在 中保護備份安全的十大安全最佳實務 AWS

AWS 方案指引

AWS 方案指引: 在 中保護備份安全的十大安全最佳實務 AWS

Table of Contents

在 中保護備份安全的十大安全最佳實務 AWS

Ibukun (IB) Oyewumi，Amazon Web Services (AWS)

2022 年 5 月 (文件歷史記錄)

安全性是 Amazon Web Services (AWS) 和客戶之間的共同責任。客戶已詢問保護其備份的方法 AWS。由於安全性實務不斷發展以減輕新風險，因此請務必定期進行風險評定以確定安全性控制的適用性，並實作多層控制以降低資料風險。

本文件將引導您完成 10 大安全最佳實務的精選清單，以保護您的備份資料和操作 AWS。本指南著重於使用 AWS Backup 服務來備份資料和操作，這些建議的安全性最佳實務可與其他備份解決方案搭配使用，例如來自 AWS Marketplace 的備份工具。

最佳實務

當您在 中保護備份時 AWS，建議使用下列方法：

主題

步驟 1. 實作備份策略

全面的備份策略是組織資料保護計畫的重要組成部分，可以抵禦、復原和減少因安全事件而可能持續存在的任何影響。建立廣泛的備份策略，以定義必須備份哪些資料，必須備份資料的頻率，以及監控備份和復原任務的方式。

當您制定備份和還原資料的全面策略時，首先要找出可能發生的中斷，以及其潛在的業務影響。

您的目標是建置復原策略，以備份工作負載，或避免在可接受的復原目標、復原時間點目標 (RTO) 以及復原點目標 (RPO) 的範圍內停機。RTO 是服務中斷與服務還原之間的可接受延遲。RPO 是自上次資料復原點以來可接受的時間量。請考慮包含下列所有項目的精細備份策略：

- 持續備份節奏
- 時間點復原 (PITR)
- 檔案層級復原
- 應用程式資料層級復原
- 磁碟區層級復原
- 執行個體層級復原

勒索軟體

精心設計的備份策略應包括可保護並復原資源以免受勒索軟體攻擊的動作，具有應用程式及其資料相依性的詳細復原要求。例如，當您建立預防性和偵測性控制以降低勒索軟體的風險時，請確保您也為跨 AWS 區域 或跨帳戶複製和還原模式設計適當的精細程度，以確保管理員不會在安全事件之後還原損毀的備份資料。

保留要求

在某些產業中，在制定備份策略時，還必須考慮資料保留要求法規。確保您的備份策略的設計符合保留要求，足以滿足每個資料分類層級和資源類型的法規需求。

合規

請洽詢您的安全合規團隊，以確認您的備份資源和操作是否應包含在合規方案的範圍內，還是從中分割出來。包含備份和復原作為安全計畫的關鍵部分，可協助您了解資料在整個環境中的位置，並適當定義合規範圍。

如需在雲端設計和操作可靠、安全、有效率且符合成本效益的工作負載的架構最佳實務，請參閱使用和可靠性支柱 – Well-Architected Framework 的備份和復原方法 AWS。 AWS

步驟 2. 將備份整合到 DR 和 BCP 中

災難復原 (DR) 是為災難做準備、響應並從中復原的過程。DR 計畫是彈性策略的重要組成部分，它涉及在災難發生時工作負載如何回應。災難可能是技術故障、人為行動或自然事件。業務連續性計畫 (BCP) 概述了組織打算如何在意外中斷期間繼續正常業務運作。

DR 計畫應該是組織 BCP 的子集。BCP 也應該包含 AWS Backup 程序。例如，影響生產資料的安全事件可能需要您調用 DR 計畫， AWS Backup 以使用 容錯移轉從另一個計畫備份資料 AWS 區域。確保您的員工熟悉並練習使用 AWS Backup 搭配您的組織程序，因此如果災難發生，您的組織可以在很少或沒有服務中斷的情況下繼續其正常操作。有關使用 的詳細資訊 AWS Backup ，請參閱本指南的其他章節。

