雲端資安最佳實踐設計

Bard Lan, AWS 解決方案架構師
bardlan@amazon.com
Jun, 2022

雲的安全與合規基於對「共同責任模型」的認識

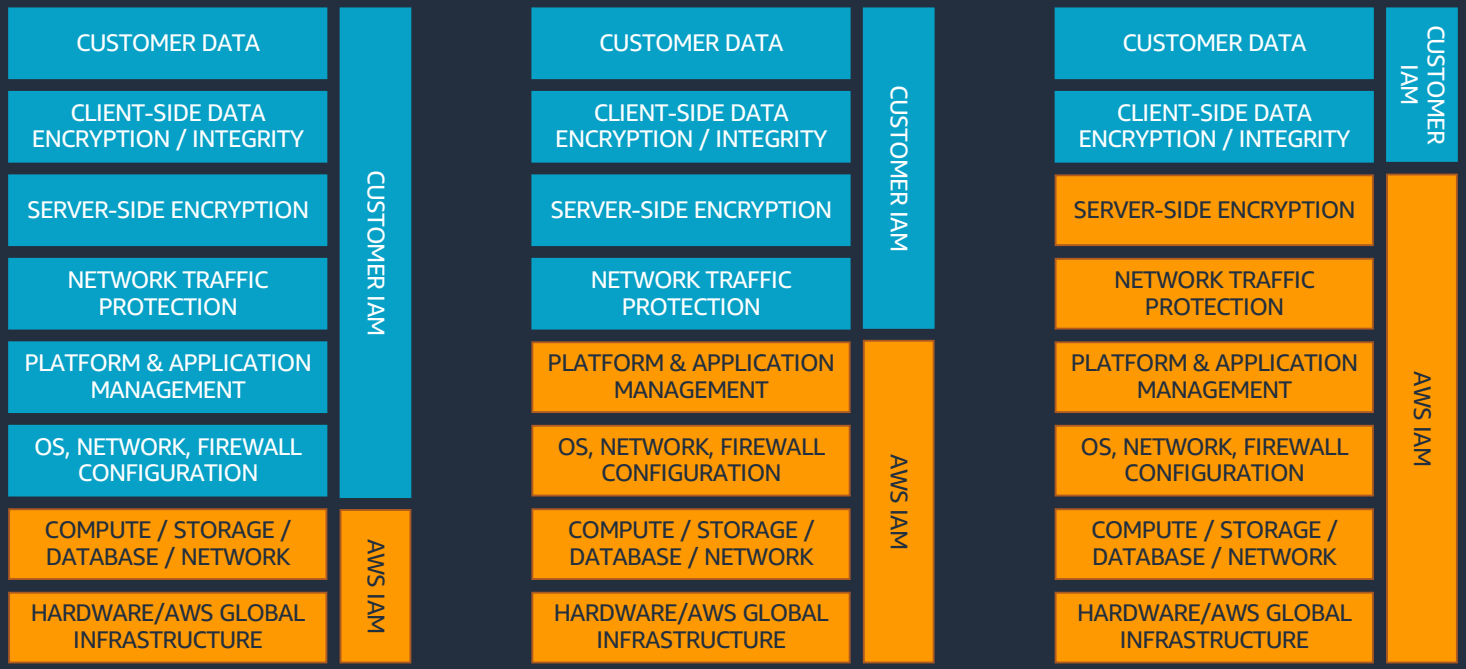
Compliance starts with the AWS "Shared Responsibility Model"

LINK: https://aws.amazon.com/tw/compliance/shared-responsibility-model/

雲上不同的服務類型具有不同的共同責任模型

Different shared responsibility model for different service types

More Customizable
+
More Customer Responsibility



Less Customizable
+
Less Customer Responsibility
+
More Best Practices built-in

AWS 定期受第三方公正組織稽核，並更新雲安全性與合規認證

Inherit global security & compliance controls

CSA cloud security alliance SM

ISO 9001 International Organization for Standardization

ISO 27001 International Organization for Standardization

ISO 27017 International Organization for Standardization

ISO 27018 International Organization for Standardization

PCI Security Standards Council PARTICIPATING ORGANIZATION

AICPA SOC — SOC 1

AICPA SOC — SOC 2

AICPA SOC — SOC 3

CJIS

FIPS 140-2 CRYPTOGRAPHY

FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA — DoD SRG

FR — FedRAMP

DEPARTMENT OF EDUCATION UNITED STATES OF AMERICA — FERPA

FFIEC Federal Financial Institutions Examination Council

C5

SECURITIES AND EXCHANGE COMMISSION — SEC Rule 17a-4(f)

