在 上達到基本八項成熟度 AWS

AWS 方案指引

AWS 方案指引: 在 上達到基本八項成熟度 AWS

Table of Contents

簡介 1
澳洲安全與合規 2
資訊安全註冊評估者計劃 2
託管憑證架構 2
AWS 共同責任模型 2
AWS Well-Architected 架構 3
重新解釋 Essential Eight 策略 4
使用佈景主題 4
重新解譯雲端的基本八項策略 5
您使用哪些 服務？ 5
您使用哪種部署模型？ 5
主題 1：受管服務 7
相關的最佳實務 8
實作此主題 8
啟用修補 8
掃描漏洞 8
監控此佈景主題 8
實作控管檢查 8
監控 Amazon Inspector 8
實作下列 AWS Config 規則 8
佈景主題 2：不可變基礎設施 10
相關的最佳實務 10
實作此主題 11
實作 AMI 和容器建置管道 11
實作安全的應用程式建置管道 11
實作漏洞掃描 12
監控此佈景主題 12
持續監控 IAM 和日誌 12
實作下列 AWS Config 規則 12
佈景主題 3：互斥基礎設施 13
相關的最佳實務 13
實作此主題 13
自動化修補 13
使用自動化而非手動程序 14

使用自動化在 EC2 執行個體上安裝下列項目 14
在任何版本之前使用對等審核，以確保變更符合最佳實務 14
使用身分層級控制項 14
實作漏洞掃描 14
監控此佈景主題 15
持續監控修補程式合規 15
持續監控 IAM 和日誌 15
實作下列 AWS Config 規則 15
佈景主題 4：身分 16
相關的最佳實務 16
實作此主題 17
實作聯合身分 17
套用最低權限許可 17
輪換登入資料 17
強制執行 MFA 18
監控此佈景主題 18
監控最低權限存取 18
實作下列 AWS Config 規則 18
佈景主題 5：資料周邊 19
相關的最佳實務 19
實作此主題 19
實作身分控制 19
實作資源控制 20
實作網路控制 20
監控此佈景主題 20
監控政策 20
實作下列 AWS Config 規則 20
主題 6：備份 21
AWS Well-Architected Framework 中的相關最佳實務 21
實作此主題 22
自動化資料備份和復原 22
相關的最佳實務 22
監控此佈景主題 22
實作下列 AWS Config 規則 22
佈景主題 7：記錄和監控 24
相關的最佳實務 24

實作此主題 24
啟用日誌記錄 24
實作記錄安全最佳實務 25
集中日誌 25
監控此佈景主題 25
實作機制 25
實作下列 AWS Config 規則 25
主題 8：手動程序的機制 27
相關的最佳實務 27
實作此主題 27
監控此佈景主題 28
案例研究 29
概觀 29
核心架構 29
無伺服器資料湖 30
容器化 Web 服務 31
COTS 軟體 33
資源 35
AWS 文件 35
其他 AWS 資源 35
澳洲網路安全中心資源 35
貢獻者 36
附錄：控制矩陣 37
應用程式控制 37
修補程式應用程式 41
設定Microsoft Office巨集設定 45
使用者應用程式強化 46
限制管理權限 48
修補程式作業系統 54
多重要素驗證 58
定期備份 60
注意 62
文件歷史紀錄 63
詞彙表 64
..... 64
A 64

B 67
C 68
D 71
E 74
F 76
G 77
H 78
I 79
L 81
M 82
O 86
P 88
Q 90
R 90
S 93
T 96
U 97
V 98
W 98
Z 99
..... c

在 上達到基本八項成熟度 AWS：澳洲組織的安全與合規

Amazon Web Services （貢獻者）

2024 年 11 月 (文件歷史記錄)

Australia Signals Directorate (ASD) 已建立並排定策略的優先順序，以協助組織降低網路安全威脅的風險。其中選擇了八個策略來形成 Essential Eight 架構。澳洲許多公有和私有部門組織都必須在 Essential Eight 架構下達到成熟度。

澳洲網路安全中心 (ACSC) 建立了 Essential Eight 架構，以協助保護以 Microsoft為基礎的網際網路連線網路。不過，許多組織需要達到其所有環境的必要八項成熟度，包括內部部署和雲端環境。

Essential Eight 架構也包含成熟度模型，旨在協助組織透過漸進式反覆運算實作架構。此模型概述成熟度層級零到三。成熟度層級 3 代表對進階網路安全策略和高度目標性攻擊的彈性。本指南提供具體的意見指引，協助您達到基本八項成熟度第三級 AWS。

澳洲組織的安全與合規

澳洲許多組織使用 AWS 雲端 來存放機密資料、處理敏感交易，以及建置關鍵服務。

雖然本指南討論如何調整雲端的 Essential Eight 架構，但 AWS 也提供下列認證和模型，協助您滿足組織的安全和合規要求：

- 資訊安全註冊評估者計劃
- 託管憑證架構
- AWS 共同責任模型
- AWS Well-Architected 架構

資訊安全註冊評估者計劃

AWS 服務 已在澳洲網路安全中心 (ACSC) 資訊安全註冊評估人員計劃 (IRAP) 的 PROTECTED 層級進行評估。獨立的澳洲訊號目錄 (ASD) 認證 IRAP 評估者已完成 的 IRAP 評估 AWS。此評估可確保針對 AWS 產品和服務，針對 PROTECTED 層級工作負載實作適用的控制項。

AWS IRAP PROTECTED 套件可透過 取得AWS Artifact。IRAP 報告是使用 ACSC 雲端安全指南 (ACSC 網站） 所開發。如需 AWS 服務 範圍內的完整清單，請參閱 AWS 服務 範圍內的 IRAP。

託管憑證架構

澳洲託管認證架構旨在支援政府系統和資料的安全管理。此架構旨在協助組織降低供應鏈和資料中心擁有權風險。 AWS 已授予認證策略層級的認證。這有助於政府機構繼續快速創新，因為 AWS 符合政府要求。

AWS 共同責任模型

AWS 共同責任模型會定義您與 共同 AWS 承擔雲端安全與合規責任的方式。 會 AWS 保護執行 中提供之所有服務的基礎設施 AWS 雲端，而且您需負責保護對這些服務的使用，例如您的資料和應用程式。

此共用模型有助於減輕您的合規和操作負擔，因為 會 AWS 操作、管理和控制許多元件，從主機作業系統和虛擬化層，到服務操作所在設施的實體安全性。您負責管理訪客作業系統 （包括更新和安全修補程式） 和其他相關聯的應用程式軟體。您也必須負責設定 AWS 提供的安全群組防火牆。

當您接近 Essential Eight 成熟度時，請務必了解 AWS 共同責任模型 AWS。您的責任會根據所使用的服務、這些服務與 IT 環境的整合，以及適用的法律和法規而有所不同。

AWS Well-Architected 架構

AWS Well-Architected 可協助雲端架構師為各種應用程式和工作負載建置安全、高效能、彈性且高效率的基礎設施。AWS Well-Architected Framework 提供架構最佳實務，協助您設計、建置和操作系統 AWS。此架構以六大支柱為基礎：卓越營運、安全性、可靠性、效能效率、成本最佳化和永續性。

AWS 也提供用於檢閱工作負載的服務。可協助您使用 AWS Well-Architected Framework 來AWS Well-Architected Tool檢閱和評估您的架構。它提供建議，讓您的工作負載更可靠、安全、有效率且符合成本效益。

重新解譯雲端的基本八項策略

以下是專為 Microsoft型網際網路連線網路設計的原始 Essential Eight 緩解策略：

- 應用程式控制
- 修補程式應用程式
- 設定Microsoft Office巨集設定
- 使用者應用程式強化
- 限制管理權限
- 修補程式作業系統
- 多重要素驗證
- 定期備份

請務必重申 Essential Eight 架構並非針對雲端環境而設計。不過，基礎原則適用，Essential Eight 策略和 AWS Well-Architected Framework 最佳實務之間存在重疊。

各種雲端原生方法可以改善安全性，並大幅降低您的合規負擔。在內部部署環境中，您必須負責所有層面的安全，而且沒有繼承的控制項。在雲端執行工作負載時， AWS 負責保護執行我們服務的基礎設施。您也可以使用自動化和受管服務來減輕合規負擔。受管服務也稱為抽象服務，其 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。如需詳細資訊，請參閱本指南中的主題 1：使用 受管服務一節。

因此，需要一些重新解譯才能使 Essential Eight 策略適用於其上的工作負載 AWS。本指南將 Essential Eight 策略轉換為 AWS 佈景主題。

使用佈景主題

本指南分為八個主題。每個 Essential Eight 策略對應至下列一或多個主題，而每個主題對應至 AWS Well-Architected Framework 中的一或多個最佳實務：

- 主題 1：使用 受管服務
- 主題 2：透過安全管道管理不可變的基礎設施
- 佈景主題 3：使用自動化管理可變基礎設施
- 佈景主題 4：管理身分

- 佈景主題 5：建立資料周邊
- 主題 6：自動化備份
- 佈景主題 7：集中記錄和監控
- 佈景主題 8：實作手動程序的機制

每個主題都包含主題的概觀、相關的 AWS Well-Architected Framework 最佳實務，以及如何實現 Essential Eight 成熟度並監控合規性的說明。這些指示提供手動步驟，或使用 AWS Config 規則協助您設定自動化。手動步驟需要機制來確保問題清單已解決。如需詳細資訊，請參閱 佈景主題 8：實作手動程序的機制. AWS Config rules 需要類似的監督或自動化，以修復不合規的資源。透過遵循與這些主題一致的指引，您可以使用同時將雲端優勢最大化的方法達到 Essential Eight 成熟度。

重新解譯雲端的基本八項策略

由於 Essential Eight 架構並非針對雲端環境而設計，因此在解決每個 Essential Eight 策略的基礎原則時，必須採取雲端原生方法。該方法取決於兩個關鍵問題。