步驟 3。自動化備份操作

應設定組織的備份計畫和資源指派，以反映企業資料保護政策。透過自動化和部署備份政策或整個組織範圍的備份計畫，可以標準化和擴展備份策略。可以使用 AWS Organizations 集中自動化備份政策，透過排程備份操作來實作、設定、管理和控管受支援的 AWS Backup 資源的備份活動。

若要在多帳戶環境中改善生產力並控管基礎設施操作，請考慮將基礎設施即程式碼 (IaC) 和事件驅動型架構作為數位轉型和備份策略的重要組成部分進行實作。自動化備份具有以下優點：

- 減少耗時的備份設定帶來的人工開銷
- 將錯誤風險降至最低
- 提供漂移偵測的可見性
- 增強跨多個 AWS 工作負載或帳戶的備份政策合規性

將備份政策作為程式碼進行實作，透過以下操作，協助您符合資料保護法規：

- 為資源類型設定不同的要求
- 擴展企業資料保護策略
- 實作生命週期規則指定復原點轉換為冷儲存或被刪除之前的時間長度，這有助於優化成本

自動化備份操作時，您可以使用 AWS 標籤和資源 IDs 來擴展資源指派選項，以自動識別存放業務關鍵應用程式資料 AWS 的資源，並使用不可變備份保護您的資料。這可協助您排定安全控制的優先順序，例如存取許可和備份計畫或政策。

步驟 4. 實作存取控制機制

考慮雲端安全時，基礎策略應該從強大的身分基礎開始，以確保使用者擁有存取資料的正確許可。合適的驗證和授權可降低安全事件的風險。共同責任模型要求 AWS 客戶實作存取控制政策。若要大規模建立和管理存取政策，可以使用 AWS Identity and Access Management (IAM)。

設定存取權限和許可時，請確保存取備份資料和文件庫的每個使用者或系統都只擁有履行其職責所需的許可，從而執行最低權限原則。使用 在備份保存庫上 AWS Backup 設定存取政策，以保護雲端工作負載。 https://docs.aws.amazon.com/aws-backup/latest/devguide/creating-a-vault-access-policy.html

例如，透過實作存取控制政策，您可以授與使用者建立備份計畫和隨選備份的存取權，同時限制他們刪除復原點的能力。使用保存庫存取政策，您可以根據您的業務需求，與來源 AWS 帳戶 或 IAM 角色共用目的地備份保存庫。也可以使用存取政策與一個或多個帳戶或 AWS Organizations中的整個組織共用備份文件庫。如需詳細資訊，請參閱 AWS Backup 文件。

當您擴展工作負載或遷移到 時 AWS，您可能需要集中管理備份保存庫和操作的許可。使用服務控制政策 (SCP) 對組織中所有帳戶可用的許可上限進行集中控制。SCP 提供深入的防禦，並確保您的使用者遵守定義的存取控制準則。如需詳細資訊，請參閱搭配使用服務控制政策與 AWS Backup來管理備份的存取權。

若要降低安全風險，例如意外存取備份資源和資料，請使用 IAM Access Analyzer 來識別與下列項目共用的任何 AWS Backup IAM 角色：

- 外部實體，例如 AWS 帳戶
- 根使用者
- IAM 使用者或角色
- 聯合身分使用者
- 一個 AWS 服務
- 匿名使用者
- 任何其他可用來建立篩選器的實體

步驟 5. 加密備份資料和文件庫

組織越來越需要改善其資料安全策略，而且在雲端中擴展時，可能需要遵守資料保護法規。正確實作加密方法可在基礎存取控制機制之上提供額外的保護層。如果主要存取控制政策失敗，此新增層可提供緩解措施。

例如，如果對 AWS Backup 資料設定過於寬鬆的存取控制政策，則金鑰管理系統或程序可以減輕安全事件的最大影響。這是因為有單獨的授權機制來存取您的資料和加密金鑰，這表示備份資料只能以加密文字的形式進行檢視。

