AWS 白皮書

導覽 AWS 上的 GDPR 合規

導覽 AWS 上的 GDPR 合規: AWS 白皮書

Table of Contents

導覽 AWS 上的 GDPR 合規

發行日期：2020 年 12 月 (文件修訂)

摘要

本文說明 Amazon Web Services (AWS) 為客戶提供之服務與資源的相關資訊，以協助客戶符合可能適用於其活動之一般資料保護規定 (GDPR) 的要求，包括了符合 IT 安全標準的 AWS Cloud Computing Compliance Controls Catalog (C5) 證明，以及符合 Cloud Infrastructure Services Providers in Europe (CISPE) 管理辦法的資料存取控制、監控與記錄工具、加密，以及金鑰管理。

一般資料保護規定概觀

一般資料保護規定 (GDPR) 是歐洲的隱私權法 (歐洲議會與理事會於 2016 年 4 月 27 日頒布的 2016/679 規定)，於 2018 年 5 月 25 日生效。GDPR 取代了歐盟資料保護命令 (95/46/EC 命令)，目的在統一施行一套資料保護法，規範各歐盟 (EU) 成員國。

GDPR 的適用範圍涵蓋登記在歐盟之組織的所有個人資料處理，或於歐盟中提供商品或服務給個人，或是監控歐盟中之歐盟居民行為時，需要處理歐盟居民之個人資料的組織。個人資料係指任何可以識別出自然人的資訊。

引進 GDPR 對在歐盟營運之組織的改變

GDPR 的關鍵要點之一，就是統一了歐盟成員國在安全處理、使用、交換個人資料的方式。組織必須實作並定期檢查各項技術與組織措施，以及個人資料處理遵循的合規政策，適用於個人資料處理的合規原則，持續不斷地證明其資料處理不僅安全，而且符合 GDPR 的規定。歐盟監督機構可以對違反 GDPR 的組織，開出高達 2,000 萬歐元或全球年營業額 4% (取其中較高者) 的罰鍰。

AWS 對於 GDPR 的準備

AWS 的合規、資料保護及安全專家將與世界各地的客戶合作，除了回答其問題之外，也會協助其準備在 GDPR 的規範之下，於雲端執行工作負載。這些團隊也會就 GDPR 的要求，檢查 AWS 的整備程度。

> **Note**
>
> 我們可以確保所有 AWS 服務的使用，均符合 GDPR 的規範。

AWS 資料處理增補合約 (DPA)

AWS 提供符合 GDPR 的資料處理增補合約 (GDPR DPA)，協助客戶符合 GDPR 合約規範的義務。AWS GDPR DPA 會整合到 AWS 服務條款，並自動全面套用到所有需要此合約來滿足 GDPR 要求的客戶。

2020 年 7 月 16 日，歐盟法院 (CJEU) 針對歐美隱私盾與標準合約條款 (SCC) (亦稱為示範條款) 發佈了一項裁定。 CJEU 裁定歐美隱私盾無效，不適用於從歐盟 (EU) 到美國 (US) 的個人資料傳輸。而在同一項裁決中，CJEU 確認了公司仍可繼續使用 SCC，作為在歐盟以外地區傳輸資料的機制。

根據這項裁決，AWS 客戶與合作夥伴可繼續使用 AWS，將其內容從歐洲傳輸到美國與其他國家/地區，以符合歐盟資料保護法律 (包括一般資料保護規定 (GDPR))。若 AWS 客戶選擇在歐盟以外地區傳輸其資料時，要遵循 GDPR 的規定，可使用 AWS 資料處理增補合約 (DPA) 中所含的 SCC。我們致力於確保客戶與合作夥伴在各地營運時，都能隨著法規與立法領域的演進，繼續享受 AWS 的好處。如需詳細資訊，請參閱歐美隱私盾常見問題集。

GDPR 規定下 AWS 的角色

在 GDPR 規定下，AWS 既是資料處理者，也是資料控制者。

根據第 32 條的規定，控制者與處理者必須「...實作適當的技術與組織措施」。這些措施須考量到「最先進的技術與實作成本，以及處理的本質、範圍、內容與用途，還有自然人權利與自由之各種可能性與嚴重性的風險」。GDPR 為需要的安全措施類型，提供了下列具體建議：

- 將個人資料假名化與加密。
- 能夠確保處理系統與服務的持續機密性、完整性、可用性與恢復力。
- 能夠在發生實體或技術事件時，及時恢復個人資料的使用與存取。
- 定期測試、評定及評估技術與組織措施之有效性的程序，可確保處理安全。

AWS 做為資料處理者

當客戶與 AWS 合作夥伴網路 (APN) 的合作夥伴使用 AWS 服務處理其內容中的個人資料時，AWS 即為資料處理者。客戶與 APN 合作夥伴可使用 AWS 服務中提供的控制 (包括安全組態控制) 處理個人資料。在這些情況下，客戶或 APN 合作夥伴可能為資料控制者或資料處理者，而 AWS 則是資料處理者或轉包處理者。符合 AWS GDPR 的資料處理增補合約 (DPA) 包含了 AWS 身為資料處理者的承諾。

AWS 作為資料控制者

當 AWS 收集個人資料，並決定處理該個人資料的目的與方法時，即為資料控制者。例如，當 AWS 處理帳戶註冊、管理與服務存取的帳戶資訊，或 AWS 帳戶的連絡人資訊，以透過客戶支援活動提供協助時，即為資料控制者。

共同安全責任模式

安全與合規是 AWS 與客戶的共同責任。當客戶將其電腦系統與資料移至雲端時，客戶與雲端服務提供者應共同負起其安全責任。當客戶移至 AWS 雲端時，AWS 負責保護執行 AWS 雲端中提供之所有服

務的全域基礎結構。對於抽象服務 (例如 Amazon S3 與 Amazon DynamoDB)，AWS 也負責作業系統與平台的安全。客戶與 APN 合作夥伴 (無論其身分為資料控制者或資料處理者) 則對其放置在雲端中或連線到雲端的所有內容負責。此責任區分通常稱為雲端的安全 (相對於雲端中的安全)。此共同模式可以減輕客戶的營運負擔，並提供客戶所需的彈性與控制，方便他們將基礎結構部署在 AWS 雲端中。如需詳細資訊，請參閱 AWS 共同責任模式。

GDPR 不會變更 AWS 共同責任模式，此模型仍然和只使用雲端運算服務的客戶與 APN 合作夥伴相關。共同責任模式這個方法非常實用，可依據 GDPR 闡明 AWS (資料處理者或轉包處理者的身分) 與客戶或 APN 合作夥伴 (資料控制者或資料處理者的身分) 之間不同的責任。

堅實的合規架構與安全標準

根據 GDPR 的規定，適當的技術與組織措施必須包括「...能夠確保處理系統與服務的持續機密性、完整性、可用性與恢復力」，以及可靠的還原、測試與總體風險管理程序。

AWS 合規計劃

AWS 始終都以高標準看待我們全球營運的安全與合規。安全一直是我們重中之重的任務。 AWS 定期接受獨立的第三方證明稽核，以確保控制活動如預期般運作。具體而言，AWS 會依據區域和產業，接受全球與區域之各式安全框架的稽核。AWS 目前參與了超過 50 項不同的稽核計劃。

評定機構記錄了這些稽核的結果，並透過 AWS Artifact 提供給所有的 AWS 客戶。AWS Artifact 是免費的自助服務入口網站，可隨需存取 AWS 合規報告。新報告會透過 AWS Artifact 發行，讓客戶能夠立即存取新報告，持續監控 AWS 的安全與合規。

這些國際公認的認證與鑑定，可以協助客戶證明符合嚴格的國際標準，例如雲端安全的 ISO 27017、雲端隱私權的 ISO 27018、SOC 1、SOC 2 與 SOC 3、PCI DSS Level 1 及其他。AWS 也能協助客戶符合當地的安全標準，例如德國政府支援的 BSI Common Cloud Computing Controls Catalogue (C5) 證明。