您使用哪些 服務？

AWS 共同責任模型 有助於減輕您的合規和操作負擔。受管服務會將更多責任轉移到 ， AWS 以維護已部署服務的可用性、效能和安全性最佳化。受管服務也會消除維護服務的營運和管理負擔，提供更多時間專注於創新。

受管服務包括無伺服器服務，例如 Amazon API GatewayAWS Lambda、 和 DynamoDB。Amazon Relational Database Service (Amazon RDS) 上的資料庫比 Amazon Elastic Compute Cloud (Amazon EC2) 上的資料庫需要較少的操作責任。

例如，如果您要為雲端調整修補程式作業系統 Essential Eight 策略，您需要考慮正在使用哪些服務，以及是否負責修補這些資源。 AWS 負責修補完全受管的服務，例如 Lambda 和 DynamoDB。對於其他 服務，例如 Amazon RDS 或 Amazon Redshift，您可能需要在維護時段期間管理修補程式。

您使用哪種部署模型？

您的組織是否使用可變或不可變的基礎設施方法？

可變基礎設施模型會更新和修改生產工作負載的現有基礎設施。 這是雲端之前的標準部署方法，當取代伺服器基礎設施非常昂貴且耗時，最實際的方法就是將變更套用至已在生產環境中的伺服器。雲端中可變方法的範例是將應用程式變更直接部署到執行中的 EC2 執行個體，無論是手動或使用 Run AWS Systems Manager Command 或 等軟體部署服務AWS CodeDeploy。

不可變的基礎設施模型會為生產工作負載部署新的基礎設施，而不是更新、修補或修改現有的基礎設施。不可變方法的範例是在 AWS CloudFormation或 中定義應用程式堆疊AWS Cloud Development Kit (AWS CDK)。您可以使用這些服務，透過持續整合和持續交付 (CI/CD) 管道來部署應用程式堆疊。此方法使用部署方法，例如滾動或藍/綠。如需此方法的詳細資訊，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。

例如，如果您要針對雲端調整修補程式作業系統 Essential Eight 策略，您需要考慮修補如何套用至部署模型。對於可變基礎設施，您可以手動修補資源，也可以透過自動化提高營運效率。如果您使用的是不可變的基礎設施，則會使用 CI/CD 管道來部署具有最新版本作業系統的新基礎設施。事實上，修補一詞是此模型下的誤判，因為基礎設施將被取代而不是修補。

主題 1：使用 受管服務

涵蓋的基本八項策略

修補程式應用程式、限制管理權限、修補程式作業系統

受管服務可讓您 AWS 管理一些安全任務，例如修補和漏洞管理，以協助您減少合規義務。

如 AWS 共同責任模型章節所述，您對 AWS 雲端安全與合規負有共同責任。這可以減輕您的操作負擔，因為 會 AWS 操作、管理和控制元件，從主機作業系統和虛擬化層到服務操作所在設施的實體安全性。

您的責任可能包括管理受管服務的維護時段，例如 Amazon Relational Database Service (Amazon RDS) 或 Amazon Redshift，以及掃描 AWS Lambda 程式碼或容器映像中的漏洞。如同本指南中的所有主題，您也保留監控和合規報告的責任。您可以使用 Amazon Inspector 來報告所有 的漏洞 AWS 帳戶。您可以在 中使用規則， AWS Config 以確保 Amazon RDS 和 Amazon Redshift 等服務已啟用次要更新和維護時段。

例如，如果您執行 Amazon EC2 執行個體，您的責任包括下列項目：

- 應用程式控制
- 修補應用程式
- 限制 Amazon EC2 控制平面和作業系統 (OS) 的管理權限
- 修補作業系統
- 強制執行多重驗證 (MFA) 以存取 AWS 控制平面和作業系統
- 備份資料和組態

不過，如果您執行 Lambda 函數，則您的責任會降低，並包含下列項目：

- 應用程式控制
- 確認程式庫是up-to-date
- 限制 Lambda 控制平面的管理權限
- 強制 MFA 存取 AWS 控制平面
- 備份 Lambda 函數程式碼和組態

AWS Well-Architected Framework 中的相關最佳實務

- SEC01-BP05 減少安全管理範圍

實作此主題

啟用修補

- 套用 Amazon RDS 更新
- 在 中啟用受管更新 AWS Elastic Beanstalk
- 請注意 Amazon Redshift 叢集維護時段

掃描漏洞

- 使用 Amazon Inspector 掃描 Amazon Elastic Container Registry (Amazon ECR) 容器映像
- 使用 Amazon Inspector 掃描 Lambda 函數

監控此佈景主題

實作控管檢查

- 在 中啟用 ACSC Essential 8 一致性套件的操作最佳實務 AWS Config

監控 Amazon Inspector

- 評估帳戶層級涵蓋範圍
- 管理多個帳戶

實作下列 AWS Config 規則

- `RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED`
- `ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED`
- `REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK`

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EKS_CLUSTER_SUPPORTED_VERSION

主題 2：透過安全管道管理不可變的基礎設施

涵蓋的基本八項策略

應用程式控制、修補程式應用程式、修補程式作業系統

對於不可變的基礎設施，您必須保護部署管道以進行系統變更。 AWS 傑出工程師 Colm MacC árthaigh 在 2022re：Invent 會議的零權限操作：執行無法存取資料 (YouTube 影片） 簡報的服務中解釋了此原則。 AWS

透過限制設定 AWS 資源的直接存取，您可以要求透過已核准、安全且自動化的管道部署或變更所有資源。通常，您會建立 AWS Identity and Access Management (IAM) 政策，讓使用者只能存取託管部署管道的帳戶。您也可以設定 IAM 政策，以允許有限數量的使用者進行破解玻璃存取。若要防止手動變更，您可以使用安全群組來封鎖 SSH 和Windows遠端桌面通訊協定 (RDP) 對伺服器的存取。Session Manager 是 的一項功能 AWS Systems Manager，可以提供執行個體的存取權，而不需要開啟傳入連接埠或維護堡壘主機。

Amazon Machine Image AMIs) 和容器映像必須以安全且重複的方式建置。對於 Amazon EC2 執行個體，您可以使用 EC2 Image Builder 建置具有內建安全功能的 AMIs，例如執行個體探索、應用程式控制和記錄。如需應用程式控制的詳細資訊，請參閱 ACSC 網站上的實作應用程式控制。您也可以使用 Image Builder 建置容器映像，也可以使用 Amazon Elastic Container Registry (Amazon ECR) 跨帳戶共用這些映像。中央安全團隊可以核准自動化程序來建置這些 AMIs 和容器映像，以便任何產生的 AMI 或容器映像都由應用程式團隊核准使用。

應用程式必須使用 AWS CloudFormation或 等服務，在基礎設施中定義為程式碼 (IaC)AWS Cloud Development Kit (AWS CDK)。程式碼分析工具 AWS CloudFormation Guard，例如 cfn-nag 或 cdk-nag，可以根據已核准管道中的安全最佳實務自動測試程式碼。

如同 主題 1：使用 受管服務，Amazon Inspector 可以報告整個 的漏洞 AWS 帳戶。集中式雲端和安全團隊可以使用此資訊來驗證應用程式團隊是否符合安全和合規要求。

若要監控和報告合規性，請持續檢閱 IAM 資源和日誌。使用 AWS Config 規則來確保僅使用核准的 AMIs，並確保 Amazon Inspector 已設定為掃描 Amazon ECR 資源是否有漏洞。

AWS Well-Architected Framework 中的相關最佳實務

- OPS05-BP04 使用建置和部署管理系統

- REL08-BP04 使用不可變基礎設施進行部署
- SEC06-BP03 減少手動管理和互動式存取

實作此主題

實作 AMI 和容器建置管道

- 使用 EC2 Image Builder，並在您的 AMIs中建置下列項目：
  - AWS Systems Manager Agent (SSM Agent)，用於執行個體探索和管理
  - 應用程式控制的安全工具，例如 Security Enhanced Linux (SELinux) (GitHub)、File Access Policy Daemon (fapolicyd) (GitHub) 或 OpenSCAP
  - Amazon CloudWatch Agent，用於記錄
- 對於所有 EC2 執行個體，請在執行個體描述檔或 Systems Manager 用來存取執行個體的 IAM 角色中包含 `CloudWatchAgentServerPolicy`和 `AmazonSSMManagedInstanceCore`政策
- 與整個組織共用 AMIs
- 共用 EC2 Image Builder 資源
- 確定應用程式團隊正在參考最新的 AMIs
- 使用您的 AMI 管道進行修補程式管理
- 實作容器建置管道：
  - 使用 EC2 Image Builder 主控台精靈建立容器映像管道
  - 使用 Amazon ECR 做為來源，為您的容器映像建置持續交付管道 (AWS 部落格文章）
- 透過多帳戶和多區域架構在整個組織中共用 ECR 容器映像

實作安全的應用程式建置管道

- 實作 IaC 的建置管道，例如使用 EC2 Image Builder 和 AWS CodePipeline (AWS 部落格文章）
- 在 CI/CD 管道中使用程式碼分析工具，例如 AWS CloudFormation Guard、cfn-nag (GitHub) 或 cdk-nag (GitHub)，以協助偵測違反最佳實務的行為，例如：
  - IAM 政策過於寬鬆，例如使用萬用字元的政策
  - 過於寬鬆的安全群組規則，例如使用萬用字元或允許 SSH 存取的安全群組規則
  - 未啟用的存取日誌
  - 未啟用的加密

  - 密碼常值
- 在管道中實作掃描工具 (AWS 部落格文章）
- 在管道 AWS Identity and Access Management Access Analyzer 中使用 (AWS 部落格文章） 來驗證 CloudFormation 範本中定義的 IAM 政策
- 設定最低權限存取的 IAM 政策和服務控制政策，以使用管道或對其進行任何修改

