AWS 隱私權參考架構

AWS 方案指引

AWS 方案指引: AWS 隱私權參考架構

Table of Contents

AWS 隱私權參考架構

Amazon Web Services （貢獻者）

2025 年 9 月 (文件歷史記錄)

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

注意

本指南僅供參考。這不是法律建議，不應倚賴 做為法律建議。 AWS 鼓勵其客戶就其隱私權和資料保護環境的實作取得適當的建議，更普遍地是與其業務相關的適用法律。

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品產品和實務，這些產品和實務可能會有所變更，恕不另行通知，且 (c) 不會對 AWS 及其附屬公司、供應商或授權方提供「原樣」的任何承諾或保證。 AWS 產品或服務不提供任何明示或暗示的保證、聲明或條件。

AWS 對其客戶的責任和責任由協議控制 AWS ，本文件不屬於，也不會修改 AWS 與其客戶之間的任何協議。

簡介

AWS 隱私權參考架構 (AWS PRA) 提供一組專門針對 中隱私權支援控制設計和組態的指導方針 AWS 服務。本指南可協助您做出有關人員、程序和技術的決策，以協助支援 中的隱私權 AWS 雲端。

AWS 共同的責任模型和隱私權

在 中 AWS 雲端，您對 的安全和合規負有共同責任 AWS。 AWS 負責雲端的安全，這表示 AWS 負責保護執行 中提供的所有服務的基礎設施 AWS 雲端。您需負責雲端的安全，這表示您需 AWS 服務 負責根據安全與隱私權要求進行設定和管理。如需詳細資訊，請參閱 AWS 共同責任模型。

AWS 服務 提供的功能可讓您在雲端中實作自己的隱私權控制，以支援您的隱私權需求。您的隱私權責任會根據許多因素而有所不同，包括 AWS 區域 您選擇的 AWS 服務 和 、將這些服務整合到您的 IT 環境，以及適用於您組織和工作負載的法律和法規。

使用 時 AWS 服務，您可以維持對內容的控制。具體而言，客戶內容定義為軟體 （包括機器映像）、資料、文字、音訊、視訊或映像，您或任何最終使用者傳輸給我們，以便處理、儲存或託管與您帳戶相關的 AWS 服務 。它還包括您或最終使用者使用 衍生的任何運算結果 AWS 服務。您負責管理下列由您控制的決策：

- 您選擇在 上收集、存放或處理的資料 AWS
- AWS 服務 您搭配資料使用的
- 您收集、存放或處理資料的 AWS 區域 。
- 資料的格式和結構，以及資料是否遮罩、匿名或加密
- 如何定義、存放、輪換和操作密碼編譯金鑰以進行加密
- 誰有權存取和何時有權存取您的資料，以及如何授予、管理和撤銷這些存取權

了解 AWS 共同責任模型及其通常如何套用到雲端操作後，您必須判斷其如何套用到您的使用案例。AWS 服務 您選擇使用的 會決定您在組織隱私權責任中必須執行的組態數量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 之類的服務被歸類為基礎設施即服務 (IaaS)。因此，如果您使用 Amazon EC2，則必須為訪客作業系統以及您在 EC2 執行個體上安裝的應用程式軟體或公用程式執行所有必要的隱私權組態。當您使用 Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 等抽象服務時， AWS 會負責基礎設施層、作業系統和平台。您的責任是管理和分類資料（客戶內容），並設定用來存取端點的政策，以存放和擷取資料。如需 如何 AWS 協助您保護資料和隱私權的詳細資訊，請參閱 的資料保護和隱私權 AWS。

了解 AWS PRA

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

本節說明 AWS 隱私權參考架構 (AWS PRA) 與其他 AWS 指引之間的關係。本節也會檢閱 AWS PRA 中 AWS 多帳戶環境範例的一般配置和結構。

本節包含下列主題：

- 使用 AWS PRA 和 AWS SRA
- AWS Organizations 和專用帳戶結構
- 操作 AWS 隱私權服務

使用 AWS PRA 和 AWS SRA

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

AWS PRA 提供客戶認為有助於為其基礎設施和工作負載規劃基礎和應用程式層級隱私權控制的模式 AWS。AWS 安全參考架構 (AWS SRA) 提供建置架構的一組準則，該架構可跨 AWS 您的登陸區域和應用程式實作並支援正確的安全控制。為了建立本指南中詳述的隱私權控制， AWS PRA 會採用許多與 AWS SRA 中所述相同的基本準則和帳戶結構。 AWS PRA 和 AWS SRA 會詳細說明許多相同的金鑰 AWS 服務。本指南僅包含這些服務的簡短描述。您可以在 AWS SRA 中進一步了解這些服務及其在安全內容中的使用方式。

AWS SRA 可協助您設計、實作和管理 AWS 安全服務，使其符合 AWS 建議的實務。您可以使用 AWS SRA 做為獨立指南，也可以使用 AWS SRA 和 AWS PRA 做為配套指南。SRA AWS 中詳述的許多安全準則，可與 AWS PRA 中詳述的隱私權控制一起遵循。與安全性類似，有一些基本的隱私權考量事項，有助於在 AWS 雲端 旅程初期進行，因為這些決策可能會影響組織帳戶結構的設計。例如，您可能會考慮的一些問題包括：

- 我的組織如何定義個人資料？

- 我的組織是否支援處理個人資料的應用程式？
- 如何處理處理其他類型管制資料的應用程式？
- 我可以實作哪些組織層級控制，讓開發人員和雲端工程師盡可能遠離個人資料？
- 如何將個人資料與其他類型的資料隔離？
- 我組織的跨邊界資料傳輸要求是什麼？

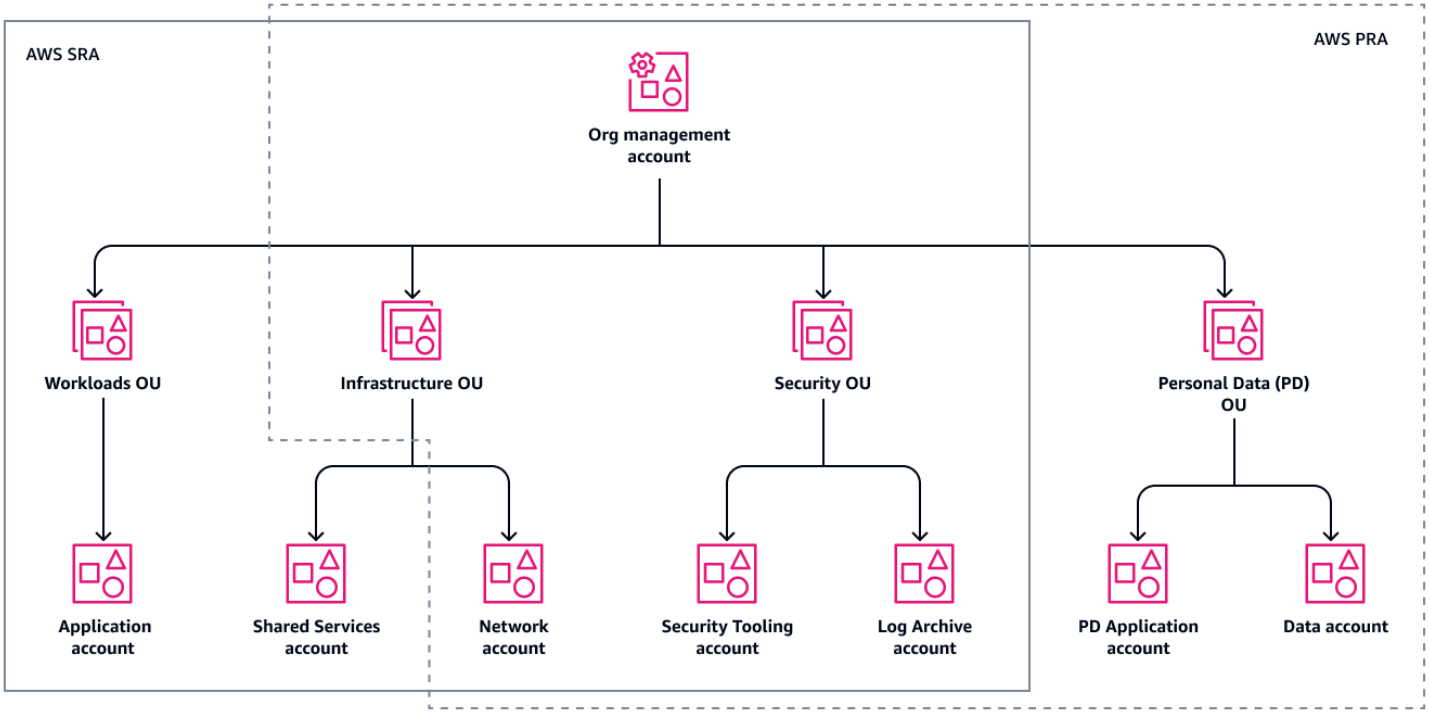
許多這些問題的答案可能會對雲端環境的設計產生影響，例如您的 AWS 帳戶 結構、服務控制政策和 AWS Identity and Access Management (IAM) 角色。

AWS Organizations 和專用帳戶結構

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

AWS Organizations 是一種帳戶管理服務，可協助您集中管理和管理多個 AWS 帳戶。使用 AWS Organizations 是架構良好的多帳戶 AWS 環境的基礎。如需詳細資訊，請參閱建立您的最佳實務 AWS 環境。

下圖顯示 AWS PRA 的高階帳戶和組織單位 (OU) 結構。在大部分情況下，PRA 的組織結構 AWS 符合 AWS SRA 的組織結構。



與 AWS SRA 組織的偏差包括：

- AWS PRA 新增個人資料 (PD) OU，專門用於收集、儲存和處理個人資料。這種結構分離提供了靈活性，因此您可以定義特定、精細的控制，以協助保護個人資料免於意外洩露。
- 在基礎設施 OU 中， AWS PRA 目前不包含 AWS SRA 中所述的共用服務帳戶的其他指引。
- AWS PRA 目前不包含 AWS SRA 中所述的工作負載 OU 的其他指引。收集或處理個人資料的應用程式位於 PD OU 中的專用帳戶中。

您可以使用 AWS Control Tower 進行整體基礎控管，並自動部署整個組織的安全性和隱私權控制。如果 目前 AWS Control Tower 在您的組織中未使用，您仍然可以在其各自服務中部署許多安全與隱私權控制， AWS Control Tower例如服務控制政策和 AWS Config 規則。

當您規劃帳戶和 OU 結構時，考慮處理個人資料可能會有所幫助，包括帳戶區隔策略。您可能需要考慮處理的唯一使用案例和適用法律和法規的資料類型。例如，持卡人資料受到支付卡產業資料安全標準 (PCI DSS) 的保護，受保護的健康資訊可能受到健康保險流通與責任法案 (HIPAA) 的約束。您可能想要檢閱哪些環境包含個人資料，並大幅規劃您的區隔策略。典型的帳戶分割策略可以包括符合軟體開發生命週期 (SDLC) 的專用 AWS 帳戶 帳戶，例如開發專用帳戶、預備或品質保證 (QA) 和生產。這類分割策略可能是整體設計討論中的關鍵元件，您的 OUs 可能需要符合您的特定法規要求。

有些多帳戶 AWS 環境需要每個 的專用應用程式帳戶 AWS 區域，或者可能需要多帳戶登陸區域。在這種情況下，您需要額外的區隔來滿足客戶和監管機構的獨特資料主權要求。如需詳細資訊，請參閱本指南中的 全球擴展的規劃。

操作 AWS 隱私權服務

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

對許多人而言，隱私權是跨截斷的。許多不同的團隊都有自己的角色，包括法規、合規和工程團隊。當您的組織開始定義隱私權計劃的關鍵人員和政策元件時，您可以將控制項對應至隱私權合規架構，以實現一致的操作。架構可做為在 AWS 環境中實作個人資料之基礎和應用程式特定隱私權控制的機制。

無論客戶用來分類其隱私權需求的架構為何，隱私權合規、隱私權工程和應用程式團隊通常都需要合作才能實現實作目標。例如，法規和合規團隊可能會提供高階需求，而工程和應用程式團隊會設定 AWS 服務 和 功能以符合這些需求。從控制架構開始，可協助您定義更具規範的組織和技術控制。

定義 AWS 服務 和 功能的技術控制項時，另一個關鍵決策是是否應將控制項套用至整個組織、OU、帳戶或特定資源。有些服務和功能非常適合在整個 AWS 組織中實作控制項。例如，封鎖對 Amazon S3 儲存貯體的公開存取是特定的控制項，最好是在組織根目錄設定，而不是針對每個帳戶個別設定。不過，您的保留政策可能因應用程式而異，這表示您可以在資源層級套用控制項。

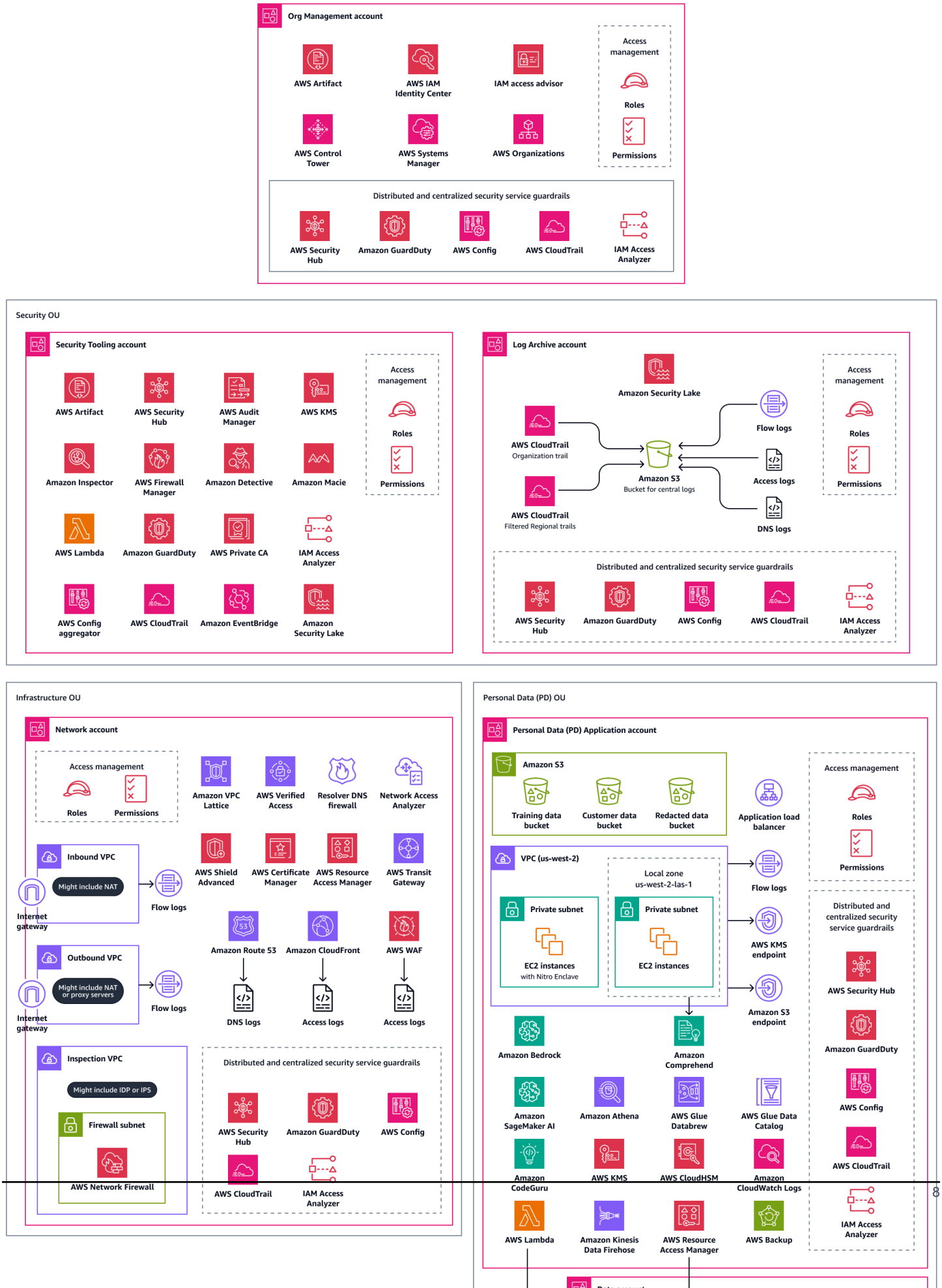
為了協助您加速組織中的隱私權操作， 為您的 AWS 工作負載 AWS 提供稽核和合規顧問服務。如需詳細資訊，請聯絡 AWS SAS。

AWS 隱私權參考架構

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

下圖說明 AWS 隱私權參考架構 (AWS PRA)。這是連接許多隱私權相關 AWS 服務 和 功能的架構範例。此架構建置在由 管理的登陸區域上 AWS Control Tower。


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Amazon Security Lake
Log Archive account
Amazon Security Lake
AWS CloudTrail
Organization trail
Flow logs
Access logs
DNS logs
Amazon S3
Bucket for central logs
AWS CloudTrail
Filtered Regional trails
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

AWS PRA 包含在個人資料 (PD) 應用程式帳戶中託管的無伺服器 Web 架構。此帳戶中的架構是直接從消費者收集個人資料的範例工作負載。在此工作負載中，使用者會透過 Web 層連線。Web 層會與應用程式層互動。此層接收來自 Web 層的輸入、處理和存放資料、允許授權的內部團隊和第三方存取資料，以及最終在不再需要資料時封存和刪除資料。架構是刻意模組化且事件驅動的，目的是示範許多基礎隱私權工程技術，而不會深入了解特定使用案例，例如資料湖、容器、運算或物聯網 (IoT)。

