AWS 隱私權參考架構 (AWS PRA)

# AWS 規範指引

# AWS 規範指引: AWS 隱私權參考架構 (AWS PRA)

# Table of Contents

# AWS 隱私權參考架構 (AWS PRA)

Amazon Web Services ( 貢獻者 )

2024 年三月 (文件歷史記錄)

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

## 注意

本指南僅供參考用途。這不是法律建議，不應該依賴於法律諮詢。 AWS 鼓勵客戶就其隱私權和資料保護環境的實施情況，以及更一般的說明，取得與其業務相關的適用法律的適用建議。

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 產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。 AWS AWS 產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。

客戶的責任和責任由 AWS 協議控制，本文件不屬於與客戶之間 AWS 的任何協議的一部分，也不會修改。 AWS

## 簡介

AWS 隱私權參考架構 (PRA) 針對中的隱私權支援控制項的設計和組態提供了一組指導方針。 AWS 服務本指南可協助您做出有關人員、流程和技術的決策，以協助支援 AWS 雲端.

### AWS 共同的責任模式和隱私

在中 AWS 雲端，您共同承擔安全性和合規性的責任 AWS。 AWS 負責雲的安全性，這意 AWS 味著負責保護運行所有在提供的服務的基礎設施 AWS 雲端. 您必須負責雲端中的安全性，這表示您有責任根據安全性和隱私權要求進行設定和管理 AWS 服務 。如需詳細資訊，請參閱AWS 共用的責任模型。

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。您的隱私權責任會因許多因素而有所不同，包括 AWS 區域 您所選擇的、這些服務整合到您的 IT 環境中，以及適用於貴組織和工作負載的法律與法規。 AWS 服務

使用時 AWS 服務，您可以保持對內容的控制權。具體而言，內容定義為軟體 (包括機器影像)、資料、文字、音訊、視訊或影像，而您或任何一般使用者透 AWS 服務 過與您的帳戶相關傳送給我們以進行

處理、儲存或託管。它還包括您或最終用 AWS 服務戶使用導出的任何計算結果。您有責任管理以下決策，這些決策由您控制：

- 您選擇收集、儲存或處理的資料 AWS
- AWS 服務 您與資料搭配使用
- 您收集、儲存或處理資料的 AWS 區域 位置
- 資料的格式和結構，以及資料是否為遮罩、匿名處理或加密
- 如何定義、儲存、輪換和操作加密金鑰以進行加密
- 誰可以存取您的資料以及他們何時可以存取您的資料，以及如何授予、管理和撤銷這些存取權

瞭解 AWS 共同的責任模型以及它通常如何套用在雲端中的作業之後，您必須決定該模型如何應用於您的使用案例。您選擇使用的決定了您在組織隱私權責任中必須執行的組態數量。 AWS 服務 例如，亞馬遜彈性運算雲端 (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，則必須針對客體作業系統以及您在 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。當您使用抽象服務 (例如 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數據，並配置用於訪問端點的策略，以便存儲和檢索數據。如需有關如何 AWS 協助您保護資料和隱私權的詳細資訊，請參閱「資料保護與隱私權」 AWS。

# 了解 AWS PRA

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

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 中範例 AWS 多帳戶環境的一般版面配置與結構。

本節包含下列主題：

- 使用 AWS PRA 和 SRA AWS
- AWS Organizations 以及專門的帳戶結構
- 營運隱私權服務 AWS

# 使用 AWS PRA 和 SRA AWS

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

AWS PRA 提供了客戶發現有助於規劃其基礎架構和工作負載的基礎設施和應用程式層級隱私權控制的模式。 AWSAWS 安全參考架構 (AWS SRA) 提供了一套建立架構的準則，該架構可在您的 AWS landing zone 和應用程式中實作並支援正確的安全控制設定。為了建立本指南中詳細介紹的隱私控制，AWS PRA 假定了 SRA 中描述的許多相同的基礎準則和帳戶結構。 AWS AWS PRA 和 AWS SRA 詳細介紹了許多相同的密鑰。 AWS 服務本指南僅包含這些服務的簡要說明。您可以深入瞭解這些服務，以及如何在 AWS SRA 中的安全性內容中使用這些服務。

AWS SRA 可協助您設計、實作和管理 AWS 安全性服務，使其符合 AWS 建議的做法。您可以將 AWS SRA 用作獨立指南，也可以使用 AWS SRA 和 AWS PRA 作為伴侶指南。 AWS SRA 中詳述的許多安全準則都可以與 PRA 中詳述的隱私控制一起遵循。 AWS 與安全性類似，有一些基本的隱私權考量可能有助於在 AWS 雲端 旅程早期做出，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？
- 處理其他類型受管制資料的應用程式呢？

- 我可以實施哪些組織層級的控制措施，以使我的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？
- 我的組織對跨境資料傳輸有何要求？

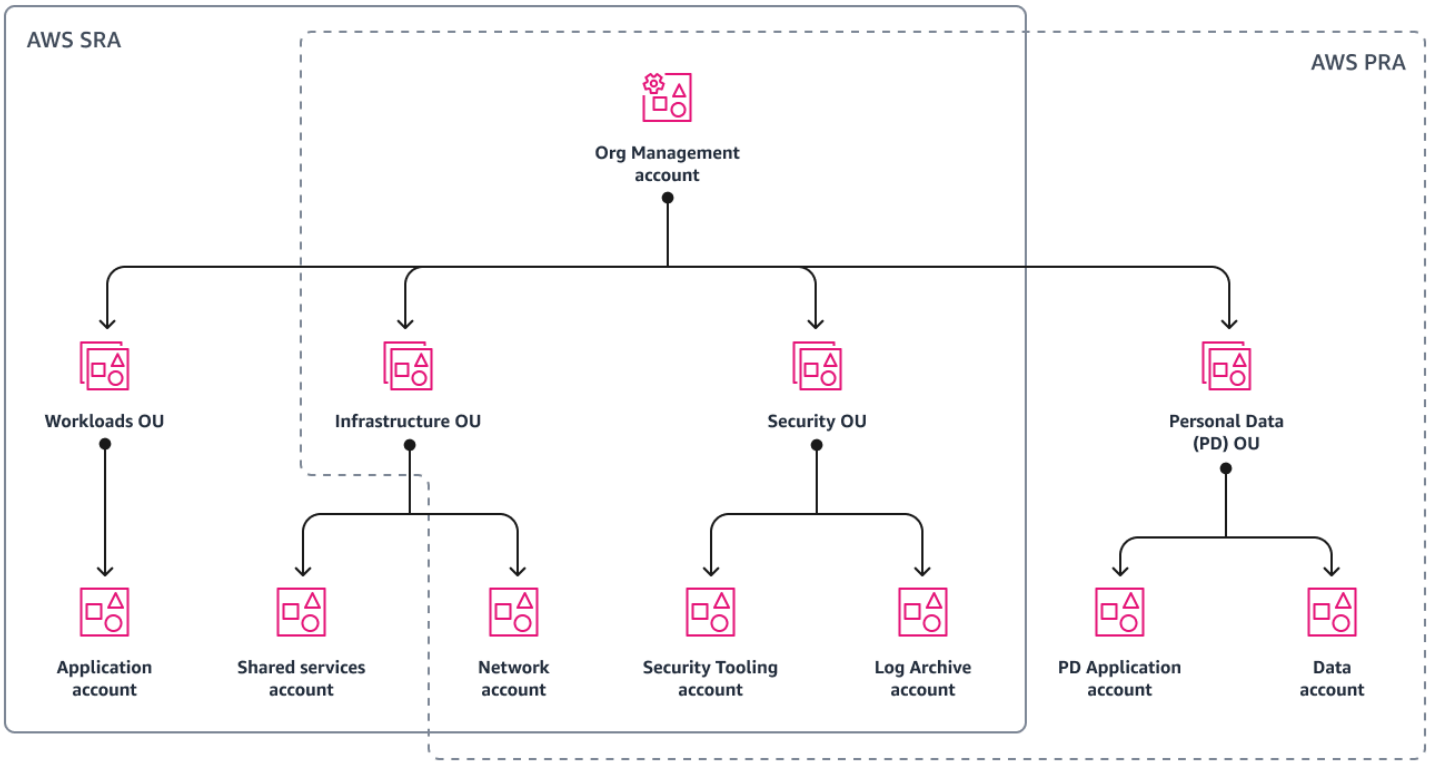
其中許多問題的答案可能會對雲端環境的設計產生影響，例如 AWS 帳戶 結構、服務控制政策和 AWS Identity and Access Management (IAM) 角色。

# AWS Organizations 以及專門的帳戶結構

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

AWS Organizations是一項帳戶管理服務，可協助您集中管理和控管多個帳戶 AWS 帳戶。使用 AWS Organizations 是架構良好、多 AWS 帳戶環境的基礎。如需詳細資訊，請參閱建立最佳實務 AWS 環境。

下圖顯示 AWS PRA 的高階帳戶與組織單位 (OU) 結構。在大多數情況下， AWS PRA 的組織結構與 AWS SRA 的組織結構相匹配。



與 AWS SRA 組織的偏差包括：

- AWS PRA 會新增個人資料 (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、精細的控制項，以協助保護個人資料免於意外揭露。
- 在基礎結構 OU 中， AWS PRA 目前不包含 AWS SRA 中所述之共用服務帳戶的其他指引。
- AWS PRA 目前不包含 AWS SRA 中所述之工作負載 OU 的其他指引。收集或處理個人資料的應用程式位於 PD OU 的專屬帳戶中。

您可以用AWS Control Tower於整個組織的整體基礎治理，以及自動化部署安全性和隱私權控制。如果您的組織目前 AWS Control Tower 未使用，您仍然可以在各自的服務中部署許多安全性和隱私權控制項 AWS Control Tower，例如服務控制原 AWS Config 則和規則。

在規劃帳戶和 OU 結構 (包括帳戶細分策略) 時，您可能會發現考慮個人資料的處理方式很有幫助。您可能需要根據其獨特的使用案例和適用的法律和法規來考慮您正在處理的資料類型。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 Health 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，並在此上大量規劃您的區段策略。典型的客戶細分策略可以包括與軟體開發生命週期 (SDLC) 保持一致的專屬客戶，例如用於開發、預備或品質保證 (QA) 以及生產環境的專屬客戶。 AWS 帳戶 像這樣的區段策略可能是整體設計討論的重要組成部分，而且您的 OU 可能需要符合您的特定法規需求。

# 營運隱私權服務 AWS

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

對於許多人來說，隱私是跨越切割的。許多不同的團隊都可以參與其中，包括監管、合規和工程團隊。當您的組織已開始定義隱私權方案的關鍵人員和政策元件時，您可以將控制項對應至隱私權法規遵循架構，以實現一致的作業。框架可以作為實施環境中個人數據的基礎和應用程序特定隱私權控制的專欄。AWS

無論客戶使用哪種架構來分類其隱私權需求，隱私權合規性、隱私權工程和應用程式團隊通常都需要共同合作以達成實作目標。例如，法規和法規遵循團隊可能會提供高階需求，而工程和應用程式團隊會配置 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性的組織和技術控制項。

定義 AWS 服務 和功能的技術控制項時，另一個重要決定是控制項應套用至整個組織、OU、帳號或特定資源。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

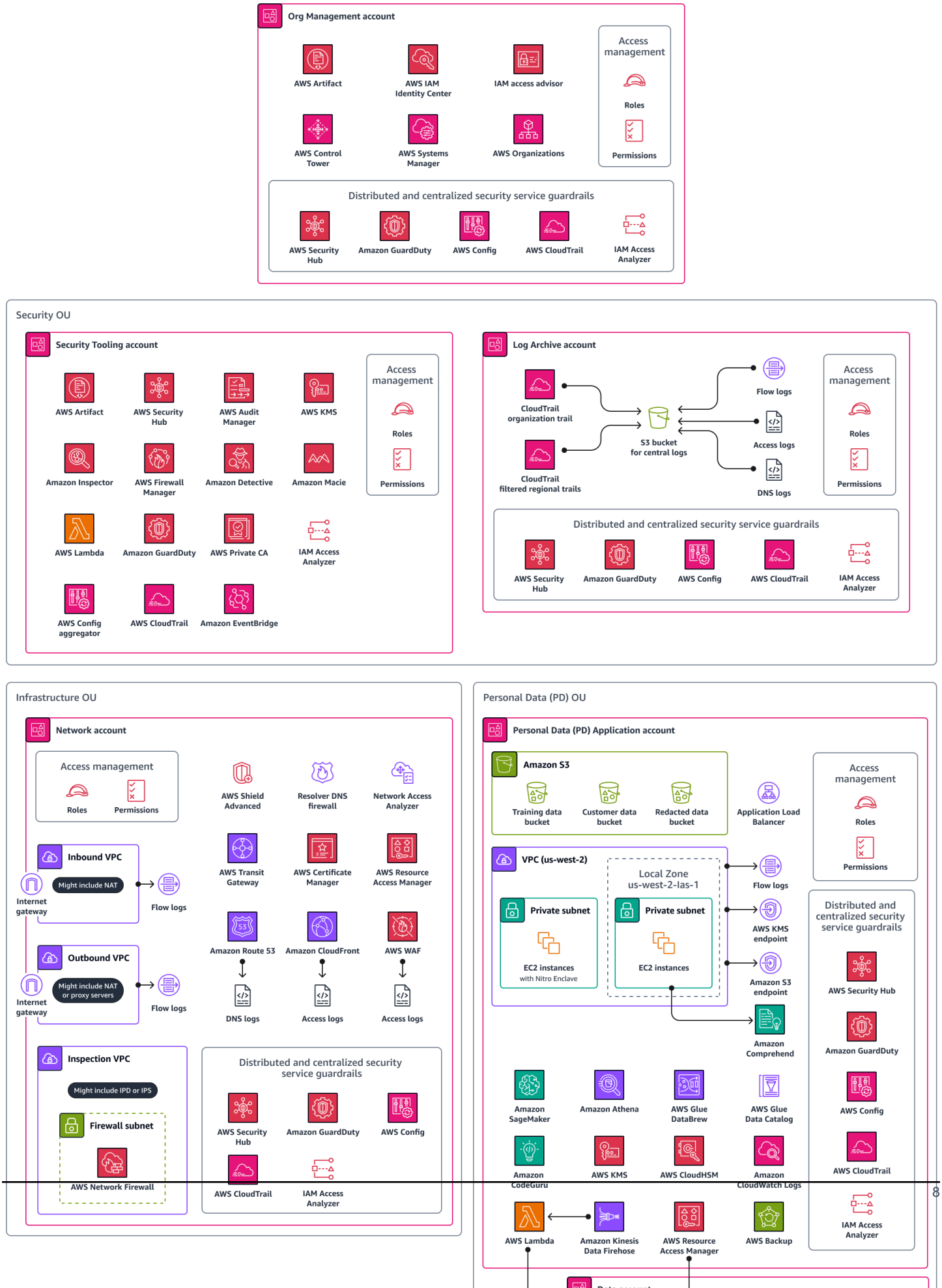
體的公開存取是一種特定的控制項，最好是在組織根目錄設定，而不是針對每個帳戶個別設定。不過，您的保留原則可能會因應用程式而異，這表示您可能會在資源層級套用控制項。