實作漏洞掃描

- 在您組織的所有帳戶中啟用 Amazon Inspector
- 使用 Amazon Inspector 掃描 AMIs 建置管道中的 AMI：
  - 在 EC2 Image Builder (GitHub) 中管理 AMIs 的生命週期 GitHub
- 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描
- 建置漏洞管理計劃來分類和修復安全問題清單

監控此佈景主題

持續監控 IAM 和日誌

- 定期檢閱您的 IAM 政策，以確保：
  - 只有部署管道可以直接存取 資源
  - 只有核准的服務可以直接存取資料
  - 使用者無法直接存取資源或資料
- 監控 AWS CloudTrail 日誌，以確認使用者正在透過管道修改資源，且未直接修改資源或存取資料
- 定期檢閱 IAM Access Analyzer 調查結果
- 設定提醒，以便在 AWS 帳戶 使用 的根使用者登入資料時通知您

實作下列 AWS Config 規則

- `APPROVED_AMIS_BY_ID`
- `APPROVED_AMIS_BY_TAG`
- `ECR_PRIVATE_IMAGE_SCANNING_ENABLED`

佈景主題 3：使用自動化管理可變基礎設施

涵蓋的基本八項策略

應用程式控制、修補程式應用程式、修補程式作業系統

與不可變基礎設施類似，您可以將可變基礎設施管理為 IaC，並透過自動化程序修改或更新此基礎設施。許多不可變基礎設施的實作步驟也適用於可變基礎設施。不過，對於可變基礎設施，您還必須實作手動控制，以確保修改後的工作負載仍遵循最佳實務。

對於可變基礎設施，您可以使用 的修補程式管理員來自動化修補程式管理 AWS Systems Manager。在您 AWS 組織的所有帳戶中啟用修補程式管理員。

防止直接 SSH 和 RDP 存取，並要求使用者使用 Session Manager 或 Run Command，這也是 Systems Manager 的功能。與 SSH 和 RDP 不同，這些功能可以記錄系統存取和變更。

若要監控和報告合規性，您必須持續審查修補程式合規性。您可以使用 AWS Config 規則來確保所有 Amazon EC2 執行個體都由 Systems Manager 管理、具有必要的許可和已安裝的應用程式，並且符合修補程式合規。

AWS Well-Architected Framework 中的相關最佳實務

- SEC06-BP03 減少手動管理和互動式存取
- SEC06-BP05 自動化運算保護

實作此主題

自動化修補

- 在您組織的所有帳戶中 AWS 實作啟用修補程式管理員中的步驟
- 對於所有 EC2 執行個體，請在 Systems Manager 用來存取執行個體的執行個體設定檔或 IAM 角色`AmazonSSMManagedInstanceCore`中包含 `CloudWatchAgentServerPolicy`和

使用自動化而非手動程序

- 在 中實作 AMI 和容器建置管道中的指引 主題 2：透過安全管道管理不可變的基礎設施
- 使用 Session Manager 或 Run Command 而非直接 SSH 或 RDP 存取

使用自動化在 EC2 執行個體上安裝下列項目

- AWS Systems Manager Agent (SSM Agent)，用於執行個體探索和管理
- 應用程式控制的安全工具，例如 Security Enhanced Linux (SELinux) (GitHub)、File Access Policy Daemon (fapolicyd) (GitHub) 或 OpenSCAP
- Amazon CloudWatch Agent，用於記錄

在任何版本之前使用對等審核，以確保變更符合最佳實務

- IAM 政策過於寬鬆，例如使用萬用字元的政策
- 過於寬鬆的安全群組規則，例如使用萬用字元或允許 SSH 存取的安全群組規則
- 未啟用的存取日誌
- 未啟用的加密
- 密碼常值
- 安全 IAM 政策

使用身分層級控制項

- 若要要求使用者透過自動化程序修改資源並防止手動設定，請允許使用者可擔任之角色的唯讀許可
- 授予僅修改資源給服務角色的許可，例如 Systems Manager 使用的角色

實作漏洞掃描

- 在 中實作漏洞掃描中的指南 主題 2：透過安全管道管理不可變的基礎設施
- 使用 Amazon Inspector 掃描 EC2 執行個體

監控此佈景主題

持續監控修補程式合規

- 使用自動化和儀表板報告修補程式合規
- 實作機制來檢閱儀表板的修補程式合規性

持續監控 IAM 和日誌

- 定期檢閱您的 IAM 政策，以確保：
  - 只有部署管道可以直接存取 資源
  - 只有核准的服務可以直接存取資料
  - 使用者無法直接存取資源或資料
- 監控 AWS CloudTrail 日誌，以確保使用者透過管道修改資源，且不會直接修改資源或存取資料
- 定期檢閱 AWS Identity and Access Management Access Analyzer 問題清單
- 設定提醒，以便在 AWS 帳戶 使用 的根使用者登入資料時通知您

實作下列 AWS Config 規則

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps
- IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC - 22, 3389

佈景主題 4：管理身分

涵蓋的基本八項策略

限制管理權限、多重要素驗證

強大的身分和許可管理是管理雲端安全性的關鍵層面。強大的身分實務會平衡必要的存取和最低權限。這有助於開發團隊快速移動，而不會犧牲安全性。

使用聯合身分來集中管理身分。這可讓您更輕鬆地跨多個應用程式和服務管理存取權，因為您管理來自單一位置的存取權。這也可協助您實作暫時許可和多重要素驗證 (MFA)。

僅授予使用者執行任務所需的許可。 AWS Identity and Access Management Access Analyzer 可以驗證政策並驗證公有和跨帳戶存取。 AWS Organizations 服務控制政策 (SCPs)、IAM 政策條件、IAM 許可界限和 AWS IAM Identity Center 許可集等功能可協助您設定精細存取控制 (FGAC)。

執行任何類型的身分驗證時，最好使用臨時憑證來降低或消除風險，例如不小心揭露、共用或遭竊的憑證。使用 IAM 角色，而非 IAM 使用者。

使用強大的登入機制，例如 MFA，以降低不慎公開或容易猜測登入資料的風險。需要根使用者的 MFA，您也可以在聯合層級要求它。如果無法避免使用 IAM 使用者，請強制執行 MFA。

若要監控和報告合規性，您必須持續努力減少許可、監控 IAM Access Analyzer 的問題清單，以及移除未使用的 IAM 資源。使用 AWS Config 規則來確保強制執行強大的登入機制、短期登入資料，以及使用 IAM 資源。

AWS Well-Architected Framework 中的相關最佳實務

- SEC02-BP01 使用強大的登入機制
- SEC02-BP02 使用臨時憑證
- SEC02-BP03 安全地儲存和使用機密
- SEC02-BP04 仰賴集中式身分提供者
- SEC02-BP05 定期稽核和輪換憑證
- SEC02-BP06 採用使用者群組和屬性
- SEC03-BP01 定義存取需求

- SEC03-BP02 授予最低權限存取權
- SEC03-BP03 建立緊急存取程序
- SEC03-BP04 持續減少許可
- SEC03-BP05 為您的組織定義許可防護機制
- SEC03-BP06 根據生命週期管理存取
- SEC03-BP07 分析公有和跨帳戶存取權
- SEC03-BP08 在組織內安全地共用資源

實作此主題

實作聯合身分

- 要求人類使用者與身分提供者聯合 AWS 使用臨時憑證存取
- 實作對您 AWS 環境的暫時提升存取

套用最低權限許可

- 保護您的根使用者憑證，不要將其用於日常任務
- 使用 IAM Access Analyzer 根據存取活動產生最低權限政策
- 使用 IAM Access Analyzer 驗證對 資源的公有和跨帳戶存取權
- 使用 IAM Access Analyzer 驗證您的 IAM 政策是否有安全且功能正常的許可
- 跨多個帳戶建立許可護欄
- 使用許可界限來設定身分型政策可授予的最大許可
- 使用 IAM 政策中的條件進一步限制存取
- 定期檢閱和移除未使用的使用者、角色、許可、政策和登入資料
- 開始使用 AWS 受管政策，並朝最低權限的許可邁進
- 使用 IAM Identity Center 中的許可集功能

輪換登入資料

- 要求工作負載使用 IAM 角色來存取 AWS
- 自動化刪除未使用的 IAM 角色

- 對於需要長期憑證的使用案例，定期輪換存取金鑰

強制執行 MFA

- 需要根使用者的 MFA
- 透過 IAM Identity Center 需要 MFA
- 考慮要求 MFA 進行服務特定的 API 動作

監控此佈景主題

監控最低權限存取

- 將 IAM Access Analyzer 調查結果傳送至 AWS Security Hub CSPM
- 考慮為關鍵 IAM Identity Center 調查結果設定通知
- 定期檢閱 的登入資料報告 AWS 帳戶

實作下列 AWS Config 規則

- ACCESS_KEYS_ROTATED
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

佈景主題 5：建立資料周邊

涵蓋的基本八項策略

限制管理權限

資料周邊是環境中 AWS 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。這些護欄可做為永遠在線的界限，協助在廣泛的 AWS 帳戶 和資源中保護您的資料。這些全組織的護欄不會取代您現有的精細存取控制。反之，它們會確保所有 AWS Identity and Access Management (IAM) 使用者、角色和資源都遵循一組定義的安全標準，以協助改善您的安全策略。

您可以使用防止從組織界限外部存取的政策來建立資料周邊，通常是在 中建立 AWS Organizations。用來建立資料周邊的三個主要周邊授權條件為：

- 信任的身分 – 您內部或代表 AWS 服務 您的委託人 (IAM 角色 AWS 帳戶或使用者）。
- 信任的資源 – 位於 中的資源 AWS 帳戶 ，或是透過代表您 AWS 服務 執行動作來管理的資源。
- 預期的網路 – 您的內部部署資料中心和虛擬私有雲端 (VPCs)，或代表 AWS 服務 您的網路。