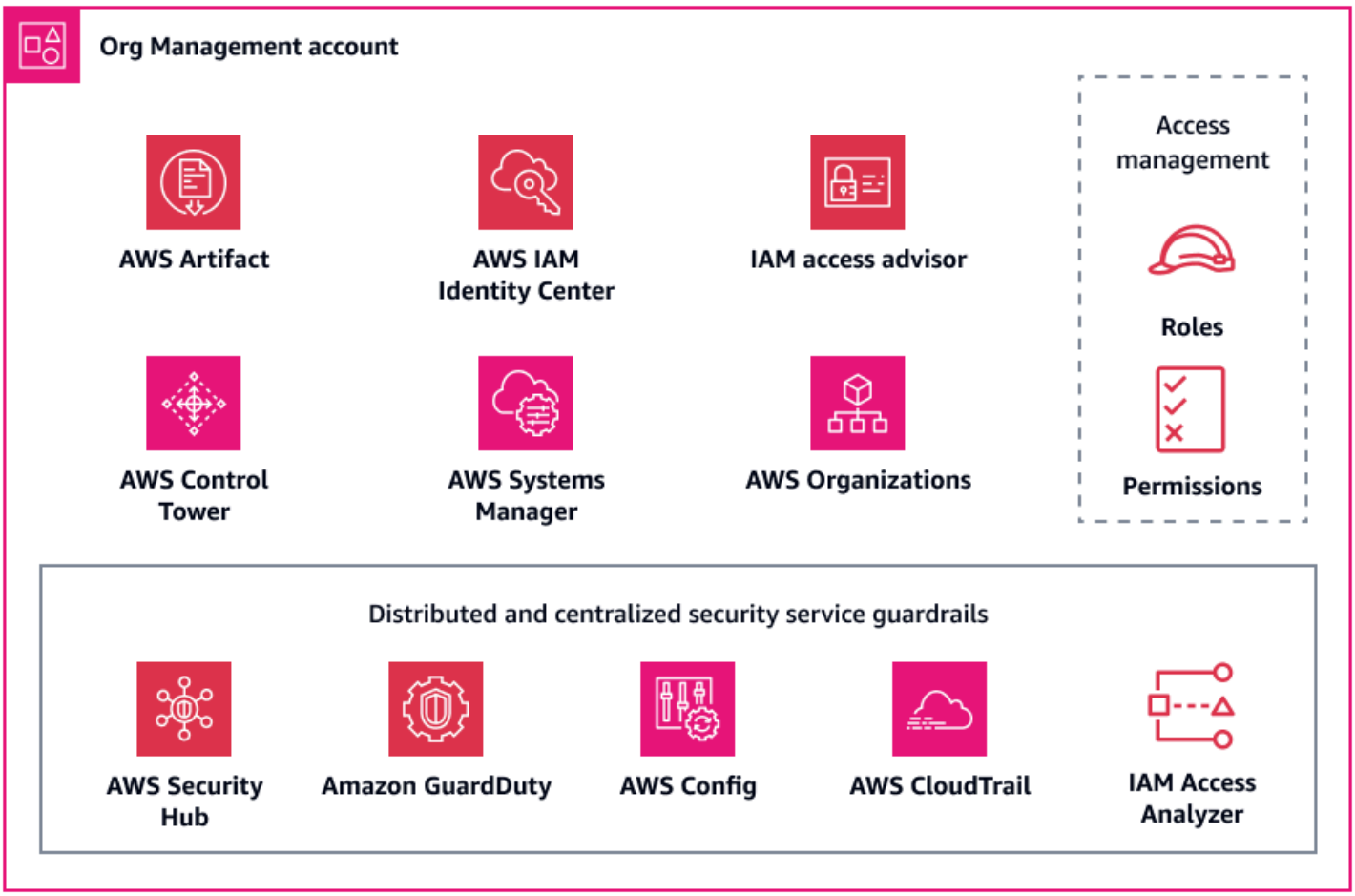
接下來，本指南會詳細說明組織中的每個帳戶。它討論了與隱私權相關的服務和功能、考量事項和建議，以及下列每個帳戶的圖表：

- 組織管理帳戶
- Security OU – 安全工具帳戶
- 安全 OU – Log Archive 帳戶
- 基礎設施 OU – 網路帳戶
- 個人資料 OU – PD 應用程式帳戶

組織管理帳戶

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

Org Management 帳戶主要用於管理組織中所有帳戶的基礎隱私權控制的資源組態偏離，這些帳戶由管理 AWS Organizations。此帳戶也是您可以一致地部署新成員帳戶的地方，具有許多相同的安全和隱私權控制。如需此帳戶的詳細資訊，請參閱AWS 安全參考架構 (AWS SRA)。下圖說明組織管理帳戶中設定 AWS 的安全性和隱私權服務。



本節提供此帳戶中 AWS 服務 所用下列項目的更多詳細資訊：

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifact 可透過隨需下載 AWS 安全與合規文件，協助您進行稽核。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

這 AWS 服務 可協助您了解繼承的 AWS 控制項，並判斷在環境中實作可能還剩哪些控制項。 AWS Artifact 提供 AWS 安全和合規報告的存取權，例如系統和組織控制 (SOC) 報告和支付卡產業 (PCI) 報告。它也提供跨地理位置和合規垂直機構的認證存取權，以驗證 AWS 控制的實作和操作有效性。使用 AWS Artifact， 您可以將 AWS 稽核成品提供給稽核人員或監管機構，做為 AWS 安全和隱私權控制的證據。下列報告可能有助於示範 AWS 隱私權控制的有效性：

- SOC 2 第 2 類隱私權報告 – 此報告示範了如何收集、使用、保留、揭露和處置個人資料的 AWS 控制的有效性。也有 SOC 3 隱私權報告，這是 SOC 2 隱私權控制的詳細描述。如需詳細資訊，請參閱 SOC 常見問答集。
- 雲端運算合規控制目錄 (C5) – 此報告是由德國國家網路安全局 Bundesamt für Sicherheit in der Informationstechnik (BSI) 所建立。它詳細說明了為了符合 C5 要求而 AWS 實作的安全控制。它還包含與資料位置、服務佈建、司法管轄區和資訊披露義務相關的其他隱私權控制要求。
- ISO/IEC 27701：2019 認證報告 –—ISO/IEC 27701：2019 說明建立和持續改善隱私權資訊管理系統 (PIMS) 的要求和指導方針。此報告會詳細說明此認證的範圍，並可做為 AWS 認證證明。如需此標準的詳細資訊，請參閱 ISO/IEC 27701：2019 (ISO 網站）。

AWS Control Tower

AWS Control Tower 可協助您設定和管理遵循規範性安全建議實務的 AWS 多帳戶環境。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

在 中 AWS Control Tower，您也可以自動化部署許多主動、預防性和偵測性控制項，也稱為護欄，這些控制項符合您的資料隱私權要求，特別是針對資料落地和主權。例如，您可以指定將資料傳輸限制為僅核准 的護欄 AWS 區域。如需更精細的控制，您可以從超過 17 個旨在控制資料駐留的 護欄中進行選擇，例如不允許 Amazon Virtual Private Network (VPN) 連線、不允許 Amazon VPC 執行個體的網際網路存取，以及 AWS 根據請求拒絕對 的存取 AWS 區域。這些護欄由許多勾 AWS CloudFormation 點、服務控制政策和 AWS Config 規則組成，可統一部署到整個組織中。如需詳細資訊，請參閱 AWS Control Tower 文件中的增強資料駐留保護的控制項。

對於資料主權， AWS Control Tower 目前提供預防性控制，例如需要將連接的 Amazon EBS 磁碟區設定為加密靜態資料，以及需要 AWS KMS 金鑰政策才能擁有限制 AWS KMS 授予建立的陳述式 AWS 服務。主權控制比資料駐留控制更廣泛。它們有助於防止可能違反資料駐留、精細存取限制、加密和彈性要求的動作。如需詳細資訊，請參閱 AWS Control Tower 文件中的協助數位主權的預防性控制。

如果您需要在資料駐留和主權控制之外部署隱私權護欄， AWS Control Tower 包含許多強制性控制。當您設定登陸區域時，這些控制項預設會部署到每個 OU。其中許多都是旨在保護日誌的預防性控制，例如不允許刪除日誌封存和啟用 CloudTrail 日誌檔案的完整性驗證。

AWS Control Tower 也與 整合 AWS Security Hub CSPM ，以提供偵測性控制。這些控制項稱為服務受管標準： AWS Control Tower。您可以使用這些控制項來監控隱私權支援控制項的組態偏離，例如 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體的靜態加密。

AWS Organizations

AWS PRA 使用 AWS Organizations 來集中管理架構中的所有帳戶。如需詳細資訊，請參閱本指南中的 AWS Organizations 和專用帳戶結構。在 中 AWS Organizations，您可以使用服務控制政策 SCPs) 和管理政策來協助保護個人資料和隱私權。

服務控制政策 (SCP)

服務控制政策 SCPs) 是一種組織政策，可用來管理組織中的許可。它們可集中控制目標帳戶、組織單位 AWS Identity and Access Management (OU) 或整個組織中 (IAM) 角色和使用者的最大可用許可。您可以從組織管理帳戶建立和套用 SCPs。

您可以使用 AWS Control Tower 在您的 帳戶間統一部署 SCPs。如需有關可套用的資料駐留控制的詳細資訊 AWS Control Tower，請參閱本指南AWS Control Tower中的 。 AWS Control Tower 包含預防性 SCPs的完整補充。如果您的組織中目前 AWS Control Tower 未使用 ，您也可以手動部署這些控制項。

使用 SCPs來處理資料駐留需求

通常透過在特定地理區域內存放和處理資料來管理個人資料駐留要求。為了確認符合司法管轄區的唯一資料落地要求，我們建議您與法規團隊緊密合作，以確認您的要求。確定這些要求後，有一些 AWS 基本的隱私權控制可以協助支援。例如，您可以使用 SCPs 來限制 AWS 區域 可用於處理和存放資料的 SCP。如需範例政策，請參閱本指南限制跨 的資料傳輸 AWS 區域中的 。

使用 SCPs 限制高風險 API 呼叫

請務必了解 AWS 負責哪些安全與隱私權控制，以及您負責哪些安全與隱私權控制。例如，您必須負責對您使用的 進行 API AWS 服務 呼叫的結果。您也必須負責了解哪些呼叫可能會導致安全性或隱私權狀態變更。如果您擔心維護特定安全性和隱私權狀態，您可以啟用拒絕特定 API 呼叫SCPs。這些 API 呼叫可能會有影響，例如意外公開個人資料或違反特定跨邊界資料傳輸。例如，您可能想要禁止下列 API 呼叫：

- 啟用對 Amazon Simple Storage Service (Amazon S3) 儲存貯體的公開存取
- 停用 Amazon GuardDuty 或為資料外洩問題清單建立抑制規則，例如木馬程式：EC2/DNSDataExfiltration 問題清單
- 刪除 AWS WAF 資料外洩規則
- 公開共用 Amazon Elastic Block Store (Amazon EBS) 快照
- 從組織移除成員帳戶
- 取消 Amazon CodeGuru Reviewer 與儲存庫的關聯

管理政策

中的管理政策 AWS Organizations 可協助您集中設定和管理 AWS 服務 及其功能。您選擇的管理政策類型會決定政策如何影響繼承政策的 OUs和帳戶。標籤政策是 中與隱私權 AWS Organizations 直接相關的管理政策範例。

使用標籤政策

標籤是可協助您管理、識別、組織、搜尋和篩選 AWS 資源的關鍵值對。套用可區分組織中處理個人資料之資源的標籤會很有用。使用標籤支援本指南中的許多隱私權解決方案。例如，您可能想要套用標籤，指出正在資源中處理或存放之資料的一般資料分類。您可以撰寫屬性型存取控制 (ABAC) 政策，限制對具有特定標籤或一組標籤的資源的存取。例如，您的政策可能會指定 SysAdmin角色無法存取具有 dataclassification:4標籤的資源。如需詳細資訊和教學課程，請參閱 IAM 文件中的根據標籤定義存取 AWS 資源的許可。此外，如果您的組織使用 AWS Backup 在許多帳戶中的備份之間廣泛套用資料保留政策，您可以套用將資源置於該備份政策範圍內的標籤。

標籤政策可協助您在整個組織中維持一致的標籤。在標籤政策中，您可以指定在資源加上標籤時套用的規則。例如，您可以要求資源加上特定金鑰的標籤，例如 DataClassification或 DataSteward，而且您可以為金鑰指定有效的大小寫處理方式或值。您也可以使用強制執行來防止不合規標記請求完成。

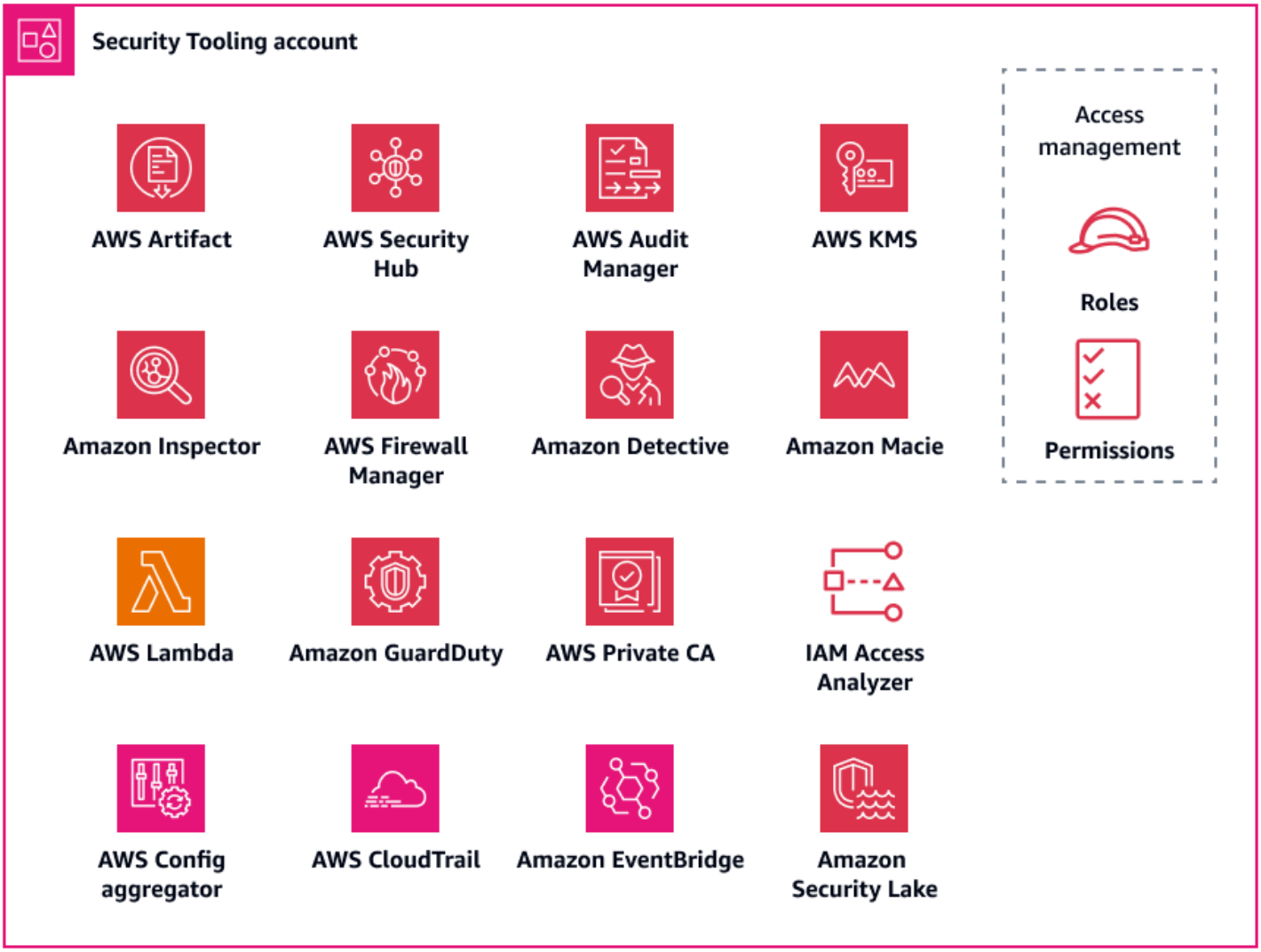
使用標籤做為隱私權控制策略的核心元件時，請考慮下列事項：

- 考慮將個人資料或其他類型的敏感資料放置在標籤索引鍵或值中的影響。當您聯絡 AWS 以取得技術協助時， AWS 可能會分析標籤和其他資源識別符，以協助解決問題。標籤資料不會加密 AWS 服務，例如 AWS 帳單與成本管理， 可以讀取這些資料。因此，您可能想要取消識別標籤值，然後使用您控制的系統重新識別它們，例如 IT 服務管理 (ITSM) 系統。 AWS 建議不要在標籤中包含個人識別資訊。
- 請考慮某些標籤值需要不可變 （不可修改），以防止規避技術控制項，例如依賴標籤的 ABAC 條件。

Security OU – 安全工具帳戶

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

Security Tooling 帳戶專用於操作安全性和隱私權基礎服務 AWS 帳戶、監控和自動化安全性和隱私權提醒和回應。如需此帳戶的詳細資訊，請參閱AWS 安全參考架構 (AWS SRA)。下圖說明 AWS Security Tooling 帳戶中設定的安全和隱私權服務。



本節提供有關此帳戶中下列項目的更多詳細資訊：

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- IAM Access Analyzer
- Amazon Macie