如需 AWS 認證計劃、報告與第三方證明的詳細資訊，請參閱 AWS 合規計劃。如需服務相關的資訊，請參閱指定範圍內的 AWS 服務。

Cloud Computing Compliance Controls Catalog

Cloud Computing Compliance Controls Catalog (C5) 是德國政府支援的證明方案，由 Federal Office for Information Security (BSI) 引進德國。此方案在協助組織證明其施行的安全，在德國政府之雲端供應商的安全建議背景下，能夠抵禦常見的網路攻擊。

資料保護的技術與組織措施，以及資訊安全措施的目標，均為資料安全，旨在確保其機密性、完整性與可用性。C5 定義的安全要求，也和資料保護相關。AWS 客戶及其合規顧問可使用 C5 證明這項資源，了解當其將工作負載移至雲端時，AWS 所提供的 IT 安全保證服務範圍。C5 新增了法規定義的 IT 安全層級，等同 IT-Grundschutz 加上其他雲端相關的控制。

C5 也新增了更多控制，以提供資料位置、服務佈建、管轄地、現有認證、資訊揭露義務及完整服務描述方面的資訊。您可以使用此資訊評估法規 (例如資料隱私權)、自己的原則，或您使用雲端運算服務相關的威脅環境。

資料存取控制

根據 GDPR 第 25 條規定，控制者應「實作適當有條理的技術方法，確保會根據預設，只在特定用途需要時，才處理個人資料」。下列 AWS 存取控制機制可協助客戶符合此要求，只允許授權的系統管理員、使用者與應用程式存取 AWS 資源與客戶資料。

AWS Identity and Access Management

建立 AWS 帳戶時，會自動為您的 AWS 帳戶建立根使用者帳戶。此使用者帳戶具有完整的存取權，可以您 AWS 帳戶中的所有 AWS 服務與資源。只有在一開始建立其他角色與使用者帳戶，以及有管理活動需要此帳戶時，才使用此帳戶，而不應將其用於日常任務。AWS 建議您從一開始就套用最低權限準則，包括為不同的任務定義不同的使用者帳戶與角色，並指定完成每項任務所需的基本許可設定。此方法是設計中用來調整 GDPR 中引入之資料保護的一種機制。AWS Identity and Access Management (IAM) 這項 Web 服務可以安全地控制您 AWS 資源的存取權。

使用者與角色定義具有特定許可的 IAM 身分。授權的使用者是具備執行特定任務能力的 IAM 角色。當角色確立之後，會建立暫時登入資料。例如，您可以使用 IAM 角色安全地為在 Amazon Elastic Compute Cloud (Amazon EC2) 中執行的應用程式，提供存取其他 AWS 資源 (如 Amazon S3 儲存貯體與 Amazon Relational Database Service (Amazon RDS)，或 Amazon DynamoDB 資料庫) 所需的暫時登入資料。同樣地，執行角色也提供具有存取其他 AWS 服務與資源 (例如：用於串流日誌的 Amazon CloudWatch Logs，或從 Amazon Simple Queue Service (Amazon SQS) 佇列中讀取訊息) 所需許可的 AWS Lambda 功能。建立角色時，您會為其新增原則，以定義授權。

若要協助客戶監控資源原則，並找出不打算提供給大眾或不同帳戶存取權的資源，可以啟用 IAM Access Analyzer 產生全面性的調查結果，從中確定可以從 AWS 帳戶外部存取的資源。IAM Access Analyzer 在評估資源原則時，會使用數學邏輯與推論，判斷原則允許的可能存取路徑。IAM Access Analyzer 會持續監控新原則或更新原則，並使用適用於 IAM 角色 (同時也適用於 Amazon S3 儲存貯體、AWS Key Management Service (AWS KMS) 金鑰、Amazon SQS 佇列，以及 Lambda 函數等等) 的原則，分析授與的許可。

當儲存貯體設定為允許存取網際網路上的任何人或其他 AWS 帳戶 (包括您組織外部的 AWS 帳戶) 時，Access Analyzer for S3 會提醒您。在檢查 Access Analyzer for Amazon S3 中存有風險的儲存貯體時，只須按一下滑鼠按鈕，就能禁止所有對儲存貯體的公開存取。AWS 建議除非您需要支援公開存取來支援特定的使用案例，否則應禁止所有對您儲存貯體的存取。在禁止所有公開存取之前，請先確定您的應用程式在沒有了公開存取權之後，仍能繼續正常運作。如需詳細資訊，請參閱使用 Amazon S3 封鎖公開存取。

IAM 也會提供上次存取的資訊，協助您找出尚未使用的許可，以便您移除其與相關主體的連結。使用上次存取的資訊或能改進原則，只允許存取所需的服務與動作。這有助於您遵循及套用最低權限的最佳實務。 您可以檢視 IAM 或整個 AWS Organizations 環境中，上次存取的實體或原則資訊。

透過 AWS STS 的暫時存取字符

您可以使用 AWS Security Token Service (AWS STS) 建立信任的使用者，並提供他們暫時安全登入資料，以存取您的 AWS 資源。暫時安全登入資料的作用，與提供給您 IAM 使用者的長期存取金鑰憑證幾乎完全相同，除了下列幾項差異：

- 暫時安全憑證適合短期使用。您可以設定這類憑證的有效期限，從 15 分鐘到最長 12 小時。暫時憑證到期之後，AWS 便無法辨識，也不允許任何藉其發出之 API 請求任何形式的存取。
- 暫時安全憑證不會儲存在使用者帳戶中，而會在收到請求後動態產生提供給使用者。有權要求新憑證的使用者，可以在暫時安全憑證到期時 (或之前) 請求新憑證。

這些差異會在您使用暫時憑證時顯現下列優點：

- 無須為應用程式散發或內嵌長期的 AWS 安全感證。
- 暫時憑證是角色與聯合身分的基礎。您可以為使用者定義暫時的 AWS 身分，將您 AWS 資源的存取權提供給他們。
- 暫時安全憑證的可以有限度地自訂生命期限。因此無須輪換憑證，也無須在不需要時明確撤銷。暫時安全憑證到期之後無法重複使用。您可以指定憑證的有效有效期限。

多重要素驗證

若要更進一步提升安全，可以為您的 AWS 帳戶及 IAM 使用者新增雙重要素驗證。啟用多重要素驗證 (MFA) 之後，當您登入 AWS 管理主控台時，就會提示您輸入使用者名稱與密碼 (第一個要素)，以及您 AWS MFA 裝置發出的驗證回應 (第二個要素)。您可以為您的 AWS 帳戶和您帳戶中建立的個別 IAM 使用者啟用 MFA。此外也可使用 MFA 控制 AWS 服務 API 的存取權。

例如，您可以定義原則，授與 Amazon EC2 中所有 AWS API 作業的完整存取權，但明確拒絕未經 MFA 驗證的使用者，存取特定的 API 作業，例如 `StopInstances` 與 `TerminateInstances`。

```
{
 “Version”: “2012-10-17”,
```

```
        “Statement”: [
            {
               “Sid”: “AllowAllActionsForEC2”,
               “Effect”: “Allow”,
               “Action”: “ec2:*”,
               “Resource”: “*”
            },
           {
               “Sid”: “DenyStopAndTerminateWhenMFAIsNotPResent”,
               “Effect”: “Deny”,
               “Action”: [
                   “ec2:StopInstances”,
                   “ec2:TerminateInstances”
              ],
               “Resource”: “*”,
               “Conditions”: {
                   “BoolIfExists”: {“aws:MultiFactorAuthPresent”:false}
               }
           }
       }
}
```

若要為 Amazon S3 儲存貯體加設一層安全性，可以設定 MFA Delete (MFA 刪除)，另外要求其他驗證，才能變更儲存貯體的版本狀態，以及永久刪除物件版本。MFA Delete (MFA 刪除) 是安全認證洩露時的另一層安全保護。