若要充分利用 AWS 雲端 加密，請同時加密傳輸中和靜態資料。為了保護傳輸中的資料， AWS 會使用已發佈的 API 呼叫，透過 AWS Backup TLS 通訊協定在您自己、應用程式和服務之間提供加密 AWS Backup 。若要保護靜態資料，您可以使用 AWS 雲端原生 AWS Key Management Service(AWS KMS) 或 AWS CloudHSM。基於雲端的硬體安全模組 (HSM)， AWS CloudHSM 使用進階加密標準 (AES) 及 256 位元金鑰 (AES-256)，這是業界所採用的強大資料加密演算法。評估資料控管和法規需求，並選取適當的加密服務來加密雲端資料和備份文件庫。

加密組態會因資源類型和跨帳戶或跨區域的備份操作而有所不同。某些資源類型支援使用與來源資源加密金鑰不同的加密金鑰來將您的備份加密。由於您負責管理存取控制，以判斷誰可以存取 AWS Backup 您的資料或保存庫加密金鑰，以及在哪些條件下，請使用 提供的政策語言 AWS KMS 來定義金鑰的存取控制。也可以使用 AWS Backup Audit Manager 以確認您的備份已正確加密。如需詳細資訊，請參閱 AWS Backup中的備份加密。

可以使用 AWS KMS 多區域金鑰將金鑰從一個區域複製到另一個區域。當您的加密資料必須複製到其他區域進行災難復原時，多區域金鑰可簡化加密管理。評估在整體備份策略中實作多區域 AWS KMS 金鑰的需求。

步驟 6. 使用不可變儲存來保護備份

組織可使用不可變儲存裝置，在「單寫多讀 (WORM)」狀態下將資料寫入其中。處於 WORM 狀態時，資料可以寫入一次，並在提交或寫入儲存媒體後視需要經常讀取和使用資料。不可變儲存裝置可協助確保維護資料的完整性。它還提供以下保護：

- 刪除
- 覆寫
- 無意和未經授權的存取
- 勒索軟體妥協

不可變儲存裝置提供有效的機制來處理可能對您的業務營運造成實際影響的潛在安全事件。

與強大的 SCP 限制搭配使用時，可以使用不可變的儲存裝置進行更好的控管。當法律條文 (例如合法保留) 要求存取不可變資料時，也可在合規 WORM 模式下使用不可變儲存裝置。

若要維護資料可用性和完整性，可以使用 AWS Backup 文件庫鎖定保護您的備份。當您使用 AWS Backup 保存庫鎖定時，未經授權的實體無法在必要的保留期間清除、變更或損毀您的客戶或商業資料。保存 AWS Backup 庫鎖定會防止下列情況，協助您符合組織的資料保護政策：

- 特殊權限使用者 （ 包括 AWS 帳戶 根使用者 ） 的刪除
- 備份生命週期設定的變更
- 會更改您定義之保留期的更新

AWS Backup 保存庫鎖定可確保不可變性，並新增額外的防禦層來保護備份保存庫中的備份 （ 復原點 ）。這在對備份和封存有嚴格完整性需求的嚴格監管產業中特別有用。 AWS Backup 保存庫鎖定可確保您的資料與備份一起保留，以便在發生意外或惡意動作時從中復原。

> **Important**
>
> - AWS Backup 尚未評估保存庫鎖定是否符合 17 C.F.R. 1.31(b)-(c) 法規中的美國證券交易委員會 (SEC) 規則 17a-4(f) 和商品未來交易委員會 (CFTC)。
> - AWS Backup 保存庫鎖定會立即生效。它給您最少三天 (72 小時) 冷靜期，以在永久鎖定文件庫之前刪除或更新其組態。可以選擇延長此冷靜期。使用此冷靜期，針對工作負載和使用案例測試 AWS Backup 保存庫鎖定。冷靜期到期後，您和 AWS 支援 都無法刪除或更改保