為了協助您加速組織中的隱私權營運，為您的工作負載 AWS 提供稽核與合規諮詢服務。 AWS 如需詳細資訊，請連絡 AWS SAS。

# AWS 隱私權參考架構

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

下圖說明 AWS 隱私權參考架構 (AWS PRA)。這是一個連接許多隱私相關和功能的體系結構的 AWS 服務 示例。這種架構建立在由管理的 landing zone 域上 AWS Control Tower。


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
AWS Control Tower
AWS Systems Manager
AWS Organizations
Access management
Roles
Permissions
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
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
Access management
Roles
Permissions
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
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
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
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
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
Amazon Comprehend
Amazon SageMaker
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
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

AWS PRA 包括託管在個人數據（PD）應用程序帳戶中的無服務器 Web 架構。此帳戶中的架構是一個範例工作負載，可直接從消費者那裡收集個人資料。在此工作負載中，使用者會透過 Web 層連線。Web 層與應用程式層互動。該層接收來自 Web 層的輸入，處理和存儲數據，允許獲得授權的內部團隊和第三方訪問數據，並最終在不再需要數據時存檔和刪除數據。該架構具有特定目的的模組化和事件驅動，以展示許多基礎隱私工程技術，而無需深入研究特定的使用案例，例如資料湖、容器、運算或物聯網 (IoT)。

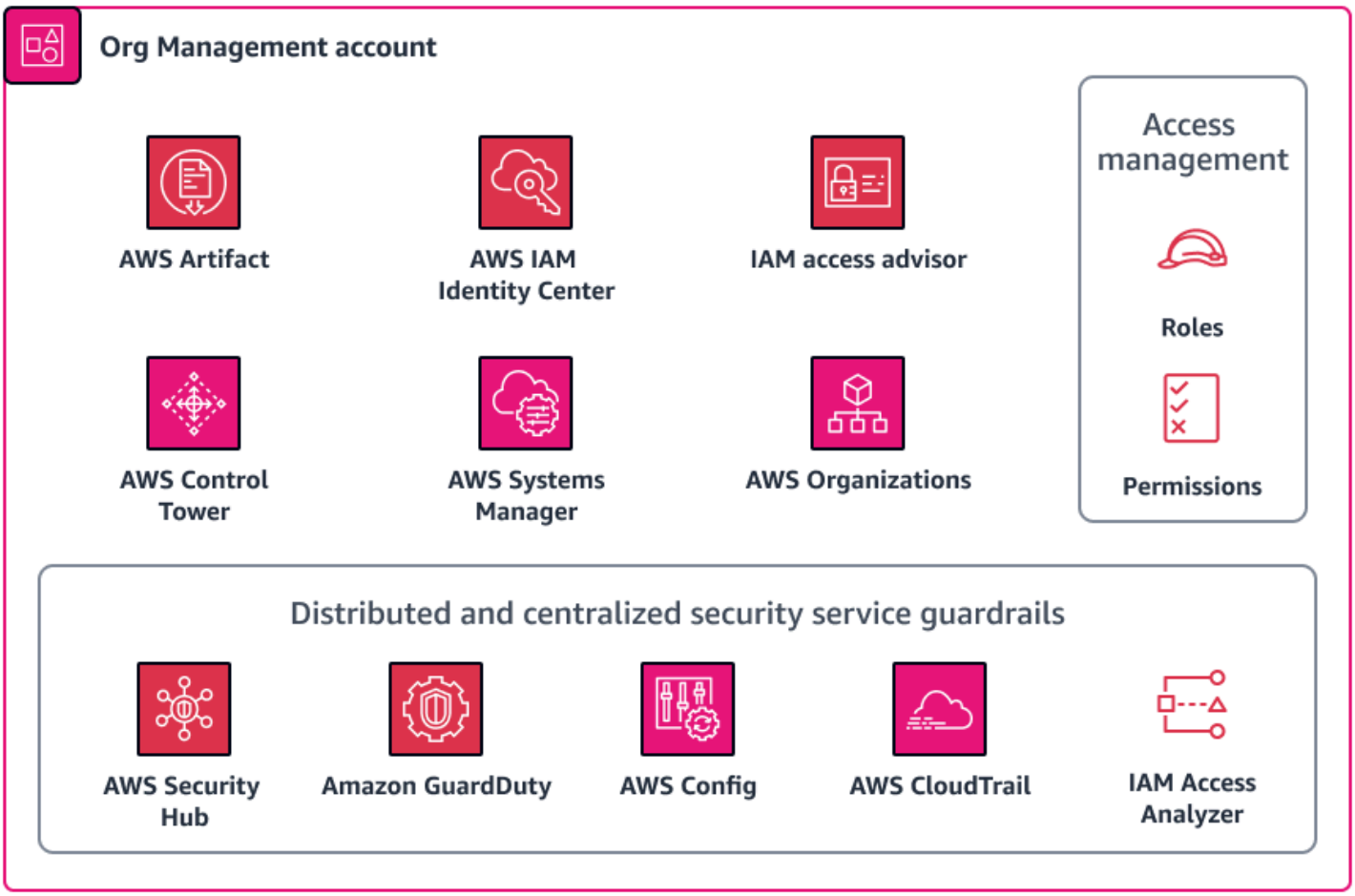
接下來，本指南詳細描述組織中的每個帳戶。它討論了與隱私權相關的服務和功能、注意事項和建議，以及下列每個帳戶的圖表：

- 組織管理帳戶
- 安全性 OU — 安全性工具帳戶
- 安全性 OU — 記錄封存帳戶
- 基礎設施 OU – 網路帳戶
- 個人資料單位 — PD 申請帳戶

# 組織管理帳戶

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

組織管理帳戶主要用於管理組織中所有帳戶 (由管理) 之基礎隱私權控制的資源組態偏移。 AWS Organizations此帳戶也是您可以一致部署新成員帳戶的地方，並具有許多相同的安全性和隱私權控制。如需有關此帳戶的詳細資訊，請參閱AWS 安全性參考架構 (AWS SRA)。下圖說明組織管理帳戶中設定的 AWS 安全性和隱私權服務。




本節提供有關此帳戶中使用的下列項目 AWS 服務 的更多詳細資訊：

- AWS Artifact
- AWS Control Tower
- AWS Organizations

## AWS Artifact

AWS Artifact提供 AWS 安全性與合規性文件的隨需下載，可協助您進行稽核。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

這可 AWS 服務 協助您瞭解繼承的控制項， AWS 並決定您可以在環境中實作哪些控制項。 AWS Artifact 提供 AWS 安全性和合規性報告的存取權，例如系統和組織控制 (SOC) 報告和支付卡產業 (PCI) 報告。它還提供來自各地區和法規遵循垂直行業的 AWS 認證機構的認證存取權，以驗證控制項的實施和營運效率。使用時 AWS Artifact，您可以將 AWS 稽核成品提供給稽核人員或監管機構，作為 AWS 安全控制的證據。以下報告可能有助於證明 AWS 隱私權控制的有效性：

- SOC 2 第 2 類隱私報告 — 本報告展示了對於收集、使用、保留、披露和處置個人資料的 AWS 控制方式的有效性。如需詳細資訊，請參閱 SOC 常見問題集。
- SOC 3 隱私權報告 — SOC 3 隱私權報告對於一般流通而言，對於 SOC 隱私權控制而言，較不詳細說明。
- ISO/IEC 27701:2019 認證報告說明了建立和持續改進隱私權資訊管理系統 (PIM) 的要求和準則。本報告詳細說明了此認證的範圍，並可作為 AWS 認證證明。如需有關此標準的詳細資訊，請參閱 ISO/IEC 27701: 2019 (ISO 網站)。

## AWS Control Tower

AWS Control Tower協助您設定和管理遵循規範安全性最佳做法的 AWS 多帳戶環境。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

在中 AWS Control Tower，您還可以自動化一些主動、預防性和偵探控制項 (也稱為護欄) 的部署，以符合您的資料存放區和資料保護需求。例如，您可以指定將資料傳輸限制為僅核准的護欄。 AWS 區域為了獲得更精細的控制，您可以從專為控制資料駐留而設計的 17 個以上的護欄中進行選擇，例如「不允許 Amazon 虛擬私人網路 (VPN) 連線」、「不允許 Amazon VPC 執行個體的網際網路存取」以及根據要求拒絕存取。 AWS AWS 區域這些護欄由許多 AWS CloudFormation 勾點、服務控制原 AWS Config 則和規則組成，這些都可以統一部署到整個組織中。如需詳細資訊，請參閱 AWS Control Tower 文件中的加強資料駐留保護的控制項。

如果您需要在資料駐留控制範圍之外部署隱私護欄，請 AWS Control Tower 包括一些強制性控制項。當您設定 landing zone 域時，預設會在每個 OU 上部署這些控制項。其中許多都是為了保護記錄而設計的預防性控制項，例如「不允許刪除記錄封存」和「啟用記錄檔的完整性驗證」。 CloudTrail

AWS Control Tower 還集成 AWS Security Hub 了提供偵探控制。這些控制項稱為服務管理標準：AWS Control Tower。您可以使用這些控制來監控隱私支援控制的組態偏移，例如 Amazon 關聯式資料庫服務 (Amazon RDS) 資料庫執行個體的靜態加密。

## AWS Organizations

AWS PRA 用 AWS Organizations 於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 以及專門的帳戶結構。在中 AWS Organizations，您可以使用服務控制政策（SCP）和管理策略來幫助保護個人數據和隱私。

服務控制政策 (SCP)

服務控制原則 (SCP) 是一種組織原則類型，可用來管理組織中的權限。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權限。您可以從「組織管理」帳戶建立及套用 SCP。

您可以使 AWS Control Tower 用在您的帳戶中統一部署 SCP。如需有關可套用的資料駐留控制項的詳細資訊 AWS Control Tower，請參閱本指南AWS Control Tower中的。 AWS Control Tower 包括預防性 SCP 的完整補充。如果您的組織目前 AWS Control Tower 未使用，您也可以手動部署這些控制項。

使用 SCP 解決資料存放需求

通常會在特定地理區域內儲存和處理資料來管理個人資料存放需求。為了驗證是否符合司法管轄區的獨特資料存放需求，我們建議您與監管團隊密切合作，以確認您的要求。確定這些要求後，有許多 AWS 基礎隱私權控制項可協助您提供支援。例如，您可以使用 SCP 來限制 AWS 區域 可用於處理和儲存資料的資料。如需原則範例，請參閱本指南限制跨越資料傳輸 AWS 區域中的。

使用 SCP 限制高風險 API 呼叫

了解負責哪些安全性和隱私權控制項，以及您負責哪些控制項 AWS 是非常重要的。例如，您需要對您使用的 API 呼叫的結果負責。 AWS 服務 您也有責任瞭解哪些通話可能會導致您的安全性或隱私權狀態發生變更。如果您擔心維護某種安全性和隱私權狀態，可以啟用 SCP 來拒絕某些 API 呼叫。這些 API 呼叫可能會產生影響，例如意外披露個人資料或違反特定跨境資料傳輸的行為。例如，您可能想要禁止下列 API 呼叫：