若要使用 MFA Delete (MFA 刪除)，可以使用硬體或虛擬 MFA 裝置產生驗證碼。如需支援硬體或虛擬 MFA 裝置的清單，請參閱多重要素驗證頁面。

AWS 資源的存取權

若要細分您 AWS 資源的存取權，可以將不同層級的許可，授予不同人員來存取不同的資源。例如，您可以只將 Amazon EC2、Amazon S3、DynamoDB、Amazon Redshift 及其他 AWS 服務的存取權，授予某些使用者。

對於其他使用者，可以只授予部分 Amazon S3 儲存貯體的唯讀存取權，也可以授予管理部分 Amazon EC2 執行個體的許可，或只允許存取您的帳單資訊。

下列範例所示的政策，是您可以用來允許對特定 Amazon S3 儲存貯體執行所有動作，以及明確拒絕存取 Amazon S3 以外之所有 AWS 服務的其中一種方法。

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Effect”: “Allow”,
                “Action”: “s3:*”,
                “Resource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ],
              },
              {
                “Effect”: “Deny”,
                “NotAction”: “s3:*”,
                “NotResource”: [
                     “arn:aws:s3:::bucket-name”,
                     “arn:aws:s3:::bucket-name/*”
                 ]
               }
            ]
}
```

您可以將政策連結到使用者帳戶或角色。如需 IAM 政策的其他範例，請參閱以 IAM 身分為基礎的政策範例。

定義區域服務存取權的界限

客戶可以保有自己內容的擁有權，並可選取處理、儲存及託管內容時所要使用的 AWS 服務。AWS 不會在未經您的同意之下，因為任何用途而擅自存取或使用您的內容。根據共同責任模式的規定，您可以選擇儲存內容的 AWS 區域，進而依照自己的特定地理需求，在所選位置部署 AWS 服務。例如，若您希望自己的內容只會儲存在歐洲，可以選擇只將 AWS 服務部署在其中一個歐洲 AWS 區域。

IAM 政策是十分簡單的方法，可以協助您限制對特定區域中之服務的存取。您可以為連結到您 IAM 主體的 IAM 政策新增全域條件 (`aws:RequestedRegion`)，以對所有 AWS 服務施行。例如，下列政策使用具有 `Deny` 效果的 `NotAction` 元素，會在請求的區域超出歐洲的範圍時，明確拒絕對陳述式中未列之所有動作的存取。因為 CloudFront、IAM、Amazon Route 53 與 AWS Support 服務是常用的 AWS 全域服務，所以不應拒絕其中的動作。