考慮在不同資料分類的環境之間實作資料周邊，例如 `OFFICIAL:SENSITIVE`或 `PROTECTED`，或不同風險層級，例如開發、測試或生產。如需詳細資訊，請參閱在 上建置資料周邊 AWS (AWS 白皮書）和在 上建立資料周邊 AWS：概觀 (AWS 部落格文章）。

AWS Well-Architected Framework 中的相關最佳實務

- SEC03-BP05 為您的組織定義許可防護機制
- SEC07-BP02 根據資料敏感度套用資料保護控制

實作此主題

實作身分控制

- 僅允許受信任的身分存取您的資源 – 使用具有條件索引鍵 和 的資源型政策`aws:PrincipalIsAWSService`。 `aws:PrincipalOrgID`這僅允許來自您 AWS 組織的主體和來自 AWS 的主體存取您的資源。

- 僅允許來自您網路的受信任身分 – 使用 VPC 端點政策搭配條件金鑰 `aws:PrincipalOrgID`和 `aws:PrincipalIsAWSService`。這僅允許來自您 AWS 組織和 的主體透過 VPC AWS 端點存取服務。

實作資源控制

- 允許您的身分僅存取信任的資源 – 使用服務控制政策 (SCPs) 搭配 條件金鑰 `aws:ResourceOrgID`。這可讓您的身分僅存取 AWS 組織中的資源。
- 僅允許從您的網路存取信任的資源 – 使用 VPC 端點政策搭配 條件金鑰 `aws:ResourceOrgID`。這可讓您的身分僅透過屬於您 AWS 組織的 VPC 端點存取服務。

實作網路控制

- 允許身分僅從預期的網路存取資源 – 使用具有條件索引鍵 `aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`和 SCPs`aws:ViaAWSService`。這可讓您的身分僅從預期的 IP 地址、VPCs 和 VPC 端點以及透過 存取資源 AWS 服務。
- 僅允許從預期的網路存取您的資源 – 使用資源型政策搭配條件索引鍵 `aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、 `aws:ViaAWSService`和 `aws:PrincipalIsAWSService`。這僅允許從預期的 IPs、預期的 VPCs、預期的 VPC 端點 AWS 服務、透過 或當呼叫身分為 時存取您的資源 AWS 服務。

監控此佈景主題

監控政策

- 實作機制來檢閱 SCPs、IAM 政策和 VPC 端點政策

實作下列 AWS Config 規則

- `SERVICE_VPC_ENDPOINT_ENABLED`

主題 6：自動化備份

涵蓋的基本八項策略

定期備份

「故障是給定的，而且一切都會隨著時間而失敗：從路由器到硬碟、從作業系統到損壞 TCP 封包的記憶體單位、從暫時性錯誤到永久故障。無論您使用的是最高品質的硬體或最低成本的元件，這是指定的。」 —Werner Vogels、CTO、Amazon、所有分散式物件

資料備份和復原是系統可靠性的關鍵部分。 AWS 旨在讓您更輕鬆地建立備份、維護備份資料的耐久性，以及確保備份資料仍可復原。

AWS Backup 是一種全受管服務，可集中和自動化跨 的資料備份 AWS 服務。它支援多種 AWS 資源類型，並可協助您針對使用多個資源的工作負載實作和維護備份策略，這些 AWS 資源必須共同備份。AWS Backup 也可協助您共同監控多個 AWS 資源的備份和還原操作。

AWS Backup 保存庫鎖定是備份保存庫的選用功能，可以提供額外的安全性和控制。當鎖定在合規模式下處於作用中狀態且寬限期結束時，使用者、帳戶或資料擁有者或 無法變更或刪除保存庫組態 AWS。每個保存庫都可以有一個保存庫鎖定。這提供一次寫入、多讀 (WORM) 組態和保留期的強制執行。

如果您遵循目前的組態指引， AWS Backup 可以提供 99.999999999% 的年度耐久性，也稱為 11 個九。它使用 AWS 全球基礎設施跨多個可用區域複寫備份。如需詳細資訊，請參閱 AWS Backup中的恢復能力。

AWS Backup 可協助您自動化備份資料的復原和測試，以驗證備份完整性和程序。

AWS Well-Architected Framework 中的相關最佳實務

- SEC09-BP01 實作安全金鑰和憑證管理
- SEC09-BP02 強制傳輸中加密
- SEC09-BP03 驗證網路通訊

實作此主題

自動化資料備份和復原

- 在 上實作資料備份 AWS
- 大規模自動化資料備份 (AWS 部落格文章)
- 使用 自動化資料復原驗證 AWS Backup (AWS 部落格文章)

在您的 AWS Backup 結果中實作控管

- 中保護備份的十大安全最佳實務 AWS(AWS 部落格文章)
- 使用 AWS Backup 保存庫鎖定來改善備份保存庫的安全性
- 使用 AWS Backup Audit Manager 稽核政策 AWS Backup 的合規性

監控此佈景主題

實作下列 AWS Config 規則

- RDS_IN_BACKUP_PLAN
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- REDSHIFT_BACKUP_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

佈景主題 7：集中記錄和監控

涵蓋的基本八項策略

應用程式控制、修補應用程式、限制管理權限、多重驗證

AWS 提供工具和功能，可讓您查看環境中發生的情況 AWS 。其中包含：

- AWS CloudTrail 透過為您的帳戶建立 AWS API 呼叫的歷史追蹤，包括透過 AWS 管理主控台、AWS SDKs和命令列工具進行的 API 呼叫，協助您監控 AWS 部署。對於支援 CloudTrail 的服務，您也可以識別哪些使用者和帳戶稱為服務的 API、呼叫的來源 IP 地址，以及呼叫的發生時間。
- Amazon CloudWatch 可協助您 AWS 即時監控 AWS 資源的指標，以及您執行的應用程式。
- 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。
- Amazon GuardDuty 是一項持續的安全監控服務，可分析和處理日誌，以識別 AWS 環境中非預期和可能未經授權的活動。GuardDuty 與 Amazon EventBridge 整合，以啟動自動回應或通知人類。
- AWS Security Hub CSPM 提供 中安全狀態的完整檢視 AWS。它還可協助您根據安全產業標準和最佳實務來檢查 AWS環境。

這些工具和功能旨在提高可見性，並協助您在問題對您的環境造成負面影響之前解決問題。這可協助您改善組織在雲端的安全狀態，並減少環境的風險設定檔。

AWS Well-Architected Framework 中的相關最佳實務

- SEC04-BP01 設定服務和應用程式日誌記錄
- SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標

實作此主題

啟用日誌記錄

- 使用 CloudWatch 代理程式將系統層級日誌發佈至 CloudWatch Logs
- 設定 GuardDuty 調查結果的提醒

- 在 CloudTrail 中建立組織追蹤

實作記錄安全最佳實務

- 實作 CloudTrail 安全最佳實務
- 使用 SCPs 防止使用者停用安全服務 (AWS 部落格文章)
- 使用 在 CloudWatch Logs 中加密日誌資料 AWS Key Management Service

集中日誌

- 從多個帳戶接收 CloudTrail 日誌
- 將日誌傳送至日誌封存帳戶
- 在 帳戶中集中 CloudWatch Logs 以進行稽核和分析 (AWS 部落格文章)
- 集中管理 Amazon Inspector
- 在 中建立整個組織的彙整工具 AWS Config (AWS 部落格文章)
- 集中管理 Security Hub CSPM
- 集中管理 GuardDuty
- 考慮使用 Amazon Security Lake

監控此佈景主題

實作機制

- 建立機制來檢閱日誌問題清單
- 建立機制來檢閱 Security Hub CSPM 問題清單
- 建立機制以回應 GuardDuty 調查結果

實作下列 AWS Config 規則

- `CLOUDTRAIL_SECURITY_TRAIL_ENABLED`
- `GUARDDUTY_ENABLED_CENTRALIZED`
- `SECURITYHUB_ENABLED`

- ACCOUNT_PART_OF_ORGANIZATIONS

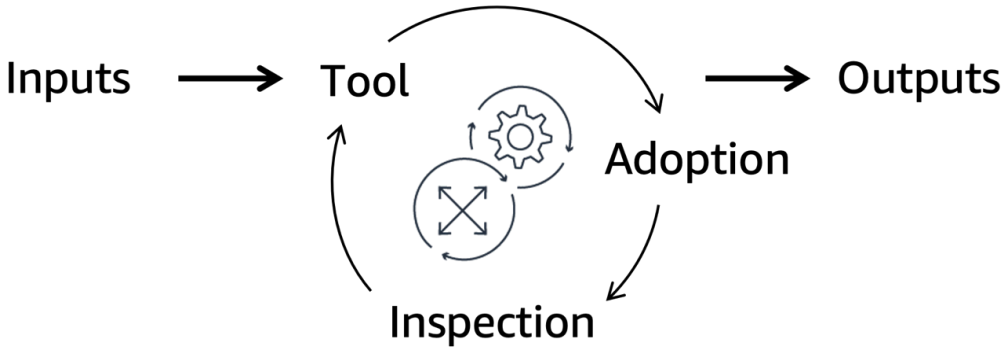
佈景主題 8：實作手動程序的機制

涵蓋的基本八項策略

應用程式控制、修補應用程式

在 Amazon，我們有一個說法：良好的意圖沒有作用，機制有作用 (AWS 部落格文章）。這表示您必須以自動化、可重複、可擴展的程序和工具取代最佳工作，才能達到所需的成果。

如下圖所示，機制是您建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。這是一個在操作時強化和改善自身的循環。它接受可控制的輸入，並將其轉換為持續的輸出，以解決經常性的業務挑戰。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。



AWS Well-Architected Framework 中的相關最佳實務

- OPS02-BP01 已為資源識別擁有者
- OPS02-BP02 流程和程序已識別擁有者
- OPS02-BP03 已為營運活動識別負責其效能的擁有者
- OPS02-BP04 存在管理責任和擁有權的機制
- OPS03-BP01 提供高層支持
- OPS03-BP03 鼓勵向上呈報