- 啟用對亞馬遜簡單儲存服務 (Amazon S3) 儲存貯體的公開存取
- 停用 Amazon GuardDuty 或為資料外洩發現項目建立抑制規則，例如特DataExfiltration洛伊木馬:EC2/DNS 尋找
- 刪除 AWS WAF 資料外洩規則
- 公開分享 Amazon Elastic Block Store (Amazon EBS) 快照
- 從組織中移除成員帳戶
- 取消 Amazon CodeGuru 審閱者與儲存庫的關聯

管理政策

中的管理原則 AWS Organizations 可協助您集中設定 AWS 服務 及管理其功能。您選擇的管理原則類型會決定原則如何影響 OU 以及繼承這些原則的帳號。標籤原則是直接與隱私權相關的管理原則範例。 AWS Organizations

使用標籤原則

標籤是索引鍵值配對，可協助您管理、識別、組織、搜尋和篩選 AWS 資源。套用標籤以區分組織中處理個人資料的資源可能很有用。標籤的使用支持本指南中的許多隱私解決方案。例如，您可能想要套用標籤，指出資源中正在處理或儲存之資料的一般資料分類。您可以撰寫以屬性為基礎的存取控制 (ABAC) 原則，以限制對具有特定標籤或一組標籤的資源的存取。例如，您的原則可能會指定`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將資料保留原則廣泛套用至許多帳戶的備份，您可以套用標記，將該資源置於該備份原則的範圍內。

標籤原則可協助您在整個組織中維持一致的標籤。在標籤策略中，您可以指定標記資源時套用至資源的規則。例如，您可以要求使用特定索引鍵 (例如`DataClassification`或) 來標記資源`DataSteward`，而且您可以為索引鍵指定有效的大小寫處理方式或值。您也可以使用強制來防止不符合標籤要求完成。

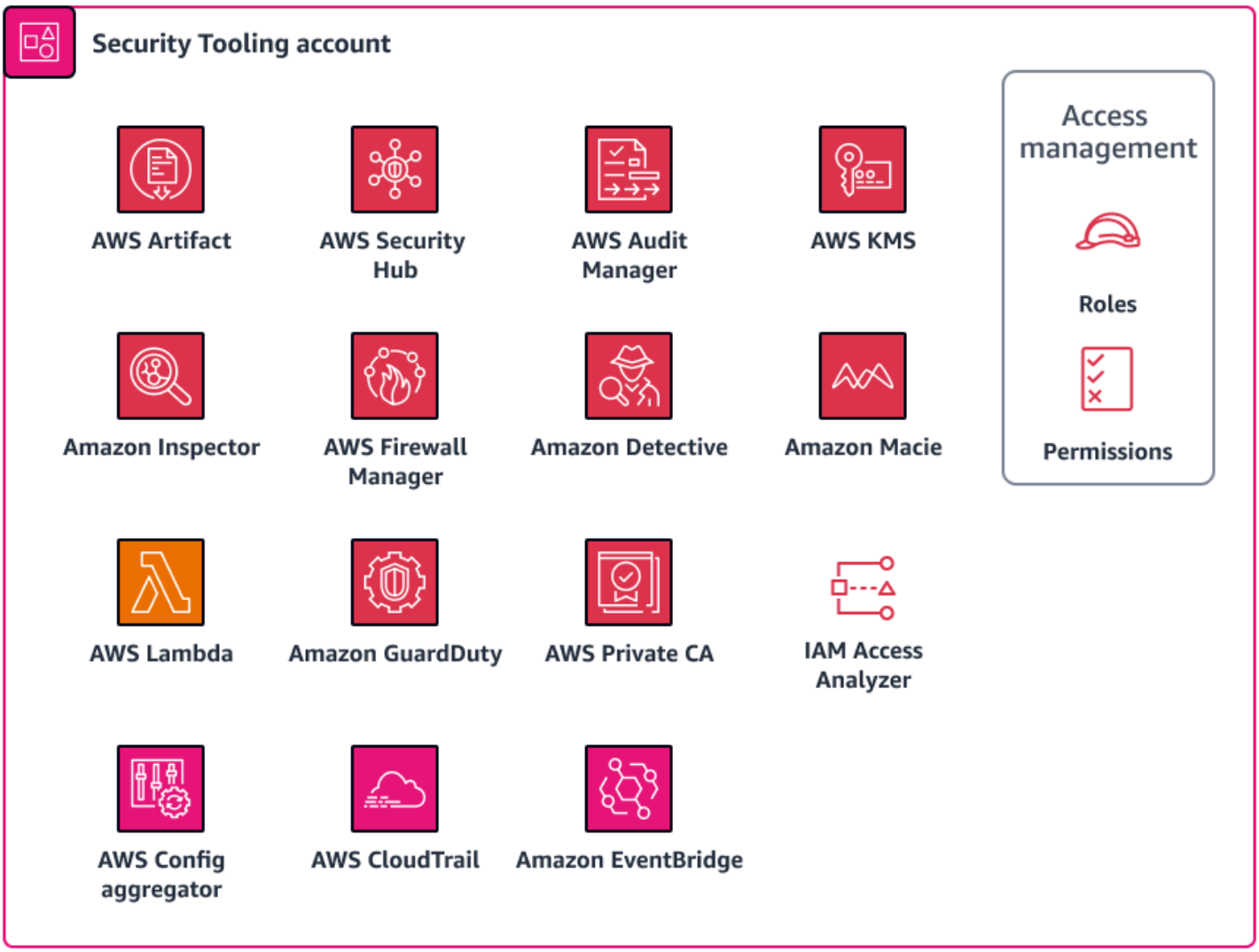
使用標籤做為隱私權控制策略的核心元件時，請考慮下列事項：

- 考慮在標籤鍵或值中放置個人資料或其他類型敏感資料的影響。當您聯絡 AWS 尋求技術協助時，AWS 可能會分析標籤和其他資源識別碼，以協助解決問題。在此情況下，您可能想要將標籤值取消識別，然後使用客戶控制的系統 (例如 IT 服務管理 (ITSM) 系統來重新識別標籤值。 AWS 建議不要在標籤中包含個人身份信息。
- 請考慮某些標籤值必須設為不可變 (不可修改)，以防止規避技術控制項，例如依賴標籤的 ABAC 條件。

# 安全性 OU — 安全性工具帳戶

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

Security Tools 帳戶致力於營運安全性與隱私權基礎服務、監控 AWS 帳戶，以及自動化安全性與隱私權警示與回應。如需有關此帳戶的詳細資訊，請參閱AWS 安全性參考架構 (AWS SRA)。下圖說明 AWS 安全性工具帳戶中設定的安全性和隱私權服務。




本節提供有關此帳戶中以下內容的更多詳細資訊：

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

## AWS CloudTrail

AWS CloudTrail可協助您稽核 AWS 帳戶. CloudTrail 在所有 AWS 帳戶 和 AWS 區域 該存儲，處理或傳輸個人數據中啟用可以幫助您跟踪此數據的使用和披露。AWS 安全參考架構建議您啟用組織追蹤，

這是一個記錄組織中所有帳戶的所有事件的單一追蹤。但是，啟用此組織追蹤會將多區域日誌資料彙總到日誌存檔帳戶中的單一 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體。對於處理個人數據的帳戶，這可能會帶來一些額外的設計考慮因素。日誌記錄可能包含對個人數據的一些引用。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在組織追蹤中包含或排除哪些區域工作負載。對於您決定要從組織追蹤中排除的工作負載，您可以考慮設定可遮罩個人資料的區域特定追蹤。有關屏蔽個人數據的更多信息，請參閱本指南的Amazon 數據 Firehose部分。最終，您的組織可能會結合組織追蹤和區域追蹤，這些追蹤彙總到集中式的日誌封存帳戶中。

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。建立組織軌跡時，您可以在中使用選擇加入設定 AWS Control Tower，或直接在CloudTrail主控台中建立追蹤。

如需整體方法以及如何管理記錄集中化和資料傳輸需求的詳細資訊，請參閱本指南中的集中式記錄儲存章節。根據 AWS SRA，無論您選擇什麼設定，您都可能想要將 Security Tools 帳戶中的追蹤管理與記錄封存帳戶中的記錄儲存區分開來。此設計可協助您為需要管理記錄檔和需要使用記錄資料的使用者建立最低權限存取原則。

## AWS Config

AWS Config提供資源的詳細檢視，以 AWS 帳戶 及資源的設定方式。它可協助您識別資源彼此之間的關聯性，以及它們的組態在一段時間內如何變更。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

在中 AWS Config，您可以部署一致性套件，這些套件是 AWS Config 規則集和修正動作。一致性套件提供一般用途架構，其設計目的是使用受管或自訂規則來進行隱私權、安全性、營運和成本最佳化治理檢查。 AWS Config 您可以使用此工具作為大型自動化工具集的一部分，以追蹤 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 1.0 一致性套件的營運最佳作法與 NIST 隱私權架構中的許多隱私權相關控制一致。每個 AWS Config 規則都適用於特定的 AWS 資源類型，並且與一或多個 NIST 隱私權架構控制項有關。您可以使用此一致性套件來追蹤帳戶中資源之間與隱私權相關的持續合規性。以下是此一致性套件中包含的一些規則：

- `no-unrestricted-route-to-igw`— 此規則可持續監控 VPC 路由表是否有預設`0.0.0.0/0`或`::/0`輸出至網際網路閘道的路由，以協助防止資料層上的資料外洩。這可協助您限制可傳送至網際網路繫結流量的位置，特別是如果有已知為惡意的 CIDR 範圍。
- `encrypted-volumes`— 此規則會檢查連接到 Amazon 彈性運算雲端 (Amazon EC2) 執行個體的亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區是否已加密。如果您的組織有特定的控制需求，這些要

求與 AWS Key Management Service (AWS KMS) 金鑰保護個人資料有關，您可以指定特定金鑰 ID 作為規則的一部分，以檢查磁碟區是否已使用特定金 AWS KMS 鑰加密。

- `restricted-common-ports`— 此規則會檢查 Amazon EC2 安全群組是否允許不受限制的 TCP 流量傳輸到指定的連接埠。安全性群組可提供資源的輸入和輸出網路流量的狀態篩選，協助您管理網路存取。 AWS 封鎖資源上通用連接埠 (例如 TCP 3389 和 TCP 21) 的輸入流量，有助於限制遠端存取。`0.0.0.0/0`

AWS Config 可用於 AWS 資源的主動和被動式合規性檢查。除了考慮在一致性包中找到的規則之外，您還可以將這些規則納入偵測和主動評估模式中。這有助於提前在軟體開發生命週期中實作隱私權檢查，因為應用程式開發人員可以開始整合部署前檢查 例如，它們可以在其模 AWS CloudFormation 板中包含掛接，以根據啟用主動模式的所有隱私相關 AWS Config 規則檢查模板中聲明的資源。如需詳細資訊，請參閱AWS Config 規則立即 Support 主動式遵循 (AWS 部落格文章)。

## Amazon GuardDuty

AWS 提供多種可用於存放或處理個人資料的服務，例如 Amazon S3、Amazon Relational Database Service 服務 (Amazon RDS) 或使用 Kubernetes 的 Amazon EC2。Amazon GuardDuty 將智慧型可見性與持續監控相結合，以偵測可能與個人資料意外洩露有關的指標。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

透過 GuardDuty，您可以在整個攻擊生命週期中識別潛在惡意、隱私權相關的活動。例如，GuardDuty 可以提醒您有關與黑名單網站的連線、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 呼叫者。您也可以設定 GuardDuty 為從您自己的信任 IP 清單中停止受信任 IP 位址的警示，並從您自己的威脅清單針對已知的惡意 IP 位址發出警示。

依照 AWS SRA 中的建議，您可以 GuardDuty 針對組織 AWS 帳戶 中的所有人啟用，並將 Security Tools 帳戶設定為 GuardDuty 委派的管理員。 GuardDuty將整個組織的搜尋結果彙總至此單一帳戶。如需詳細資訊，請參閱使用管理 GuardDuty 帳戶 AWS Organizations。您還可以考慮在事件響應過程中識別所有與隱私相關的利益相關者，從檢測和分析到遏制和消除，並將其涉及數據洩露的任何事件涉及到。

## IAM Access Analyzer

許多客戶都希望持續保證個人資料會適當地與預先核准的協力廠商處理器分享，而不會與其他實體分享。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 環境中的信任資源。當您定義個人資料外洩和預期洩露的控制項時，您可以定義受信任的身分識別、受信任的資源和預期的網路。

使用 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)，組織可以定義信任 AWS 帳戶 區域，並針對該信任區域的違規設定警示。IAM Access Analyzer 會分析 IAM 政策，協助識別和解決非預期的公開或跨帳戶存取潛在敏感資源。IAM Access Analyzer 使用數學邏輯和推論，針對可從外部存取的資源產生全面的發現結果。 AWS 帳戶最後，為了回應和修復過於寬鬆的 IAM 政策，您可以使用 IAM Access Analyzer 來驗證現有政策與 IAM 最佳實務的比較，並提供建議。IAM 存取分析器可以根據 IAM 主體先前的存取活動產生最低權限 IAM 政策。它會分析 CloudTrail 記錄檔並產生策略，該策略僅授與繼續執行這些工作所需的權限。

如需有關如何在安全性內容中使用 IAM Access Analyzer 的詳細資訊，請參閱AWS 安全參考架構。

### Amazon Macie

Amazon Macie 是一項服務，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，並協助您自動防範這些風險。當 Macie 偵測到潛在的政策違規或 Amazon S3 儲存貯體的安全性或隱私問題時，會產生發現結果。Macie 是組織可用來實作自動化以支援合規性工作的另一種工具。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