存 AWS Backup 庫鎖定或鎖定保存庫的內容。如需詳細資訊，請參閱 AWS Backup 文件庫鎖定中的文件。

步驟 7. 實作備份監控和警報

備份作業可能會失敗。失敗的作業 (例如備份、還原或複製任務) 可能會影響程序中的後續步驟。當初始備份作業失敗時，其他後續任務也會失敗的可能性很高。在這種情況下，您可以透過監控和通知最好地了解事件的經過。監控和警報可以提供備份作業的組織意識，協助您回應備份失敗。

啟動並設定通知以監控 AWS Backup 作業具有以下優點：

- 讓您了解備份活動
- 協助確保您滿足重要的服務水準協議 (SLA)
- 增強一如往常的業務監控
- 協助您履行合規義務

您可以 AWS Backup 與其他 AWS 服務 和 票證系統整合，以執行自動化調查和呈報流程，藉此實作工作負載的備份監控。例如，您可以執行下列動作：

- 使用 Amazon CloudWatch 以追蹤指標、建立警示並檢視儀表板。
- 使用 Amazon EventBridge 來監控 AWS Backup 程序和事件。
- 使用 AWS CloudTrail 來監控 AWS Backup API 呼叫以及有關進行這些呼叫的時間、來源 IP、使用者和帳戶的詳細資訊。
- 使用 Amazon Simple Notification Service (Amazon SNS) 訂閱 AWS Backup 相關主題，例如備份、還原和複製事件。

您可以使用 AWS Backup Audit Manager 自動為每個帳戶和區域產生每日備份稽核報告的證據。您也可以使用一組自動化範本和儀表板（稱為備份觀察者解決方案）來取得彙總的每日跨帳戶多區域 AWS Backup 報告，藉此跨多個帳戶擴展備份監控。

步驟 8. 稽核備份組態

為了確保備份程式如預期般執行，並識別和更正備份程序的任何異常，請針對定義的備份頻率等已定義的控制項稽核 AWS Backup 政策合規性。若要找到並調查不符合業務需求的備份操作或資源，請持續且自動追蹤您的備份活動並產生自動報告。

AWS Backup Audit Manager 提供內建、可自訂的合規控制，以符合您的商業合規和法規要求。您可以使用預建且可自訂的控制作為稽核框架來評估您的 AWS Backup 做法。控制包括：

- 受備份計畫保護的備份資源
- 備份計畫最低頻率和最低保留
- 備份復原點已加密
- 備份復原點手動刪除
- 備份復原點最小保留
- 跨區域複製
- 跨帳戶複製
- 備份文件庫鎖定

對於基礎設施即程式碼 (IaC) 自動化，您可以使用 AWS Backup Audit Manager 搭配 AWS CloudFormation。

AWS Security Hub CSPM 可讓您全面檢視 的安全狀態 AWS。它還可以協助您根據安全最佳實務和業界標準來檢查環境，例如 AWS 基礎安全最佳實務控制。如果您在雲端環境中使用 Security Hub CSPM，我們建議您啟用 AWS 基礎安全最佳實務標準，因為它包含有助於保護備份安全的偵測性控制項 AWS。 AWS Backup Audit Manager 和 Security Hub CSPM 中的大多數偵測性控制項也可以作為AWS Config 受管規則使用。

步驟 9. 測試資料復原功能

備份策略必須包括測試備份。如果無法還原備份的資料，則備份策略無效。定期測試您找到某些復原點並將其能力還原。

雖然 AWS Backup 會自動將標籤從其保護的資源複製到復原點，根據預設，標籤不會從復原點複製到對應的還原資源。若要擴展庫存管理和尋找復原點，請考慮使用 AWS Backup 事件來對 AWS Backup 還原任務建立的資源啟動標籤複寫程序。