AWS CloudTrail

AWS CloudTrail 可協助您稽核 中的整體 API 活動 AWS 帳戶。在儲存、 AWS 區域 處理或傳輸個人資料的所有 AWS 帳戶 和 中啟用 CloudTrail，可協助您追蹤此資料的使用和揭露。AWS 安全參考架構建議啟用組織線索，這是記錄組織中所有帳戶所有事件的單一線索。不過，啟用此組織追蹤會將多區域日誌資料彙總到 Log Archive 帳戶中的單一 Amazon Simple Storage Service (Amazon S3) 儲存貯體。對於處理個人資料的帳戶，這可能會帶來一些額外的設計考量。日誌記錄可能包含一些對個人資料的參考。為了滿足您的資料駐留和資料傳輸需求，您可能需要重新考慮將跨區域日誌資料彙總到 S3 儲存貯體所在的單一區域。您的組織可能會考慮應該在組織追蹤中包含或排除哪些區域工作負載。對於您決定從組織追蹤中排除的工作負載，您可以考慮設定遮蔽個人資料的區域特定追蹤。如需遮罩個人資料的詳細資訊，請參閱本指南的 Amazon Data Firehose一節。最後，您的組織可能有組織追蹤和區域追蹤的組合，這些追蹤會彙總到集中式 Log Archive 帳戶。

如需設定單一區域追蹤的詳細資訊，請參閱使用 AWS Command Line Interface (AWS CLI) 或 主控台的指示。當您建立組織追蹤時，您可以使用 中的選擇加入設定AWS Control Tower，也可以直接在 CloudTrail 主控台中建立追蹤。

如需整體方法以及如何管理日誌和資料傳輸需求的集中的詳細資訊，請參閱本指南中的 集中式日誌儲存一節。無論您選擇何種組態，您可能想要根據 AWS SRA，將安全工具帳戶中的線索管理與日誌封存帳戶中的日誌儲存區分開。此設計可協助您為需要管理日誌和需要使用日誌資料的人員建立最低權限的存取政策。

AWS Config

AWS Config 提供 中資源的詳細檢視 AWS 帳戶 及其設定方式。它可協助您識別資源彼此之間的關聯，以及其組態隨著時間的變化。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

在 中 AWS Config，您可以部署一致性套件，這是一組 AWS Config 規則和修補動作。一致性套件提供一般用途架構，旨在使用受管或自訂 AWS Config 規則來啟用隱私權、安全性、營運和成本最佳化控管檢查。您可以使用此工具做為較大型自動化工具的一部分，來追蹤 AWS 資源組態是否符合您自己的控制架構需求。

NIST 隱私權架構 v1.0 一致性套件的操作最佳實務符合 NIST 隱私權架構中的許多隱私權相關控制項。每個 AWS Config 規則都適用於特定 AWS 資源類型，並且與一或多個 NIST 隱私權架構控制項相關。您可以使用此一致性套件來追蹤帳戶中資源的隱私權相關持續合規。以下是此一致性套件中包含的一些規則：

- `no-unrestricted-route-to-igw` – 此規則透過持續監控 VPC 路由表的預設`0.0.0.0/0`或`::/0`輸出路由至網際網路閘道，協助防止資料平面上的資料外洩。這可協助您限制可傳送網際網路流量的位置，尤其是在已知有惡意 CIDR 範圍的情況下。
- `encrypted-volumes` – 此規則會檢查連接至 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的 Amazon Elastic Block Store (Amazon EBS) 磁碟區是否加密。如果您的組織有與使用 AWS Key Management Service (AWS KMS) 金鑰來保護個人資料相關的特定控制要求，您可以將特定金鑰 IDs 指定為規則的一部分，以檢查磁碟區是否使用特定 AWS KMS 金鑰加密。
- `restricted-common-ports` – 此規則會檢查 Amazon EC2 安全群組是否允許指定連接埠不受限制的 TCP 流量。安全群組可以透過提供傳入和傳出資源網路流量的狀態篩選，來協助您管理網路存取 AWS 。在 資源上封鎖從 `0.0.0.0/0`到 TCP 3389 和 TCP 21 等常見連接埠的輸入流量，可協助您限制遠端存取。

AWS Config 可用於主動 AWS 和被動的 資源合規檢查。除了考量一致性套件中的規則之外，您還可以在偵測和主動評估模式中整合這些規則。這有助於在軟體開發生命週期的早期實作隱私權檢查，因為應用程式開發人員可以開始整合部署前檢查。例如，他們可以在其 AWS CloudFormation 範本中包含勾點，根據所有已啟用主動模式的隱私權相關 AWS Config 規則，檢查範本中宣告的資源。如需詳細資訊，請參閱AWS Config 規則現在支援主動式合規 (AWS 部落格文章）。

Amazon GuardDuty

AWS 提供多種服務，可用於存放或處理個人資料，例如 Amazon S3、Amazon Relational Database Service (Amazon RDS) 或 Amazon EC2 搭配 Kubernetes。Amazon GuardDuty 結合了智慧型可見性與持續監控，可偵測可能與意外洩漏個人資料相關的指標。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

使用 GuardDuty，您可以在整個攻擊生命週期中識別潛在的惡意隱私權相關活動。例如，GuardDuty 可以提醒您有關黑名單網站的連線、不尋常的網路連接埠流量或流量、DNS 洩漏、非預期的 EC2 執行個體啟動，以及不尋常的 ISP 發起人。您也可以設定 GuardDuty 來停止來自您信任 IP 清單的信任 IP 地址提醒，以及來自您威脅清單的已知惡意 IP 地址提醒。

如 AWS SRA 中建議，您可以為 AWS 帳戶 組織中的所有 啟用 GuardDuty，並將安全工具帳戶設定為 GuardDuty 委派管理員。GuardDuty 會將整個組織的調查結果彙總到此單一帳戶。如需詳細資訊，請參閱使用 管理 GuardDuty 帳戶 AWS Organizations。您也可以考慮在事件回應程序中識別所有與隱私權相關的利益相關者，從偵測和分析到遏制和消除，並讓他們參與任何可能涉及資料外洩的事件。

IAM Access Analyzer

許多客戶希望持續確保與預先核准和預期的第三方處理器適當共用個人資料，而不是其他實體。資料周邊是一組預防性護欄，旨在僅允許來自預期網路的受信任身分存取您 AWS 環境中的受信任資源。當您定義意外和預期公開個人資料的控制時，您可以定義信任的身分、信任的資源和預期的網路。

透過 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)，組織可以定義信任 AWS 帳戶 區域，並設定該信任區域的違規提醒。IAM Access Analyzer 會分析 IAM 政策，以協助識別和解決對潛在敏感資源的意外公有或跨帳戶存取。IAM Access Analyzer 使用數學邏輯和推論，為可從 外部存取的資源產生全面的調查結果 AWS 帳戶。最後，為了回應和修復過度寬鬆的 IAM 政策，您可以使用 IAM Access Analyzer 根據 IAM 建議的做法驗證現有政策並提供建議。IAM Access Analyzer 可以根據 IAM 主體先前的存取活動產生最低權限的 IAM 政策。它會分析 CloudTrail 日誌並產生僅授予繼續執行這些任務所需許可的政策。

如需如何在安全內容中使用 IAM Access Analyzer 的詳細資訊，請參閱 AWS 安全參考架構。

Amazon Macie

Amazon Macie 是一種服務，使用機器學習和模式比對來探索敏感資料、提供資料安全風險的可見性，並協助您自動化對這些風險的保護。Macie 在偵測到 Amazon S3 儲存貯體的安全性或隱私權潛在政策違規或問題時產生調查結果。Macie 是另一個工具，組織可用來實作自動化，以支援合規工作。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

Macie 可以偵測大量且不斷增長的敏感資料類型清單，包括個人身分識別資訊 (PII)，例如名稱、地址和其他可識別屬性。您甚至可以建立自訂資料識別符，以定義可反映組織個人資料定義的偵測條件。

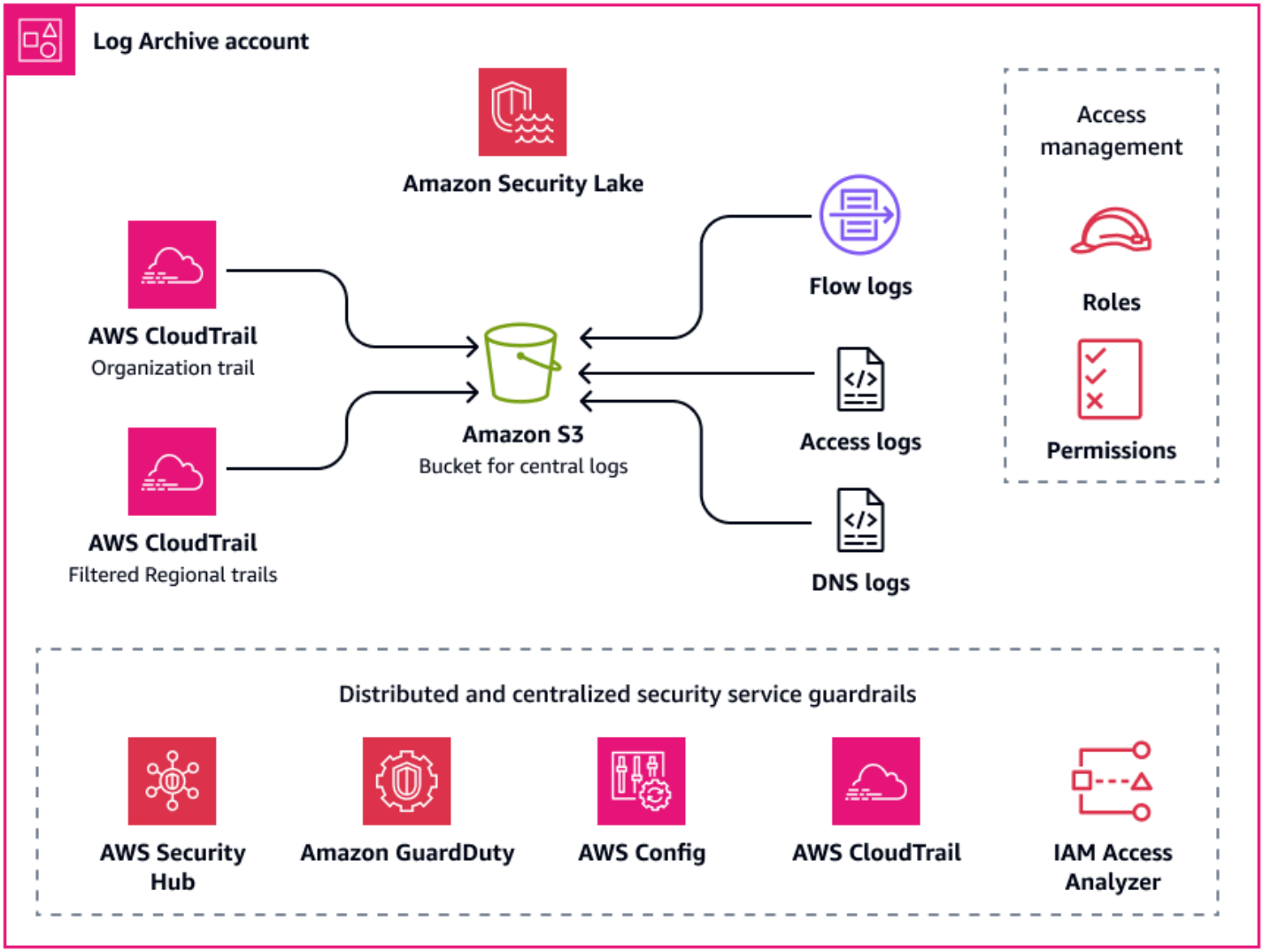
當您的組織為包含個人資料的 Amazon S3 儲存貯體定義預防性控制時，您可以使用 Macie 作為驗證機制，以持續確保個人資料的所在位置及其保護方式。若要開始，請啟用 Macie 並設定自動敏感資料探索。Macie 會持續分析所有 S3 儲存貯體中跨帳戶和 的物件 AWS 區域。Macie 會產生並維護互動式熱度圖，描述個人資料所在的位置。自動化敏感資料探索功能旨在降低成本，並將手動設定探索任務的需求降至最低。您可以在自動化敏感資料探索功能的基礎上建置 ，並使用 Macie 自動偵測現有儲存貯體中的新儲存貯體或新資料，然後根據指派的資料分類標籤驗證資料。設定此架構，以及時通知適當的開發和隱私權團隊分類錯誤或未分類的儲存貯體。

您可以使用 為組織中的每個帳戶啟用 Macie AWS Organizations。如需詳細資訊，請參閱在 Amazon Macie 中整合和設定組織。

安全 OU – Log Archive 帳戶

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

Log Archive 帳戶可讓您集中基礎設施、服務和應用程式日誌類型。如需此帳戶的詳細資訊，請參閱AWS 安全參考架構 (AWS SRA)。透過日誌的專用帳戶，您可以在所有日誌類型中套用一致的提醒，並確認事件回應者可以從單一位置存取這些日誌的彙總。您也可以從一個位置設定安全控制和資料保留政策，這可以簡化隱私權營運開銷。下圖說明在 AWS Log Archive 帳戶中設定的安全性和隱私權服務。



集中式日誌儲存

日誌檔案 （例如 AWS CloudTrail 日誌） 可能包含可視為個人資料的資訊。有些組織選擇使用組織線索，將跨帳戶 AWS 區域 和跨帳戶的 CloudTrail 日誌彙總到一個集中位置，以便可見。如需詳細資訊，請參閱本指南中的 AWS CloudTrail。實作 CloudTrail 日誌的集中化時，日誌通常會存放在單一區域的 Amazon Simple Storage Service (Amazon S3) 儲存貯體中。

根據您組織對個人資料的定義、您對客戶的合約義務，以及適用的區域隱私權法規，您可能需要在記錄彙總時考慮跨邊界資料傳輸。判斷各種日誌類型內的個人資料是否屬於這些限制。例如，CloudTrail 日誌可能包含您組織的員工資料，但可能不包含您客戶的個人資料。如果您的組織需要遵守受限的資料傳輸要求，下列選項有助於支援：

- 如果您的組織在 中 AWS 雲端 向多個國家/地區的資料主體提供服務，您可以選擇彙總具有最嚴格資料駐留要求的國家/地區中的所有日誌。例如，如果您在德國營運，且要求最嚴格，您可以在 的 S3 儲存貯體中彙總資料，`eu-central-1` AWS 區域 以便在德國收集的資料不會離開德國邊界。對於此選項，您可以在 CloudTrail 中設定單一組織線索，將日誌從所有帳戶彙總 AWS 區域 到目標區域。
- 在將資料複製並彙總到另一個區域 AWS 區域 之前，修改需要保留在 中的個人資料。例如，您可以在將日誌轉移到不同區域之前，遮蔽應用程式主機區域中的個人資料。如需遮罩個人資料的詳細資訊，請參閱本指南的 Amazon Data Firehose一節。
- 如果您有嚴格的資料主權問題，您可以在 中維護單獨的多帳戶登陸區域 AWS 區域 ，以強制執行這些要求。如此一來，您就可以簡化 區域中的登陸區域組態，以進行集中式記錄。它還提供額外的基礎設施隔離優勢，並有助於將日誌保留在自己的區域本機。與您的法律顧問合作，判斷哪些個人資料在範圍內，以及允許哪些Region-to-Region傳輸。如需詳細資訊，請參閱本指南中的 全球擴展的規劃。

透過服務日誌、應用程式日誌和作業系統 (OS) 日誌，您可以依預設使用 Amazon CloudWatch 來監控其對應帳戶和區域中的 AWS 服務 或 資源。許多選擇將這些日誌和指標從多個帳戶和區域集中到單一帳戶。根據預設，這些日誌會保留在其對應的 帳戶和其來源的區域中。對於集中化，您可以使用訂閱篩選條件和 Amazon S3 匯出任務，將資料共用到集中位置。從具有跨邊界資料傳輸需求的工作負載彙總日誌時，包含適當的篩選條件和匯出任務可能很重要。如果工作負載的存取日誌包含個人資料，您可能需要確保這些資料會傳輸至或保留在特定帳戶和區域中。