Macie 可以偵測龐大且不斷增長的敏感資料類型清單，包括個人識別資訊 (PII)，例如姓名、地址和其他可識別屬性。您甚至可以建立自訂資料識別碼，以定義反映組織對個人資料定義的偵測準則。

當您的組織針對包含個人資料的 Amazon S3 儲存貯體定義預防性控制時，您可以使用 Macie 做為驗證機制，持續保證您的個人資料存放位置及其受到保護的方式。若要開始，請啟用 Macie 並設定自動化敏感資料探索。Macie 持續分析所有 S3 儲存貯體中的物件、跨帳戶和 AWS 區域. Macie 生成並維護一個交互式熱圖，描繪了個人數據所在的位置。自動化敏感資料探索功能旨在降低成本，並將手動設定探索工作的需求降至最低。您可以在自動化敏感資料探索功能之上進行建置，並使用 Macie 自動偵測新值區或現有值區中的新資料，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與隱私權團隊有關錯誤分類或未分類值區的相關資訊。

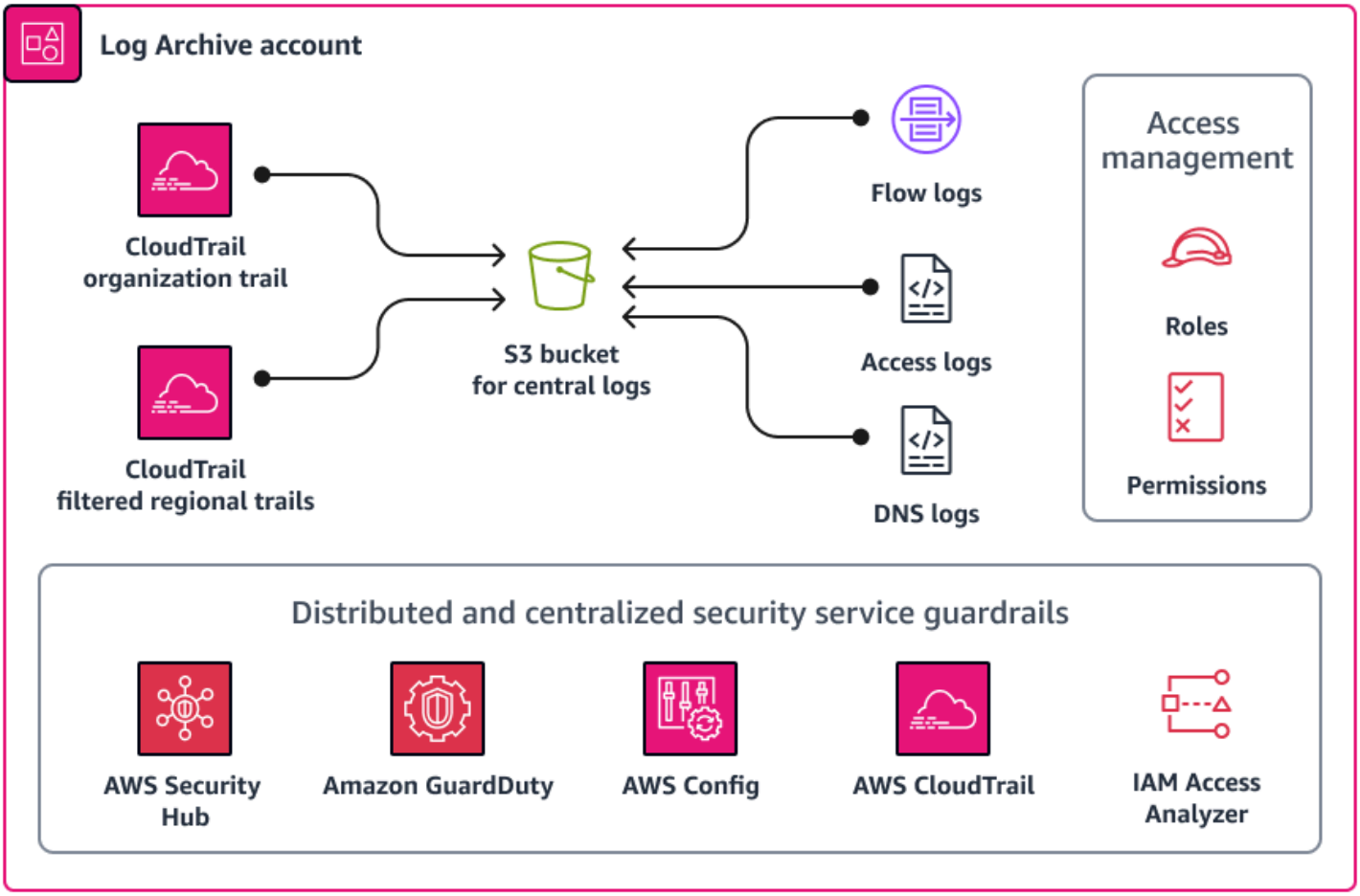
您可以使用來為組織中的每個帳戶啟用 AWS Organizations Macie。如需詳細資訊，請參閱在 Amazon Macie 中整合和設定組織。

## 安全性 OU — 記錄封存帳戶

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

記錄封存帳戶是您集中基礎結構、服務和應用程式記錄檔類型的地方。如需有關此帳戶的詳細資訊，請參閱AWS 安全性參考架構 (AWS SRA)。使用專屬的記錄帳戶，您可以在所有記錄類型中套用一致的警示，並確認事件回應者可以從單一位置存取這些記錄的彙總。您也可以從單一位置設定安全控制和資

料保留政策，這樣可以簡化隱私權營運額外負荷。下圖說明記錄封存帳戶中設定的 AWS 安全性和隱私權服務。




## 集中式記錄儲存

記錄檔案 (例如 AWS CloudTrail 記錄檔) 可能包含可視為個人資料的資訊。有些組織選擇使用組織追蹤，以便將跨帳戶 AWS 區域 和跨帳戶的 CloudTrail 記錄彙總到一個中央位置，以達到可見性的目的。如需詳細資訊，請參閱本指南中的 AWS CloudTrail。實作集中化 CloudTrail 日誌時，日誌通常存放在單一區域的 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體中。

根據您組織對個人資料的定義和適用的區域隱私權法規，您可能需要考慮跨境資料傳輸。如果您的組織需要符合區域隱私權法規的資料傳輸需求，下列選項可協助您提供支援：

1. 如果您的組織向多個國家/地區的 AWS 雲端 資料主體提供服務，您可以選擇彙總該國家/地區中符合最嚴格資料落地要求的所有記錄。例如，如果您在德國營運，而且它的要求最嚴格，則可能會在中彙總 S3 儲存貯體中的資料，`eu-central-1` AWS 區域 以便在德國收集的資料不會離開德國的邊

界。對於此選項，您可以在其中設定單一組織追蹤 CloudTrail ，以彙總所有帳戶和目標區域 AWS 區域 的記錄。

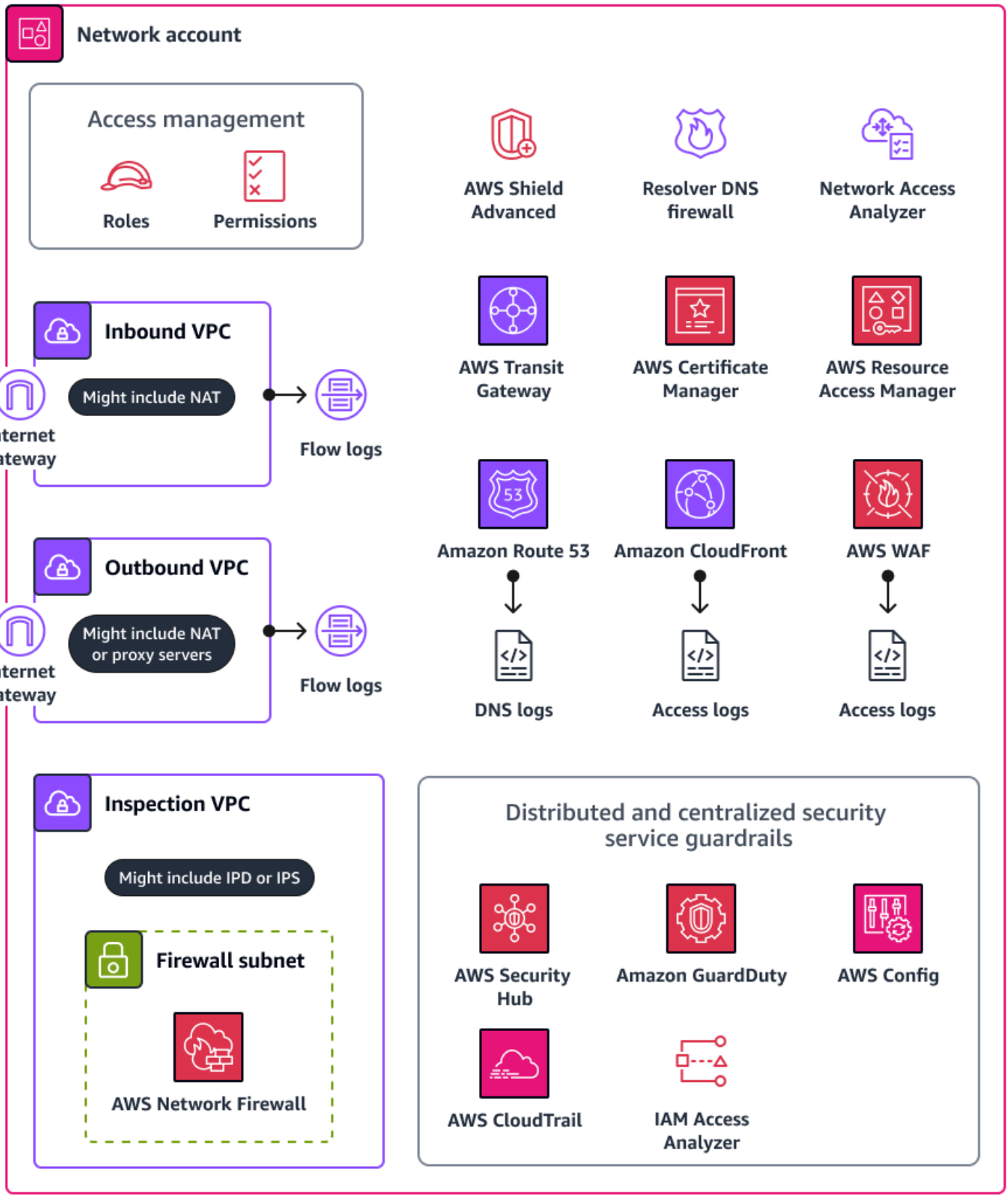
2. 在將資料複製並彙總到其他區域之 AWS 區域 前，編輯需要保留在其中的個人資料。例如，您可以在將記錄傳輸到其他區域之前，先遮罩應用程式主機區域中的個人資料。有關屏蔽個人數據的更多信息，請參閱本指南的Amazon 數據 Firehose部分。

與您的法律顧問合作，以確定哪些個人數據在範圍內，以及允許哪些 AWS 地區到地區的傳輸。

# 基礎設施 OU – 網路帳戶

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

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




本節提供有關此帳戶中使用的下列項目 AWS 服務 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可透過稱為節點位置的全球資料中心網路傳遞內容。當使用者要求您提供服務的內容時 CloudFront，會將要求路由至提供最低延遲的節點位置。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

您可以使用 CloudFront 地理限制來防止位於特定地理位置的使用者存取您透過散佈發 CloudFront佈的內容。如需地理限制的詳細資訊和設定選項，請參閱 CloudFront文件中的限制內容的地理分佈。

您也可以設定 CloudFront 產生存取記錄，其中包含有關 CloudFront 接收之每個使用者要求的詳細資訊。如需詳細資訊，請參閱 CloudFront 文件中的設定和使用標準記錄 (存取記錄)。最後，如果設定 CloudFront 為在一系列邊緣位置快取內容，您可能會考慮在何處發生快取。對於某些組織而言，跨區域快取可能會受到跨境資料傳輸需求的限制。

## AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) 可協助您安全地共用資源， AWS 帳戶 以減少營運開銷，並提供可見性和可稽核性。使用時 AWS RAM，組織可以限制哪些 AWS 資源可以與其組織 AWS 帳戶 中的其他人或協力廠商帳號共用。如需詳細資訊，請參閱可共用 AWS 資源。在網路帳戶中，您可以用 AWS RAM 來共用 VPC 子網路和傳輸閘道連線。如果您使 AWS RAM 用與其他人共用資料平面連線 AWS 帳戶，請考慮建立程序以檢查是否已與預先核准 AWS 區域建立連線。

除了共用 VPC 和傳輸閘道連線之外，還 AWS RAM 可用於共用不支援 IAM 資源型政策的資源。對於「個人資料 OU」中託管的工作負載，您可 AWS RAM 以使用存取位於單獨的個人資料 AWS 帳戶。如需詳細資訊，請參閱 AWS Resource Access Manager「個人資料 OU — PD 應用程式帳戶」一節。