```
      {
         “Version”: “2012-10-17”,
         “Statement”: [
             {
                “Sid”: “DenyAllOutsideRequestedRegions”,
                “Effect”: “Deny”,
                “NotAction”: [
                     “cloudfront:*”,
                     “iam:*”,
                     ”route53:*”,
                     “support:*”
                 ],
                 “Resource”: “*”,
                 “Condition”: {
                    “StringNotLike”: {
                        “aws:RequestedRegion”: [
                              “eu-*”
                        ]
                    }
                 }
            }
          ]
}
```

此 IAM 政策範例也可實作為 AWS Organizations 的服務控制政策 (SCP)，定義組織中特定 AWS 帳戶或組織單位 (OU) 適用的許可界限，以便您可以控制複雜的多帳戶環境中，使用者對區域服務的存取權。

新推出的區域提供地理限制功能。2019 年 3 月 20 日之後推出的地區預設為停用。您必須先啟用這些區域才能使用。對於預設為停用的 AWS 區域，您可以使用 AWS 管理主控台啟用及停用該區域。啟用及停用 AWS 區域可讓您控制 AWS 帳戶中的使用者，能否存取該區域中的資源。如需詳細資訊，請參閱管理 AWS 區域。

控制 Web 應用程式與行動應用程式的存取權

AWS 提供各種服務，讓您用來管理客戶應用程式中的資料存取控制。若您需要為您的 Web 應用程式與行動應用程式，新增使用者登入與存取控制功能，可以使用 Amazon Cognito。Amazon Cognito 使用者集區是安全的使用者目錄，可擴展至上億名使用者。若要保護使用者的身分，可為您的使用者集區新增多重要素驗證 (MFA)。您也可以使用調整式身分驗證。此法採用的模型會依風險分級，可以預測您可能需要其他驗證要素的時機。

若是使用 Amazon Cognito Identity Pools (聯合身分)，您可以查看誰存取了您的資源，以及存取動作的來源位置 (行動應用程式或 Web 應用程式)。您可以使用此資訊建立 IAM 角色與政策，根據存取來源 (行動應用程式或 Web 應用程式) 與身分供應商的類型，允許或拒絕存取資源。

監控與記錄

GDPR 第 30 條規定，「...每個控制者 (如其適用) 及控制者代表均應保留一份其責任下處理之活動的記錄」。本文也包括在監控所有個人資料處理時，必須記錄之資訊的詳細資料。因為控制者與處理者也必須及時傳送缺口通知，所以快速偵測事件十分重要。AWS 提供下列監控與記錄服務，協助客戶達成這些義務。

使用 AWS Config 管理及設定資產

AWS Config 可以為您 AWS 帳戶中許多 AWS 資源類型的組態提供詳細的資訊，包括資源彼此之間的關聯性，以及資源先前的設定，方便您了解設定與關聯性在不同時間的變化。

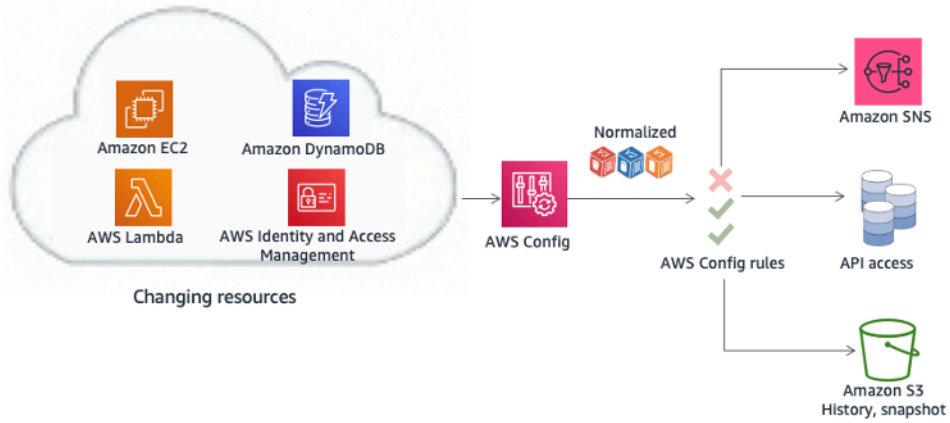

圖 1 – 使用 AWS Config 監控不同時間的組態變化

AWS 資源是可以在 AWS 中運作的實體，例如 EC2 執行個體、Amazon Elastic Block Store (Amazon EBS) 磁碟區、安全群組，或 Amazon Virtual Private Cloud (Amazon VPC)。如需 AWS Config 支援的 AWS 資源完整清單，請參閱支援的 AWS 資源類型。

您可以使用 AWS Config 執行下列作業：

- 評估您的 AWS 資源設定用途，以確認組態的正確性。
- 取得支援並與您 AWS 帳戶連結之資源目前的組態快照。
- 取得帳戶中一或多項資源的組態。
- 取得一或多項資源的歷史組態。
- 在建立、修改或刪除資源時取得通知。

- 查看資源之間的關聯性。例如，尋找使用特定安全群組的所有資源。

合規稽核與安全分析

您可以使用 AWS CloudTrail 持續監控 AWS 帳戶活動。其會擷取您帳戶透過 AWS 管理主控台、AWS 開發套件、命令列工具，以及更高層級之 AWS 服務呼叫 API 的歷史記錄。您也可以為支援 CloudTrail 的服務，指定哪些使用者與帳戶呼叫了 AWS API、發出呼叫的來源 IP 地址，以及呼叫發出的時間。您可以使用 API 將 CloudTrail 整合至應用程式，自動為您的組織建立追蹤、檢查追蹤狀態，以及控制管理員啟用及停用 CloudTrail 記錄的方式。

CloudTrail 日誌檔可以從多個區域與多個 AWS 帳戶彙總至單一 Amazon S3 儲存貯體中。AWS 建議您將日誌 (特別是 AWS CloudTrail 日誌) 寫入日誌專用帳戶 (日誌封存) 中，設有存取限制的 Amazon S3 儲存貯體。儲存貯體的許可應禁止刪除記錄，並應使用 Amazon S3 管理的加密金鑰 (SSE-S3) 或 AWS KMS 管理的金鑰 (SSE-KMS)，以伺服器端加密對靜態日誌進行加密。CloudTrail 日誌檔的完整性驗證可用於判斷日誌檔在經過傳遞之後是否遭到修改、刪除或未變更。此功能遵循產業標準演算法，雜湊採用 SHA-256，數位簽署採用 SHA-256 加 RSA，讓日誌檔很難經由計算方式修改、刪除或偽造 CT; 日誌檔，而且免除了偵測的程序。您可以使用 AWS 命令列界面 (AWS CLI)，驗證 CloudTrail 傳遞檔案所在位置上的檔案。

Amazon S3 儲存貯體中彙總的 CloudTrail 記錄加以分析之後，可供稽核或疑難排解活動之用。集中日誌之後，就能和 Security Information and Event Management (SIEM) 解決方案整合，或是交由 AWS 服務 (例如 Amazon Athena 或 CloudTrail Insights) 分析，然後使用 Amazon QuickSight 儀表板製作成圖表。集中 CloudTrail 日誌之後，也能使用相同的日誌封存帳戶，集中其他來源的日誌，例如 CloudWatch Logs 與 AWS 負載平衡器。