Amazon Security Lake

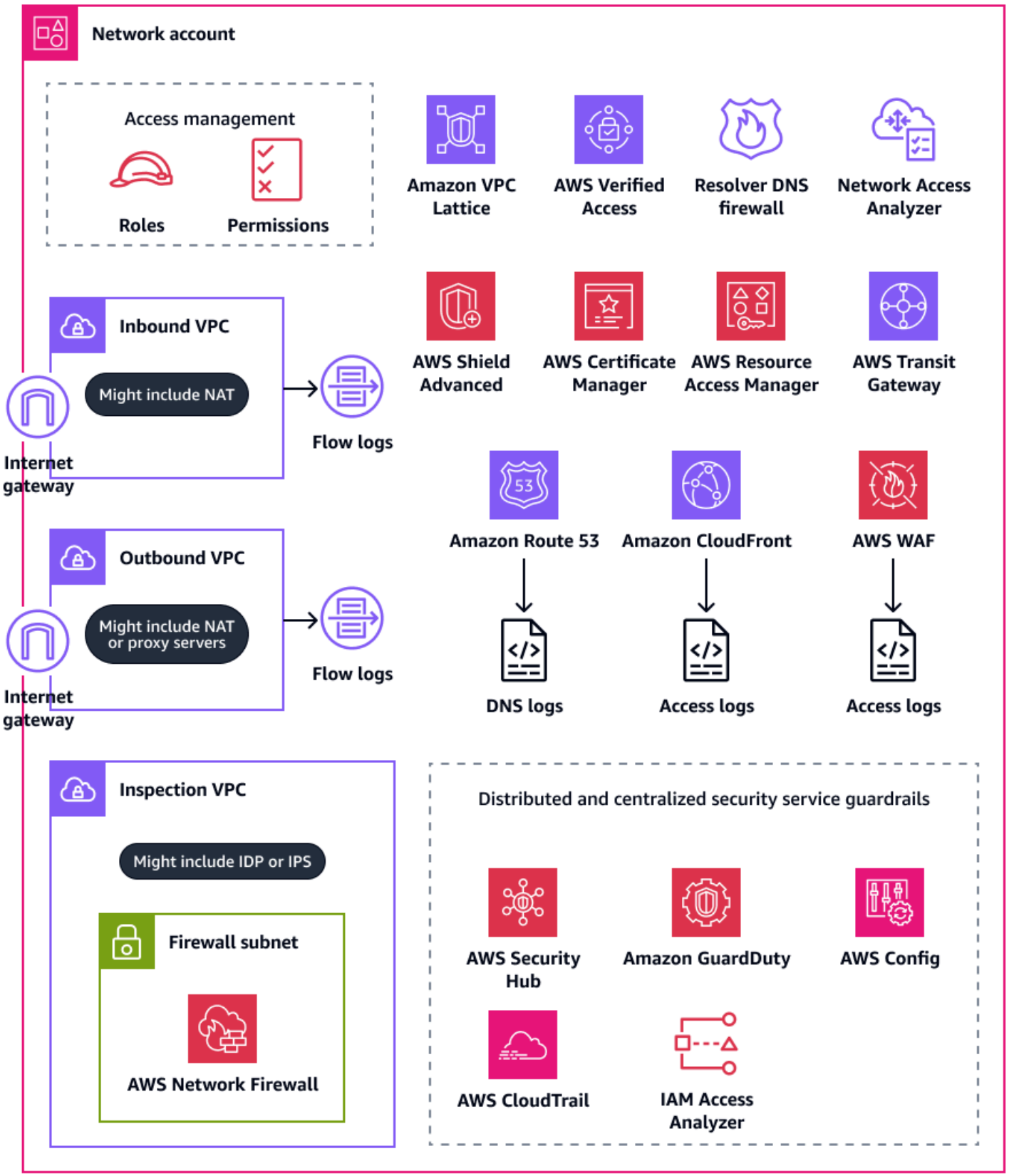
如 AWS SRA 中建議，您可能想要使用 Log Archive 帳戶做為 Amazon Security Lake 的委派管理員帳戶。當您這樣做時，Security Lake 會在與其他 SRA 建議的安全性日誌相同的帳戶中的專用 Amazon S3 儲存貯體中收集支援的日誌。

從隱私權的角度來看，事件回應者必須能夠從 AWS 環境、SaaS 供應商、內部部署、雲端來源和第三方來源存取日誌。這有助於他們更快封鎖和修復對個人資料的未經授權存取。日誌儲存的相同考量最可能適用於 Amazon Security Lake 內的日誌落地和區域移動。這是因為 Security Lake 會從您啟用服務的 AWS 區域 收集安全日誌和事件。若要符合資料駐留要求，請考慮您的彙總區域組態。 彙總區域是 Security Lake 合併您選取的一或多個貢獻區域中的資料的區域。您的組織可能需要符合資料駐留的區域合規要求，才能設定 Security Lake 和彙總區域。

基礎設施 OU – 網路帳戶

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

在網路帳戶中，您可以管理虛擬私有雲端 (VPCs) 與更廣泛的網際網路之間的聯網。在此帳戶中，您可以使用 AWS WAF、使用 AWS Resource Access Manager (AWS RAM) 共用 VPC 子網路和 AWS Transit Gateway 附件，以及使用 Amazon CloudFront 支援目標服務用量，來實作廣泛的揭露控制機制。如需此帳戶的詳細資訊，請參閱AWS 安全參考架構 (AWS SRA)。下圖說明網路帳戶中設定 AWS 的安全和隱私權服務。



本節提供此帳戶中 AWS 服務 所用下列項目的更多詳細資訊：

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront 支援前端應用程式和檔案託管的地理限制。CloudFront 可以透過稱為節點的資料中心全球網路交付內容。當使用者請求您使用 CloudFront 提供的內容時，請求會路由到提供最低延遲的節點。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

您的隱私權計劃目前可能支援遵守特定區域法律。如果您的工作負載的範圍僅限於為僅位於這些區域內的客戶提供服務，您可以實作技術措施來防止來自其他區域的使用。您可以使用 CloudFront 地理限制，防止特定地理位置的使用者存取您透過 CloudFront 分佈分佈的內容。如需地理限制的詳細資訊和組態選項，請參閱 CloudFront 文件中的限制內容的地理分佈。

您也可以設定 CloudFront 產生存取日誌，其中包含 CloudFront 收到的每個使用者請求的詳細資訊。如需詳細資訊，請參閱 CloudFront 文件中的設定和使用標準日誌（存取日誌）。最後，如果 CloudFront 設定為在一系列節點快取內容，您可能會考慮快取發生的位置。對於某些組織，跨區域快取可能會受到跨邊界資料傳輸要求的約束。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) 可協助您安全地跨 共用資源 AWS 帳戶 ，以減少營運開銷並提供可見性和可稽核性。透過 AWS RAM，組織可以限制哪些 AWS 資源可以與其 AWS 帳戶 組織中的其他 或第三方帳戶共用。如需詳細資訊，請參閱可共用 AWS 資源。在網路帳戶中，您可以使用 AWS RAM 來共用 VPC 子網路和傳輸閘道連線。如果您使用 與其他 AWS RAM 共用資料平面連線 AWS 帳戶，您可以考慮建立程序，以檢查是否已進行預先核准的連線， AWS 區域 並遵守您的資料駐留需求。

除了共用 VPCs和傳輸閘道連線之外， AWS RAM 還可以用來共用不支援 IAM 資源型政策的資源。對於在個人資料 OU 中託管的工作負載，您可以使用 AWS RAM 存取位於個別 中的個人資料 AWS 帳戶。如需詳細資訊，請參閱個人資料 OU – PD 應用程式帳戶一節AWS Resource Access Manager中的 。

AWS Transit Gateway

如果您想要部署在 中收集、存放或處理個人資料 AWS 的資源 AWS 區域 ，以符合組織資料駐留需求，而且您有適當的技術保護措施，請考慮實作護欄，以防止控制項和資料平面上未經核准的跨邊界資料流程。在控制平面上，您可以使用 IAM 和服務控制政策來限制區域用量，進而限制跨區域資料流程。

有多種選項可在資料平面上控制跨區域資料流程。例如，您可以使用路由表、VPC 對等互連和 AWS Transit Gateway 附件。 AWS Transit Gateway 是連接虛擬私有雲端 (VPCs) 和內部部署網路的中央中樞。作為大型 AWS 登陸區域的一部分，您可以考慮資料周遊的各種方式 AWS 區域，包括透過網際網路閘道、透過直接 VPC-to-VPC 對等互連，以及透過區域間對等互連 AWS Transit Gateway。例如，您可以在 中執行下列動作 AWS Transit Gateway：

- 確認 VPCs 與內部部署環境之間的東西和南北連線符合您的隱私權要求。
- 根據您的隱私權需求設定 VPC 設定。
- 在 AWS Organizations 和 IAM 政策中使用服務控制政策，以協助防止修改您的 AWS Transit Gateway 和 Amazon Virtual Private Cloud (Amazon VPC) 組態。如需服務控制政策範例，請參閱本指南限制對 VPC 組態的變更中的 。

AWS WAF

為了協助防止意外洩漏個人資料，您可以為 Web 應用程式部署defense-in-depth方法。您可以在應用程式中建置輸入驗證和速率限制，但 AWS WAF 可以做為另一道防線。 AWS WAF 是一種 Web 應用程式防火牆，可協助您監控轉送至受保護 Web 應用程式資源的 HTTP 和 HTTPS 請求。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

您可以使用 AWS WAF定義和部署規則，以檢查特定條件。下列活動可能與個人資料的意外揭露相關聯：

- 來自不明或惡意 IP 地址或地理位置的流量
- Open Worldwide Application Security Project (OWASP) 前 10 大攻擊，包括外洩相關攻擊，例如 SQL Injection
- 請求率高
- 一般機器人流量
- 內容抓取器

您可以部署由 管理的 AWS WAF 規則群組 AWS。的某些受管規則群組 AWS WAF 可用於偵測隱私權和個人資料的威脅，例如：

- SQL 資料庫 – 此規則群組包含的規則旨在封鎖與利用 SQL 資料庫相關聯的請求模式，例如 SQL Injection 攻擊。如果您的應用程式與 SQL 資料庫界面，請考慮此規則群組。
- 已知錯誤輸入 – 此規則群組包含的規則旨在封鎖已知無效的請求模式，並與漏洞的利用或探索相關聯。
- 機器人控制 – 此規則群組包含專為管理來自機器人的請求而設計的規則，這些規則可能會消耗過多的資源、扭曲業務指標、造成停機時間，以及執行惡意活動。
- 帳戶接管預防 (ATP) – 此規則群組包含旨在防止惡意帳戶接管嘗試的規則。此規則群組會檢查傳送至應用程式登入端點的登入嘗試。

個人資料 OU – PD 應用程式帳戶

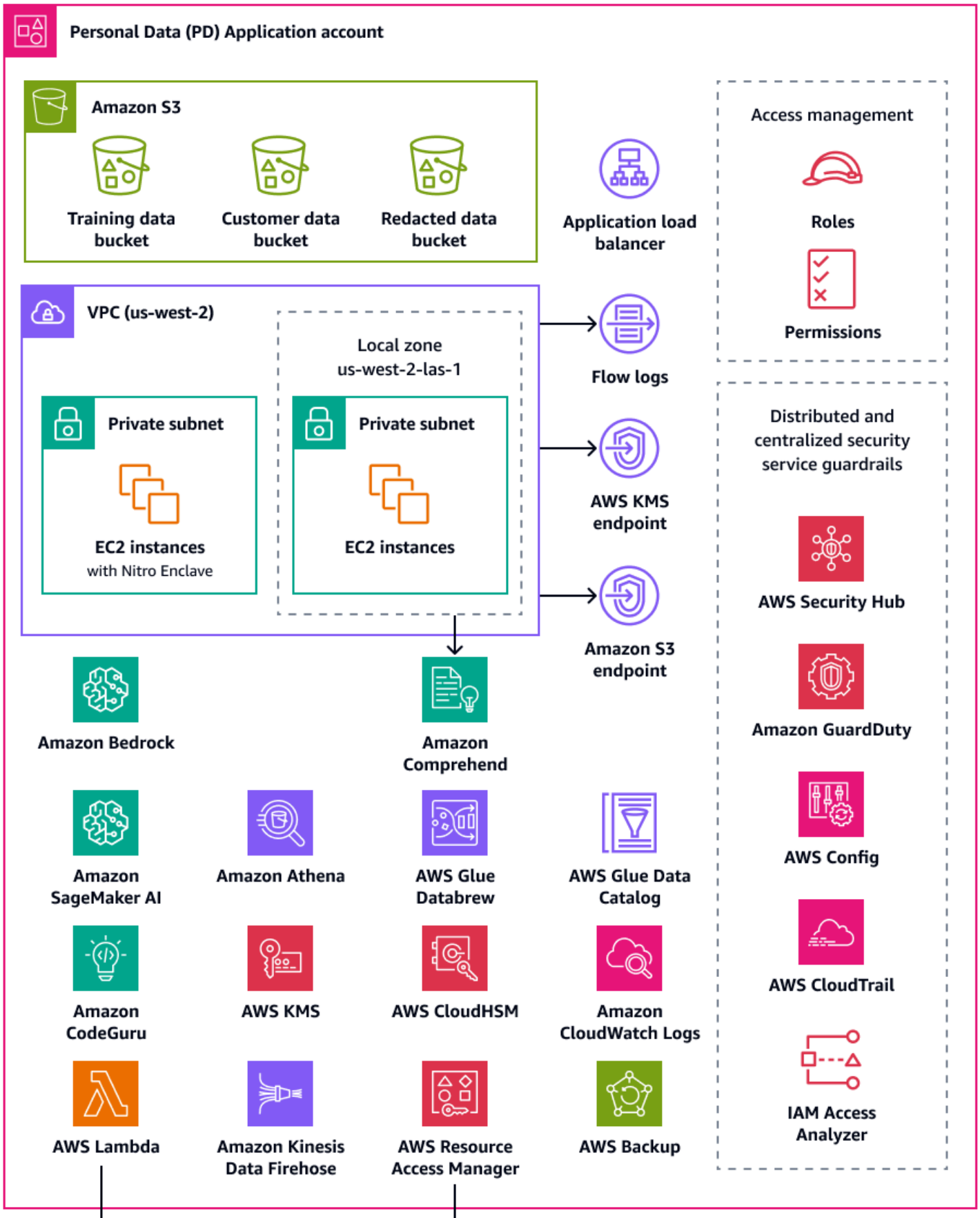
> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

Personal Data (PD) 應用程式帳戶是您的組織託管收集和處理個人資料的服務。具體而言，您可以將定義為個人資料的內容存放在此帳戶中。 AWS PRA 透過多層無伺服器 Web 架構示範許多隱私權組態範例。涉及到跨 AWS 登陸區域的操作工作負載時，不應將隱私權組態視為one-size-fits-all解決方案。例如，您的目標是了解基礎概念、它們如何增強隱私權，以及您的組織如何將解決方案套用至您的特定使用案例和架構。

對於 AWS 帳戶 組織中收集、存放或處理個人資料的 ，您可以使用 AWS Organizations 和 AWS Control Tower 部署基礎和可重複的護欄。為這些帳戶建立專用組織單位 (OU) 至關重要。例如，您可能只想將資料駐留護欄套用至一部分帳戶，其中資料駐留是核心設計考量。對於許多組織而言，這些是存放和處理個人資料的帳戶。

您的組織可能會考慮支援專用資料帳戶，這是您存放個人資料集授權來源的位置。授權資料來源是您存放主要資料版本的位置，這可能會被視為最可靠且準確的資料版本。例如，您可以將授權資料來源中的資料複製到其他位置，例如 PD 應用程式帳戶中的 Amazon Simple Storage Service (Amazon S3) 儲存貯體，這些儲存貯體用於存放訓練資料、一部分客戶資料和修訂後的資料。透過採取這種多帳戶方法，將資料帳戶中的完整和確定性個人資料集與 PD 應用程式帳戶中的下游消費者工作負載分開，您可以在未經授權存取您的帳戶時減少影響範圍。

下圖說明 PD 應用程式和資料帳戶中設定 AWS 的安全性和隱私權服務。


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application load balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
Amazon Athena
AWS Glue Databrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Access management

本節提供有關這些帳戶中 AWS 服務 所用下列項目的更多詳細資訊：

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- Amazon CloudWatch Logs
- Amazon CodeGuru Reviewer
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- AWS Local Zones
- AWS Nitro Enclaves
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS 可協助管理資料生命週期的 功能
- AWS 服務 和 功能，可協助分段資料
- AWS 服務 和 功能，可協助探索、分類或分類資料

Amazon Athena

您可以考慮資料查詢限制控制，以符合您的隱私權目標。Amazon Athena 是一種互動式查詢服務，可協助您使用標準 SQL 直接在 Amazon S3 中分析資料。您不需要將資料載入 Athena；它可直接處理存放在 S3 儲存貯體中的資料。

Athena 的常見使用案例是為資料分析團隊提供量身打造且經過清理的資料集。如果資料集包含個人資料，您可以透過遮罩為資料分析團隊提供少量價值的整個個人資料欄來淨化資料集。如需詳細資訊，請參閱使用 Amazon Athena 匿名化和管理資料湖中的資料，以及 AWS Lake Formation(AWS 部落格文章）。

如果您的資料轉換方法在 Athena 支援的函數之外需要額外的彈性，您可以定義自訂函數，稱為使用者定義的函數 (UDF)。您可以在提交至 Athena UDFs，並在其上執行 AWS Lambda。您可以在 SELECT和 FILTER SQL查詢中使用 UDFs，也可以在相同的查詢中叫用多個 UDFs。對於隱私權，您可以建立執行特定類型資料遮罩的 UDFs，例如只顯示資料欄中每個值的最後四個字元。

Amazon Bedrock

Amazon Bedrock 是一項全受管服務，可從 AI21 實驗室、Anthropic、Meta、Mistral AI 和 Amazon 等領導 AI 公司存取基礎模型。它可協助組織建置和擴展生成式 AI 應用程式。無論使用何種平台，使用生成式 AI 時，組織都可能面臨隱私權風險，包括可能暴露個人資料、未經授權的資料存取，以及其他違規。

Amazon Bedrock Guardrails 旨在透過在 Amazon Bedrock 中跨生成式 AI 工作負載強制執行安全和合規最佳實務，協助緩解這些風險。AI 資源的部署和使用不一定符合組織的隱私權和合規要求。組織在使用生成式 AI 模型時可能會難以維護資料隱私權，因為這些模型可能會記住或重現敏感資訊。Amazon Bedrock Guardrails 透過評估使用者輸入和模型回應，協助保護隱私權。整體而言，如果輸入資料包含個人資料，則可能會有在模型輸出中公開此資訊的風險。

Amazon Bedrock Guardrails 提供機制來強制執行資料保護政策，並協助防止未經授權的資料暴露。它提供內容篩選功能，可在輸入中偵測和封鎖個人資料、主題限制以協助防止存取不適當或風險的主題，以及在模型提示和回應中遮罩或修訂敏感詞彙的字詞篩選條件。這些功能有助於防止可能導致隱私權違規的事件，例如回應偏差或客戶信任遭到侵蝕。這些功能可協助您確保 AI 模型不會不小心處理或揭露個人資料。Amazon Bedrock Guardrails 也支援評估 Amazon Bedrock 外部的輸入和回應。如需詳細資訊，請參閱使用 Amazon Bedrock Guardrails 實作與模型無關的安全措施 (AWS 部落格文章）。