可以透過建立資料復原模式，然後定期對其進行測試，來啟動資料復原工作流程。為了提高您復原備份資料能力的信心，請建立一個基礎且可重複的過程來執行持續的資料復原測試。例如，您可以建立一個模式，測試從使用客戶受管 AWS KMS 金鑰加密的中央 DR 備份文件庫到使用不同的客戶受管 AWS KMS 金鑰加密的來源帳戶備份文件庫的跨帳戶、跨區域還原操作。

如果您不經常測試這類還原操作，您可能會發現跨帳戶、跨區域操作 AWS KMS 加密的假設不正確。通常，唯一可以實際運作的備份復原模式是您經常測試的路徑。透過對支援的備份資源類型進行例行測

試，您會發現可能導致未來干擾和遺失重要資料的早期警告。如果可能，請維持有限但可行的復原路徑和模式數量，以避免浪費儲存空間、優化成本並節省時間。在復原測試失敗時修正問題比遺失寶貴或重要資料更容易。

步驟 10. 將備份納入事件回應計畫中

安全事件反應模擬 (SIRS) 是內部事件，提供了一個結構化機會，以便在實際情況中實踐您的事件反應計畫和程序。在創造性 SIRS 活動中測試備份資料和操作很有價值，可以針對意外情況自行測試。這有助於您驗證組織的準備情況，並在罕見和意外情況發生時不會恐慌。模擬必須是現實的，並且其應該涉及到對事件做出反應時所需的跨職能組織團隊。

從基礎模擬練習開始，並朝著完整、複雜的事件努力。例如，您可以建置一個由虛擬私有雲端 (VPC) 和相關資源組成的現實模型，以模擬因政策和存取控制清單變更而導致資訊意外過度暴露或潛在資料洩露。若要評估事件反應計畫如何工作，請記錄經驗教訓，並確定需要對未來的反應程序進行的改進。

您可以使用 AWS Backup 將自動執行個體層級備份設定為 Amazon Machine Image (AMIs)，並將磁碟區層級備份設定為跨多個 的快照 AWS 帳戶。這可以協助事件反應團隊加強他們的鑑識流程，例如自動鑑識磁碟收集，方法是提供一個還原點，它可減少潛在安全事件 (例如勒索軟體) 的範圍和影響。

後續步驟

本指南涵蓋前 10 項保護備份資料的最佳實務和控制項 AWS。建議您使用這些最佳實務來設計和實作具有多層控制的備份與復原策略及架構，以擴展並達成您的業務需求。如需詳細資訊 AWS Backup，請參閱 AWS Backup 文件。

如果您對本指南有任何疑問，請在 AWS Backup 論壇上開始新的帖子，或聯絡 AWS 支援。

資源

AWS 規範指引

- AWS上的備份與復原方法 (指南)

AWS 文件

- AWS Backup
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon EventBridge
- IAM
- AWS KMS
- AWS Organizations
- AWS Security Hub CSPM
- Amazon SNS

部落格文章

- AWS 服務 使用 將大規模集中備份自動化 AWS Backup
- 開啟災難復原 (DR) 架構 AWS，第 I 部分：雲端中復原的策略
- 加密的重要性以及 AWS 如何提供協助
- 使用保存 AWS Backup 庫鎖定增強備份的安全狀態
- 使用 AWS Backup Audit Manager 監控、評估和示範備份合規
- 使用 在帳戶和區域之間建立和共用加密備份 AWS Backup
- 使用 AWS Backup Audit Manager 簡化稽核資料保護政策
- 透過 使用服務控制政策管理對備份的存取 AWS Backup

- 取得彙總的每日跨帳戶多區域 AWS Backup 報告

GitHub 儲存庫

下列程式碼儲存庫為您提供管理和部署解決方案，以 AWS Backup 跨多個帳戶和 AWS Organizations 跨組織使用 實作備份和復原 AWS 區域。

- AWS Backup 使用 實作 AWS
- AWS Backup 使用 CI/CD 管道實作

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2022 年 5 月 13 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。