G X P — GxP

HIPAA

International Traffic in Arms Regulations Compliant ITAR

MPAA

iDA SINGAPORE

マイナンバー — My Number Act

VPAT Section 508

FIEC

irap

정보보호관리체계인증 ISMS

G-Cloud

TISAX ENX ASSOCIATION

GDPR

CYBER ESSENTIALS PLUS

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad — Categoría ALTA — RD 3/2010

LINK: https://aws.amazon.com/tw/compliance/programs/

aws

提醒：使用 AWS 服務不表示您的應用就地合規

Applications built on top of AWS services are not implicitly compliant, customers need to get certified separately

Customer Applications

Your own accreditation

Your own certifications

Your own external audits

AWS Services

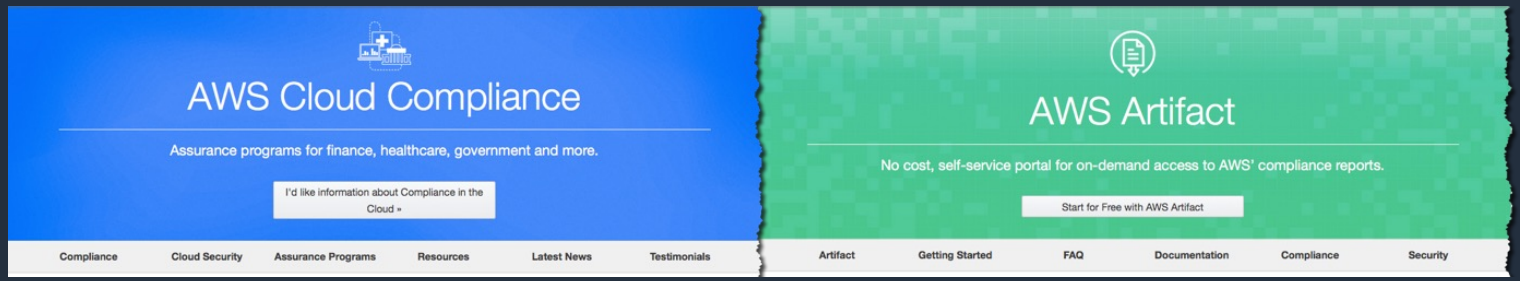
Applications built on top of AWS services, **are not implicitly compliant** to security controls (that AWS services are complaint with).

Customers need to **certify applications separately** by engaging with external auditors.

aws

Security **IN** the Cloud

Managed by **customers**



Security **OF** the Cloud

Managed by **AWS**

Well-Architected Tool

https://aws.amazon.com/well-architected-tool/

AWS Well-Architected Tool

Learn, measure, and build using architectural best practices

The AWS Well-Architected Tool helps you review your workloads against current AWS best practices and provides guidance on how to improve your cloud architectures. This tool is based on the AWS Well-Architected Framework.

Define a workload

Define a workload based on one of your existing cloud applications.

Define workload

Pricing (US)

Any usage	Free

Getting started

What is the AWS Well-Architected Tool?

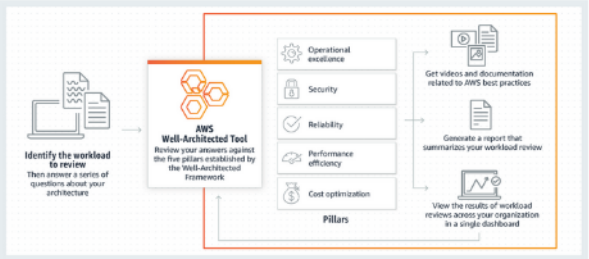
Getting started video

More resources

FAQ

AWS Well-Architected Partners

How it works



Benefits and features

Get architectural guidance

Access the

Enable consistent governance

Apply a consistent

Continuously improve architectures

Support continuous

AWS Well-Architected Framework

Identify the workload to review
Then answer a series of questions about your architecture

AWS Well-Architected Tool
Review your answers against the five pillars established by the Well-Architected Framework

Operational excellence

Security

Reliability

Performance efficiency

Cost optimization

Pillars

Get videos and documentation related to AWS best practices

Generate a report that summarizes your workload review

View the results or workload reviews across your organization in a single dashboard