## AWS Transit Gateway

如果您想要部署收集、儲存或處理符合您組織資料存放需求的個人資料的 AWS 資源，而且您有適當的技術保護措施，請考慮實施保護措施，以防止未經核准的跨境資料在 AWS 區域 控制和資料層面上流動。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，因此跨區域資料流量。

有多個選項可用來控制資料平面上的跨區域資料流程。例如，您可以使用路由表、VPC 對等和 AWS Transit Gateway 附件。 AWS Transit Gateway是連接虛擬私人雲端 (VPC) 和內部部署網路的中央集線器。作為大型 AWS landing zone 域的一部分，您可以考慮資料可以遍歷的各種方式 AWS 區域，包括透過網際網路閘道、透過直接 VPC 到 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 VPC 與內部部署環境之間的東西向和南北連線符合您的隱私權需求。
- 根據您的隱私權需求設定 VPC 設定。
- 使用中的服務控制政策 AWS Organizations 和 IAM 政策來協助防止對您 AWS Transit Gateway 和 Amazon Virtual Private Cloud (Amazon VPC) 組態進行修改。如需服務控制原則的範例，請參閱本指南限制對 VPC 組態的變更中的。

## AWS WAF

為了防止意外洩露個人資料，您可以為 Web 應用程式部署一 defense-in-depth 種方法。您可以在應用程式中建立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，可協助您監控轉寄至受保護 Web 應用程式資源的 HTTP 和 HTTPS 要求。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

使用 AWS WAF，您可以定義和部署用於檢查特定準則的規則。以下活動可能與意外披露個人資料有關：

- 來自未知或惡意 IP 位址或地理位置的流量
- 開放全球應用程式安全專案 (OWASP) 十大攻擊，包括 SQL 注入等漏洞相關攻擊
- 要求率高
- 一般機器人流量
- 內容抓取工具

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 可用來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 SQL 資料庫利用相關聯的要求模式，例如 SQL 插入攻擊。如果您的應用程式與 SQL 資料庫連接，請考慮這個規則群組。
- 已知錯誤輸入 — 此規則群組包含的規則旨在封鎖已知無效且與惡意利用或發現弱點相關聯的要求模式。

- 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、扭曲商業指標、造成停機時間以及執行惡意活動。
- 帳號接管預防 (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。

# 個人資料單位 — PD 申請帳戶

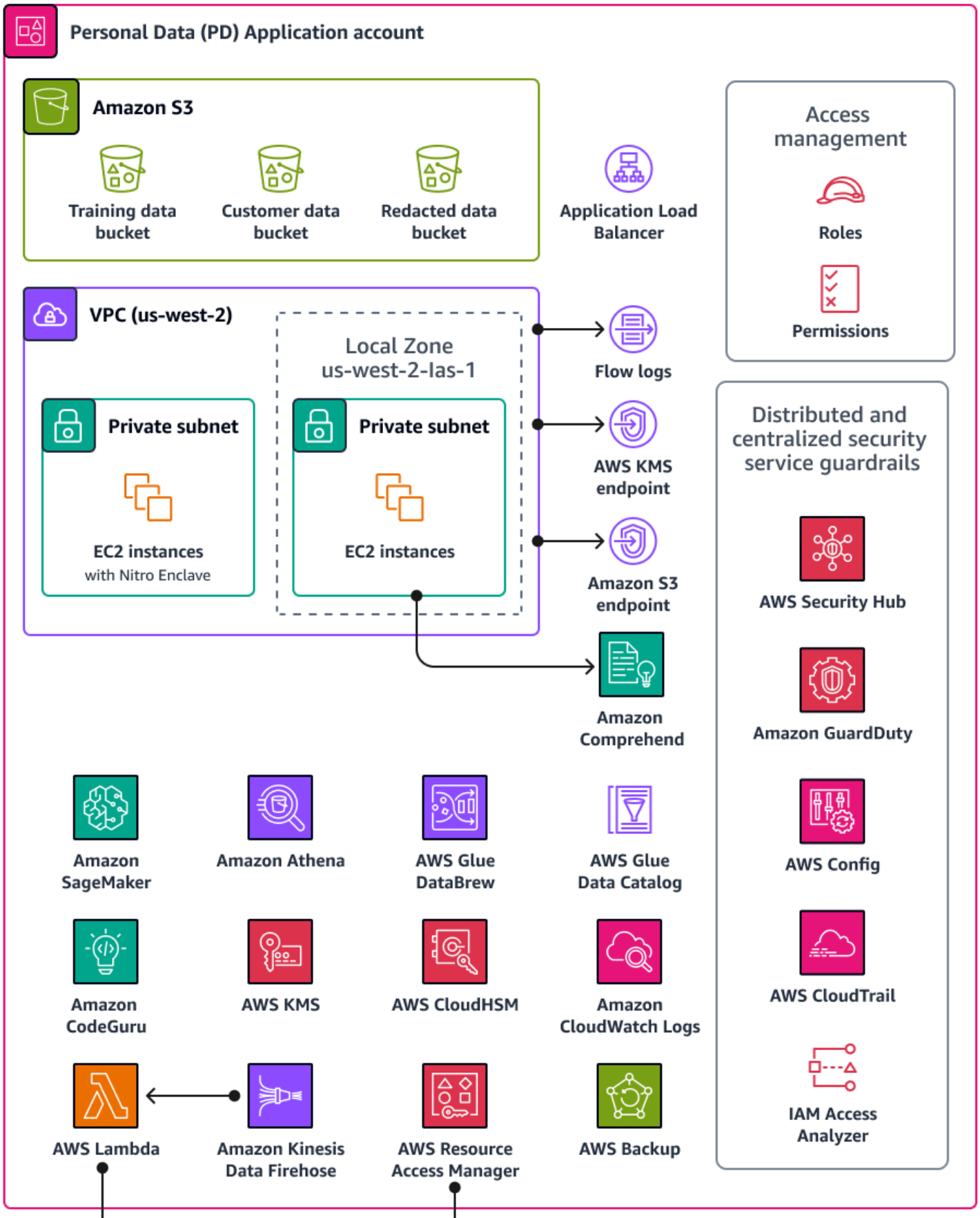
我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

個人資料 (PD) 應用程式帳戶是貴組織託管收集和處理個人資料之服務的地方。具體而言，您可能會將定義為個人資料的內容儲存在此帳戶中。 AWS PRA 透過多層無伺服器 Web 架構示範一些隱私權設定範例。當涉及到跨 AWS landing zone 域操作工作負載時，隱私配置不應被視為 one-size-fits-all 解決方案。例如，您的目標可能是了解基礎概念，它們如何增強隱私權，以及您的組織如何將解決方案應用於您的特定使用案例和架構。

對 AWS 帳戶 於收集、儲存或處理個人資料的組織中，您可以使用 AWS Organizations 和部署基礎且 AWS Control Tower 可重複的防護裝置。為這些帳戶建立專屬的組織單位 (OU) 非常重要。例如，您可能只想將資料存放區護欄套用到資料存放區是核心設計考量的帳戶子集。對於許多組織而言，這些是存儲和處理個人數據的帳戶。

您的組織可能支援專用的資料帳戶，您可以在此帳戶儲存個人資料集的權威來源。授權資料來源是您儲存資料的主要版本的位置，這可能被認為是資料最可靠、最準確的版本。例如，您可以將資料從授權資料來源複製到其他位置，例如 PD 應用程式帳戶中用於存放訓練資料的 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體、客戶資料子集和編修資料。透過採用這種多帳戶方法，將資料帳戶中完整且明確的個人資料集與 PD Application 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。

下圖說明在 PD 應用程式和資料帳戶中設定的 AWS 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
Amazon Comprehend
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
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
Log Archive

本節提供有關這些帳戶中使用 AWS 服務 的下列項目的更多詳細資訊：

- Amazon Athena
- Amazon CloudWatch 日誌
- Amazon 評論 CodeGuru 家
- Amazon Comprehend
- Amazon 數據 Firehose
- AWS Glue
- AWS Key Management Service
- AWS Local Zones
- AWS 硝基飛地
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker
- AWS 協助管理資料生命週期的功能
- 協助區段資料的 AWS 服務和功能

## Amazon Athena

您也可以考慮資料查詢限制控制項，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。您不必將資料載入 Athena；它可以直接與存放在 S3 儲存貯體中的資料搭配使用。

Athena 的一個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，您可以透過遮罩對資料分析團隊帶來極少價值的整個個人資料欄來清理資料集。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 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，稱為使用者定義函數 (UDF)。您可以在提交至 Athena 的 SQL 查詢中叫用 UDF，然後它們在上 AWS Lambda 執行。您可以在`SELECT`和`FILTER` SQL查詢中使用 UDF，也可以在同一個查詢中叫用多個 UDF。為了保護隱私，您可以建立 UDF 來執行特定類型的資料遮罩，例如僅顯示資料行中每個值的最後四個字元。

## Amazon CloudWatch 日誌

Amazon CloudWatch Logs 可協助您集中管理所有系統、應用程式的日誌，以 AWS 服務 便您可以監控和安全地存檔日誌。在 CloudWatch Logs 中，您可以針對新的或現有的記錄群組使用資料保護政策，以協助將個人資料洩露的風險降到最低。資料保護政策可以偵測記錄中的敏感資料，例如個人資料。當使用者透過存取記錄檔時，資料安全防護原則可以遮罩該資料 AWS Management Console。當使用者需要直接存取個人資料時，您可以根據工作負載的整體用途規格，為這些使用者指派`logs:Unmask`權限。您也可以建立全帳戶的資料保護政策，並在組織中的所有帳戶中一致地套用此政策。這會預設為「記錄檔」中 CloudWatch 所有目前和 future 的記錄群組設定遮罩。我們也建議您啟用稽核報告，並將其傳送到另一個日誌群組、Amazon S3 儲存貯體或 Amazon Data Firehose。這些報告包含每個記錄群組中資料保護發現項目的詳細記錄。

## Amazon 評論 CodeGuru 家

對於隱私和安全性，對於許多組織來說，在部署和部署後階段都支持持續合規性至關重要。 AWS PRA 在處理個人資料的應用程式的部署管道中包含主動式控制。Amazon CodeGuru 審核者可以偵測可能會在 Java 和 Python 程式碼中暴露個人資料的潛在缺陷。 JavaScript它為開發人員提供了改進代碼的建議。 CodeGuru 審核者可以識別各種安全性、隱私權和一般最佳做法中的缺陷。如需詳細資訊，請參閱 Amazon CodeGuru 偵測器程式庫。它旨在與多個來源供應商合作 AWS CodeCommit，包括 Bitbucket 和 Amazon S3。 GitHub CodeGuru 審核者可以偵測到的一些隱私權相關瑕疵包括：

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

## Amazon Comprehend

Amazon Comprehend 是一種自然語言處理 (NLP) 服務，它使用機器學習來發掘英文文字文件中的寶貴見解和連結。Amazon Comprehend 可以偵測和編輯結構化、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 文件中的個人識別資訊 (PII)。

您可以使用 AWS 開發套件和 Amazon Comprehend API，將 Amazon Comprehend 與許多應用程式整合。一個例子是使用 Amazon Comprehend，使用 Amazon S3 對象 Lambda 來偵測和編輯個人資料。Organizations 可以使用 S3 物件 Lambda 將自訂程式碼新增至 Amazon S3 GET 請求，以便在資料傳回至應用程式時修改和處理資料。S3 Object Lambda 可以篩選列、動態調整影像大小、編輯個人資料等。程式碼由 AWS Lambda 功能提供支援，在完全受管理的基礎架構上執行 AWS，無需建立

和儲存資料衍生副本，或執行 Proxy。您不需要變更應用程式即可使用 S3 物件 Lambda 轉換物件。您可以使用中的 `ComprehendPiiRedactionS3Object` Lambda 函數 AWS Serverless Application Repository 來編輯個人資料。此函數使用 Amazon Comprehend 偵測個人資料實體，並以星號取代這些實體來編輯這些實體。如需詳細資訊，請參閱 Amazon S3 文件中的使用 S3 物件 Lambda 和 Amazon Comprehend 偵測和編輯 P II 資料。

由於 Amazon Comprehend 提供許多透過 AWS 開發套件整合應用程式的選項，因此您可以使用 Amazon Comprehend 在收集、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，偵測和編輯應用程式日誌 (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針對 Amazon EC2 上的應用程式日誌執行此功能。Amazon Comprehend 提供兩種密文模式：

- `REPLACE_WITH_PII_ENTITY_TYPE`以其類型取代每個 PII 實體。例如，李俊將被取代為名稱。
- `MASK`以您選擇的字元取代 PII 實體中的字元 (! 、#、$、%、& 、或 @)。例如，朵珍可以用 **** *** 代替。

## Amazon 數據 Firehose

Amazon 資料 Firehose 可用於擷取、轉換串流資料，並將其載入下游服務，例如 Amazon Apache Flink 或 Amazon S3 受管服務。Firehose 通常用於傳輸大量串流資料，例如應用程式記錄檔，而不必從頭開始建置處理管線。