實作此主題

- 建立機制來檢閱和解決合規差距

- 建立機制以更新安全政策
- 移除不支援的應用程式，然後將其新增至 AWS Config 規則拒絕清單
- 使用 驗證存取政策 AWS Identity and Access Management Access Analyzer
- 啟用 Amazon Inspector，自動讓漏洞註冊up-to-date
- 至少每年檢閱應用程式控制規則集
- 考慮實作自動化，例如AWS Config 規則，以減少手動程序的負擔
- 考慮使用AWS Systems Manager 庫存來了解哪些執行個體正在執行軟體政策所需的軟體

監控此佈景主題

- 為 的執行發起人建立監督，以追蹤目標的進度，包括合規、檢查差距和評估機制。

在 上達到基本八項成熟度的指示性案例研究 AWS

本章針對目標為 Essential Eight 成熟度的政府機構提供指示性案例研究 AWS。

本章中的章節：

- 案例和架構概觀
- 工作負載範例：無伺服器資料湖
- 工作負載範例：容器化 Web 服務
- 工作負載範例：Amazon EC2 上的 COTS 軟體

案例和架構概觀

政府機構在 中有三個工作負載 AWS 雲端：

- 使用 Amazon Simple Storage Service (Amazon S3) 進行儲存和擷取、轉換和載入 AWS Lambda (ETL) 操作的無伺服器資料湖
- 在 Amazon Elastic Container Service (Amazon ECS) 上執行並使用 Amazon Relational Database Service (Amazon RDS) 中資料庫的容器化 Web 服務
- 在 Amazon EC2 上執行的商業off-the-shelf(COTS) 軟體

雲端團隊為組織提供集中式平台，為 AWS 環境執行核心服務。雲端團隊提供 AWS 環境的核心服務。每個工作負載都由不同的應用程式團隊擁有，也稱為開發人員團隊或交付團隊。

核心架構

雲端團隊已在 中建立下列功能 AWS 雲端：

- 聯合身分 AWS IAM Identity Center 連結至其 Microsoft Entra ID （ 先前稱為 Azure Active Directory) 執行個體。聯合會透過 AWS Identity and Access Management (IAM) 角色強制執行 MFA、使用者帳戶的自動過期，以及短期憑證的使用。
- 集中式 AMI 管道用於使用 EC2 Image Builder OSs和核心應用程式。
- Amazon Inspector 已啟用以識別漏洞，所有安全調查結果都會傳送至 Amazon GuardDuty 進行集中管理。
- 建立的機制用於更新應用程式控制規則、回應網路安全事件，以及檢閱合規漏洞。

- AWS CloudTrail 用於記錄和監控。
- 安全事件，例如根使用者的登入，會啟動提醒。
- SCPs和 VPC 端點政策會為您的 AWS 環境建立資料周邊。
- SCPs可防止應用程式團隊停用安全性和記錄服務，例如 CloudTrail 和 AWS Config。
- AWS Config 為了安全 AWS 帳戶 起見，問題清單會從整個 AWS 組織彙總到單一 。
- AWS 帳戶 ACS AWS Config C Essential 8 一致性套件在您的組織中已啟用。

工作負載範例：無伺服器資料湖

此工作負載是 的範例主題 1：使用 受管服務。

資料湖使用 Amazon S3 儲存和 AWS Lambda ETL。這些資源在 AWS Cloud Development Kit (AWS CDK) 應用程式中定義。透過 部署對系統所做的變更 AWS CodePipeline。此管道僅限於應用程式團隊。當應用程式團隊對程式碼儲存庫提出提取請求時，會使用兩人規則。

對於此工作負載，應用程式團隊會採取下列動作來解決 Essential Eight 策略。

應用程式控制

- 應用程式團隊會在 GuardDuty 中啟用 Lambda 保護，並在 Amazon Inspector 中啟用 Lambda 掃描。
- 應用程式團隊實作機制來檢查和管理 Amazon Inspector 調查結果。

修補程式應用程式

- 應用程式團隊會在 Amazon Inspector 中啟用 Lambda 掃描，並設定已棄用或易受攻擊程式庫的提醒。
- 應用程式團隊可讓 AWS Config 追蹤資產探索 AWS 的資源。

限制管理權限

- 如 核心架構節所述，應用程式團隊已透過其部署管道上的核准規則，限制對生產部署的存取。
- 應用程式團隊倚賴 核心架構節所述的集中式聯合身分和集中式記錄解決方案。
- 應用程式團隊會建立 AWS CloudTrail 追蹤和 Amazon CloudWatch 篩選條件。
- 應用程式團隊會設定 CodePipeline 部署和 AWS CloudFormation 堆疊刪除的 Amazon Simple Notification Service (Amazon SNS) 提醒。

修補程式作業系統

- 應用程式團隊會在 Amazon Inspector 中啟用 Lambda 掃描，並設定已棄用或易受攻擊程式庫的提醒。

多重要素驗證

- 應用程式團隊依賴 核心架構節所述的集中式聯合身分解決方案。此解決方案會強制執行 MFA、記錄身分驗證，以及提醒或自動回應可疑的 MFA 事件。

定期備份

- 應用程式團隊會將程式碼，例如 AWS CDK 應用程式和 Lambda 函數和組態，存放在程式碼儲存庫中。
- 應用程式團隊會啟用版本控制和 Amazon S3 物件鎖定，以協助防止物件遭到刪除或修改。
- 應用程式團隊依賴內建的 Amazon S3 耐用性，而不是將其整個資料集複寫到另一個資料集 AWS 區域。
- 應用程式團隊會在另一個 中執行工作負載的副本 AWS 區域 ，以符合其資料主權需求。它們使用 Amazon DynamoDB 全域資料表和 Amazon S3 跨區域複寫，將資料從主要區域自動複寫到次要區域。

工作負載範例：容器化 Web 服務

此工作負載是 的範例主題 2：透過安全管道管理不可變的基礎設施。

Web 服務會在 Amazon ECS 上執行，並使用 Amazon RDS 中的資料庫。應用程式團隊會在 CloudFormation 範本中定義這些資源。使用 EC2 Image Builder 建立容器，並存放在 Amazon ECR 中。應用程式團隊透過 部署變更至系統 AWS CodePipeline。此管道僅限於應用程式團隊。當應用程式團隊對程式碼儲存庫提出提取請求時，會使用兩個人規則。

對於此工作負載，應用程式團隊會採取下列動作來解決 Essential Eight 策略。

應用程式控制

- 應用程式團隊可在 Amazon Inspector 中掃描 Amazon ECR 容器映像。
- 應用程式團隊會在 EC2 Image Builder 管道中建置檔案存取政策協助程式 (fapolicyd) 安全工具。如需詳細資訊，請參閱 ACSC 網站上的實作應用程式控制。

- 應用程式團隊會設定 Amazon ECS 任務定義，將輸出記錄到 Amazon CloudWatch Logs。
- 應用程式團隊實作機制來檢查和管理 Amazon Inspector 調查結果。

修補程式應用程式

- 應用程式團隊可在 Amazon Inspector 中掃描 Amazon ECR 容器映像，並設定已棄用或易受攻擊程式庫的提醒。
- 應用程式團隊會將對 Amazon Inspector 調查結果的回應自動化。新的問題清單會透過 Amazon EventBridge 觸發程序啟動其部署管道，而 CodePipeline 是目標。
- 應用程式團隊可讓 AWS Config 追蹤資產探索 AWS 的資源。

限制管理權限

- 應用程式團隊已透過其部署管道上的核准規則，限制對生產部署的存取。
- 應用程式團隊倚賴集中式雲端團隊的聯合身分來輪換登入資料和集中式記錄。
- 應用程式團隊會建立 CloudTrail 追蹤和 CloudWatch 篩選條件。
- 應用程式團隊會為 CodePipeline 部署和 CloudFormation 堆疊刪除設定 Amazon SNS 警示。

修補程式作業系統

- 應用程式團隊可在 Amazon Inspector 中掃描 Amazon ECR 容器映像，並設定作業系統修補程式更新的提醒。
- 應用程式團隊會自動回應 Amazon Inspector 問題清單。新的問題清單會透過 EventBridge 觸發程序啟動其部署管道，而 CodePipeline 是目標。
- 應用程式團隊會訂閱 Amazon RDS 事件通知，以便通知他們更新。他們與其業務擁有者一起做出以風險為基礎的決策，以決定是否要手動套用這些更新，或讓 Amazon RDS 自動套用這些更新。
- 應用程式團隊會將 Amazon RDS 執行個體設定為多可用區域叢集，以減少維護事件的影響。

多重要素驗證

- 應用程式團隊依賴 核心架構節所述的集中式聯合身分解決方案。此解決方案會強制執行 MFA、記錄身分驗證，以及提醒或自動回應可疑的 MFA 事件。

定期備份

- 應用程式團隊會設定 AWS Backup 來自動備份其 Amazon RDS 叢集的資料。
- 應用程式團隊會將 CloudFormation 範本存放在程式碼儲存庫中。
- 應用程式團隊開發自動化管道，在另一個區域中建立工作負載的副本，並執行自動化測試 (AWS 部落格文章）。自動化測試執行後，管道會銷毀堆疊。此管道每月自動執行一次，並驗證復原程序的有效性。