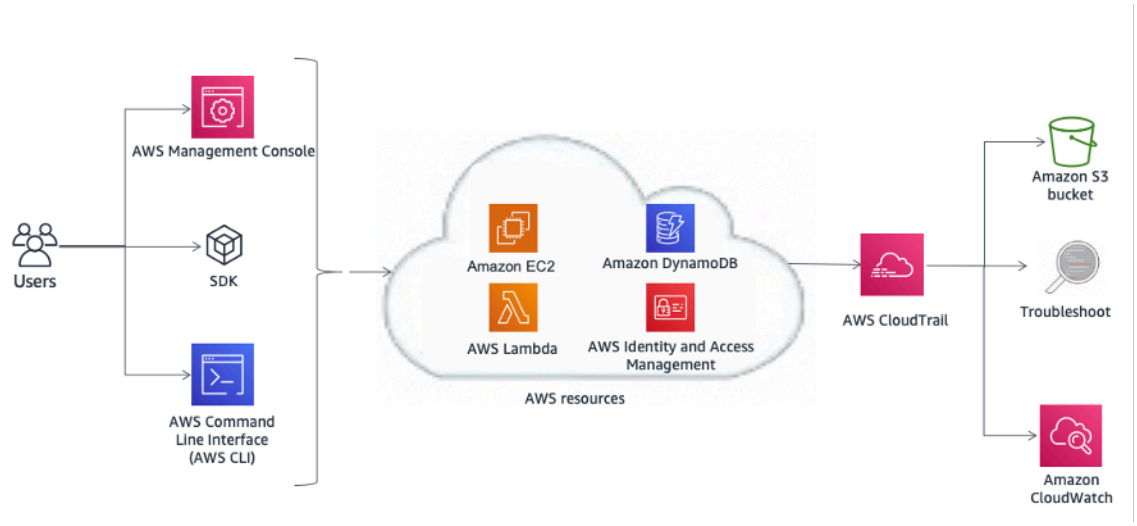

圖 2 – AWS CloudTrail 之合規稽核與安全分析的範例架構

AWS CloudTrail 日誌也能觸發預先設定的 Amazon CloudWatch Events。您可以使用這些事件通知使用者或系統有事件發生，或是執行修復動作。例如，若要監控您 Amazon EC2 執行個體上的活動，可以建立 CloudWatch 事件規則。當 Amazon EC2 執行個體上發生特定活動，並被擷取到日誌中時，該規則會觸發 AWS Lambda 函數，將事件的通知電子郵件傳送給管理員(請參閱圖 3)。 電子郵件中會提供詳細資料，例如事件發生的時間、執行動作的使用者、Amazon EC2 詳細資料等等。下圖顯示事件通知的架構。

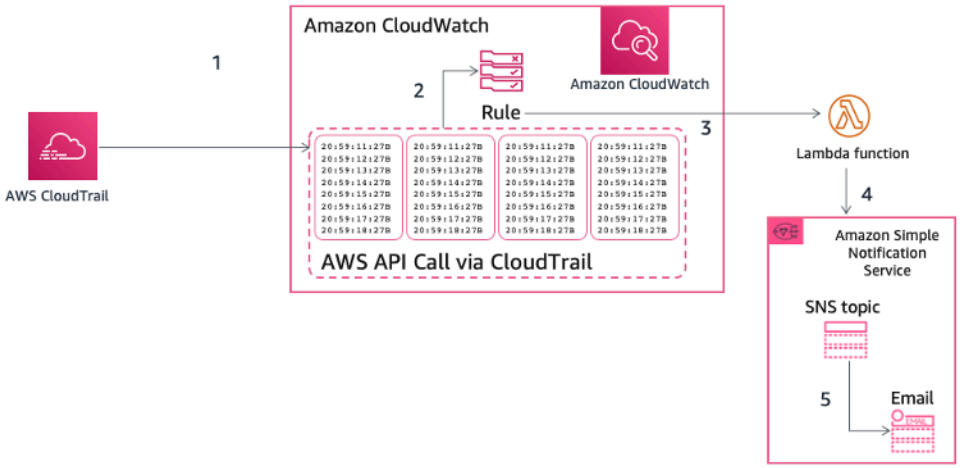

圖 3 – AWS CloudTrail 事件通知範例

收集及處理日誌

CloudWatch Logs 可用於監控、儲存及存取來自 Amazon EC2 執行個體、AWS CloudTrail、Route 53 及其他來源的日誌檔。請參閱將日誌發佈至 CloudWatch Logs 的 AWS 服務文件頁面。

舉例來說，日誌資訊可能包括：

- 對 Amazon S3 物件之存取的詳細記錄
- VPC 流程日誌會提供網路中流程的詳細資訊
- 規則型組態會依據 AWS Config 規則執行驗證及動作
- 使用 CloudFront 中的 Web 應用程式防火牆 (WAF) 功能，篩選及監控對應用程式的 HTTP 存取

在 Amazon EC2 執行個體或內部部署伺服器上安裝 CloudWatch Agent，也可將自訂應用程式指標與日誌發佈至 CloudWatch Logs。

使用 CloudWatch Logs Insights，可以互動方式分析日誌，而執行查詢則能讓您更快更有效率地應變操作問題。

設定訂閱篩選條件，可以幾近即時地處理 CloudWatch Logs，並將其傳遞至其他服務，例如 Amazon OpenSearch Service (OpenSearch Service) 叢集、Amazon Kinesis 串流、Amazon Kinesis Data Firehose 串流，或是可用於自訂處理、分析或載入其他系統的 Lambda。

CloudWatch 指標篩選條件可用於在日誌檔資料中定義用來查看日誌資料的模式、將模式成 CloudWatch 的數字指標，以及依據您的商務要求設定警示。例如，若要遵循 AWS 建議，不使用根使用者執行日常任務，可以為 CloudTrail 日誌 (傳遞至 CloudWatch Logs) 設定特定的 CloudWatch 指標篩選條件，以建立自訂指標，以及設定警示，在有人使用根認證存取您的 AWS 帳戶時，通知相關利害關係人。

諸如 Amazon S3 伺服器存取日誌檔、Elastic Load Balancing 存取日誌檔、VPC 流程日誌檔，以及 AWS Global Accelerator 流程日誌檔等日誌檔，都可直接傳遞至 Amazon S3 儲存貯體。例如，當您啟用 Amazon Simple Storage Service 伺服器存取日誌時，可取得對 Amazon S3; 儲存貯體發出之請求的詳細資訊。存取日誌記錄包含請求的詳細資料，例如請求類型、請求中指定的資源，以及請求的處理時間與日期。如需日誌訊息的詳細資訊，請參閱《Amazon Simple Storage Service 開發人員指南》(Amazon Simple Storage Service Developer Guide) 中的 Amazon Simple Storage Service 伺服器存取日誌的格式 (Amazon Simple Storage Service Server Access Log Format)。因為伺服器存取日誌可以為儲存貯體擁有者，提供不在其控制下之用戶端所發請求的詳情，所以許多應用程式都會使用。根據預設，Amazon S3 不會收集服務存取日誌，但您如有啟用日誌，Amazon S3 就會在幾小時內，將存取日誌傳遞至您的儲存貯體。若您需要更快的傳遞方式，或需要將日誌傳遞到多個目的地，可考慮使用 CloudTrail 日誌，或並用 CloudTrail 日誌與 Amazon S3。靜態日誌可以加密，方法是在目的地儲存貯體中，設定預設物件加密。該物件會使用儲存於 AWS Key Management Service (AWS KMS) 中 Amazon S3 管理之金鑰 (SSE-S3) 或客戶主金鑰 (CMK) 的伺服器端加密進行加密。

儲存於 Amazon S3 儲存貯體中的日誌，可以使用 Amazon Athena 進行查詢及分析。Amazon Athena 是互動式查詢服務，可讓您使用標準 SQL 分析 S3 中的資料。您可以透過 Athena，使用 ANSI SQL 執行臨機操作查詢，無須彙總資料或將資料載入 Athena。Athena 可以處理非結構化、半結構化與結構化的資料集，並整合到 Amazon QuickSight 中，輕鬆產生圖表。

日誌檔也是自動化威脅偵測的實用資訊來源。Amazon GuardDuty 是持續執行的安全監控服務，可分析及處理來自幾個來源的事件，例如 VPC 流程日誌、CloudTrail 管理事件日誌、CloudTrail Amazon S3 資料事件日誌，以及 DNS 日誌。此服務使用威脅情報摘要 (例如惡意 IP 地址與網域的清單) 與機器學習，找出您 AWS 環境中，未預期且疑似未經授權的惡意活動。當您在某個地區啟用 GuardDuty 時，該功能會立即開始分析您的 CloudTrail 事件日誌。其透過獨立重複的事件串流，直接從 CloudTrail 取用 CloudTrail 管理與 Amazon S3 資料事件。

使用 Amazon Macie 大規模地探索及保護資料

GDPR 第 32 條規定：「…控制者與處理者應實作適當的技術與組織措施，確認風險的安全層級，包括除但不限於：[…]

(b) 能夠確保處理系統與服務的持續機密性、完整性、可用性與恢復力；

[…]

(d) 定期測試、評定及評估技術與組織措施之有效性的程序，以確保處理安全。」