使用 Amazon Bedrock Guardrails，您可以使用情境接地檢查來評估事實接地和回應相關性，以限制模型幻覺的風險。例如，部署生成式 AI 客戶面向應用程式，該應用程式在擷取增強生成 (RAG) 應用程式中使用第三方資料來源。內容基礎檢查可用來驗證對這些資料來源的模型回應，並篩選掉不正確的回應。在 AWS PRA 的內容中，您可以跨工作負載帳戶實作 Amazon Bedrock Guardrail，在其中強制執行針對每個工作負載需求量身打造的特定隱私權護欄。

AWS Clean Rooms

當組織透過分析交集或重疊的敏感資料集來尋找彼此協作的方法時，維護共用資料的安全性和隱私權是一大問題。 AWS Clean Rooms可協助您部署資料無塵室，這是安全、中立的環境，讓組織可以分析合併的資料集，而無需共用原始資料本身。它也可以透過提供存取權給 上的其他組織來產生唯一的洞見， AWS 而無需從自己的帳戶移動或複製資料，也不會洩露基礎資料集。所有資料會保留在來源位置。內建分析規則會限制輸出並限制 SQL 查詢。系統會記錄所有查詢，協同合作成員可以檢視其資料的查詢方式。

您可以建立 AWS Clean Rooms 協同合作，並邀請其他 AWS 客戶成為該協同合作的成員。您授予一個成員查詢成員資料集的能力，您可以選擇其他成員來接收這些查詢的結果。如果多個成員需要查詢資料集，您可以建立與相同資料來源和不同成員設定的其他協同合作。每個成員都可以篩選與協同合作成員共用的資料，而且您可以使用自訂分析規則來設定如何分析他們提供給協同合作的資料的限制。

除了限制提供給協同合作的資料以及其他成員如何使用資料之外， AWS Clean Rooms 還提供下列功能，可協助您保護隱私權：

- 差異隱私權是一種數學技術，透過在資料中新增仔細校正的雜訊量來增強使用者隱私權。這有助於降低資料集內個別使用者重新識別的風險，而不會遮蔽感興趣的值。使用AWS Clean Rooms 差異隱私權不需要差異隱私權專業知識。
- AWS Clean Rooms ML 允許兩個或多個方在其資料中識別類似的使用者，而無需直接彼此共用資料。這可降低成員身分推論攻擊的風險，其中協作的成員可以識別其他成員資料集中的個人。透過建立外觀相似的模型並產生外觀相似的區段， AWS Clean Rooms ML 可協助您比較資料集，而不會公開原始資料。這不需要任何成員具備 ML 專業知識或在 之外執行任何工作 AWS Clean Rooms。您可以保留訓練模型的完整控制權和擁有權。
- 適用於無塵室的密碼編譯運算 (C3R) 可與分析規則搭配使用，以從敏感資料衍生洞見。它以密碼編譯方式限制協作的任何其他方可以學習的內容。使用 C3R 加密用戶端，資料會先在用戶端加密，再提供給 AWS Clean Rooms。由於資料表在上傳至 Amazon S3 之前是使用用戶端加密工具加密，因此資料會保持加密，並透過處理持續存在。

在 AWS PRA 中，我們建議您在資料帳戶中建立 AWS Clean Rooms 協同合作。您可以使用它們與第三方共用加密的客戶資料。只有在提供的資料集中有重疊時才使用它們。如需如何判斷重疊的詳細資訊，請參閱 AWS Clean Rooms 文件中的列出分析規則。

Amazon CloudWatch Logs

Amazon CloudWatch Logs 可協助您集中所有系統、應用程式和 AWS 服務 的日誌，以便您可以對其進行監控並安全地進行封存。在 CloudWatch Logs 中，您可以針對新的或現有的日誌群組使用資料保護政策，以協助將個人資料的揭露風險降至最低。資料保護政策可以偵測日誌中的敏感資料，例如個人資料。當使用者透過 存取日誌時，資料保護政策可以遮罩該資料 AWS 管理主控台。當使用者需要直接存取個人資料時，根據您的工作負載的整體用途規格，您可以為這些使用者指派`logs:Unmask`許可。您也可以建立整個帳戶的資料保護政策，並一致地將此政策套用至組織中的所有帳戶。根據預設，這會為 CloudWatch Logs 中的所有目前和未來日誌群組設定遮罩。我們也建議您啟用稽核報告，並將其傳送至另一個日誌群組、Amazon S3 儲存貯體或 Amazon Data Firehose。這些報告包含每個日誌群組中資料保護問題清單的詳細記錄。

Amazon CodeGuru Reviewer

對於隱私權和安全性，許多組織在部署和部署後階段都支援持續合規至關重要。PRA 在 AWS 處理個人資料之應用程式的部署管道中包含主動控制。Amazon CodeGuru Reviewer 可以偵測可能以 Java、JavaScript 和 Python 程式碼公開個人資料的潛在瑕疵。它為開發人員提供改善程式碼的建議。CodeGuru Reviewer 可以識別各種安全性、隱私權和一般建議實務中的瑕疵。它旨在與多個來源提供者搭配使用，包括 AWS CodeCommit、Bitbucket、GitHub 和 Amazon S3。CodeGuru Reviewer 可以偵測的一些隱私權相關瑕疵包括：

- SQL 注入
- 不安全的 Cookie
- 缺少授權
- 用戶端 AWS KMS 重新加密

如需 CodeGuru Reviewer 可偵測項目的完整清單，請參閱 Amazon CodeGuru Detector Library。

Amazon Comprehend

Amazon Comprehend 是一種自然語言處理 (NLP) 服務，使用機器學習在英文文字文件中發現寶貴的洞見和連線。Amazon Comprehend 可以偵測和修訂結構化、半結構化或非結構化文字文件中的個人資料。如需詳細資訊，請參閱 Amazon Comprehend 文件中的個人身分識別資訊 (PII)。

由於 Amazon Comprehend 有許多透過 AWS SDKs 進行應用程式整合的選項，因此您可以使用 Amazon Comprehend 在您收集、存放和處理資料的許多不同位置識別個人資料。您可以使用 Amazon Comprehend ML 功能來偵測和修訂應用程式日誌 (AWS 部落格文章）、客戶電子郵件、支援票證等中的個人資料。PD 應用程式帳戶的架構圖顯示如何在 Amazon EC2 上為應用程式日誌執行此函數。Amazon Comprehend 提供兩種修訂模式：

- `REPLACE_WITH_PII_ENTITY_TYPE` 會將每個 PII 實體取代為其類型。例如，Jane Doe 將被取代為 NAME。
- `MASK` 以您選擇的字元（！、#、$、%、&、 或 @) 取代 PII 實體中的字元。例如，Jane Doe 可以取代為 **** ***。

Amazon Data Firehose

Amazon Data Firehose 可用來擷取、轉換串流資料，並將資料載入下游服務，例如 Amazon Managed Service for Apache Flink 或 Amazon S3。Firehose 通常用於傳輸大量串流資料，例如應用程式日誌，而無需從頭開始建置處理管道。

您可以使用 Lambda 函數在資料傳送至下游之前執行自訂或內建處理。為了隱私權，此功能支援資料最小化和跨邊界資料傳輸需求。例如，您可以使用 Lambda 和 Firehose 在將多區域日誌資料集中在日誌存檔帳戶中之前進行轉換。如需詳細資訊，請參閱「Biogen：多帳戶集中記錄解決方案」(YouTube 影片）。在 PD 應用程式帳戶中，您可以設定 Amazon CloudWatch 和 AWS CloudTrail ，將日誌推送至 Firehose 交付串流。Lambda 函數會轉換日誌，並將其傳送至 Log Archive 帳戶中的中央 S3 儲存貯體。您可以設定 Lambda 函數來遮罩包含個人資料的特定欄位。這有助於防止跨 傳輸個人資料 AWS 區域。透過使用此方法，個人資料會在傳輸和集中化之前遮罩，而不是在傳輸和集中之後遮罩。對於不受跨邊界傳輸要求約束的司法管轄區中的應用程式，透過 CloudTrail 中的組織追蹤彙總日誌通常更具營運效率和成本效益。如需詳細資訊，請參閱本指南AWS CloudTrail安全 OU – 安全工具帳戶一節中的 。

Amazon DataZone

隨著組織擴展其共用資料的方法， AWS 服務 例如 AWS Lake Formation，他們想要確保差異存取是由最熟悉資料的人員所控制：資料擁有者。不過，這些資料擁有者可能知道隱私權要求，例如同意或跨邊界資料傳輸考量。Amazon DataZone 會根據您的資料管控政策，協助資料擁有者和資料控管團隊跨組織共用和使用資料。在 Amazon DataZone 中，業務單位 (LOBs) 會管理自己的資料，而目錄會追蹤此擁有權。感興趣的對象可以在業務任務中尋找和請求存取資料。只要遵守資料發佈者建立的政策，資料擁有者就可以授予基礎資料表的存取權，而無需管理員或移動資料。

在隱私權環境中，Amazon DataZone 在下列範例使用案例中很有幫助：

- 面向客戶的應用程式會產生用量資料，可與個別的行銷 LOB 共用。您需要確保只有選擇加入行銷的客戶的資料才會發佈至 目錄。
- 歐洲客戶資料已發佈，但只能由位於歐洲經濟區域 (EEA) 的 LOBs 訂閱。如需詳細資訊，請參閱使用 Amazon DataZone 中的精細存取控制增強資料安全性。

在 AWS PRA 中，您可以將共用 Amazon S3 儲存貯體中的資料以資料生產者身分連線至 Amazon DataZone。

AWS Glue

維護包含個人資料的資料集是設計隱私的關鍵組成部分。組織的資料可能以結構化、半結構化或非結構化的形式存在。沒有結構的個人資料集可能難以執行許多隱私權增強操作，包括資料最小化、追蹤屬於單一資料主體的資料作為資料主體請求的一部分、確保一致的資料品質，以及資料集的整體分割。AWS Glue 是一種全受管的擷取、轉換和載入 (ETL) 服務。它可協助您分類、清理、豐富和移動資料存放區和資料串流之間的資料。 AWS Glue 功能旨在協助您探索、準備、建構和結合資料集，以進行分析、機器學習和應用程式開發。您可以使用 在現有資料集上 AWS Glue 建立可預測且通用的結構。AWS Glue Data Catalog AWS Glue DataBrew、 和 AWS Glue Data Quality 是可協助支援組織隱私權需求的 AWS Glue 功能。

AWS Glue Data Catalog

AWS Glue Data Catalog 可協助您建立可維護的資料集。Data Catalog 包含資料參考，做為擷取、轉換和載入 (ETL) 任務的來源和目標 AWS Glue。Data Catalog 中的資訊會儲存為中繼資料資料表，而每個資料表都會指定單一資料存放區。您可以執行 AWS Glue 爬蟲程式來清查各種資料存放區類型中的資料。您可以將內建和自訂分類器新增至爬蟲程式，而這些分類器會推斷個人資料的資料格式和結構描述。爬蟲程式接著會將中繼資料寫入 Data Catalog。集中式中繼資料表可以更輕鬆地回應資料主體請求（例如刪除權），因為它可新增 AWS 環境中不同個人資料來源的結構和可預測性。如需如何使用 Data Catalog 自動回應這些請求的完整範例，請參閱使用 Amazon S3 Find and Forget 處理資料湖中的資料清除請求 (AWS 部落格文章）。最後，如果您的組織使用 AWS Lake Formation來管理和提供跨資料庫、資料表、資料列和儲存格的精細存取，則 Data Catalog 是關鍵元件。Data Catalog 提供跨帳戶資料共用，並協助您使用標籤型存取控制大規模管理資料湖 (AWS 部落格文章）。如需詳細資訊，請參閱本節AWS Lake Formation中的 。

AWS Glue DataBrew

AWS Glue DataBrew 可協助您清理和標準化資料，並對資料執行轉換，例如移除或遮罩個人身分識別資訊，以及加密資料管道中的敏感資料欄位。您也可以視覺化地映射資料的歷程，以了解資料經過的各種資料來源和轉換步驟。隨著您的組織努力更好地了解和追蹤個人資料來源，此功能變得越來越重要。DataBrew 可協助您在資料準備期間遮罩個人資料。您可以在資料分析任務中偵測個人資料，並收集統計資料，例如可能包含個人資料和潛在類別的資料欄數。然後，您可以使用內建的可逆或不可逆資料轉換技術，包括替換、雜湊、加密和解密，而無須撰寫任何程式碼。然後，您可以使用下游已清理和遮罩的資料集進行分析、報告和機器學習任務。DataBrew 中提供的一些資料遮罩技術包括：

- 雜湊 – 將雜湊函數套用至資料欄值。
- 替代 - 將個人資料取代為其他外觀真實的值。
- 剔除或刪除 – 將特定欄位取代為 null 值，或刪除資料欄。

- 遮罩 – 使用角色亂碼，或遮罩欄中的某些部分。

以下是可用的加密技術：

- 確定性加密 – 將確定性加密演算法套用至資料欄值。確定性加密一律會為值產生相同的加密文字。
- 概率加密 – 將概率加密演算法套用至資料欄值。機率式加密會在每次套用時產生不同的加密文字。

如需 DataBrew 中提供的個人資料轉換配方的完整清單，請參閱個人身分識別資訊 (PII) 配方步驟。

AWS Glue 資料品質

AWS Glue Data Quality 可協助您在交付至資料消費者之前，主動自動化和操作跨資料管道的高品質資料交付。 AWS Glue Data Quality 提供跨資料管道的資料品質問題的統計分析，可在 Amazon EventBridge 中觸發警示，並提出修補的品質規則建議。 AWS Glue Data Quality 也支援使用特定網域的語言建立規則，讓您可以建立自訂資料品質規則。

AWS Key Management Service

AWS Key Management Service (AWS KMS) 可協助您建立和控制密碼編譯金鑰，以協助保護您的資料。 會根據 AWS KMS keys FIPS 140-2 密碼編譯模組驗證計畫， AWS KMS 使用硬體安全模組來保護和驗證。如需如何在安全內容中使用此服務的詳細資訊，請參閱 AWS 安全參考架構。

AWS KMS 與大多數提供加密 AWS 服務 的 整合，您可以在應用程式中使用 KMS 金鑰來處理和儲存個人資料。您可以使用 AWS KMS 協助支援各種隱私權要求，並保護個人資料，包括：

- 使用客戶受管金鑰來更好地控制強度、旋轉、過期和其他選項。
- 使用專用客戶受管金鑰來保護允許存取個人資料的個人資料和秘密。
- 定義資料分類層級，並為每個層級指定至少一個專用客戶受管金鑰。例如，您可能有一個金鑰用於加密操作資料，另一個用於加密個人資料。
- 防止意外跨帳戶存取 KMS 金鑰。
- 將 KMS 金鑰存放在與要加密之資源 AWS 帳戶 相同的 內。
- 實作 KMS 金鑰管理和使用的責任分離。如需詳細資訊，請參閱如何使用 KMS 和 IAM 為 S3 中的加密資料啟用獨立安全控制 (AWS 部落格文章）。
- 透過預防性和被動護欄強制執行自動金鑰輪換。

根據預設，KMS 金鑰會儲存，且只能在建立金鑰的區域中使用。如果您的組織對資料落地和主權有特定要求，請考慮多區域 KMS 金鑰是否適合您的使用案例。多區域金鑰是不同 中的特殊用途 KMS 金鑰

AWS 區域 ，可以互換使用。建立多區域金鑰的程序會將您的金鑰材料跨 AWS 區域 邊界移動到內部 AWS KMS，因此缺乏區域隔離可能與組織的主權和駐留目標不相容。解決此問題的一種方法是使用不同類型的 KMS 金鑰，例如區域特定的客戶受管金鑰。

外部金鑰存放區

對於許多組織而言， 中的預設 AWS KMS 金鑰存放區 AWS 雲端 可以滿足其資料主權和一般法規要求。但是，有些可能需要在雲端環境之外建立和維護加密金鑰，並且您有獨立的授權和稽核路徑。使用 中的外部金鑰存放區 AWS KMS，您可以使用組織擁有的金鑰材料來加密個人資料，並在 外部控制 AWS 雲端。您仍然照常與 AWS KMS API 互動，但只會與您提供的外部金鑰存放區代理 (XKS 代理) 軟體 AWS KMS 互動。您的外部金鑰存放區代理接著會調解 AWS KMS 與外部金鑰管理器之間的所有通訊。

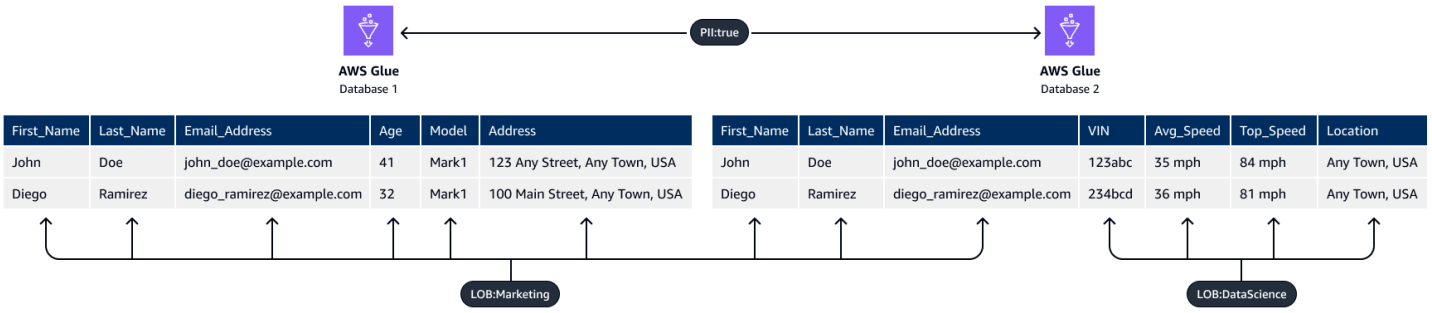
使用外部金鑰存放區進行資料加密時，相較於在 中維護金鑰，請務必考慮額外的操作開銷 AWS KMS。使用外部金鑰存放區，您必須建立、設定和維護外部金鑰存放區。此外，如果您必須維護的其他基礎設施發生錯誤，例如 XKS 代理，且連線中斷，使用者可能暫時無法解密和存取資料。與您的合規和法規利益相關者緊密合作，以了解個人資料加密的法律和合約義務，以及您的服務水準協議的可用性和彈性。