您可以使用 Lambda 函數在下游傳送資料之前執行自訂或內建的處理。為了保護隱私，此功能支持數據最小化和跨境數據傳輸要求。例如，您可以使用 Lambda 和 Firehose 來轉換多區域日誌資料，然後再將其集中到日誌存檔帳戶中。如需詳細資訊，請參閱 Biogen：多帳戶集中式記錄解決方案 (YouTube 影片)。在 PD 應用程式帳戶中，您可以設定 Amazon CloudWatch 並 AWS CloudTrail 將日誌推送到 Firehose 交付串流。Lambda 函數會轉換日誌，並將其傳送到日誌存檔帳戶中的中央 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。這有助於防止個人數據在其中傳輸 AWS 區域。通過使用這種方法，個人數據在傳輸和集中管理之前被屏蔽，而不是之後。對於不受跨境傳輸要求限制的司法管轄區中的應用程式，透過中的組織追蹤彙總記錄檔通常會更有效率且符合成本效益。 CloudTrail如需詳細資訊，請參閱AWS CloudTrail本指南的安全性 OU — 資訊安全工具帳戶一節。

## AWS Glue

維護包含個人資料的資料集是設計隱私權的關鍵要素。組織的資料可能以結構化、半結構化或非結構化表單存在。沒有結構的個人資料集可能會使得執行許多增強隱私權的操作變得困難，包括資料最小化、

追蹤作為資料主體請求一部分歸因於單一資料主體的資料，以確保一致的資料品質，以及資料集的整體細分。 AWS Glue是完全受管的擷取、轉換和載入 (ETL) 服務。它可以協助您在資料存放區和資料串流之間對資料進行分類、清理、充實和移動資料。 AWS Glue 功能旨在協助您探索、準備、建構和結合用於分析、機器學習和應用程式開發的資料集。您可以使 AWS Glue 用在現有資料集之上建立可預測且通用的結構。 AWS Glue Data Catalog AWS Glue DataBrew、和「 AWS Glue 資料品質」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協助您建立可維護的資料集。資料目錄包含資料的參考，這些資料在 AWS Glue中用作擷取、轉換和載入 (ETL) 工作的來源和目標。「資料目錄」中的資訊會儲存為中繼資料表，且每個表格指定單一資料存放區。您可以執行 AWS Glue 爬行者程式來取得各種資料存放區類型中的資料清查。您可以將內建和自訂分類器新增至爬行者程式，這些分類器會推斷個人資料的資料格式和結構描述。然後爬行者程式會將中繼資料寫入「資料目錄」。集中式中繼資料表可讓您更輕鬆地回應資料主體要求 (例如清除權)，因為它可以增加環境中不同個人資料來源的結構和可預測性。 AWS 如需如何使用資料型錄自動回應這些請求的完整範例，請參閱使用 Amazon S3 尋找並忘記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、列和儲存格的精細存取，則「資料目錄」是一個關鍵元件。Data Catalog 提供跨帳戶資料共用功能，並協助您使用以標籤為基礎的存取控制來大規模管理資料湖 (AWS 部落格文章)。

AWS Glue DataBrew

AWS Glue DataBrew協助您清理和標準化資料，並且可以對資料執行轉換，例如移除或遮罩個人識別資訊，以及加密資料管線中的敏感資料欄位。您也可以直觀地對應資料的歷程，以瞭解資料經歷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跟踪個人數據來源，此功能變得越來越重要。DataBrew 幫助您在數據準備過程中掩蓋個人數據。您可以將個人資料偵測為資料剖析工作的一部分，並收集統計資料，例如可能包含個人資料和潛在類別的欄數。然後，您可以使用內建的可逆或不可逆轉的資料轉換技術，包括替代、雜湊、加密和解密，所有這些都不需要撰寫任何程式碼。然後，您可以在下游使用已清理和遮罩的資料集來進行分析、報告和機器學習工作。中可用的一些資料遮罩技術 DataBrew 包括：

- 雜湊 — 將雜湊函數套用至資料行值。
- 替代 — 以其他具有真實外觀的值取代個人資料。
- 清空或刪除 — 以空值取代特定欄位，或刪除該欄。
- 遮罩掉 — 使用字元加擾，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行值。確定性加密永遠會為值產生相同的密文。
- 概率加密 — 將概率加密演算法套用至資料行值。概率加密會在每次套用時產生不同的密文。

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

AWS Glue 資料品質

AWS Glue 資料品質可協助您在資料管道交付高品質資料之前，主動將高品質資料交付給資料消費者。 AWS Glue 資料品質可針對整個資料管道的資料品質問題提供統計分析，可在 Amazon 觸發警示 EventBridge，並提出修復的品質規則建議。 AWS Glue 資料品質也支援使用領域特定語言建立規則，以便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加密金鑰，以協助保護您的資料。AWS KMS 使用硬體安全模組在 FIPS 140-2 密碼編譯模組驗證程式 AWS KMS keys 下進行保護和驗證。如需有關如何在安全性內容中使用此服務的詳細資訊，請參閱AWS 安全性參考架構。

AWS KMS 與大多數提供加密 AWS 服務 的項目整合，您可以在處理和儲存個人資料的應用程式中使用 KMS 金鑰。您可以用 AWS KMS 來協助支援各種隱私權要求，並保護個人資料，包括：

- 使用客戶管理的金鑰可以更好地控制強度、輪換、到期日和其他選項。
- 使用專屬的客戶管理金鑰來保護允許存取個人資料的個人資料和機密。
- 定義資料分類層級，並在每個層級指定至少一個專用的客戶管理金鑰。例如，您可能擁有一個密鑰來加密操作數據，另一個用於加密個人數據的密鑰。
- 防止意外的跨帳戶存取 KMS 金鑰。
- 將 KMS 金鑰儲存在與 AWS 帳戶 要加密的資源相同。
- 針對 KMS 金鑰管理和使用實作職責分離。如需詳細資訊，請參閱如何使用 KMS 和 IAM 對 S3 中的加密資料啟用獨立安全控制 (AWS 部落格文章)。
- 透過預防性和反應式護欄執行自動按鍵旋轉。

根據預設，KMS 金鑰會儲存，並且只能在建立 KMS 金鑰的區域中使用。如果您的組織對資料存放和主權有特定需求，請考慮多區域 KMS 金鑰是否適合您的使用案例。多區域金鑰是不同的特殊用途 KMS 金鑰 AWS 區域 ，可互換使用。建立多區域金鑰的程序會將您的關鍵材料跨越 AWS 區域 界限移動 AWS KMS，因此缺乏區域隔離可能與您組織的合規目標不相容。解決此問題的一種方法是使用不同類型的 KMS 金鑰，例如特定區域的客戶管理金鑰。

## AWS Local Zones

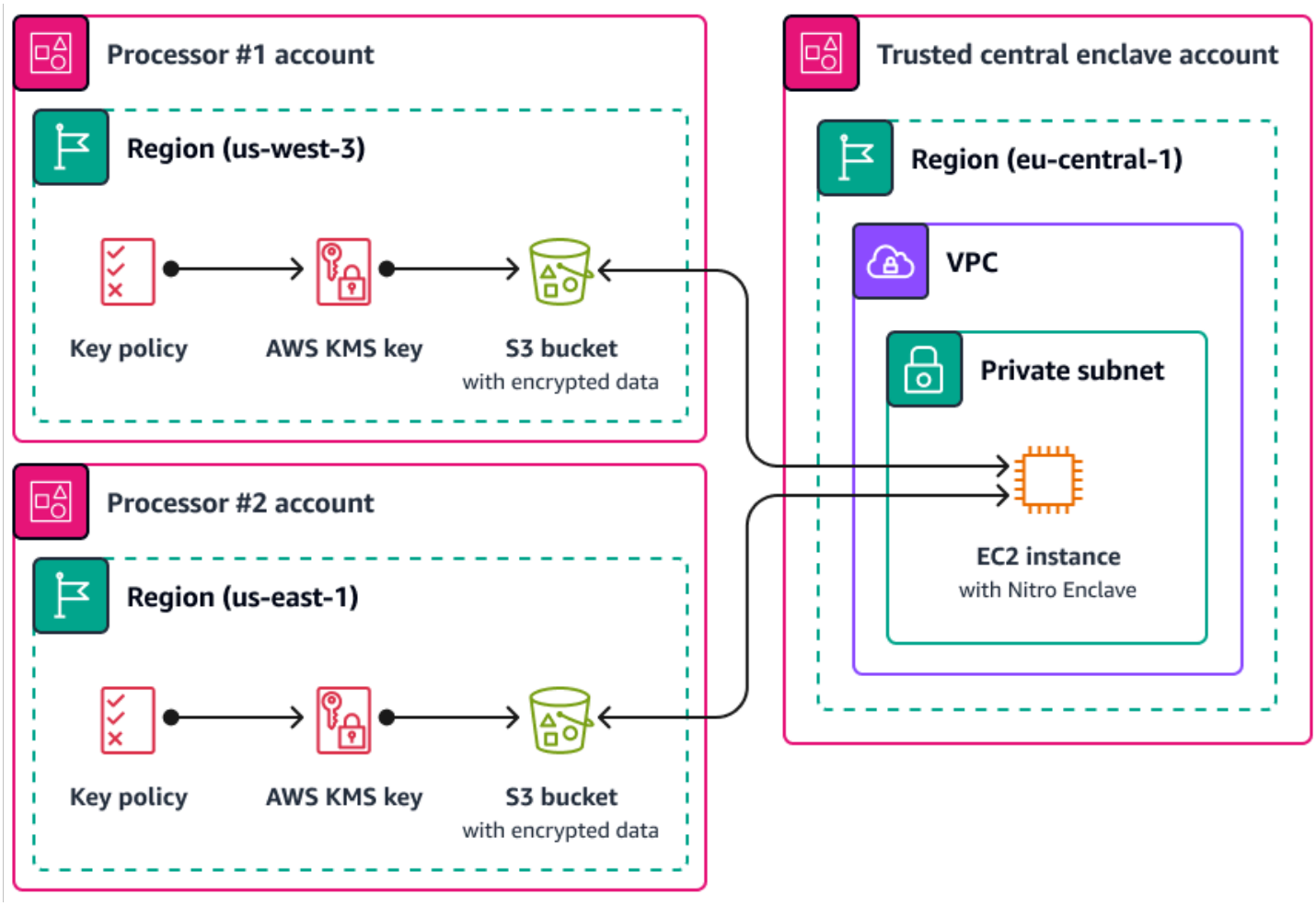
如果您需要遵守資料存放區要求，您可以部署儲存和處理個人資料的特定資源， AWS 區域 以支援這些需求。您也可以使用 L AWS ocal Zones，協助您將運算、儲存、資料庫和其他特定 AWS 資源放置在靠近大型人口和產業中心的地方。本地區域是地理位置靠近大都會區域的延伸。 AWS 區域 您可以將特定類型的資源放置在本地區域內，靠近本地區域對應的區域。當某個區域在相同法律管轄區內無法使用時，Local Zones 可協助您滿足資料落地需求。使用 Local Zones 時，請考慮組織內部署的資料存放控制項。例如，您可能需要控制項來防止從特定本地區域傳輸資料到另一個區域。如需有關如何使用 SCP 維護跨境資料傳輸護欄的詳細資訊，請參閱使用 landing zone 控制管理 L AWS ocal Zones 中資料駐留的最佳做法 (AWS 部落格文章)。

## AWS 硝基飛地

從處理角度考慮您的資料細分策略，例如使用 Amazon 彈性運算雲端 (Amazon EC2) 等運算服務處理個人資料。機密運算是更大型架構策略的一部分，可協助您將個人資料處理隔離在隔離、受保護且受信任的 CPU 隔離區中。Enclave 是獨立、強化且受到高度限制的虛擬機器。AWS 硝基隔離區是 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 系統的安全性設計 (AWS 白皮書)。

Nitro Enclaves 部署了一個與父實例的內核分開的內核。父執行個體的核心無法存取 Enclave。使用者無法透過 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隔離區中，並設定為使用 Enclave 的 Vsock，也就是可促進隔離區域與上層執行個體之間通訊的通訊端。

Nitro Enclaves 可能很有用的一個用例是在兩個單獨 AWS 區域 的數據處理器之間進行聯合處理，這些數據處理器可能不相互信任。下圖顯示如何使用 Enclave 進行中央處理、KMS 金鑰在傳送至 Enclave 之前加密個人資料，以及驗證 Enclave 請求解密區是否具有唯一度量值的 AWS KMS key 原則。如需詳細資訊和指示，請參閱搭配使用密碼編譯驗證。 AWS KMS如需金鑰原則範例，請參閱本指南需要驗證才能使用金鑰 AWS KMS中的。




透過此實作，只有相應的資料處理者和基礎 enclave 才能存取純文字個人資料。唯一會公開資料的位置，位於個別資料處理器的環境之外，位於 Enclave 本身，其設計目的是防止存取和竄改。