工作負載範例：Amazon EC2 上的 COTS 軟體

此工作負載是 的範例佈景主題 3：使用自動化管理可變基礎設施。

Amazon EC2 上執行的工作負載是使用 手動建立 AWS 管理主控台。開發人員登入 EC2 執行個體並更新軟體，以手動更新系統。

對於此工作負載，雲端和應用程式團隊會採取下列動作來解決 Essential Eight 策略。

應用程式控制

- 雲端團隊會設定其集中式 AMI 管道，以安裝和設定 AWS Systems Manager Agent (SSM Agent)、CloudWatch 代理程式和 SELinux。他們會在組織中的所有帳戶中共用產生的 AMI。
- 雲端團隊使用 AWS Config 規則來確認所有執行中的 EC2 執行個體都由 Systems Manager 管理，並已安裝 SSM Agent、CloudWatch 代理程式和 SELinux。
- 雲端團隊會將 Amazon CloudWatch Logs 輸出傳送至在 Amazon OpenSearch Service 上執行的集中式安全資訊和事件管理 (SIEM) 解決方案。
- 應用程式團隊實作機制，以檢查和管理來自 AWS Config GuardDuty 和 Amazon Inspector 的問題清單。雲端團隊會實作自己的機制，以擷取應用程式團隊遺漏的任何調查結果。如需建立漏洞管理計劃以解決調查結果的更多指引，請參閱在 上建立可擴展的漏洞管理計劃 AWS。

修補程式應用程式

- 應用程式團隊會根據 Amazon Inspector 調查結果來修補執行個體。
- 雲端團隊會修補基本 AMI，而應用程式團隊會在 AMI 變更時收到提醒。
- 應用程式團隊透過設定安全群組規則來限制對其 EC2 執行個體的直接存取，以僅允許工作負載所需的連接埠上的流量。
- 應用程式團隊使用修補程式管理員來修補執行個體，而不是登入個別執行個體。
- 若要在 EC2 執行個體群組上執行任意命令，應用程式團隊會使用 Run Command。

- 在極少數情況下，當應用程式團隊需要直接存取執行個體時，他們會使用 Session Manager。此存取方法使用聯合身分，並記錄任何工作階段活動以進行稽核。

限制管理權限

- 應用程式團隊會設定安全群組規則，僅允許工作負載所需連接埠上的流量。這會限制對 Amazon EC2 執行個體的直接存取，並要求使用者透過 Session Manager 存取 EC2 執行個體。
- 應用程式團隊倚賴集中式雲端團隊的聯合身分來輪換登入資料和集中式記錄。
- 應用程式團隊會建立 CloudTrail 追蹤和 CloudWatch 篩選條件。
- 應用程式團隊會為 CodePipeline 部署和 CloudFormation 堆疊刪除設定 Amazon SNS 警示。

修補程式作業系統

- 雲端團隊會修補基本 AMI，而應用程式團隊會在 AMI 變更時收到提醒。應用程式團隊使用此 AMI 部署新的執行個體，然後使用 Systems Manager 的 State Manager 安裝必要的軟體。
- 應用程式團隊使用修補程式管理員來修補執行個體，也就是登入個別執行個體的執行個體。
- 若要在 EC2 執行個體群組上執行任意命令，應用程式團隊會使用 Run Command。
- 在極少數情況下，當應用程式團隊需要直接存取時，他們會使用 Session Manager。

多重要素驗證

- 應用程式團隊依賴 核心架構節所述的集中式聯合身分解決方案。此解決方案會強制執行 MFA、記錄身分驗證，以及提醒或自動回應可疑的 MFA 事件。

定期備份

- 應用程式團隊會為其 EC2 執行個體和 Amazon Elastic Block Store (Amazon EBS) 磁碟區建立 AWS Backup 計劃。
- 應用程式團隊會實作機制，每月手動執行備份還原。

資源

AWS 文件

- AWS 安全參考架構 (AWS SRA)
- AWS 安全文件
- AWS Well-Architected 架構的安全支柱

其他 AWS 資源

- AWS 雲端安全性
- AWS 雲端採用架構（安全性觀點）

澳洲網路安全中心資源

- Essential Eight 已說明
- 基本八項成熟度模型
- Essential Eight 評估程序指南

貢獻者

本文件的貢獻者包括：

- AWS 解決方案架構資深解決方案架構師，James Kingsmill
- Chris Harding，資深解決方案架構師， AWS 解決方案架構
- Jess Modini，諮詢解決方案架構師， AWS解決方案架構
- Justin Bowden，安全保證委託人， AWS 安全保證
- Rob Powell，資深解決方案架構師， AWS 解決方案架構
- Tony Mihaljevic | AWS Professional Services 資深雲端架構師
- Volker Rath， AWS Global Services Security 首席安全顧問

附錄：Essential Eight 控制項矩陣

下表將 Essential Eight 策略連結至 AWS Well-Architected Framework 中的 AWS 實作指引和相關最佳實務。對於 中不適用的基本八項控制項 AWS 雲端，資料表包含澳洲網路安全中心 (ACSC) 的其他指導連結。

控制矩陣：

- 應用程式控制
- 修補程式應用程式
- 設定Microsoft Office巨集設定
- 使用者應用程式強化
- 限制管理權限
- 修補程式作業系統
- 多重要素驗證
- 定期備份

應用程式控制

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
應用程式控制會在工作站和伺服器上實作，將可執行檔、軟體程式庫、指令碼、安裝程式、編譯的 HTML、HTML 應用程式、控制面板小程式和驅動程式的執行限制為組織核准的集合。	主題 2：透過安全管道管理不可變的基礎設施：實作 AMI 和容器建置管道	使用 EC2 Image Builder 並建置： • AWS Systems Manager 代理程式 (SSM 代理程式) • 應用程式控制的安全工具，例如 Security Enhanced Linux (SELinux) (GitHub)、File Access Policy Daemon (fapolicy	SEC06-BP02 從強化影像佈建運算

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
		d) (GitHub) 或 OpenSCAP Amazon CloudWatch 代理程式 與整個組織共用 AMIs 確定應用程式團隊正在參考最新的 AMIs 使用您的 AMI 管道進行修補程式管理	
Microsoft已實作 的「建議區塊規則」。	請參閱實作應用程式控制 (ACSC 網站)	不適用	不適用
Microsoft已實作 的「建議驅動程式區塊規則」。			
每年或更頻繁地驗證應用程式控制規則集。	佈景主題 8：實作手動程序的機制：實作機制以更新安全政策	不適用	SEC01-BP08 定期評估和實作新的安全服務和功能

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
工作站和伺服器上允許的和封鎖的執行會集中記錄和保護，避免未經授權的修改和刪除、監控入侵跡象，以及在偵測到網路安全事件時採取動作。	佈景主題 7：集中記錄和監控：啟用記錄	使用 CloudWatch 代理程式將系統層級日誌發佈至 CloudWatch Logs 設定 GuardDuty 調查結果的提醒 在 CloudTrail 中建立組織追蹤 使用版本控制和 Amazon S3 S3 中的資料	SEC04-BP01 設定服務和應用程式日誌記錄 SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標
	佈景主題 7：集中記錄和監控：實作記錄安全最佳實務	實作 CloudTrail 安全最佳實務 使用 SCPs 防止使用者停用安全服務 (AWS 部落格文章） 使用 在 CloudWatch Logs 中加密日誌資料 AWS Key Management Service	SEC04-BP01 設定服務和應用程式日誌記錄 SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
	佈景主題 7：集中記錄和監控：集中日誌	從多個帳戶接收 CloudTrail 日誌 將日誌傳送至日誌封存帳戶 在 帳戶中集中 CloudWatch Logs 以進行稽核和分析 (AWS 部落格文章） 集中管理 Amazon Inspector 在 中建立整個組織的彙整工具 AWS Config (AWS 部落格文章） 集中管理 Security Hub CSPM 集中管理 GuardDuty 考慮使用 Amazon Security Lake	SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標
	佈景主題 8：實作手動程序的機制：實作機制來檢閱和解決合規差距	考慮實作自動化，例如AWS Config 規則，以減少手動程序的負擔	OPS02-BP02 流程和程序已識別擁有者 OPS02-BP03 已為營運活動識別負責其效能的擁有者 OPS02-BP04 存在管理責任和擁有權的機制

修補程式應用程式

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
資產探索的自動化方法至少會於今晚使用，以支援後續漏洞掃描活動的資產偵測。	主題 1：使用 受管服務：掃描漏洞 主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描 佈景主題 3：使用自動化管理可變基礎設施：實作漏洞掃描	在您組織的所有帳戶中啟用 Amazon Inspector 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描 建置漏洞管理計劃來分類和修復安全問題清單	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護
	佈景主題 7：集中記錄和監控：集中日誌	從多個帳戶接收 CloudTrail 日誌 將日誌傳送至日誌封存帳戶 在 帳戶中集中 CloudWatch Logs 以進行稽核和分析 (AWS 部落格文章) 集中管理 Amazon Inspector 在 (AWS 部落格文章) 中建立整個組織的彙整工具 AWS Config 集中管理 Security Hub CSPM	SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
		集中管理 GuardDuty 考慮使用 Security Lake	
具有up-to-date漏洞資料庫的漏洞掃描器會用於漏洞掃描活動。 漏洞掃描器至少每天使用一次，以識別面向網際網路服務中安全漏洞的遺失或更新。	主題 1：使用 受管服務：掃描漏洞 主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描 佈景主題 3：使用自動化管理可變基礎設施：實作漏洞掃描	在您組織的所有帳戶中啟用 Amazon Inspector 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描 建置漏洞管理計劃來分類和修復安全問題清單	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護
漏洞掃描器至少每週使用一次，以識別辦公室生產力套件、網頁瀏覽器及其延伸模組、電子郵件用戶端、PDF 軟體和安全產品中缺少的安全漏洞修補程式或更新。	請參閱技術範例：修補程式應用程式 (ACSC 網站)	不適用	不適用