AWS Lake Formation

許多組織透過結構化中繼資料目錄來編目和分類資料集，希望在其組織中共用這些資料集。您可以使用 AWS Identity and Access Management (IAM) 許可政策來控制對整個資料集的存取，但對於包含不同敏感度之個人資料的資料集，通常需要更精細的控制。例如，用途規格和使用限制 (FPC 網站 ） 可能表示行銷團隊需要存取客戶地址，但資料科學團隊不需要。

資料湖也有相關的隱私權挑戰，以其原始格式集中存取大量敏感資料。大多數組織的資料都可以集中存取，因此資料集的邏輯分隔，特別是包含個人資料的資料集，是至關重要的。 AWS Lake Formation可協助您在共用資料時設定控管和監控，無論是來自單一來源還是資料湖中包含的許多來源。在 AWS PRA 中，您可以使用 Lake Formation 對資料帳戶中的共用資料儲存貯體中的資料提供精細的存取控制。

您可以使用 Lake Formation 中的標籤型存取控制功能。標籤型存取控制是一種授權策略，可根據屬性定義許可。在 Lake Formation 中，這些屬性稱為 LF 標籤。使用 LF 標籤，您可以將這些標籤連接到 Data Catalog 資料庫、資料表和資料欄，並將相同的標籤授予 IAM 主體。Lake Formation 允許在委託人被授予存取符合資源標籤值的標籤值時對這些資源進行操作。下圖顯示如何指派 LF 標籤和許可，以提供對個人資料的差異化存取。



此範例使用標籤的階層性質。兩個資料庫都包含個人身分識別資訊 (PII:true)，但單欄式層級的標籤會將特定資料欄限制為不同的團隊。在此範例中，擁有 LF-Tag PII:true 的 IAM 主體可以存取具有此標籤的 AWS Glue 資料庫資源。具有 LOB:DataScience LF-Tag 的主體可以存取具有此標籤的特定資料欄，具有 LF-Tag LOB:Marketing 的主體只能存取具有此標籤的資料欄。行銷只能存取與行銷使用案例相關的 PII，資料科學團隊只能存取與其使用案例相關的 PII。

AWS Local Zones

如果您需要遵守資料駐留要求，您可以部署資源，以在特定 中存放和處理個人資料 AWS 區域 ，以支援這些要求。您也可以使用 AWS Local Zones，這可協助您將運算、儲存、資料庫和其他特定 AWS 資源放在接近大型人口和產業中心的位置。Local Zone 是 的延伸 AWS 區域 ，地理位置接近大型都會區域。您可以將特定類型的資源放在 Local Zone 內，靠近 Local Zone 對應的區域。當區域在相同的法律司法管轄區內無法使用時，Local Zones 可協助您滿足資料駐留要求。當您使用 Local Zones 時，請考慮在您的組織內部署的資料駐留控制。例如，您可能需要控制以防止從特定 Local Zone 到另一個區域的資料傳輸。如需如何使用 SCPs 維護跨邊界資料傳輸護欄的詳細資訊，請參閱AWS Local Zones 使用登陸區域控制在 中管理資料駐留的最佳實務 (AWS 部落格文章)。

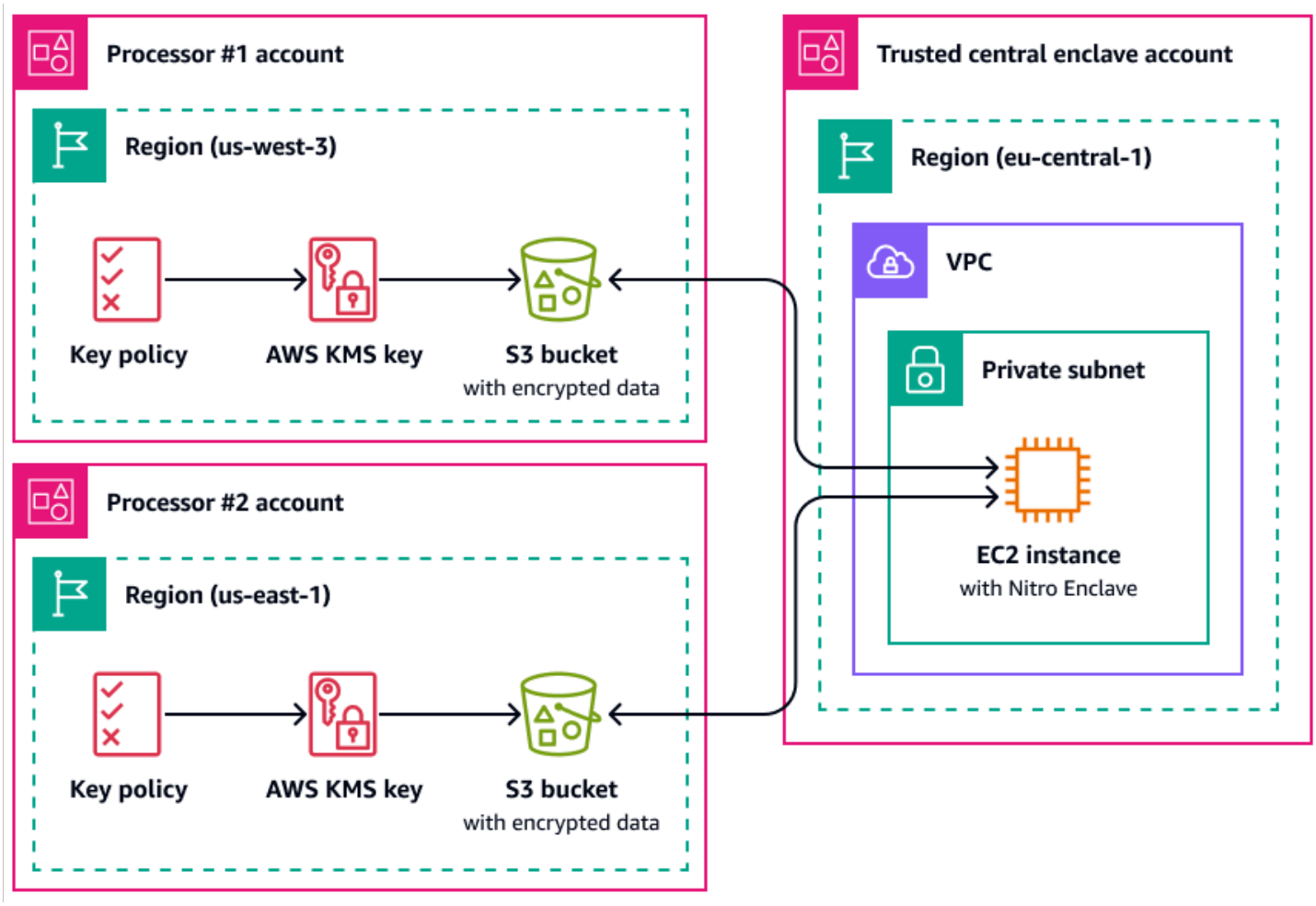
AWS Nitro Enclaves

從處理角度考慮您的資料分割策略，例如使用 Amazon Elastic Compute Cloud (Amazon EC2) 等運算服務處理個人資料。作為較大架構策略一部分的機密運算，可協助您在隔離、受保護且信任的 CPU 環境中隔離個人資料處理。Enclaves 是獨立、強化且受到高度限制的虛擬機器。AWS Nitro Enclaves 是一種 Amazon EC2 功能，可協助您建立這些隔離的運算環境。如需詳細資訊，請參閱 AWS Nitro 系統的安全設計 (AWS 白皮書)。

Nitro Enclaves 部署與父執行個體核心分開的核心。父執行個體的核心無法存取 enclave。使用者無法 SSH 或遠端存取 enclave 中的資料和應用程式。處理個人資料的應用程式可以內嵌在 enclave 中，並設定為使用 enclave 的 Vsock，這是促進 enclave 與父執行個體之間通訊的通訊端。

Nitro Enclaves 可能很有用的一個使用案例是在兩個資料處理器之間進行關節處理，這兩個資料處理器位於不同的 中， AWS 區域 但彼此可能不信任。下圖顯示如何使用 enclave 進行中央處理、在傳送至

enclave 之前加密個人資料的 KMS 金鑰，以及驗證請求解密的 enclave 在其證明文件中具有唯一測量值 AWS KMS key 的政策。如需詳細資訊和說明，請參閱搭配 使用密碼編譯證明 AWS KMS。如需範例金鑰政策，請參閱本指南需要證明才能使用 AWS KMS 金鑰中的 。



透過此實作，只有個別的資料處理者和基礎 enclave 可以存取純文字個人資料。資料在個別資料處理者環境外公開的唯一位置是 enclave 本身，其設計可防止存取和竄改。

AWS PrivateLink

許多組織想要將個人資料暴露限制在不受信任的網路。例如，如果您想要增強整體應用程式架構設計的隱私權，您可以根據資料敏感性來分割網路（類似於AWS 服務 和 功能，可協助分段資料一節中討論的資料集邏輯和實體分離）。 AWS PrivateLink可協助您從虛擬私有雲端 (VPCs) 建立與 VPC 外部服務的單向私有連線。使用 AWS PrivateLink，您可以設定在環境中存放或處理個人資料的 服務的專用私有連線；不需要連線到公有端點，並透過不受信任的公有網路傳輸此資料。當您啟用範圍內 AWS PrivateLink 服務的服務端點時，不需要網際網路閘道、NAT 裝置、公有 IP 地址、 AWS Direct Connect 連線或 AWS Site-to-Site VPN 連線即可通訊。當您使用 AWS PrivateLink 連線到提供個人資料存取權的服務時，您可以根據您組織的資料周邊定義，使用 VPC 端點政策和安全群組來控制存取。

如需僅允許信任組織中 IAM 原則 AWS 和資源存取服務端點的範例 VPC 端點政策，請參閱本指南需要組織成員資格才能存取 VPC 資源中的 。

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) 可協助您安全地跨 共用資源 AWS 帳戶 ，以減少營運開銷並提供可見性和可稽核性。當您規劃多帳戶分割策略時，請考慮使用 AWS RAM 來共用存放在個別隔離帳戶中的個人資料存放區。您可以與其他可信任的帳戶共用該個人資料，以進行處理。在 中 AWS RAM，您可以管理許可，以定義可以在共用資源上執行的動作。所有對 的 API 呼叫 AWS RAM 都會記錄在 CloudTrail 中。此外，您可以設定 Amazon CloudWatch Events 自動通知您 中的特定事件 AWS RAM，例如變更資源共享的時間。

雖然您可以在 IAM AWS 帳戶 中使用以資源為基礎的政策，或在 Amazon S3 中使用儲存貯體政策，以與其他 共用許多類型的 AWS 資源，但 為隱私權 AWS RAM 提供額外的優點。 為資料擁有者 AWS 提供額外的可見性，讓您了解跨 共用資料的方式和對象 AWS 帳戶，包括：

- 能夠與整個 OU 共用資源，而不是手動更新帳戶 IDs清單
- 如果消費者帳戶不屬於您的組織，請強制執行共用啟動的邀請程序
- 特定 IAM 主體可存取每個個別資源的可見性

如果您先前已使用以資源為基礎的政策來管理資源共用，並想要 AWS RAM 改用 ，請使用 PromoteResourceShareCreatedFromPolicy API 操作。

Amazon SageMaker AI

Amazon SageMaker AI 是一種受管機器學習 (ML) 服務，可協助您建置和訓練 ML 模型，然後將模型部署到生產就緒的託管環境中。SageMaker AI 旨在讓您更輕鬆地準備訓練資料和建立模型功能。

Amazon SageMaker Model Monitor

許多組織在訓練 ML 模型時考慮資料偏離。資料偏離是生產資料與用來訓練 ML 模型的資料之間有意義的變化，或隨著時間的推移，輸入資料的有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。如果 ML 模型在生產環境中接收的資料的統計性質偏離訓練的基準資料的性質，預測的準確性可能會下降。Amazon SageMaker Model Monitor 可以持續監控生產環境中 Amazon SageMaker AI 機器學習模型的品質，並監控資料品質。及早主動偵測資料偏離可協助您實作修正動作，例如重新訓練模型、稽核上游系統或修正資料品質問題。Model Monitor 可以減輕手動監控模型或建置其他工具的需求。

Amazon SageMaker Clarify

Amazon SageMaker Clarify 提供模型偏差和可解釋性的洞見。SageMaker Clarify 通常用於 ML 模型資料準備和整體開發階段。開發人員可以指定感興趣的屬性，例如性別或年齡，SageMaker Clarify 會執行一組演算法來偵測這些屬性中是否有任何偏差。演算法執行後，SageMaker Clarify 會提供視覺化報告，其中包含可能偏差的來源和測量說明，讓您可以識別修復偏差的步驟。例如，在只包含幾個商業貸款範例的金融資料集中，SageMaker 可以標記不平衡，因此您可以避免不利於該年齡群組的模型。您也可以透過檢閱其預測並持續監控這些 ML 模型是否有偏差，來檢查已訓練的模型是否有偏差。最後，SageMaker Clarify 與 Amazon SageMaker AI Experiments 整合，提供圖形說明哪些功能對模型的整體預測制定程序貢獻最大。此資訊可能有助於滿足可解釋性結果，而且可協助您判斷特定模型輸入是否比對整體模型行為的影響更大。

Amazon SageMaker 模型卡

Amazon SageMaker 模型卡可協助您記錄 ML 模型的關鍵詳細資訊，以供控管和報告之用。這些詳細資訊可能包括模型擁有者、一般用途、預期使用案例、所做的假設、模型的風險評分、訓練詳細資訊和指標，以及評估結果。如需詳細資訊，請參閱AWS 使用人工智慧和Machine Learning解決方案的模型可解釋性 (AWS 白皮書）。

Amazon SageMaker Data Wrangler

Amazon SageMaker Data Wrangler 是一種機器學習工具，可協助簡化資料準備和特徵工程程序。它提供視覺化界面，可協助資料科學家和機器學習工程師快速輕鬆地準備和轉換資料，以用於機器學習模型。使用 Data Wrangler，您可以從各種來源匯入資料，例如 Amazon S3、Amazon Redshift 和 Amazon Athena。然後，您可以使用超過 300 個內建資料轉換來清理、標準化和合併功能，而無需撰寫任何程式碼。

Data Wrangler 可作為 AWS PRA 中資料準備和特徵工程程序的一部分。它使用 支援靜態和傳輸中的資料加密 AWS KMS，並使用 IAM 角色和政策來控制對資料和資源的存取。它支援透過 AWS Glue 或 Amazon SageMaker Feature Store 進行資料遮罩。如果您將 Data Wrangler 與 整合 AWS Lake Formation，則可以強制執行精細的資料存取控制和許可。您甚至可以將 Data Wrangler 與 Amazon Comprehend 搭配使用，以自動修訂表格式資料中的個人資料，做為更廣泛的 ML Ops 工作流程的一部分。如需詳細資訊，請參閱使用 Amazon SageMaker Data Wrangler 自動修訂機器學習的 PII (AWS 部落格文章）。

Data Wrangler 的多樣性可協助您遮罩許多產業的敏感資料，例如帳號、信用卡號碼、社會安全號碼、病患姓名，以及醫療和軍事記錄。您可以限制對任何敏感資料的存取，或選擇加以修訂。

AWS 可協助管理資料生命週期的 功能

當不再需要個人資料時，您可以將生命週期和time-to-live政策用於許多不同資料存放區中的資料。設定資料保留政策時，請考慮下列可能包含個人資料的位置：

- 資料庫，例如 Amazon DynamoDB 和 Amazon Relational Database Service (Amazon RDS)
- Amazon S3 儲存貯體
- 來自 CloudWatch 和 CloudTrail 的日誌
- AWS Database Migration Service (AWS DMS) 和 AWS Glue DataBrew 專案中遷移的快取資料
- 備份和快照

下列 AWS 服務 和 功能可協助您在 AWS 環境中設定資料保留政策：

- Amazon S3 生命週期 – 一組規則，定義 Amazon S3 套用至一組物件的動作。在 Amazon S3 Lifecyle 組態中，您可以建立過期動作，定義 Amazon S3 代表您刪除過期物件的時間。如需詳細資訊，請參閱管理儲存生命週期。
- Amazon Data Lifecycle Manager – 在 Amazon EC2 中，建立可自動建立、保留和刪除 Amazon Elastic Block Store (Amazon EBS) 快照和 EBS 支援的 Amazon Machine Image (AMIs) 的政策。
- DynamoDB 存留時間 (TTL) – 定義每個項目時間戳記，決定何時不再需要項目。在指定時間戳記的日期和時間之後不久，DynamoDB 會從資料表中刪除項目。
- CloudWatch Logs 中的日誌保留設定 – 您可以將每個日誌群組的保留政策調整為介於 1 天到 10 年之間的值。
- AWS Backup – 集中部署資料保護政策，以設定、管理和控管各種 AWS 資源的備份活動，包括 S3 儲存貯體、RDS 資料庫執行個體、DynamoDB 資料表、EBS 磁碟區等。透過指定資源類型或根據現有 AWS 資源標籤套用 ，將備份政策套用至資源。從集中式主控台稽核和報告備份活動，以協助滿足備份合規要求。