持續的資料分類程序，對於調整資料本質的安全資料處理而言非常重要。若您的組織會管理敏感資料，就必須監控其位置、適當施以保護，以提供證據證明，您已照法規與合規要求，施行資料安全與隱私權。為協助客戶大規模地識別及保護其敏感資料，AWS 提供了 Amazon Macie 這項管理完善的資料安全與資料隱私服務，其使用模式比對與機器學習模型偵測個人識別資訊 (PII)，從而探索及保護儲存在 S3 儲存貯體中的敏感資料。Amazon Macie 會掃描這些儲存貯體，並提供專為偵測幾類敏感資料而設計的受管資料識別符，分類儲存貯體的資料。Macie 可以偵測 PII，例如全名、電子郵件地址、出生日期、身分證號碼、納稅人身分或參考號碼等等。客戶可以定義自訂資料識別符來反映其組織的特定案例 (例如客戶帳戶號碼或內部資料分類)。

Amazon Macie 會持續評估儲存貯體中的物件，並自動提供所找到符合資料類別定義，但未加密或可公開存取之資料的結果摘要 (圖 4)。這些資料可能包括提供給您未在 AWS Organizations 中定義之 AWS 帳戶，任何未經加密並可公開存取之物件或儲存貯體的警示。Amazon Macie 與其他 AWS 服務整合 (例如 AWS Security Hub)，可產生可採取動作的安全結果，並針對該結果 (圖 5) 建議自動與被動的動作。

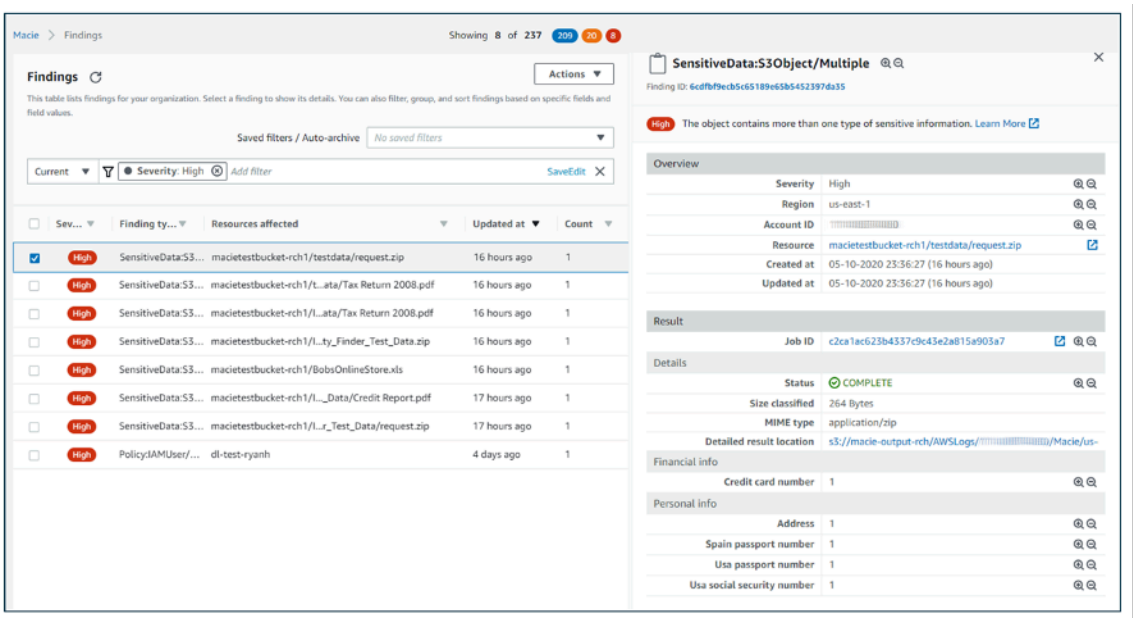

圖 4 – 資料檢查與結果範例

集中式安全管理

許多組織在掌握和集中管理其環境上，都面臨各種挑戰。隨着您的操作影響層面擴大，若不仔細思考安全設計，可能會讓此項挑戰愈趨複雜。缺乏知識，再加上治理與安全程序上分散且不平均的管理，可能會讓您的環境容易受到攻擊。

AWS 提供各種工具協助您解決 IT 管理與治理上，一些最具挑戰性的問題，以及協助您從設計達成保護資料的目的。

AWS Control Tower 提供方法讓您設定及治理安全、新穎的多帳戶 AWS 環境。此服務會依照最佳實務的藍圖，自動設定多帳戶環境的登陸區域，並允許您從預先封裝的清單中，選擇防護機制來實現治理。防護機制會針對安全、合規與營運實作治理規則。AWS Control Tower 使用 AWS IAM Identity Center (IAM Identity Center) 的預設目錄，提供身分識別管理，並使用 IAM Identity Center 與 IAM，允許跨帳戶進行稽核。此外也集結了儲存於 Amazon S3 中，來自 CloudTrail 與 AWS Config 日誌的日誌。

AWS Security Hub 是另一項支援集中功能，並能提升組織掌握度的服務。Security Hub 可集中管理來自 AWS 帳戶與服務 (例如 Amazon GuardDuty 與 Amazon Inspector) 的安全與合規結果，並排列其優先順序，同時還能和第三方合作夥伴的安全軟件整合，協助您分析安全趨勢，從中找出最高優先順序的安全問題。

Amazon GuardDuty 是智慧型威脅偵測服務，可協助客戶更精確而且輕鬆地監控及保護其 AWS 帳戶、工作負載，以及儲存於 Amazon S3 中的資料。GuardDuty 可以分析幾個來源中，您 AWS 帳戶的數十億個事件，包括 AWS CloudTrail 管理事件、CloudTrail Amazon S3 資料事件、Amazon Virtual Private Cloud 流程日誌，以及 DNS 日誌例如，其可偵測異常的 API 呼叫、對已知惡意之 IP 位址發出的可疑輸出通訊，或是利用 DNS 查詢作為傳輸機制，企圖竊取資料的行為。GuardDuty 能夠利用機器學習支援的威脅情報，以及第三方的安全合作夥伴，提供更精確的結果。

Amazon Inspector 是自動安全評定服務，可協助改善在 AWS EC2 執行個體上部署之應用程式的安全與合規。Amazon Inspector 可自動評定應用程式的暴露程度、弱點，以及和最佳實務之間的偏差。在執行評定之後，Amazon Inspector 會產生一份詳細的安全問題清單，並依據嚴重程度排列其內容。

Amazon CloudWatch Events 可讓您將 AWS 帳戶設定為將事件傳送給其他 AWS 帳戶，或是做為其他帳戶或組織的事件接收者。此機制在實作跨帳戶事件回應案例時非常實用，可以採取及時的修正動作 (例如呼叫 Lambda 函數，或對 Amazon EC2 執行個體執行命令)，以在發生安全事件時隨時執行。

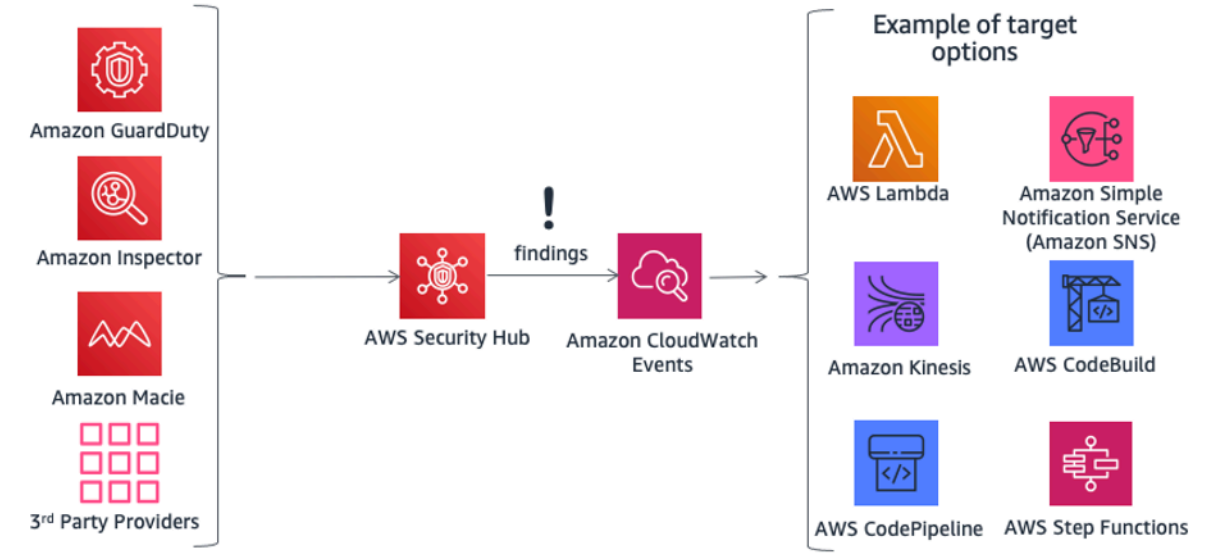

圖 5 – 採取 AWS Security Hub 與 Amazon CloudWatch Events 的行動

AWS Organizations 可協助您集中管理及治理複雜的環境，並可讓您控制多帳戶環境中的存取、合規與安全。AWS Organizations 支援服務控制政策 (SCP)，其定義了可以對組織中之特定帳戶或組織單位 (OU) 執行的 AWS 服務動作的。

AWS Systems Manager 可協助您掌握及控制 AWS 上的基礎結構。您可以從整合的主控台中，檢視來自多個 AWS 服務的操作資料，並自動執行這些服務中的操作任務。您可以獲取有關近期 API 活動、資源組態變更、操作警示、軟體庫存，以及與修補合規狀態的資訊。您也可以將這項整合與其他 AWS 服務搭配使用，依據您的營運需求，對資源採取動作，以達成環境合規的目的。

例如將 Amazon Inspector 與 AWS Systems Manager 整合，可簡化及自動執行安全評定，原因是您可以在啟動 Amazon EC2 執行個體時，使用 Amazon Elastic Compute Cloud Systems Manager，自動安裝 Amazon Inspector 代理程式。您也可以使用 Amazon EC2 System Manager 與 Lambda 函數，自動修復 Amazon Inspector 結果。

保護您在 AWS 上的資料

GDPR 第 32 條規定，組織必須「...實作適當的技術與組織措施，確認風險的安全層級，包括 ...個人資料的假名化與加密[...]」。此外，組織必須禁止未經授權而揭露或存取個人資料。」

因為沒有正確金鑰，就無法讀取資料，所以加密可以降低個人資料儲存的風險。完整的加密策略有助於降低各種安全事件 (包括一些安全缺口) 的影響。

加密靜態資料

加密靜態資料對於法規合規與資料保護而言非常重要。此作法有助於確保不具有效金鑰的使用者或應用程式，無法讀取儲存在磁碟上的敏感資料。AWS 除了提供多種選項，可以為加密靜態資料及管理加密金鑰。例如，您可以使用在 AWS KMS 中建立及管理 CMK 的 AWS 加密開發套件，為任何資料加密。