## AWS PrivateLink

許多組織希望限制個人數據暴露在不受信任的網絡中。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度來區隔網路 (類似於本協助區段資料的 AWS 服務和功能節中討論的資料集的邏輯和實體區隔)。 AWS PrivateLink協助您建立從虛擬私有雲端 (VPC) 到 VPC 外部服務的單向私有連線。使用時 AWS PrivateLink，您可以設定專用的私人連線，以便在您的環境中儲存或處理個人資料的服務；不需要連線到公用端點，也不需要透過不受信任的公用網路傳輸此資料。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、公用 IP 位址、 AWS Direct Connect 連線或 AWS Site-to-Site VPN 連線即可進行通訊。當您使用連線 AWS PrivateLink 至可存取個人資料的服務時，您可以根據組織的資料周邊定義，使用 VPC 端點原則和安全群組來控制存取。如需僅允許受信任組織中的 IAM 原則和 AWS 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。當您規劃多帳戶區隔策略時，請考慮使 AWS RAM 用分享儲存在個別獨立帳戶中的個人資料儲存區。您可以與其他受信任的帳戶共享該個人數據，以進行處理。在中 AWS RAM，您可以管理定義可對共用資源執行哪些動作的權限。所有的 API 呼叫 AWS RAM 都會登入 CloudTrail。此外，您可以設定 Amazon E CloudWatch vents 以自動通知您中的特定事件 AWS RAM，例如資源共用變更時。

雖然您可以使用 IAM 中的 AWS 資源型政策或 Amazon S3 中 AWS 帳戶 的儲存貯體政策與其他人共用許多類型的資源，但為隱私權 AWS RAM 提供了一些額外的好處。 AWS 為資料擁有者提供更多資料在您共用資料的方式以及與誰共用資料的可見性 AWS 帳戶，包括：

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

如果您之前已使用以資源為基礎的政策來管理資源共用， AWS RAM 而且想要改用，請使用 PromoteResourceShareCreatedFromPolicyAPI 作業。

## Amazon SageMaker

Amazon SageMaker 是一種受管機器學習 (ML) 服務，可協助您建立和訓練機器學習模型，然後將其部署到生產就緒的託管環境中。 SageMaker 旨在更輕鬆地準備訓練資料和建立模型特徵。

### Amazon SageMaker 模型監控

許多組織在訓練 ML 模型時會考慮資料漂移。資料漂移是生產資料與用來訓練 ML 模型的資料之間有意義的變化，或輸入資料隨著時間的推移有意義的變化。資料漂移可降低機器學習模型預測中的整體品質、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所依據的基準資料的性質，則預測的準確性可能會下降。Amazon SageMaker 模型監控器可以持續監控生產過程中 Amazon SageMaker 機器學習模型的品質，並監控資料品質。及早且主動地偵測資料漂移可協助您實作修正措施，例如再訓練模型、稽核上游系統或修正資料品質問題。模型監視器可減輕手動監控模型或建立其他工具的需求。

### Amazon SageMaker 澄清

Amazon SageMaker 澄清提供了有關模型偏見和解釋性的洞察力。 SageMaker在 ML 模型資料準備和整體開發階段通常使用澄清。開發人員可以指定感興趣的屬性，例如性別或年齡，並 SageMaker 且

Carrier 運行一組算法來檢測這些屬性中存在的任何偏見。演算法執行之後， SageMaker Cleven 會提供視覺化報告，其中包含來源和可能偏差測量值的說明，以便您識別修正偏差的步驟。例如，在一個財務資料集中，只包含一個年齡組別與其他年齡組別相比的幾個商業貸款範例， SageMaker 可以標記不平衡情況，以便避免使該年齡組別不適合的模型。您也可以檢閱其預測並持續監控這些 ML 模型是否存在偏差，以檢查已訓練過的模型是否存在偏差。最後， SageMaker澄清與 Amazon SageMaker 實驗集成，以提供一個圖表，該圖表說明哪些功能對模型的整體預測製作過程最有貢獻。這項資訊對於達到無法解釋的結果很有用，而且可協助您判斷特定模型輸入的影響力是否超過對整體模型行為的影響。

Amazon SageMaker 模型卡

Amazon SageMaker 模型卡可協助您記錄機器學習模型的重要詳細資料，以供管理和報告之用。這些詳細資料可以包括模型擁有者、一般用途、預期使用案例、做出的假設、模型的風險評等、訓練詳細資料和量度，以及評估結果。如需詳細資訊，請參閱使用 AWS 人工智慧和 Machine Learning 解決方案的模型說明功能 (AWS 白皮書)。

## AWS 協助管理資料生命週期的功能

當不再需要個人資料時，您可以對許多不同資料倉庫中的資料使用生命週期和 time-to-live政策。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 庫和 Amazon Relational Database Service 服務 (Amazon RDS)
- Amazon S3 儲存貯體
- 記錄來源 CloudWatch 和 CloudTrail
- 來自 AWS Database Migration Service (AWS DMS) 和 AWS Glue DataBrew 專案中移轉的快取資料
- 備份和快照

下列功能 AWS 服務 和功能可協助您設定 AWS 環境中的資料保留原則：

- Amazon S3 生命週期 — 一組規則，用於定義 Amazon S3 套用至一組物件的動作。在 Amazon S3 生命週期組態中，您可以建立到期動作，以定義 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，建立一個政策，自動建立、保留和刪除 Amazon Elastic Block Store (Amazon EBS) 快照和 EBS 支援的 Amazon 機器映像 (AMI)。
- DynamoDB 存留時間 (TTL) — 定義每個項目的時間戳記，以決定不再需要項目的時間戳記。在指定時間戳記的日期和時間之後不久，DynamoDB 會從表格中刪除該項目。
- CloudWatch 防護記錄中的防護記錄保留設定 — 您可以將每個記錄群組的保留原則調整為 1 天到 10 年之間的值。

- AWS Backup— 集中部署資料保護政策，以便跨多種 AWS 資源 (包括 S3 儲存貯體、RDS 資料庫執行個體、DynamoDB 表格、EBS 磁碟區等) 設定、管理和控管備份活動。透過指定 AWS 資源類型或根據現有資源標籤套用來提供其他細微性，將備份政策套用至您的資源。透過集中式主控台稽核和報告備份活動，以協助符合備份合規性需求。

## 協助區段資料的 AWS 服務和功能

資料區段是您將資料儲存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驗證措施，並減少曝光對整體資料集的影響範圍。例如，您可以將這些數據細分為更小，更易於管理的組，而不是將所有客戶數據存儲在一個大型數據庫中。

您可以使用實體和邏輯分隔來區隔個人資料：

- 物理分離 — 將數據存儲在單獨的數據存儲中或將數據分配到單獨的 AWS 資源中的行為。雖然資料實際上是分開的，但是相同的主體可以存取這兩個資源。這就是為什麼我們建議將物理分離與邏輯分離結合起來。
- 邏輯分離 — 使用存取控制來隔離資料的行為。不同的工作職能需要不同級別的個人資料子集的存取權限。如需實作邏輯分隔的範例原則，請參閱本指南授與特定 Amazon DynamoDB 屬性的存取權中的〈〉。

邏輯與實體分隔的組合可在撰寫以身分識別為基礎的政策和資源型政策時，提供彈性、簡易性和細微性，以支援跨工作職能的差異化存取。例如，建立在單一 S3 儲存貯體中以邏輯方式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。

# 隱私權相關政策範例

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

許多處理敏感資料的組織都採用預防性前瞻性的方法，並在整個過程中實施了多層偵探和反應式控制。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這些政策可透過使用預防性方法，協助您的組織達成各種使用、揭露限制和跨境資料傳輸隱私權目標。本指南前面的章節中有許多參考了這些策略。

本節包含下列範例原則：

- 需要從特定 IP 位址存取
- 需要組織成員資格才能存取 VPC 資源
- 限制跨越資料傳輸 AWS 區域
- 授與特定 Amazon DynamoDB 屬性的存取權
- 限制對 VPC 組態的變更
- 需要驗證才能使用金鑰 AWS KMS

## 需要從特定 IP 位址存取

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

只有在呼叫來自範圍`192.0.2.0/24`或範圍內的 IP 位址時，此政策才允許`john_stiles`使用者擔任 IAM 角色`203.0.113.0/24`。本政策有助於防止意外披露個人資料及不必要的跨境資料傳輸。例如，如果您的組織有需要存取個人資料的客戶支援人員，您可能希望該支援人員只能從位於特定子集中的辦公室存取該資料 AWS 區域。

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

```
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::account-id: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

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

此 VPC 私人雲端點政策僅允許 AWS Identity and Access Management (IAM) 來自o-1abcde123組織的主體和資源存取 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。如需有關本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"
                }
            }
        }
    ]
}
```

# 限制跨越資料傳輸 AWS 區域

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

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eu-central-1以 AWS 區域 外的區域 AWS 服務進行 API 呼叫。此 SCP 可協助防止在未核准的 AWS 區域中建立儲存和處理服務。這有助 AWS 服務 於防止在這些地區完全處理個人資料。此政策使用NotAction參數，因為它涵蓋了全球 AWS 服務 (例如 IAM)，以及與全球服務 (例如 AWS Key Management Service (AWS KMS) 和 Amazon 整合的服務 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。如需有關本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:*",
                "chime:*",
                "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"
                    ]
                }
            }
        }
    ]
}
```

# 授與特定 Amazon DynamoDB 屬性的存取權

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

當您的組織討論實體和邏輯區分個人資料的策略時，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。下列以身分識別為基礎的政策只允許從名為的 UserID Amazon DynamoDB 表格擷取SignUpTime、和LastLoggedIn屬性。Users例如，您可以將此政策附加到客戶支援角色，而不是授予此角色存取完整個人資料集的權限。如需有關本政策如何協助保護組織中隱私權和個人資料的詳細資訊，請參閱本指南協助區段資料的 AWS 服務和功能中的。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan",
            "dynamodb:TransactGetItems"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
```

```
            },
            "StringEquals":{
               "dynanamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

# 限制對 VPC 組態的變更

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

在您設計並部署支援跨境資料傳輸需求的 AWS 基礎結構 (包括網路資料流程) 之後，您可能會想要防止修改。下列服務控制原則有助於防止 VPC 組態偏移或意外修改。它會拒絕新的網際網路閘道附件、VPC 對等連線、傳輸閘道附件和新的 VPN 連線。如需有關本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:AttachEgressOnlyInternetGateway",
                "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"
                    ]
                }
            }
        }
    ]
}
```