AWS 服務 和 功能，可協助分段資料

資料分割是您將資料存放在不同容器中的程序。這可協助您為每個資料集提供差異化的安全性和身分驗證措施，並減少整體資料集的暴露影響範圍。例如，您可以將此資料分割為更小、更易於管理的群組，而不是將所有客戶資料儲存在一個大型資料庫中。

您可以使用實體和邏輯分隔來分割個人資料：

- 實體分離 – 將資料儲存在個別資料存放區中，或將資料分散至個別 AWS 資源的行為。雖然資料實際上是分開的，但兩個資源都可以供相同的主體存取。這就是為什麼我們建議將實體分離與邏輯分離結合。
- 邏輯分離 – 使用存取控制隔離資料的行為。不同的任務函數需要對個人資料子集的不同層級存取權。如需實作邏輯分隔的範例政策，請參閱本指南授予特定 Amazon DynamoDB 屬性的存取權中的 。

編寫以身分為基礎的和資源為基礎的政策時，邏輯和物理分隔的組合可提供靈活性、簡單性和精細性，以支援跨任務職能的差異化存取。例如，建立在單一 S3 儲存貯體中邏輯上分隔不同資料分類的政策，在操作上可能很複雜。針對每個資料分類使用專用 S3 儲存貯體，可簡化政策組態和管理。

AWS 服務 和 功能，可協助探索、分類或分類資料

有些組織尚未開始在其環境中使用擷取、載入和轉換 (ELT) 工具來主動為其資料編製目錄。這些客戶可能處於早期資料探索階段，他們希望更了解他們存放和處理的資料 AWS ，以及其結構和分類方式。您可以使用 Amazon Macie 進一步了解 Amazon S3 中的 PII 資料。不過，Amazon Macie 無法協助您分析其他資料來源，例如 Amazon Relational Database Service (Amazon RDS) 和 Amazon Redshift。您可以在大型資料映射練習開始時，使用兩種方法來加速初始探索：

- 手動方法 – 製作一個資料表，其中包含兩個資料欄和任意數量的資料列。在第一欄中，撰寫可能位於網路封包標頭或內文或您提供的任何服務的資料特性 （例如使用者名稱、地址或性別）。請您的合規團隊完成第二欄。在第二欄中，如果資料被視為個人資料，請輸入「是」，如果資料不是，請輸入「否」。指出被視為特別敏感的任何類型的個人資料，例如宗教面額或健康資料。
- 自動化方法 – 使用透過 提供的工具 AWS Marketplace。其中一個這類工具是 Securiti。這些解決方案提供的整合，可讓它們跨多種 AWS 資源類型掃描和探索資料，以及其他雲端服務平台中的資產。其中許多相同的解決方案可以持續收集和維護集中式資料目錄中的資料資產和資料處理活動的庫存。如果您依賴工具來執行自動分類，則可能需要調校探索和分類規則，以符合組織對個人資料的定義。

隱私權相關政策範例

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

許多處理敏感資料的組織採取預防性的向前方法，並在整個過程中實作偵測性和反應性控制層。本節提供 AWS Identity and Access Management (IAM) AWS Organizations、 和 AWS Key Management Service () 的隱私權相關政策範例AWS KMS。這些政策可協助您的組織使用預防性方法，達成各種使用、揭露限制和跨邊界資料傳輸隱私權目標。本指南先前章節會參考其中許多政策。

本節包含下列範例政策：

- 需要從特定 IP 地址存取
- 需要組織成員資格才能存取 VPC 資源
- 限制跨 的資料傳輸 AWS 區域
- 授予特定 Amazon DynamoDB 屬性的存取權
- 限制對 VPC 組態的變更
- 需要證明才能使用 AWS KMS 金鑰

需要從特定 IP 地址存取

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

只有在呼叫來自範圍 `192.0.2.0/24`或 中的 IP 地址時，此政策才允許使用者`john_stiles`擔任 IAM 角色`203.0.113.0/24`。此政策有助於防止意外洩露個人資料和不必要的跨邊界資料傳輸。例如，如果您的組織有客戶支援人員需要存取個人資料，您可能希望該支援人員只能從位於特定子集的辦公室存取該資料 AWS 區域。此外，請驗證組織的 PII 定義，因為某些政策可能需要 `Condition`或 `Principal`區段，以限制對特定使用者或 IP 地址的存取。

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

需要組織成員資格才能存取 VPC 資源

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

此 VPC 端點政策僅允許來自o-1abcde123組織的 AWS Identity and Access Management (IAM) 主體和資源存取 Amazon Personalize (Amazon S3) 端點。此預防性控制有助於建立信任區域，並定義個人資料周邊。如需此政策如何協助保護組織中隱私權和個人資料的詳細資訊，請參閱本指南AWS PrivateLink中的 。

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

```
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

限制跨 的資料傳輸 AWS 區域

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

除了兩個 AWS Identity and Access Management (IAM) 角色之外，此服務控制政策會拒絕對 eu-west-1和 AWS 區域 以外的區域 AWS 服務進行 API 呼叫eu-central-1。此 SCP 可協助防止在未經核准的區域中建立 AWS 儲存和處理服務。這有助於防止 AWS 服務 這些區域中的 一起處理個人資料。此政策使用 NotAction 參數，因為它會考慮全域 AWS 服務，例如 IAM，以及與全域服務整合的服務，例如 AWS Key Management Service (AWS KMS) 和 Amazon CloudFront。在參數值中，您可以將這些全域和其他不適用的服務指定為例外狀況。如需此政策如何協助保護組織中隱私權和個人資料的詳細資訊，請參閱本指南AWS Organizations中的 。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
```

```
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
```

```
                    "eu-west-1"
                ]
            },
            "ArnNotLike": {
                "aws:PrincipalARN": [
                    "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                    "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                ]
            }
        }
    }
  ]
}
```

授予特定 Amazon DynamoDB 屬性的存取權

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

當您的組織討論實體和邏輯上分隔個人資料的策略時，請考慮哪些 AWS 儲存服務支援 AWS Identity and Access Management (IAM) 中的精細存取控制政策。下列身分型政策僅允許從名為 的 `UserID`Amazon DynamoDB 資料表擷取 `SignUpTime`、 和 `LastLoggedIn` 屬性`Users`。例如，您可以將此政策連接至客戶支援角色，而不是讓此角色存取完整的個人資料集。如需此政策如何協助保護組織中隱私權和個人資料的詳細資訊，請參閱本指南AWS 服務 和 功能，可協助分段資料中的 。

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
```

```
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

限制對 VPC 組態的變更

> **調查**
>
> 我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

在設計和部署支援您跨邊界資料傳輸需求的 AWS 基礎設施之後，包括網路資料流程，您可能想要防止修改。下列服務控制政策有助於防止 VPC 組態偏離或意外修改。它拒絕新的網際網路閘道連接、VPC 互連連線、傳輸閘道連接和新的 VPN 連接。如需此政策如何協助保護組織中隱私權和個人資料的詳細資訊，請參閱本指南AWS Transit Gateway中的 。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
```

```
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

需要證明才能使用 AWS KMS 金鑰

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

下列 AWS Key Management Service (AWS KMS) 金鑰政策允許 AWS Nitro Enclave 執行個體只有在請求中的 enclave 證明文件符合條件陳述式中的測量結果時，才能使用 KMS 金鑰。此政策僅允許受信任的 enclav 解密資料。如需此政策如何協助保護組織中隱私權和個人資料的詳細資訊，請參閱本指南AWS Nitro Enclaves中的 。如需可用於金鑰政策和 in AWS Identity and Access Management (IAM) 政策之條件金鑰的完整清單 AWS KMS ，請參閱 的條件金鑰 AWS KMS。

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

```
        "Sid": "Enable enclave data processing",
        "Effect": "Allow",
        "Principal": {
           "AWS": "arn:aws:iam::123456789012:role/data-processing"
        },
        "Action": [
           "kms:Decrypt",
           "kms:GenerateDataKey",
           "kms:GenerateRandom"
        ],
        "Resource": "*",
        "Condition": {
           "StringEqualsIgnoreCase": {
              "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
              "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
              "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
              "kms:RecipientAttestation:PCR2":
 "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
              "kms:RecipientAttestation:PCR3":
 "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
              "kms:RecipientAttestation:PCR4":
 "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
              "kms:RecipientAttestation:PCR8":
 "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
           }
        }
     }
  ]
}
```

全球擴展的規劃

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

AWS Security Assurance Services 經常收到有關在全球擴展 AWS 時 的隱私權架構的問題。問題涉及維持對唯一隱私權要求的合規性，例如資料主權義務或客戶合約，同時避免額外的成本和營運開銷。設計考量因素通常包括資料落地、操作員存取限制、彈性和存活能力，以及整體獨立性。如需詳細資訊，請參閱 上的滿足數位主權要求 AWS(AWS re：Invent 2022 簡報）。

下列問題很常見，只有您可以針對使用案例回答這些問題：

- 我客戶的個人資料需要存放在何處？
- 我的客戶資料存放在哪裡？
- 個人資料可以跨越邊界的方式和位置？
- 跨區域存取資料的人工或服務是否構成傳輸？
- 如何確定沒有外國政府存取我客戶的個人資料？
- 在哪裡可以存放備份和熱或冷網站？
- 為了將資料保留在本機，我應該在提供服務的每個區域中維護 AWS 登陸區域嗎？ 或者，我可以使用現有的 AWS Control Tower 登陸區域嗎？

對於資料駐留需求，不同的架構部署可能更適合不同的組織。有些組織可能要求其客戶的個人資料保留在特定區域內。如果是這樣，您可能會擔心如何在維護這些義務的同時，通常遵守法規。無論情況如何，選擇多帳戶部署策略時有多個考量。

若要定義關鍵架構設計元件，請與您的合規和合約團隊緊密合作，以確認個人資料可以跨越 的位置、時間和方式的需求 AWS 區域。判斷哪些內容符合資料傳輸的資格，例如移動、複製或檢視。此外，了解是否有必須實作的特定彈性和資料保護控制。備份和災難復原策略是否需要跨區域容錯移轉？ 若是如此，請判斷您可以使用哪些區域來存放備份資料。判斷資料加密是否有任何需求，例如特定加密演算法或用於產生金鑰的專用硬體安全模組。與這些主題的合規利益相關者保持一致之後，開始考慮多帳戶環境的設計方法。

以下是三種方法，您可以用來以基礎設施隔離的遞增順序來規劃 AWS 多帳戶策略：

- 具有受管區域的中央登陸區域
- 區域登陸區域
- AWS 歐洲主權雲端

也請務必記住，隱私權合規可能不會只停止資料主權。檢閱本指南的其餘部分，以了解許多其他挑戰的可能解決方案，例如同意管理、資料主體的請求、資料控管和 AI 偏差。

具有受管區域的中央登陸區域

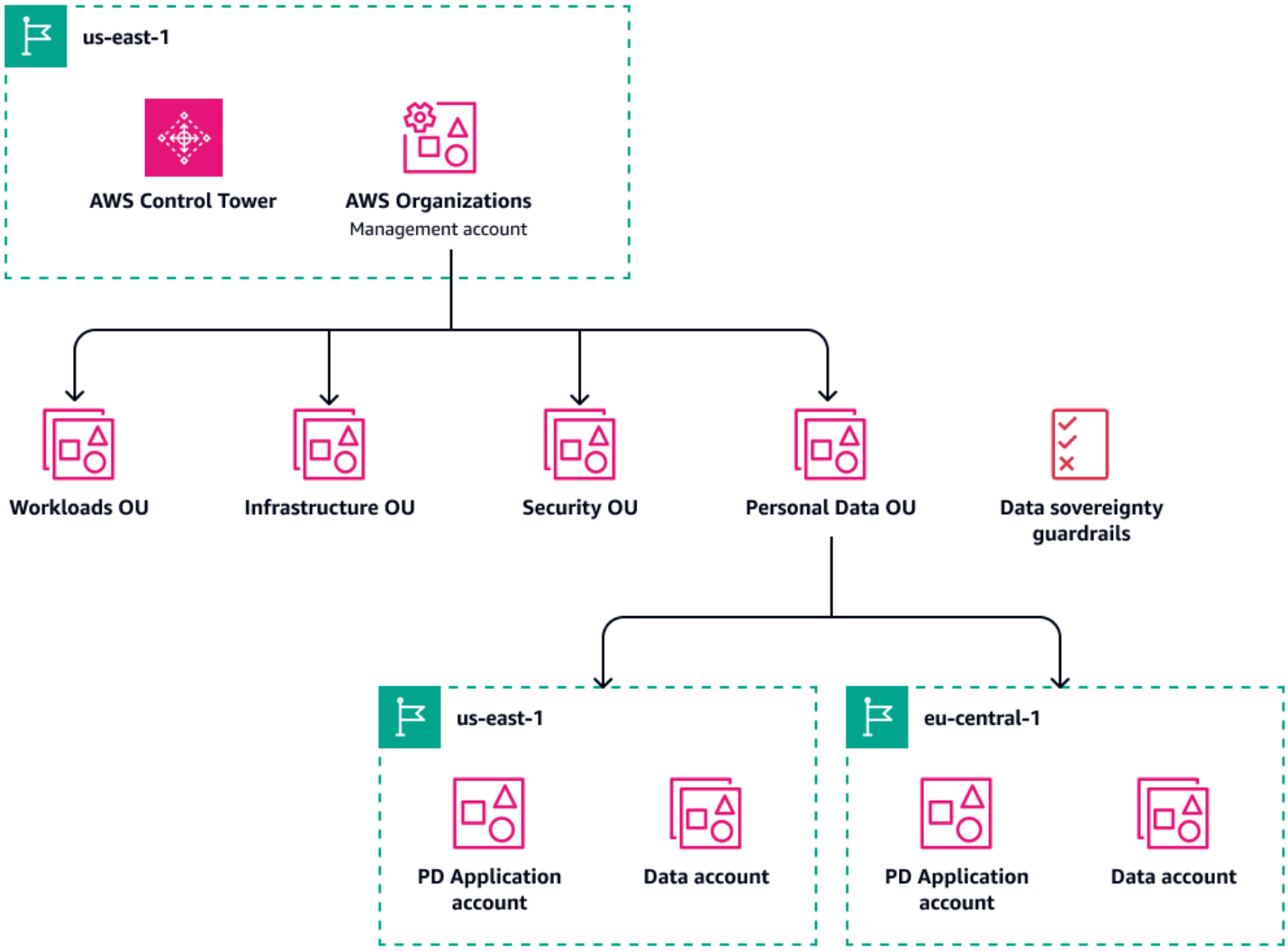
如果您想要全域擴展，但已在其中建立多帳戶架構 AWS，則通常會想要使用相同的多帳戶登陸區域 (MALZ) 來管理其他 AWS 區域。在此組態中，您會繼續在建立基礎設施的區域中，從現有的 AWS Control Tower 登陸區域操作基礎設施服務，例如記錄、帳戶工廠和一般管理。

對於生產工作負載，您可以透過將 AWS Control Tower 登陸區域擴展到新的區域來操作區域部署。透過這樣做，您可以將控管擴展 AWS Control Tower 到新的區域。如此一來，您就可以將個人資料存放區保留在特定受管區域中，資料仍然位於受益於基礎設施服務和 AWS Control Tower 控管的帳戶。在 中 AWS Organizations，包含個人資料的帳戶仍會在專用個人資料 OU 下彙總，其中 AWS Control Tower 會實作 中的所有資料主權護欄。此外，區域特定的工作負載包含在專用帳戶中，而不是在多個區域中建立可能包含相同工作負載的生產帳戶。

此部署可以最具成本效益，但需要考慮控制跨 AWS 帳戶 和區域邊界的個人資料流程。考慮下列各項：

- 日誌可能包含個人資料，因此可能需要一些額外的組態來包含或修改敏感欄位，以防止在彙總期間進行跨區域傳輸。如需控制跨區域日誌彙總的詳細資訊和建議實務，請參閱本指南集中式日誌儲存中的 。
- 考慮在 AWS Transit Gateway 設計中隔離 VPCs 和適當的雙向網路流量流程。您可以限制允許和核准的 Transit Gateway 附件，也可以限制可變更 VPC 路由表的人員或內容。
- 您可能需要防止雲端營運團隊的成員存取個人資料。例如，包含客戶交易資料的應用程式日誌可能會被視為比其他日誌來源更敏感。可能需要其他核准和技術護欄，例如角色型存取控制和屬性型存取控制。此外，資料在存取時可能受到駐留限制。例如，一個區域 A 中的資料只能從該區域內存取。