加密資料可安全地儲存靜態資料，而且只有具備 CMK 授權之存取權的一方才能解密。因此，您可以從 AWS CloudTrail 取得信封加密的機密資料、用於授權與驗證加密的政策機制及稽核記錄。有一些 AWS 基礎服務內建了加密靜態資料的功能，讓您可以選擇在將資料寫入非揮發性儲存體之前先行加密。例如，您可以使用 AES-256 加密，為 Amazon EBS 磁碟區加密，以及為 Amazon S3 儲存貯體設定伺服器端加密 (SSE)。Amazon S3 也支援用戶端加密，可讓您在將資料傳送至 Amazon S3 之前先行加密。AWS 開發套件支援用戶端加密，有利於物件的加密與解密作業。Amazon RDS 也支援透明資料加密 (TDE)。

其在 Linux Amazon EC2 執行個體存放區上，可以使用內建的 Linux 程式庫加密資料。此方法會透明地加密檔案，保護機密資料。因此，處理資料的應用程式將不會知道磁碟層級加密。

您有兩種方法可以用來加密執行個體存放區上的檔案：

- 磁碟層級加密：若採用此方法，將會使用一或多組加密金鑰，為整個磁碟或磁碟中的區塊加密。磁碟加密會在檔案系統層級之下運作，不會區分作業系統，並會隱藏目錄與檔案資訊，例如名稱與大小。比方說，Encrypting File System 是 Windows NT 作業系統之新技術檔案系統 (NTFS) 的 Microsoft 擴充套件，可提供磁碟加密。
- 檔案系統層級加密：此方法會加密檔案與目錄，但不會加密整個磁碟或分割區。檔案系統層級加密會在檔案系統之上運作，具備跨作業系統的可攜性。

對於非揮發性記憶體界面 (NVMe) 的 SSD 執行個體存放區磁碟區而言，磁碟層級加密是預設選項。NVMe 執行個體儲存體中的資料，會使用執行個體上硬體模組中實作的 XTS-AES-256 區塊編碼器加密。加密金鑰是以硬體模組來產生，且對每個 NVMe 執行個體儲存體設備而言是唯一的。所有加密金鑰會在執行個體停止或終止時銷毀，且無法復原。您不可使用自己的加密金鑰。

加密傳輸資料

AWS 強烈建議您為系統 (含 AWS 內外部的資源) 之間傳輸的資料加密。

當您建立 AWS 帳戶時，會同時在其中佈建邏輯分隔的 AWS 雲端 (Amazon Virtual Private Cloud, Amazon VPC)。您可以在該處您定義的虛擬網絡中，啟動 AWS 資源。您可以完全掌控自己的虛擬網路環境，包括選取自己的 IP 地址範圍、建立子網路，以及設定路由表與網路閘道。您也可以在公司的資料中心與 Amazon VPC 之間，建立硬體的虛擬私有網路 (VPN) 連線，使用 AWS 雲端來擴充您公司的資料中心。

如需了解如何保護您 Amazon VPC 與企業資料中心之間的通訊，有幾個 VPN 連線選項可以選擇。請選擇最符合您需求的連線選項。您可以使用 AWS Client VPN，利用用戶端上的 VPN 服務來安全存取您的 AWS 資源。您也可以使用 AWS Marketplace 中的第三方軟體 VPN 設備，在 Amazon VPC 的 Amazon EC2 執行個體上安裝該設備。或者，您可以建立 IPsec VPN 連線，藉此保護 VPC 與遠端網絡之間的通訊。若要建立從遠端網路到您 Amazon VPC 的專用私有連線，可以使用 AWS Direct Connect。您可以將此連線與 AWS Site-to-Site VPN 合併，建立 IPsec 加密的私有連線。

AWS 提供 TLS 協定的 HTTPS 端點進行通訊，可以在您使用 AWS API 時，為傳輸資料加密。您可以使用 AWS Certificate Manager (ACM) 服務產生、管理及部署您您工作負載系統之間，建立加密傳輸時所使用的私有與公有憑證。Elastic Load Balancing 與 ACM 整合用於支援 HTTPS 協定。若您的內容由 Amazon CloudFront 進行散發，便支援加密端點。

加密工具

AWS 提供各種調整彈性高的資料加密服務、工具與機制，協助保護您儲存於 AWS 上處理的資料。如需 AWS 服務功能與隱私權的相關資訊，請參閱 AWS 服務功能的隱私權注意事項。

AWS 的密碼編譯服務使用各種加密與儲存體技術，以維護靜態或傳輸資料的完整性。AWS 為加密作業提供四種主要工具。

- AWS Key Management Service (AWS KMS) 是 AWS 管理的服務，可產生及管理主金鑰與資料金鑰。AWS KMS 會與許多 AWS 服務整合，以使用客戶帳戶的 AWS KMS 金鑰，為資料進行伺服器端加密。AWS KMS 硬體安全模組 (HSM) 通過 FIPS 140-2 Level 2 驗證。
- AWS CloudHSM 提供通過 FIPS 140-2 Level 3 驗證的 HSM。這些模組可以安全地儲存各種您自我管理的密碼編譯金鑰，包括主金鑰與資料金鑰。
- AWS 密碼編譯服務與工具
  - AWS 加密開發套件提供用戶端加密程式庫，可對所有類型的資料，實作加密與解密作業。

- Amazon DynamoDB 加密用戶端提供用戶端加密程式庫，可在將資料表傳送至資料庫服務 (如 Amazon DynamoDB) 之前先行加密。

AWS Key Management Service

AWS Key Management Service 為受管服務，可讓您輕鬆建立及控制加密資料時所用的加密金鑰，並能使用硬體安全模組 (HSM) 保護金鑰的安全。AWS KMS 與其他幾個 AWS 服務整合，可協助您保護儲存在這些服務上的資料。AWS KMS 也會與 AWS CloudTrail 整合，為您提供記錄依據法規與合規要求而使用之所有金鑰的日誌。

您可以輕鬆建立、匯入及輪換金鑰，也可以從 AWS Management Console 或使用 AWS 開發套件或 AWSAWS CLI，定義使用政策與稽核使用。

無論是自行匯入或由 KMS 代為建立，AWS KMS 中的 CMK 都會以加密格式儲存在高耐用性的儲存體中，以確保其能夠隨需使用。您可選擇讓 KMS 每年一次自動輪換在 KMS 中建立的 CMK，而不需要重新加密已使用主金鑰加密的資料。因為 KMS 可以隨時提供這些 CMK，自動為先前加密的資料解密，所以您無須追蹤先前的 CMK 版本。

對於 AWS KMS 中的任何 CMK，您都可以透過許多存取控制 (包括授予)，以及金鑰政策或 IAM 政策中的金鑰政策條件，控制誰可存取這些金鑰，以及這些人員能夠使用的服務。您也可以從自己的金鑰管理基礎結構中匯入金鑰在 KMS 中使用。

例如，下列政策使用 `kms:ViaService` 條件，允許客戶管理的 CMK，只能請求來自代表特定使用者 (`ExampleUser`) 之特定區域 (us-west-2) 的 Amazon EC2 或 Amazon RDS 時，才能用於指定的動作。