LINK: https://aws.amazon.com/architecture/well-architected/

AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

讓人員遠離資料
Keep people away from data

為安全事件做準備
Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

讓人員遠離資料
Keep people away from data

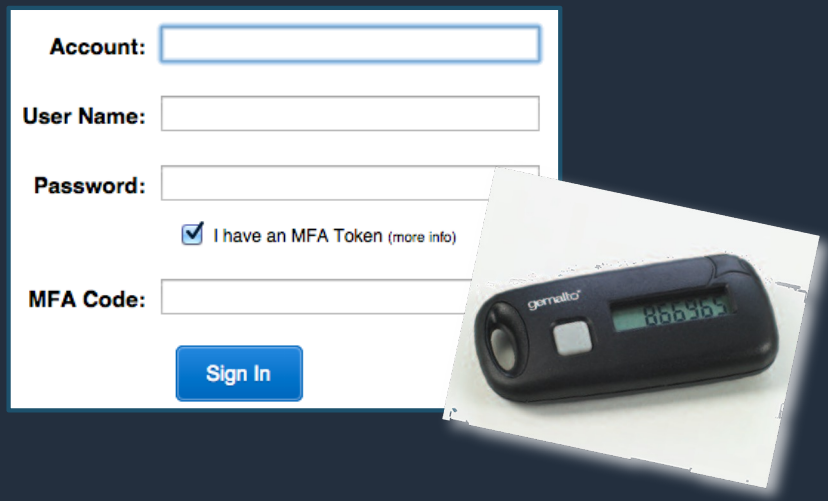
為安全事件做準備
Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

最佳實踐：啟用多重驗證 (Multi-factor Authentication)

AWS Management Console

Login with **Username/Password** with optional **MFA** (recommended)



API access

Access API using **Access Key + Secret Key**, with optional MFA

ACCESS KEY ID

Ex: `AKIAIOSFODNN7EXAMPLE`

SECRET KEY

Ex: `UtnFEMI/K7MDENG/bPxRfiCYEX`

最佳實踐：避免將憑證直接存放於硬碟或程式碼中

Assign Role to EC2 Instances instead of kept Access Key and Secret Access Key in disk

- 無需事先產生與分發憑證
  NO distribution of credentials
- 自動憑證變更 (rotation) 以避免固定憑證長期使用
  Automatic credentials rotation to mitigate the use of long term credentials

建立 IAM 角色以授予 S3 的存取權限
Create an IAM role to grant permissions to access S3

啟用 EC2 虛擬機，並套用該 IAM 角色
Launch an instance with the role

EC2 套用角色，並取得臨時憑證
assumes the role and delivers temporary credentials to the instance (metadata)

AWS CLI 及 SDK 自動使用該憑證
AWS CLI and SDK automatically use the credentials

LINK: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

最佳實踐：適當地授與所需的最低權限
Least Privilege Access to Data

安全最佳實踐 Security best practice

- 從最小的權限範圍開始
  Start with a minimum set of permissions
- 再根據需要賦予其他所需權限
  Grant additional permissions as necessary

僅定義所需的權限範圍 Define only the required set of permissions

- 個別服務的可操作動作
  What actions a particular service supports
- 特定任務的操作範圍
  What collection of API actions are required for the specific task
- 執行任務操作所需的具體權限
  What permissions are required to perform those actions

定期檢視未被利用的使用者、角色或權限
Review unused users/roles/policies periodically

AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

讓人員遠離資料
Keep people away from data

為安全事件做準備
Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

Amazon Virtual Private Cloud (VPC) 安全元件

Security Components

Virtual Private Cloud

設置 AWS 的邏輯隔離環境，使企業能在獨立的虛擬網路環境中使用各種 AWS 服務與資源

Provision a logically isolated cloud where you can launch AWS resources into a virtual network