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
漏洞掃描器至少會於今晚使用，以識別其他應用程式中安全漏洞缺少的修補程式或更新。	主題 1：使用 受管服務：掃描漏洞 主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描 佈景主題 3：使用自動化管理可變基礎設施：實作漏洞掃描	在您組織的所有帳戶中啟用 Amazon Inspector 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描 建置漏洞管理計劃來分類和修復安全問題清單	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護
面向網際網路服務中安全漏洞的修補程式、更新或廠商緩解措施會在發行後兩週內套用，如果存在漏洞，則會在 48 小時內套用。	主題 1：使用 受管服務：掃描漏洞 主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描 佈景主題 3：使用自動化管理可變基礎設施：實作漏洞掃描	在您組織的所有帳戶中啟用 Amazon Inspector 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描 建置漏洞管理計劃來分類和修復安全問題清單	SEC06-BP01 執行漏洞管理
	佈景主題 3：使用自動化管理可變基礎設施：自動化修補	在您 AWS 組織的所有帳戶中啟用修補程式管理員	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
針對辦公室生產力套件、網頁瀏覽器及其延伸模組、電子郵件用戶端、PDF 軟體和安全產品中安全漏洞的修補程式、更新或廠商緩解措施，會在發行後兩週內套用，如果存在漏洞，則會在 48 小時內套用。	請參閱技術範例：修補程式應用程式 (ACSC 網站)	不適用	不適用
其他應用程式中安全漏洞的修補程式、更新或廠商緩解措施會在發行後一個月內套用。	主題 1：使用 受管服務：掃描漏洞 主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描 佈景主題 3：使用自動化管理可變基礎設施：實作漏洞掃描	在您組織的所有帳戶中啟用 Amazon Inspector 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描 建置漏洞管理計劃來分類和修復安全問題清單	SEC06-BP01 執行漏洞管理
	佈景主題 3：使用自動化管理可變基礎設施：自動化修補	在您 AWS 組織的所有帳戶中啟用修補程式管理員	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護
已移除不再由廠商支援的應用程式。	佈景主題 8：實作手動程序的機制：實作機制來檢閱和解決合規差距	考慮使用AWS Systems Manager 庫存來了解哪些執行個體正在執行軟體政策所需的軟體	SEC06-BP02 從強化影像佈建運算

設定Microsoft Office巨集設定

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
Microsoft Office 對於沒有已證實業務需求的使用者，巨集會停用。	請參閱技術範例：設定巨集設定 (ACSC 網站)	不適用	不適用
只有從沙盒環境、信任位置或由信任發佈者數位簽署的Microsoft Office巨集才能執行。			
只有負責驗證Microsoft Office巨集是否不含惡意程式碼的特權使用者，才能寫入和修改信任位置中的內容。			
Microsoft Office 無法透過訊息列或後台檢視啟用由不受信任發佈者數位簽署的巨集。			
Microsoft Office的信任發佈者清單會每年或更頻繁地進行驗證。			
Microsoft Office 來自網際網路的檔案中的巨集會遭到封鎖。			

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
Microsoft Office 巨集防毒掃描已啟用。			
Microsoft Office 巨集會遭到封鎖，無法進行 Win32 API 呼叫。			
Microsoft Office 使用者無法變更巨集安全設定。			
允許和封鎖的Microsoft Office巨集執行會集中記錄並受到保護，免於未經授權的修改和刪除、監控入侵跡象，以及在偵測到網路安全事件時採取動作。			

使用者應用程式強化

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
Web 瀏覽器不會Java從網際網路處理。	請參閱技術範例：使用者應用程式強化 (ACSC 網站)	不適用	不適用
Web 瀏覽器不會處理來自網際網路的 Web 廣告。			
Internet Explorer 11 已停用或移除。			

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
Microsoft Office 被封鎖，無法建立子程序。			
Microsoft Office 被封鎖，無法建立可執行內容。			
Microsoft Office 被封鎖，無法將程式碼注入其他程序。			
Microsoft Office 已設定為防止啟用 OLE 套件。			
PDF 軟體無法建立子程序。			
已實作網頁瀏覽器的 ACSC 或廠商強化指引，Microsoft Office以及 PDF 軟體。			
使用者無法變更 Web 瀏覽器Microsoft Office 和 PDF 軟體安全設定。			
.NET Framework 3.5（包括 .NET 2.0 和 3.0) 已停用或移除。			
Windows PowerShell 2.0 已停用或移除。			

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
PowerShell 設定為使用受限語言模式。			
封鎖的PowerShell 指令碼執行會集中記錄並受到保護，免於未經授權的修改和刪除、監控入侵跡象，以及在偵測到網路安全事件時採取動作。			

限制管理權限

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
首次請求時，系統會驗證對系統和應用程式的特權存取請求。	佈景主題 4：管理身分：實作聯合身分	要求人類使用者與身分提供者聯合 AWS 使用臨時憑證存取	SEC02-BP04 仰賴集中式身分提供者 SEC03-BP01 定義存取需求
除非重新驗證，否則系統與應用程式的權限存取會在 12 個月後自動停用。	佈景主題 4：管理身分：實作聯合身分	要求人類使用者與身分提供者聯合 AWS 使用臨時憑證存取	SEC02-BP04 仰賴集中式身分提供者
	佈景主題 4：管理身分：輪換登入資料	要求工作負載使用 IAM 角色來存取 AWS 自動化刪除未使用的 IAM 角色	SEC02-BP05 定期稽核和輪換憑證

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
		針對需要長期憑證的使用案例，定期輪換存取金鑰 AWS Summit ANZ 2023：您前往雲端臨時登入資料的旅程 (YouTube 影片)	
系統與應用程式的權限存取會在閒置 45 天後自動停用。	佈景主題 4：管理身分：實作聯合身分 佈景主題 4：管理身分：輪換登入資料	要求人類使用者與身分提供者聯合 AWS 使用臨時憑證存取 要求工作負載使用 IAM 角色來存取 AWS 自動化刪除未使用的 IAM 角色 針對需要長期憑證的使用案例，定期輪換存取金鑰 AWS Summit ANZ 2023：您前往雲端臨時登入資料的旅程 (YouTube 影片)	SEC02-BP04 仰賴集中式身分提供者 SEC02-BP05 定期稽核和輪換憑證

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
系統和應用程式的特權存取僅限於使用者和服務履行其職責所需的內容。	佈景主題 4：管理身分：套用最低權限許可	保護您的根使用者憑證，不要將其用於日常任務 使用 IAM Access Analyzer 根據存取活動產生最低權限政策 使用 IAM Access Analyzer 驗證對 資源的公有和跨帳戶存取權 使用 IAM Access Analyzer 驗證您的 IAM 政策是否有安全且功能正常的許可 跨多個帳戶建立許可護欄 使用許可界限來設定身分型政策可授予的最大許可 使用 IAM 政策中的條件進一步限制存取 定期檢閱和移除未使用的使用者、角色、許可、政策和登入資料 開始使用 AWS 受管政策並邁向最低權限許可	SEC01-BP02 安全帳戶根使用者和屬性 SEC03-BP02 授予最低權限存取權

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
		使用 IAM Identity Center 中的許可集功能	
特殊權限帳戶無法存取網際網路、電子郵件和 Web 服務。	請參閱技術範例：限制管理權限 (ACSC 網站）	考慮實作 SCP，以防止任何尚未擁有網際網路存取權的 VPC 取得它	不適用
特殊權限使用者使用不同的特殊權限和無特殊權限操作環境。 特殊權限操作環境不會在無特殊權限的操作環境中虛擬化。 無權限帳戶無法登入有權限的操作環境。 特殊權限帳戶（本機管理員帳戶除外）無法登入無特殊權限的操作環境。	佈景主題 5：建立資料周邊	建立資料周邊。考慮在不同資料分類的環境之間實作資料周邊，例如 `OFFICIAL:SENSITIVE` 或 `PROTECTED` ，或不同的風險層級，例如開發、測試或生產。	SEC06-BP03 減少手動管理和互動式存取
Just-in-time管理用於管理系統和應用程式。	佈景主題 4：管理身分：實作聯合身分	要求人類使用者使用臨時憑證與身分提供者聯合 AWS 存取 實作對您 AWS 環境的暫時提升存取 (AWS 部落格文章）	SEC02-BP04 仰賴集中式身分提供者

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
管理活動是透過跳轉伺服器執行。	主題 1：使用 受管服務 佈景主題 3：使用自動化管理可變基礎設施：使用自動化而非手動程序	使用 Session Manager 或 Run Command 而非直接 SSH 或 RDP 存取	SEC01-BP05 減少安全管理範圍 SEC06-BP03 減少手動管理和互動式存取
本機管理員帳戶和服務帳戶的登入資料是唯一、無法預測和管理的。	請參閱技術範例：限制管理權限 (ACSC 網站)	不適用	不適用
Windows Defender Credential Guard 和 Windows Defender Remote Credential Guard已啟用。			

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
系統會集中記錄並保護特殊權限存取的使用，避免未經授權的修改和刪除、監控入侵跡象，以及在偵測到網路安全事件時採取動作。	佈景主題 7：集中記錄和監控：啟用記錄 佈景主題 7：集中記錄和監控：集中日誌	使用 CloudWatch Agent 將作業系統層級日誌發佈至 CloudWatch Logs 為您的組織啟用 CloudTrail 在 帳戶中集中 CloudWatch Logs 以進行稽核和分析 (AWS 部落格文章） 集中管理 Amazon Inspector 集中管理 Security Hub CSPM 在 (AWS 部落格文章） 中建立整個組織的彙整工具 AWS Config 集中管理 GuardDuty 考慮使用 Amazon Security Lake 從多個帳戶接收 CloudTrail 日誌 將日誌傳送至日誌封存帳戶	SEC04-BP01 設定服務和應用程式日誌記錄 SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標
系統會集中記錄特殊權限帳戶和群組的變更，並防止未經授權的修改和刪除、監控入侵跡象，以及在偵測到網路安全事件時採取動作。			