```
{
 “Version”: “2012-10-17”,
 “Statement”: [
     {
        “Effect”: “Allow”,
        “Principal”: {
            “AWS”: “arn:aws:iam::111122223333:user/ExampleUser”
         }
        “Action”: [
             “kms:Encrypt*”,
             “kms:Decrypt”,
             ”kms:ReEncrypt*”,
             “kms:GenerateDataKey*”,
```

```
                    “kms:CreateGrant”,
                    “kms:ListGrants”,
                    “kms:DescribeKey”
                ],
                “Resource”: “*”,
                “Condition”: {
                   “ForAnyValue:StringEquals”: {
                       “kms:ViaService”: [
                            “ec2.us-west-2.amazonaws.com”,
                            “rds.us-west-2.amazonaws.com”
                       ]
                    }
            }
}
```

AWS 服務整合

AWS KMS 已與許多 AWS 服務整合 – 如需整合服務的完整清單，請參閱 KMS 網站。這些整合可讓您輕鬆地使用 AWS KMS CMK，加密您儲存在這些服務上的資料。除了使用客戶管理的 CMK 之外，許多整合服務也可讓您使用自動為您建立並由 AWS 管理的 CMK，但只能在建立該 CMK 的特定服務中使用。

稽核功能

當您每次使用儲存在日誌檔 AWS KMS 中的金鑰時，AWS CloudTrail 都會加以記錄 (該日誌檔會傳遞至您在 CloudTrail 組態中指定的 Amazon S3 儲存貯體)。記錄的資訊包括使用者、時間、日期、執行的作業，以及使用的金鑰等等。

安全性

AWS KMS 的設計在確保無人能夠存取您的主金鑰。此服務採用專為保護您主金鑰而設計的系統，採用大量強化技術，例如一律不將純文字主金鑰儲存在磁碟中、不將這些主金鑰保存在記憶體中，以及限制哪些系統可以存取使用金鑰的主機。所有對服務上之更新軟體的存取，皆由多方存取控制加以控制，亦即稽核與審核是 AWS 內部的獨立小組執行。

如需 AWS KMS 的詳細資訊，請參閱 AWS Key Management Service 白皮書：

AWS CloudHSM

AWS CloudHSM 是位於雲端的硬體安全模組 (HSM)，可讓您在通過 FIPS 140-2 Level 3 驗證的硬體上，產生及使用您的加密金鑰，從而協助您達成資料安全中，公司、合約與法規的合規要求。

您可以使用 AWS CloudHSM 控制加密金鑰與 HSM 所執行的密碼編譯作業。

AWS 與 AWS Marketplace 合作夥伴為保護 AWS 平台中的敏感資料提供了各種解決方案，但對於管理密碼編譯金鑰方面訂有嚴格合約或法規要求的應用程式與資料，有時必須施以更多的保護。之前在儲存敏感性資料 (或保護敏感性資料的加密金鑰) 時，只能選擇在內部部署資料中心，致使您無法將這些應用程式移轉至雲端，或是會大幅降低其效能。AWS CloudHSM 依據政府針對安全管理金鑰的標準而設計，而且通過驗證。您可以使用 HSM 保護您的加密金鑰。您可以安全地產生、儲存及管理加密資料時所用的密碼編譯金鑰，確保只有您可以存取這些金鑰。AWS CloudHSM 不僅能讓您符合嚴格的金鑰管理要求，也能保有應用程式的效能。

AWS CloudHSM 服務可與 Amazon VPC 搭配使用。AWS CloudHSM 執行個體會使用您指定的 IP 地址，佈建在 Amazon VPC 中，以為您的 Amazon EC2 執行個體提供簡單的私有網絡連線。若定位在 Amazon EC2 執行個體附近的 HSM 執行個體，將能減少網路延遲，從而提高應用程式的效能。AWS 為 HSM 執行個體提供專屬專用 (單一租用戶) 的存取權，而這些 HSM 執行個體也會與其他 AWS 客戶區隔。許多區域與可用區域皆有提供 AWS CloudHSM，讓您可以為您的應用程式，新增安全耐用的金鑰儲存體。

整合 AWS 服務與第三方應用程式

您可以將 CloudHSM 搭配 Amazon Redshift、Amazon RDS for Oracle 或第三方應用程式 (例如 SafeNet Virtual KeySecure) 一起使用，做為您的信任根目錄、Apache (SSL 橋接) 或 Microsoft SQL Server (透明資料加密) 等等。您撰寫自己的應用程式時，也可以使用 AWS CloudHSM，以繼續使用標準密碼編譯程式庫，包括 PKCS #11、Java JCA/JCE，以及 Microsoft CAPI 與 CNG。

稽核活動

若您需要追蹤資源變更，或基於安全與合規理由，需要稽核活動，可以使用 AWS CloudTrail，經由 AWS CloudHSM 審核您帳戶發出的管理 API 呼叫。此外也可使用 syslog 稽核對 HSM 設備的作業，或將 syslog 日誌訊息，傳送到自己的收集器。

AWS 密碼編譯服務與工具

AWS 提供了多種符合各種密碼編譯安全標準的機制，讓您用於實作最適切的加密。AWS Encryption 開發套件是用戶端加密程式庫，可於 Java、Python、C、JavaScript，以及支援 Linux、macOS 與 Windows 的命令列界面中使用。該程式庫提供進階的資料保護功能，包括經驗證安全的對稱金鑰演算法套件，像是可以衍生及簽署金鑰的 256 位元 AES-GCM。因為 DynamoDB Encryption Client 專為使用 Amazon DynamoDB 的應用程式所設計，所以使用者可以在將其資料表資料傳送至資料庫之前，先對其施加保護。其也可在擷取資料時，執行驗證與解密。此用戶端可在 Java 與 Python 中使用。

Linux DM-Crypt 基礎結構

Dm-crypt 是 Linux 核心層級的加密機制，可讓使用者掛載加密的檔案系統。在掛載檔案系統的過程中，檔案系統會連結到目錄 (掛載點) 供作業系統使用。掛載之後，檔案系統中的所有檔案無須額外的互動，就能供應用程式使用。然而，當這些檔案儲存於磁碟上時會進行加密。

裝置映射器是 Linux 2.6 與 3.x 核心中的基礎結構，為建立區塊裝置的虛擬層提供了一般性方法。裝置映射器的密碼目標使用核心加密 API，對區塊裝置進行透明加密。這篇文章中的解決方案使用 dm-crypt 與 Logical Volume Manager (LVM) 映射到邏輯磁碟區，搭載了磁碟的檔案系統。LVM 為 Linux 核心提供邏輯磁碟區管理。

經由設計自動保護資料

無論何時，當使用者或應用程式嘗試使用 AWS Management Console、AWS API 或 AWS CLI 時，就會傳送請求給 AWS。AWS 服務收到請求之後，會根據特定的政策評估邏輯，執行一系列的步驟，決定要允許或拒絕請求。除了根憑證請求之外，AWS 預設會拒絕所有對其提出的請求 (套用了預設的拒絕政策)。這表示政策未明確允許的事項，一律會予以拒絕。根據政策定義與最佳實務，AWS 建議您套用最低權限原則，這表示每個元件 (例如使用者、模組或服務) 只能存取完成其任務所需的資源。

此法符合 GDPR 第 25 條所述，「控制者應實作適當的技術與組織措施，實作適當有條理的技術方法，確保會根據預設，只在特定用途需要時，才處理個人資料」。

AWS 也提供工具讓您實作基礎結構即程式碼，在您開始架構設計時，可以使用這套強大的機制加入安全措施。AWS CloudFormation 提供通用語言描述及佈建所有基礎結構資源，包括安全政策與程序。有了這些工具與實務，安全便成為程式碼的一部分，可以根據您組織的要求使用版本控制、監控及修改 (使用版本控制系統)。因為安全程序與政策都能包含在架構定義中，也可以透過組織的安全措施持續監控，使得資料保護可以經由設計來實現。

AWS 如何提供協助

表 1 – AWS 如何協助您導覽 GDPR 合規

區域	描述	AWS 服務與工具
強大的合規架構	適當的技術與組織措施，必須包括「能夠確保處理系統與服務的持續機密性、完整性、可用性與恢復力」。	SOC 1/SSAE 16/ISAE 3402 (前身為 SAS 70) / SOC 2 / SOC 3 PCI DSS 第 1 級 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5)
資料存取控制	控制者「…應實作適當的技術與組織措施，實作適當有條理的技術方法，確保會根據預設，只在特定用途需要時，才處理個人資料。」	AWS Identity and Access Management (IAM) Amazon Cognito AWS Shield 與 AWS WAF AWS Resource Access Manager Amazon CloudFront AWS Organizations AWS CloudTrail
監控與記錄	「每個控制者 (如其適用) 及控制者代表均應保留一份其責任下處理之活動的記錄。」	AWS Config Amazon CloudWatch AWS Control Tower

區域	描述	AWS 服務與工具
	「…控制者與處理者應實作適當的技術與組織措施，確認風險的安全層級 […]」	Amazon GuardDuty Amazon Inspector Amazon Macie AWS Systems Manager AWS Security Hub AWS 工具與開發套件
保護您在 AWS 上的資料	組織必須「實作適當的技術與組織措施，確認風險的安全層級，包括個人資料的假名化與加密」。	AWS Certificate Manager AWS CloudHSM AWS Key Management Service

作者群

此文件的作者包括：

- Tim Anderson，Amazon Web Services 技術產業專家
- Carmela Gambardella，Amazon Web Services 公部門解決方案架構師
- Giuseppe Russo，Amazon Web Services 安全保證經理
- Marta Taggart，Amazon Web Services 資深方案經理
- Luca Iannario，Amazon Web Services 公部門解決方案架構師

文件修訂

日期	描述
2017 年 11 月	首次發行
2020 年 12 月	更新以加入新增的 AWS 服務與功能。

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品與慣例，如有變更，恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶的責任與義務，由 AWS 協議管轄，本文不屬於 AWS 與其客戶之間的任何協議，也並非上述協議的修改。