# 需要驗證才能使用金鑰 AWS KMS

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

下列 AWS Key Management Service (AWS KMS) 金鑰原則只允許 AWS Nitro Enclave 執行個體使用 KMS 金鑰，只有在要求中的 Enclave 驗證文件符合條件陳述式中的度量值時，才能使用 KMS 金鑰。此原則只允許受信任的保護區解密資料。如需有關本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 硝基飛地中的。如需可在金鑰政策和 AWS Identity and Access Management (IAM) 政策中使用的 AWS KMS 條件金鑰的完整清單，請參閱 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
               }
            }
         }
      ]
}
```

# 資源

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

## AWS 規定指引

- AWS 安全參考架構 (AWS SRA)

## AWS 文件

- 資料保護 (AWS Well-Architected 的架構)
- 資料分類 (AWS 白皮書)
- Amazon Web Services：風險與合規 (AWS 白皮書)
- 滿足個人資料處理需求的混合式架構 (AWS 白皮書)
- 瞭解 GDPR 合規性 AWS (AWS 白皮書)
- 建立資料周邊 AWS (AWS 白皮書)
- AWS 安全性文件

## 其他 AWS 資源

- AWS 合規計劃
- AWS 共同責任模式
- 資料隱私問答集
- AWS 安全保證服務
- AWS 數位主權承諾：毫不妥協的控制 (AWS 部落格文章)
- AWS 安全學習

# 貢獻者

我們希望收到您的來信。請通過進行簡短的調查來提供有關 AWS PRA 的反饋。

本指南由 AWS 安全保證服務團隊撰寫。如需支援實作本指南中的建議並操作您的工作負載，請聯絡AWS 安全保證服務團隊。

主要作者

- 丹尼爾·尼特斯，首 AWS 席隱私顧問
- 琥珀·韋爾奇, AWS 高級隱私顧問
- 羅伯特·卡特， AWS 技術計劃經理

貢獻者

- 艾維克穆克吉，高級安全顧問 AWS
- 大衛邊界， AWS 高級解決方案架構
- 傑夫·隆巴多， AWS 高級安全解決方案架構師
- 拉姆拉瑪尼， AWS 首席安全解決方案架構師
- 凡妮莎·雅各布斯, AWS 高級安全顧問

# 文件歷史紀錄

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

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 信號更新 | 我們在整個過程中做了重大更 | 2024年3月26日 |
| 初次出版 | — | 2023 年 10 月 2 日 |

# AWS 規範指引詞彙表

以下是 AWS Prescriptive Guidance 所提供策略、指南和模式的常用術語。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：將內部部署 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：將您的內部部署 Oracle 資料庫遷移至 中的 Oracle 的 Amazon Relational Database Service (Amazon RDS) 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：將內部部署 Oracle 資料庫遷移至 中的 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至相同平台的雲端服務。範例：遷移 Microsoft Hyper-V 應用程式 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、一致性、隔離、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，但需要比主動被動遷移更多的工作。

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，但只有來源資料庫處理來自連接應用程式的交易，同時將資料複寫至目標資料庫。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

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

反模式

經常用於重複性問題的解決方案，其解決方案具有反效益、無效或效果不如替代方案。

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侵害。

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。如需如何在遷移策略中使用 AWS 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、一致性、隔離、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 (ABAC) 文件中的 Word for AWS。IAM

權威性資料來源

您存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將資料從權威資料來源複製到其他位置，以處理或修改資料，例如匿名化、修訂或擬匿名化資料。

可用區域

中與其他可用區域中的故障 AWS 區域 隔離的不同位置，並對相同區域中的其他可用區域提供便宜的低延遲網路連線。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地遷移至雲端。AWS CAF 將指引整理成六個重點領域：業務、人員、治理、平台、安全和操作。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 提供人員開發、訓練和通訊的指引，協助組織準備好成功採用雲端。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估算的工具。 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。您可以搭配 Amazon Detective 使用行為圖表來檢查失敗的登入嘗試、可疑的 API 呼叫和類似的動作。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。另請參閱端點。

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。此策略可協助您在影響最小的情況下快速復原。

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。有些機器人很有用或有益，例如在網際網路上為資訊編製索引的 Web 爬蟲程式。某些其他機器人，稱為不良機器人，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由單一方控制的機器人網路，稱為機器人繼承者或機器人運算子。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，使用者取得其通常無權存取 AWS 帳戶 之 存取權的快速方法。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作碎片程序指標。

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

版本向最終使用者緩慢且增量的版本。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。您可以使用 CDC 進行各種用途，例如稽核或複寫目標系統中的變更，以維持同步。

混亂工程

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，以強調 AWS 工作負載並評估其回應。

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。

Cloud Center of Excellence (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營運模型。

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您的雲端採用 （例如，建立登陸區域、定義 CCoE、建立操作模型）
- 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

這些階段由 Stephen Orban 在部落格文章 The Journey Toward Cloud-First 和企業策略部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱遷移準備指南。

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。 每個版本的程式碼都稱為分支。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

很少存取且通常為歷史資料的資料。查詢此類資料時，通常可接受慢查詢。將此資料移至效能較低且價格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映像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如， AWS Panorama 提供將 CV 新增至內部部署攝影機網路的裝置，而 Amazon SageMaker 則提供 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變得不合規，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。您通常會在遷移的產品組合探索和分析階段使用來自 CMDB 的資料。

一致性套件

您可以組合的 AWS Config 規則和修復動作集合，以自訂合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或跨組織的單一實體。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 is commonly described as a pipeline. CI/CD 可協助您自動化程序、提高生產力、改善程式碼品質，以及更快交付。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化。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

架構架構架構，提供分散式、分散式的資料擁有權，並具有集中式的管理和治理。

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，可協助確保只有受信任的身分才能從預期的網路存取受信任的資源。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。

資料庫操作語言 (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。

defense-in-depth

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，a defense-in-depth 方法可能會結合多重要素驗證、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，以管理組織的帳戶並管理該服務的許可。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。

部署

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)

用於識別和排定限制的流程，這些限制會對軟體開發生命週期中的速度和品質產生不利影響。DVSM 延伸了最初為精實生產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、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

在星狀結構描述中，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為文字欄位或像文字那樣行為的離散數字。這些屬性通常用於查詢限制、篩選和結果集標籤。

災難

阻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，例如意外錯誤組態或惡意軟體攻擊。

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 上的工作負載災難復原 AWS：雲端中的復原。

DML

請參閱資料庫操作語言。

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。如需有關如何搭配 strangler fig 模式使用網域驅動設計的資訊，請參閱使用容器和 Amazon ASMX Gateway 逐步現代化舊版 Microsoft ASP.NET (API) Web 服務。

DR

請參閱災難復原。

漂移偵測

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 來偵測可能會影響對治理要求合規性的登陸區域中的變更。 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縮短回應時間。

電子資料交換 (EDI)

組織之間的商業文件自動交換。如需詳細資訊，請參閱什麼是電子資料交換。

加密

將純文字資料轉換為人類可讀取的運算程序。

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) 主體。這些帳戶或主體可以透過建立介面 VPC 端點，私下連線至您的端點服務。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)

可自動化和管理企業關鍵業務流程 （例如會計、MES 和專案管理） 的系統。

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 安全特徵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。EDA 是透過計算摘要統計資料和建立資料視覺化來執行。

# 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：包含量值的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

使用頻繁且增量測試來縮短開發生命週期的哲學。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，邊界，例如可用區域 AWS 區域、控制平面或資料平面，這些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。這通常表示為數值分數，可透過各種技術計算，例如 Shapley 累加解釋 (SHAP) 和整合漸層。如需詳細資訊，請參閱使用 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。

幾下提示

在請求 LLM 執行類似任務之前，提供少量示範任務和所需輸出的範例。此技術是內文學習的應用，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式設定、推理或網域知識的任務，少量擷取提示非常有效。另請參閱零擷取提示。

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，以及以自然語言進行交談。如需詳細資訊，請參閱什麼是基礎模型。

# G

生成式 AI

經過大量資料訓練的 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)

在 Amazon CloudFront 中，此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 Word 文件中的限制內容的地理分佈。 CloudFront

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，而以中繼線為基礎的工作流程是現代的首選方法。

金色影像

系統或軟體的快照，用作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

高階規則，可協助管理跨組織單位 (OUs) 的資源、政策和合規性。預防性防護機制會強制執行政策，以確保符合合規標準。其實作方式是使用服務控制政策和 IAM 許可界限。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、Amazon GuardDuty、 AWS Trusted Advisor、Amazon Inspector 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)

工作負載在遇到挑戰或災難時持續運作的能力，無需介入。HA 系統設計為自動容錯移轉、持續提供高品質效能，以及處理不同的負載和故障，且對效能的影響最小。

歷史現代化

一種用於現代化和升級操作技術 (OT) 系統的方法，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠的不同來源收集和存放資料。

保留資料

從用來訓練機器學習模型的資料集中保留的歷程記錄、已標記資料的一部分。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。

常用資料

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，修正程式通常在典型的 DevOps 發行工作流程之外建立。

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

在 90 天內的平均 CPU 和記憶體用量介於 5% 到 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、修補或修改現有基礎設施。與可變基礎設施相比，不可避免的基礎設施本質上更一致、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 Security Reference Architecture 建議使用傳入、傳出和檢查 VPCs 設定您的網路帳戶，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

由 Klaus Schwab 於 2016 年推出的術語，指透過連線能力、即時資料、自動化、分析和 AI/ML 的進步來現代化製造程序。

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，請參閱建置工業物聯網 (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 Security Reference Architecture 建議使用傳入、傳出和檢查 VPCs 設定您的 Network 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 AWS 的機器學習模型可解譯性。

IoT

請參閱物聯網。

IT 資訊程式庫 (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 提供 ITSM 的基礎。

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。如需整合雲端操作與 ITSM 工具的相關資訊，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，其中每個使用者和資料本身都會明確指派安全標籤值。使用者安全標籤與資料安全標籤之間的交集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、彙整文件、將文字翻譯為其他語言，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 Rs。

小端序系統

首先儲存最低有效位元組的系統。另請參閱端點。

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、特洛伊木馬程式、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 可 AWS 操作基礎設施層、作業系統和平台，而且您可以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)

用於追蹤、監控、記錄和控制生產程序的軟體系統，可將原物料轉換為工廠的成品。

MAP

請參閱遷移加速計畫。

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。機制是在運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

除了屬於 組織的管理帳戶 AWS 帳戶 之外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

MES

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

小型的獨立服務，透過定義明確的 APIs 進行通訊，通常由小型、獨立的團隊擁有。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 APIs 透過定義明確的界面進行通訊。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。

遷移加速計畫 (MAP)

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遷移至雲端，並協助抵銷遷移的初始成本的 AWS 計畫。MAP 包含以系統化方式執行舊版遷移的遷移方法，以及一組可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操作、業務分析師和擁有者、遷移工程師、開發人員，以及從事衝刺工作的 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。

遷移產品組合評估 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的產品組合評估（伺服器大小調整、定價、TCO 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、遷移優先順序和波規劃）。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。

遷移就緒狀態評估 (MRA)

使用 AWS CAF 取得組織雲端就緒狀態的洞見、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

用於將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 7 個 Rs 項目，並請參閱將您的組織動員以加速大規模遷移。

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 中的應用程式現代化策略 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

請參閱開啟程序通訊 - Unified Architecture。

開放程序通訊 - Unified Architecture (OPC-UA)

工業自動化的 A machine-to-machine (M2M) 通訊協定。OPC-UA 提供與資料加密、身分驗證和授權方案的互通性標準。

操作層級協議 (OLA)

闡明哪些功能 IT 群組承諾相互交付的協議，以支援服務層級協議 (SLA)。

操作預備檢閱 (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 中的操作就緒審核 (ORR)。

操作技術 (OT)

與實體環境搭配使用的硬體和軟體系統，以控制工業操作、設備和基礎設施。在製造中，OT 和資訊技術 (IT) 系統的整合是 Industry 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 建立的追蹤 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有事件 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 文件中的為組織建立追蹤。

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 透過加速變革採用、解決轉型問題，以及推動文化和組織變革，協助組織準備和轉換至新系統和策略。在 AWS 遷移策略中，由於雲端採用專案所需的變更速度，因此此架構稱為人員加速。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

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

原始存取身分 (OAI)

In CloudFront，用於限制存取以保護您的 Amazon S3 內容的選項。當您使用 OAI 時， CloudFront 會建立 Amazon S3 可以驗證的主體。已驗證的主體只能透過特定 CloudFront 分佈存取 S3 儲存貯體中的內容。另請參閱 OAC，它提供更精細和增強的存取控制。

ORR

請參閱操作準備檢閱。

OT

請參閱操作技術。

傳出（傳出）VPC

在 AWS 多帳戶架構中，處理從應用程式內起始之網路連線的 VPC。AWS 安全參考架構建議設定具有傳入、傳出和檢查 VPCs 的網路帳戶，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

連接至 IAM 主體的 IAM 管理政策，用於設定使用者或角色可擁有的最大許可。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（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最大許可的物件 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。如需詳細資訊，請參閱在微服務中啟用資料持久性。

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。

設計隱私

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

容器，其中包含有關您希望 Amazon Route 53 如何回應一個或多個 DNS 內網域及其子網域的 VPCs 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，並參閱在 實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

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

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 提示的輸出作為下一個提示的輸入，以產生更好的回應。此技術用於將複雜的任務分解為子任務，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關聯性，並允許更精細的個人化結果。

擬匿名化

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

publish/subscribe (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以訂閱的頻道。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、知情 (RACI)。

RAG

請參閱擷取增強型生成。

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、知情 (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 Rs。

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)

服務中斷和服務還原之間的可接受延遲上限。

重構

請參閱 7 Rs。

區域

地理區域 AWS 的資源集合。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 Rs。

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 Rs。

轉譯形式

請參閱 7 Rs。

回購

請參閱 7 Rs。

彈性

應用程式抵抗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、負責、諮詢、知情 (RACI) 矩陣

定義所有涉及遷移活動和雲端操作各方的角色和責任的矩陣。矩陣名稱衍生自矩陣中定義的責任類型：責任 (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，如果您排除該矩陣，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 Rs。

淘汰

請參閱 7 Rs。

擷取增強產生 (RAG)

一種生成式 AI 技術，其中 LLM 在產生回應之前，會參考其訓練資料來源以外的權威資料來源。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，讓攻擊者更難存取憑證。

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 由資料列許可和資料欄遮罩組成。

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 (IdPs) 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 Management Console 或呼叫 AWS API 操作，而不必在 IAM 中為組織中的每個人建立使用者。如需 SAML 2.0 型聯合的詳細資訊，請參閱 SAML 文件中的關於 Word 2.0 型聯合。 IAM

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，例如密碼或使用者憑證。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 秘密中的內容？。

設計安全性

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。

安全資訊和事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具和服務。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，並產生警示。

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 執行個體或輪換憑證。

伺服器端加密

由接收資料的 AWS 服務 加密其目的地的資料。

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。SCPs 會定義管理員可委派給使用者或角色之動作的防護機制或設定限制。您可以使用 SCPs 作為允許清單或拒絕清單，以指定允許或禁止的服務或動作。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。

服務層級協議 (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)

目標指標，代表服務的運作狀態，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，而您要負責雲端的安全。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。

單一失敗點 (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

請參閱服務層級指示器。

SLO

請參閱服務層級目標。

split-and-seed 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

請參閱單一失敗點。

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。此結構專為資料倉儲或商業智慧用途而設計。

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 ASMX.NET (API) Web 服務。

子網

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

提供內容、指示或指引給 LLM 以指示其行為的技術。系統提示可協助設定內容，並建立與使用者互動的規則。

# T

標籤

作為中繼資料的鍵值對，用於組織您的 AWS 資源。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

可用來互連 VPCs 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，以代表您在組織中在其帳戶中 AWS Organizations 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 AWS Organizations 搭配使用其他 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

一個小型 DevOps 團隊，您可以使用兩個披薩來餵送。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

也稱為繁重型，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。未區分的任務範例包括採購、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

兩個 VPCs 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 Word 對等。 VPC

漏洞

損害系統安全性的軟體或硬體缺陷。

# 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，通常可接受中等慢的查詢。

視窗函數

SQL 函數，對以某種方式與目前記錄相關聯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，讀取許多。

WQF

請參閱 AWS Workload Qualification Framework。

寫入一次，讀取許多 (WORM)

一次性寫入資料的儲存模型，可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

零時差漏洞

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。威脅實施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。

零擷取提示

為 LLM 提供執行任務的指示，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。零擷取提示的有效性取決於任務的複雜性和提示的品質。另請參閱微拍提示。

殭屍應用程式

平均 CPU 和記憶體用量低於 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。