修補程式作業系統

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
面向網際網路服務作業系統中安全漏洞的修補程式、更新或廠商緩解措施會在發行後兩週內套用，如果存在漏洞，則會在 48 小時內套用。	主題 2：透過安全管道管理不可變的基礎設施：實作 AMI 和容器建置管道	使用 EC2 Image Builder 並建置： • AWS Systems Manager 代理程式 (SSM 代理程式) • 應用程式控制的安全工具，例如 Security Enhanced Linux (SELinux) (GitHub)、File Access Policy Daemon (fapolicyd) (GitHub) 或 OpenSCAP • Amazon CloudWatch 代理程式 與整個組織共用 AMIs 確定應用程式團隊正在參考最新的 AMIs 使用您的 AMI 管道進行修補程式管理	SEC01-BP05 減少安全管理範圍 SEC06-BP01 執行漏洞管理 SEC06-BP03 減少手動管理和互動式存取
	主題 1：使用 受管服務：啟用修補 佈景主題 3：使用自動化管理可變基礎設施：自動化修補	在您 AWS 組織的所有帳戶中啟用修補程式管理員	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
工作站、伺服器和網路裝置作業系統中安全漏洞的修補程式、更新或廠商緩解措施會在發行後兩週內套用，如果存在漏洞，則會在 48 小時內套用。	主題 2：透過安全管道管理不可變的基礎設施：實作 AMI 和容器建置管道	使用 EC2 Image Builder 並建置： • AWS Systems Manager 代理程式 (SSM 代理程式) • 應用程式控制的安全工具，例如 Security Enhanced Linux (SELinux) (GitHub)、File Access Policy Daemon (fapolicyd) (GitHub) 或 OpenSCAP • Amazon CloudWatch 代理程式 與整個組織共用 AMIs 確定應用程式團隊正在參考最新的 AMIs 使用您的 AMI 管道進行修補程式管理	SEC01-BP05 減少安全管理範圍 SEC06-BP01 執行漏洞管理 SEC06-BP02 從強化影像佈建運算
	主題 1：使用 受管服務：啟用修補 佈景主題 3：使用自動化管理可變基礎設施：自動化修補	在您 AWS 組織的所有帳戶中啟用修補程式管理員	SEC06-BP01 執行漏洞管理 SEC06-BP05 自動化運算保護

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
漏洞掃描器至少每天使用一次，以識別面向網際網路服務作業系統中安全漏洞缺少的修補程式或更新。 漏洞掃描器至少每週使用一次，以識別工作站、伺服器和網路裝置作業系統中安全漏洞缺少的修補程式或更新。	主題 1：使用 受管服務：掃描漏洞 主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描 佈景主題 3：使用自動化管理可變基礎設施：實作漏洞掃描	在您組織的所有帳戶中啟用 Amazon Inspector 使用 Amazon Inspector 設定 Amazon ECR 儲存庫的增強型掃描 建置漏洞管理計劃來分類和修復安全問題清單	SEC01-BP05 減少安全管理範圍 SEC06-BP01 執行漏洞管理 SEC06-BP02 從強化影像佈建運算

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
作業系統的最新版本或先前版本用於工作站、伺服器和網路裝置。 已取代不再由廠商支援的作業系統。	主題 2：透過安全管道管理不可變的基礎設施：實作漏洞掃描	使用 EC2 Image Builder 並建置： • AWS Systems Manager 代理程式 (SSM 代理程式) • 應用程式控制的安全工具，例如 Security Enhanced Linux (SELinux) (GitHub)、File Access Policy Daemon (fapolicyd) (GitHub) 或 OpenSCAP • Amazon CloudWatch 代理程式 與整個組織共用 AMIs 確定應用程式團隊正在參考最新的 AMIs 使用您的 AMI 管道進行修補程式管理	SEC01-BP05 減少安全管理範圍 SEC06-BP01 執行漏洞管理 SEC06-BP02 從強化影像佈建運算

多重要素驗證

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
如果組織的使用者向組織的面向網際網路服務進行身分驗證，則會使用多重要素身分驗證。	佈景主題 4：管理身分：實作聯合身分	要求人類使用者與身分提供者聯合 AWS 使用臨時憑證存取 實作暫時提升對您 AWS 環境的存取	SEC02-BP04 仰賴集中式身分提供者
	佈景主題 4：管理身分：強制執行 MFA	需要根使用者的 MFA 需要 MFA 到 AWS IAM Identity Center 考慮要求 MFA 進行服務特定的 API 動作	SEC02-BP01 使用強大的登入機制
如果組織使用者向處理、存放或通訊其組織的敏感資料的第三方面向網際網路服務進行身分驗證，則會使用多重要素驗證。	請參閱實作多重要素驗證 (ACSC 網站)	不適用	不適用
如果組織使用者向處理、存放或通訊其組織非敏感資料的第三方網際網路面向服務進行身分驗證，則會使用多重要素驗證（如果可用）。			
非組織使用者預設會啟用多重要素驗證（但使用者可以選擇			

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
選擇退出），如果他們向組織的面向網際網路服務進行身分驗證。			
多重要素驗證用於驗證系統的特權使用者。	佈景主題 4：管理身分：實作聯合身分	要求人類使用者與身分提供者聯合 AWS 使用臨時憑證存取 實作暫時提升對您 AWS 環境的存取	SEC02-BP04 仰賴集中式身分提供者
	佈景主題 4：管理身分：強制執行 MFA	需要根使用者的 MFA 透過 IAM Identity Center 需要 MFA 考慮要求 MFA 進行服務特定的 API 動作	SEC02-BP01 使用強大的登入機制
多重要素驗證用於驗證存取重要資料儲存庫的使用者。	佈景主題 4：管理身分：強制執行 MFA	考慮要求 MFA 進行服務特定的 API 動作	SEC02-BP01 使用強大的登入機制
多重要素驗證具有驗證器模擬的防護能力，並使用下列其中一種方法：使用者擁有的內容和使用者知道的內容，或使用者擁有的內容會由使用者知道或知道的內容解除鎖定。	請參閱實作多重要素驗證 (ACSC 網站）	不適用	不適用

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
成功和失敗的多重要素驗證會集中記錄並受到保護，免於未經授權的修改和刪除、監控入侵跡象，以及在偵測到網路安全事件時採取動作。	佈景主題 7：集中記錄和監控：啟用記錄 佈景主題 7：集中記錄和監控：集中日誌	在 帳戶中集中 CloudWatch Logs 以進行稽核和分析 (AWS 部落格文章） 集中管理 Amazon Inspector 集中管理 Security Hub CSPM 在 (AWS 部落格文章） 中建立整個組織的彙整工具 AWS Config 集中管理 GuardDuty 考慮使用 Security Lake 從多個帳戶接收 CloudTrail 日誌 將日誌傳送至日誌封存帳戶	SEC04-BP01 設定服務和應用程式日誌記錄 SEC04-BP02 在標準化位置中擷取日誌、調查結果和指標

定期備份

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
重要資料、軟體和組態設定的備份會根據業務連續性需求，以	主題 6：自動化備份：自動化資料備份和復原	在 上實作資料備份 AWS	REL09-BP01 識別並備份所有需要備份的

Essential Eight 控制	實作指引	AWS 資源	AWS Well-Architected 指引
協調和彈性的方式執行和保留。		大規模自動化資料備份 (AWS 部落格文章)	資料，或從來源複製資料 REL09-BP02 保護和加密備份 REL09-BP03 自動執行資料備份
從備份還原系統、軟體和重要資料都會以協調的方式進行測試，做為災難復原練習的一部分。	主題 6：自動化備份：自動化資料備份和復原 主題 6：自動化備份：跨 AWS Backup 結果實作控管	使用 自動化資料復原驗證 AWS Backup (AWS 部落格文章) 使用 AWS Backup Audit Manager 稽核政策 AWS Backup 的合規性	REL09-BP04 定期執行資料復原以驗證備份的完整性和程序
無權限帳戶和特殊權限帳戶（備份管理員除外）無法存取備份。	主題 6：自動化備份：在您的 AWS Backup 結果中實作控管	中保護備份的十大安全最佳實務 AWS(AWS 部落格文章) 使用 AWS Backup 保存庫鎖定來改善備份保存庫的安全性 使用 AWS Backup Audit Manager 稽核政策 AWS Backup 的合規性	SEC08-BP04 強制存取控制
無權限帳戶和特殊權限帳戶（不包括備份中斷玻璃帳戶）無法修改或刪除備份。			

注意

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。

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
最佳實務更新	我們已更新本指南，以反映 AWS Well-Architected Framework 安全支柱中的最新最佳實務。	2024 年 11 月 6 日
初次出版	—	2023 年 10 月 20 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

經常用於經常性問題的解決方案，其中解決方案具有反生產力、無效或比替代解決方案更有效。

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 ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、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。因此， 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)

一種工具，可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。 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。有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，並透過核准的程序，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的版本。

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) 執行試驗，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

部落格文章中的 Stephen Orban 定義了這些階段： AWS 雲端 企業策略部落格上的邁向雲端優先之旅和採用階段。如需有關它們如何與 AWS 遷移策略相關的詳細資訊，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

正在收集和處理其資料的個人。

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並排定優先順序。DVSM 擴展了最初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，其行為類似於文字。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 () 文件中的信封加密。 AWS Key Management Service AWS KMS

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給 LLM。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，已在廣義和未標記資料的大量資料集上進行訓練。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，以及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、特洛伊木馬程式、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

除了屬於組織一部分的管理帳戶 AWS 帳戶 之外的所有 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)

此 AWS 計畫提供諮詢支援、訓練和服務，以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 建議使用不可變基礎設施做為最佳實務。

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)

用於工業自動化的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，整合 OT 和資訊技術 (IT) 系統是工業 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)

當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。

設計隱私權

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)

管理產品整個生命週期的資料和程序，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

以預留位置值取代資料集中個人識別符的程序。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 Rs。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新放置

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 Rs。

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。

斯卡達

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 秘密中的內容？ Secrets Manager 文件中的 。

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。

未區分的任務

也稱為繁重工作，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，通常可接受中等速度的查詢。

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，讀取許多。

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瑕疵或漏洞。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。