下圖顯示具有區域部署的集中式登陸區域。



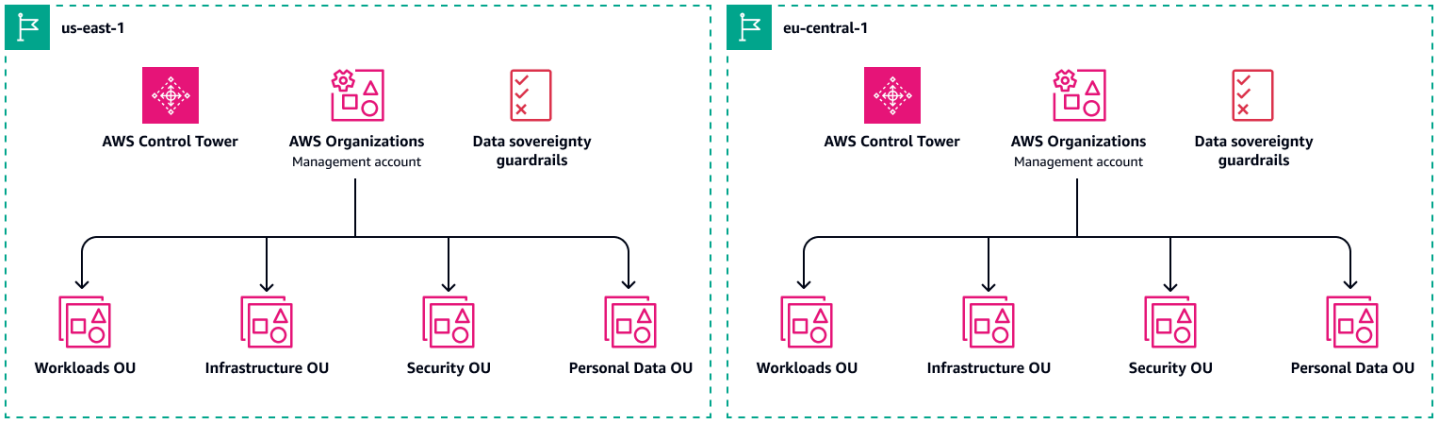
區域登陸區域

與非材料工作負載相比，具有多個 MALZ 可以完全隔離處理個人資料的工作負載，從而協助您實現更嚴格的合規要求。根據預設，可以設定 AWS Control Tower 集中記錄彙總，從而簡化。透過此方法，您不需要使用需要修訂的個別日誌串流來維護記錄的例外狀況。您甚至可以擁有每個 MALZ 的本機和專用雲端操作團隊，這會限制操作員存取本機駐留。

許多組織都有個別的美國和歐洲登陸區域部署。每個區域登陸區域都有單一的空白安全狀態，以及區域中帳戶的相關控管。例如，在一個 MALZ 中的工作負載中可能不需要使用專用 HSMs 來加密個人資料，但在另一個 MALZ 中可能需要。

雖然此策略可以擴展以滿足許多目前和未來的需求，但請務必了解與維護多個 MALZs 相關的額外成本和營運開銷。如需詳細資訊，請參閱 AWS Control Tower 定價。

下圖顯示兩個區域中的個別登陸區域。



AWS 歐洲主權雲端

有些組織需要徹底分離其在歐洲經濟區 (EEA) 中操作的工作負載，以及在其他地方操作的工作負載。在這種情況下，請考慮AWS 歐洲主權雲端。 AWS 歐洲主權雲端是歐洲的全新獨立雲端，旨在協助客戶滿足區域不斷發展的主權需求，包括嚴格的資料駐留權、營運自主權和彈性需求。

AWS 歐洲主權雲端在實體上和邏輯上與現有的 分開 AWS 區域，同時提供相同的安全性、可用性和效能。只有位於歐洲 AWS 的員工才能控制 AWS 歐洲主權雲端的操作和支援。如果您有嚴格的資料駐留需求， AWS 歐洲主權雲端會保留您在歐洲建立的所有中繼資料 （例如其用來執行的角色、許可、資源標籤和組態 AWS)。 AWS 歐洲主權雲端也具有自己的帳單和用量計量系統。

對於此方法，您會使用與上一節區域登陸區域類似的模式。不過，對於您提供給歐洲客戶的服務，您可以在 AWS 歐洲主權雲端中部署專用的 MALZ。

資源

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

AWS 方案指引

- AWS 安全參考架構 (AWS SRA)

AWS 文件

- 資料保護 (AWS Well-Architected Framework)
- 資料分類 (AWS 白皮書)
- Amazon Web Services：風險與合規 (AWS 白皮書)
- 解決個人資料處理需求的混合架構 (AWS 白皮書)
- 在 上導覽 GDPR 合規 AWS (AWS 白皮書)
- 在 上建置資料周邊 AWS (AWS 白皮書)
- AWS 安全文件

其他 AWS 資源

- AWS 合規計劃
- AWS 共同的責任模型
- 資料隱私權常見問答集
- AWS 安全保證服務
- AWS 數位主權承諾：控制不受影響 (AWS 部落格文章)
- AWS 安全學習

貢獻者

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

本指南是由 AWS 安全保證服務團隊撰寫。如需實作本指南中建議和操作工作負載的支援，請聯絡AWS 安全保證服務團隊。

主要作者

- AWS 高級隱私權顧問，Amber Welch
- Daniel Nieters， AWS 首席隱私權顧問
- Robert Carter， AWS 技術計畫經理

貢獻者

- Avik Mukherjee， AWS 資深安全顧問
- David Bounds， AWS 資深解決方案架構師
- Jeff Lombardo， AWS 資深安全解決方案架構師
- Ram Ramani， AWS 首席安全解決方案架構師
- VanessaKinds， AWS 資深安全顧問
- Thomas Nicholson， AWS 資深隱私權顧問
- Jose DeJesus， AWS 資深保證顧問
- Doug Pardue， AWS Solutions Architect Manager

技術作者

- 資深 AWS 技術作者，Lilly AbouHarb

文件歷史紀錄

調查

我們希望聽到您的意見。請進行簡短的問卷，以提供對 AWS PRA 的意見回饋。

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
重大更新	我們已將雲端運算合規控制目錄 (C5) 新增至 AWS Artifact區段。我們已將 Amazon Security Lake 新增至 Log Archive 帳戶。我們已將 Amazon Bedrock AWS Clean Rooms、Amazon DataZone AWS Lake Formation 、Amazon SageMaker AI 以及 AWS 服務 和 功能新增至 PD 應用程式帳戶，以協助探索、分類或分類資料。 https://docs.aws.amazon.com/prescriptive-guidance/latest/privacy-reference-architecture/personal-data-account.html我們新增了全球擴展策略一節。	2025 年 9 月 16 日
重大更新	我們全面進行了重大更新。	2024 年 3 月 26 日
初次出版	—	2023 年 10 月 2 日

AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的現場部署 Oracle 資料庫 遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將內部部署 Oracle 資料庫 遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統 遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫 遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式 遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但比主動-被動遷移需要更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。目標資料庫在遷移期間不接受任何交易。

彙總函數

在一組資料列上運作的 SQL 函數，會計算群組的單一傳回值。彙總函數的範例包括 SUM和 MAX。

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

永久刪除資料集中個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常性問題的常用解決方案，其中解決方案具有反效益、無效或比替代解決方案效率更低。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是產品組合探索和分析程序的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱什麼是人工智慧？

人工智慧操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何在 AWS 遷移策略中使用 AIOps 的詳細資訊，請參閱操作整合指南。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性、一致性、隔離性、耐久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱《 AWS Identity and Access Management (IAM) 文件》中的 ABAC for AWS。

授權資料來源

存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線能力。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定有效率且有效的計劃，以成功移至雲端。 AWS CAF 會將指導方針整理成六個重點領域：業務、人員、控管、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。為此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

評估資料庫遷移工作負載、建議遷移策略並提供工作預估值的工具。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的行為圖中的資料。

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 （藍色） 中執行目前的應用程式版本，並在另一個環境 （綠色） 中執行新的應用程式版本。此策略可協助您快速復原，並將影響降至最低。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上編製資訊索引的 Web 爬蟲程式。某些其他機器人稱為惡意機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到惡意軟體感染且受單一方控制之機器人的網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱關於分支 (GitHub 文件)。

碎片存取

在特殊情況下，以及透過核准的程序，讓使用者快速取得他們通常無權存取 AWS 帳戶 之 的存取權。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作打破玻璃程序指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 AWS上執行容器化微服務白皮書的圍繞業務能力進行組織部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

版本對最終使用者的緩慢和增量版本。當您有信心時，您可以部署新版本並完全取代目前版本。

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，為您的 AWS 工作負載帶來壓力，並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端 企業策略部落格上的 CCoE 文章。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲端運算通常連接到邊緣運算技術。

雲端操作模型

在 IT 組織中，用於建置、成熟和最佳化一或多個雲端環境的操作模型。如需詳細資訊，請參閱建置您的雲端操作模型。

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)

- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段是由 Stephen Orban 在部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中所定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub或 Bitbucket Cloud。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

使用機器學習從數位影像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如，Amazon SageMaker AI 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或整個組織的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的一致性套件。

持續整合和持續交付 (CI/CD)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱持續交付的優點。CD 也可表示持續部署。如需詳細資訊，請參閱持續交付與持續部署。

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

僅收集和處理嚴格必要資料的原則。在 中實作資料最小化 AWS 雲端 可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性防護機制，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個生命週期中追蹤資料的原始伺服器和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如 分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重驗證、網路分割和加密。

委派的管理員

在 中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶，以管理組織的帳戶和管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的可搭配 AWS Organizations運作的服務。

deployment

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 環境。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS上實作安全控制中的偵測性控制。

開發值串流映射 (DVSM)

一種程序，用於識別並優先考慮對軟體開發生命週期中的速度和品質造成負面影響的限制。DVSM 延伸了原本專為精簡製造實務設計的價值串流映射程序。它著重於透過軟體開發程序建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬呈現，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在星星結構描述中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為與文字相似。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

防止工作負載或系統在其主要部署位置實現其業務目標的事件。這些事件可能是自然災難、技術故障或人為動作的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您用來將災難造成的停機時間和資料遺失降至最低的策略和程序。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 上工作負載的災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

DR

請參閱災難復原。

偏離偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源中的偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲端運算相比，邊緣運算可以減少通訊延遲並改善回應時間。

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

將人類可讀取的純文字資料轉換為加密文字的運算程序。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱 服務端點。

端點服務

您可以在虛擬私有雲端 (VPC) 中託管以與其他使用者共用的服務。您可以使用 建立端點服務，AWS PrivateLink 並將許可授予其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 委託人。這些帳戶或主體可以透過建立介面 VPC 端點私下連接至您的端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud (Amazon VPC) 文件中的建立端點服務。

企業資源規劃 (ERP)

一種系統，可自動化和管理企業的關鍵業務流程 （例如會計、MES 和專案管理）。

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service (AWS KMS) 文件中的信封加密。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如， AWS CAF 安全概念包括身分和存取管理、偵測控制、基礎設施安全、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱計畫實作指南。

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。透過計算摘要統計並建立資料可視化來執行 EDA。

F

事實資料表

星狀結構描述中的中央資料表。它存放有關業務操作的量化資料。一般而言，事實資料表包含兩種類型的資料欄：包含度量的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等邊界會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱AWS 故障隔離界限。

功能分支

請參閱分支。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

少量擷取提示

在要求 LLM 執行類似的任務之前，提供少量示範任務和所需輸出的範例。此技術是內容內學習的應用程式，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式、推理或網域知識的任務，少量的提示非常有效。另請參閱零鏡頭提示。

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過變更資料擷取使用連續資料複寫，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及以自然語言交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的限制內容的地理分佈。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於提高裝置製造操作的速度、可擴展性和生產力。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為棕地。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。它們是透過使用 AWS Config AWS Security Hub CSPM、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如，Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分，而轉換結構描述可能是一項複雜任務。AWS 提供有助於結構描述轉換的 AWS SCT。

高可用性 (HA)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，並處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

一種方法，用於現代化和升級操作技術 (OT) 系統，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠中的各種來源收集和存放資料。

保留資料

從用於訓練機器學習模型的資料集中保留的部分歷史標記資料。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如，Microsoft SQL Server 至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱資料

經常存取的資料，例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別，才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性，通常會在典型 DevOps 發行工作流程之外執行修補程式。

超級護理期間

在切換後，遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常，此期間的長度為 1-4 天。在超級護理期間結束時，遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

I

IaC

將基礎設施視為程式碼。

身分型政策

連接至一或多個 IAM 主體的政策，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱工業物聯網。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有的基礎設施。不可變基礎設施本質上比可變基礎設施更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的使用不可變基礎設施的部署最佳實務。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

2016 年 Klaus Schwab 推出的術語，透過連線能力、即時資料、自動化、分析和 AI/ML 的進展，指製造程序的現代化。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC，可管理 VPCs（在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱什麼是 IoT？

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM 提供了基礎。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需有關將雲端操作與 ITSM 工具整合的資訊，請參閱操作整合指南。

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會獲得明確指派的安全標籤值。使用者安全標籤和資料安全標籤之間的交集會決定使用者可以看到哪些資料列和資料欄。

登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱設定安全且可擴展的多帳戶 AWS 環境。

大型語言模型 (LLM)

預先訓練大量資料的深度學習 AI 模型。LLM 可以執行多個任務，例如回答問題、摘要文件、將文字翻譯成其他語言，以及完成句子。如需詳細資訊，請參閱什麼是 LLMs。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的套用最低權限許可。

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱機器學習。

主要分支

請參閱分支。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊，或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在操作時強化和改善自身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。

成員帳戶

屬於組織一部分的管理帳戶 AWS 帳戶 以外的所有 AWS Organizations。帳戶一次只能是一個組織的成員。

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

根據發佈/訂閱模式的輕量型machine-to-machine(M2M) 通訊協定，適用於資源受限的 IoT 裝置。

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用無 AWS 伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行

更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱在 上實作微服務 AWS。

Migration Acceleration Program (MAP)

一種 AWS 計畫，提供諮詢支援、訓練和服務，協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 AWS 遷移策略的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的遷移工廠的討論和雲端遷移工廠指南。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。MPA 工具 （需要登入） 可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移準備程度評定 (MRA)

使用 AWS CAF 取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱此詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱《》中的現代化應用程式的策略 AWS 雲端。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱《》中的評估應用程式的現代化準備 AWS 雲端程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱將單一體系分解為微服務。

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」 或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性， AWS Well-Architected Framework 建議使用不可變的基礎設施作為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱開放程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

用於工業自動化machine-to-machine(M2M) 通訊協定。OPC-UA 提供資料加密、身分驗證和授權機制的互通性標準。

操作水準協議 (OLA)

一份協議，闡明 IT 職能群組承諾向彼此提供的內容，以支援服務水準協議 (SLA)。

操作整備審查 (ORR)

問題及相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作準備度審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造中，OT 和資訊技術 (IT) 系統的整合是工業 4.0 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱操作整合指南。

組織追蹤

由 建立的線索 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱 CloudTrail 文件中的建立組織追蹤。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

CloudFront 中的增強型選項，用於限制存取以保護 Amazon Simple Storage Service (Amazon S3) 內容。OAC 支援所有 S3 儲存貯體中的所有伺服器端加密 AWS KMS (SSE-KMS) AWS 區域，以及對 S3 儲存貯體的動態PUT和DELETE請求。

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從應用程式內啟動之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

附接至 IAM 主體的 IAM 管理政策，可設定使用者或角色擁有的最大許可。如需詳細資訊，請參閱 IAM 文件中的許可界限。

個人身分識別資訊 (PII)

直接檢視或與其他相關資料配對時，可用來合理推斷個人身分的資訊。PII 的範例包括名稱、地址和聯絡資訊。

PII

請參閱個人身分識別資訊。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

可定義許可的物件（請參閱身分型政策）、指定存取條件（請參閱資源型政策），或定義組織中所有帳戶的最大許可 AWS Organizations（請參閱服務控制政策）。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則可以更輕鬆地實作並達到更好的效能和可擴展性。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱評估遷移準備程度。

述詞

傳回 `true`或 的查詢條件`false`，通常位於 `WHERE`子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS上實作安全控制中的預防性控制。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中角色術語和概念中的主體。

依設計的隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。如需詳細資訊，請參閱 Route 53 文件中的使用私有託管區域。

主動控制

旨在防止部署不合規資源的安全控制。這些控制項會在佈建資源之前對其進行掃描。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的控制項參考指南，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

產品整個生命週期的資料和程序管理，從設計、開發和啟動，到成長和成熟，再到拒絕和移除。

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

使用一個 LLM 提示的輸出做為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以提高可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強生成。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

區域

地理區域中的 AWS 資源集合。每個 AWS 區域 都獨立於其他 ，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用哪些。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新定位

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

應用程式抵禦中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

矩陣，定義所有參與遷移活動和雲端操作之各方的角色和責任。矩陣名稱衍生自矩陣中定義的責任類型：負責人 (R)、責任 (A)、已諮詢 (C) 和知情 (I)。支援 (S) 類型為選用。如果您包含支援，則矩陣稱為 RASCI 矩陣，如果您排除它，則稱為 RACI 矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS上實作安全控制中的回應性控制。

保留

請參閱 7 個 R。

淘汰

請參閱 7 個 R。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者 (IdP) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS 管理主控台 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。它由秘密值及其中繼資料組成。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 Secrets Manager 文件中的 Secrets Manager 秘密中的什麼內容？。

依設計的安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：預防性、偵測性、回應性和主動性。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生提醒。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為偵測或回應式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

由接收資料的 AWS 服務 在其目的地加密資料。

服務控制政策 (SCP)

為 AWS Organizations中的組織的所有帳戶提供集中控制許可的政策。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制政策。

服務端點

的進入點 URL AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 服務 端點。

服務水準協議 (SLA)

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務層級指標 (SLI)

服務效能方面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

描述您與 共同 AWS 承擔雲端安全與合規責任的模型。 AWS 負責雲端的安全，而 負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱 中的階段式應用程式現代化方法 AWS 雲端。

SPOF

請參閱單一故障點。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構旨在用於資料倉儲或商業智慧用途。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 Amazon CloudWatch Synthetics 來建立這些測試。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

T

標籤

做為中繼資料以組織 AWS 資源的鍵值對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱 環境。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可以用於互連 VPC 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的什麼是傳輸閘道。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中 AWS Organizations 及其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 文件中的 AWS Organizations 搭配使用 AWS Organizations 與其他 AWS 服務。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

兩個比薩就能吃飽的小型 DevOps 團隊。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱量化深度學習系統的不確定性指南。

未區分的任務

也稱為繁重工作，這是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危及系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等緩慢的查詢。

視窗函數

SQL 函數，對與目前記錄在某種程度上相關的資料列群組執行計算。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，多次讀取。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

儲存模型，可一次性寫入資料，並防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為不可變。

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的缺陷或漏洞。威脅行為者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

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。