Security Groups & ACLs

NAT Gateway

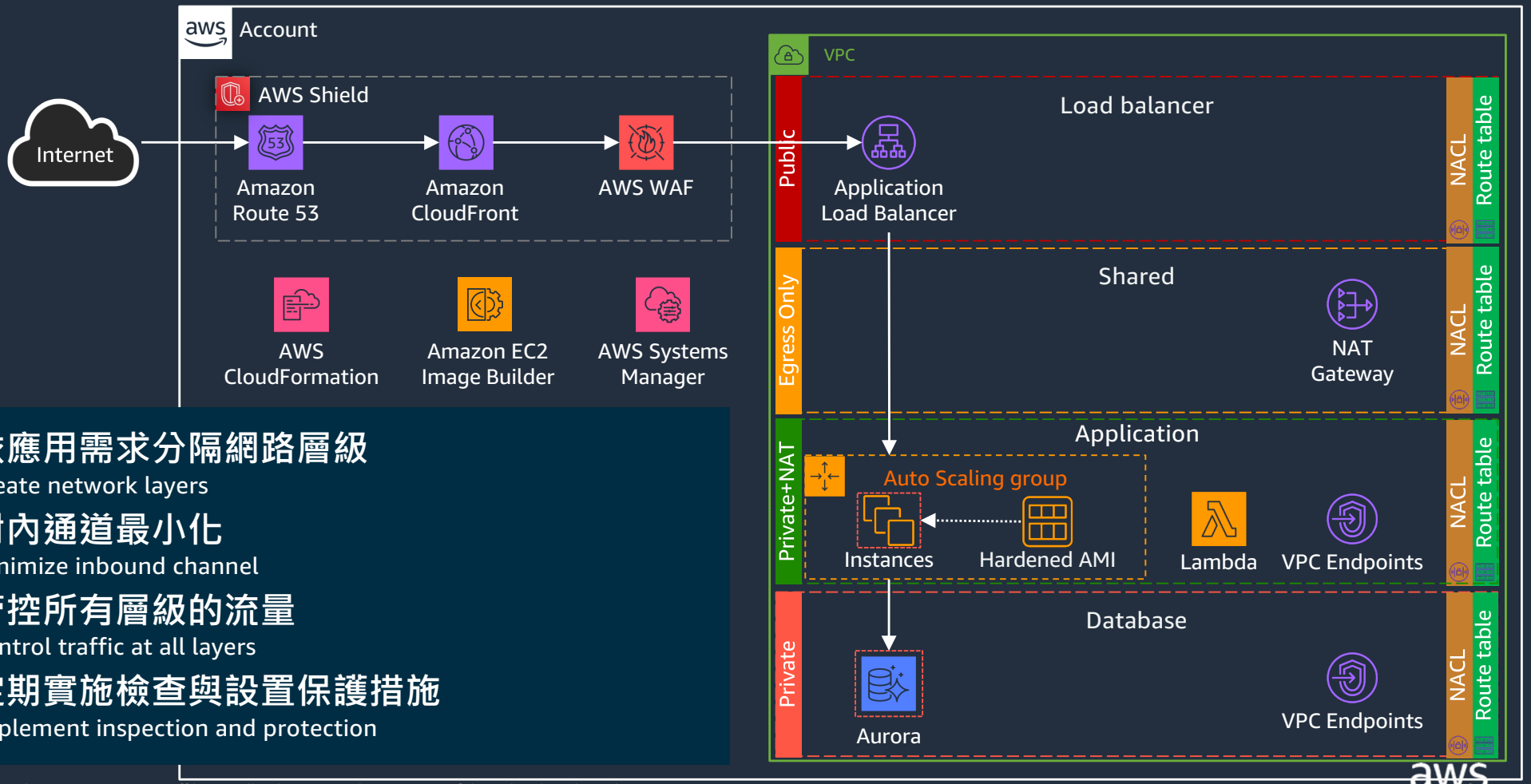
Flow Logs

VPC Endpoints

Private and secure connectivity to Amazon S3 and Amazon DynamoDB

最佳實踐：建構良善架構以最小化網路攻擊面

Well-architected



- **依應用需求分隔網路層級**
  Create network layers
- **對內通道最小化**
  Minimize inbound channel
- **管控所有層級的流量**
  Control traffic at all layers
- **定期實施檢查與設置保護措施**
  Implement inspection and protection

AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

讓人員遠離資料
Keep people away from data

為安全事件做準備
Prepare for security events

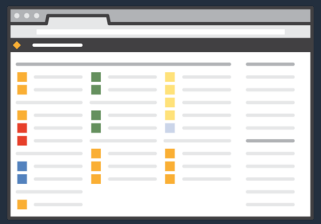
LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

AWS CloudTrail – 記錄帳號的 AWS API 存取日誌

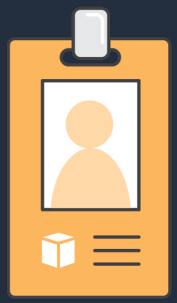
Web service that records AWS API calls for your account and delivers logs

John

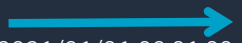
2021/01/01 00:01:00



Web console
54.2.1.100



Peter



2021/01/01 00:01:00

CLI
54.2.1.102

人 (Who)　時 (When)　地 (Where)

事 (What)

RunInstances

StopInstances

UpdateInstanceInformation

TerminateInstances

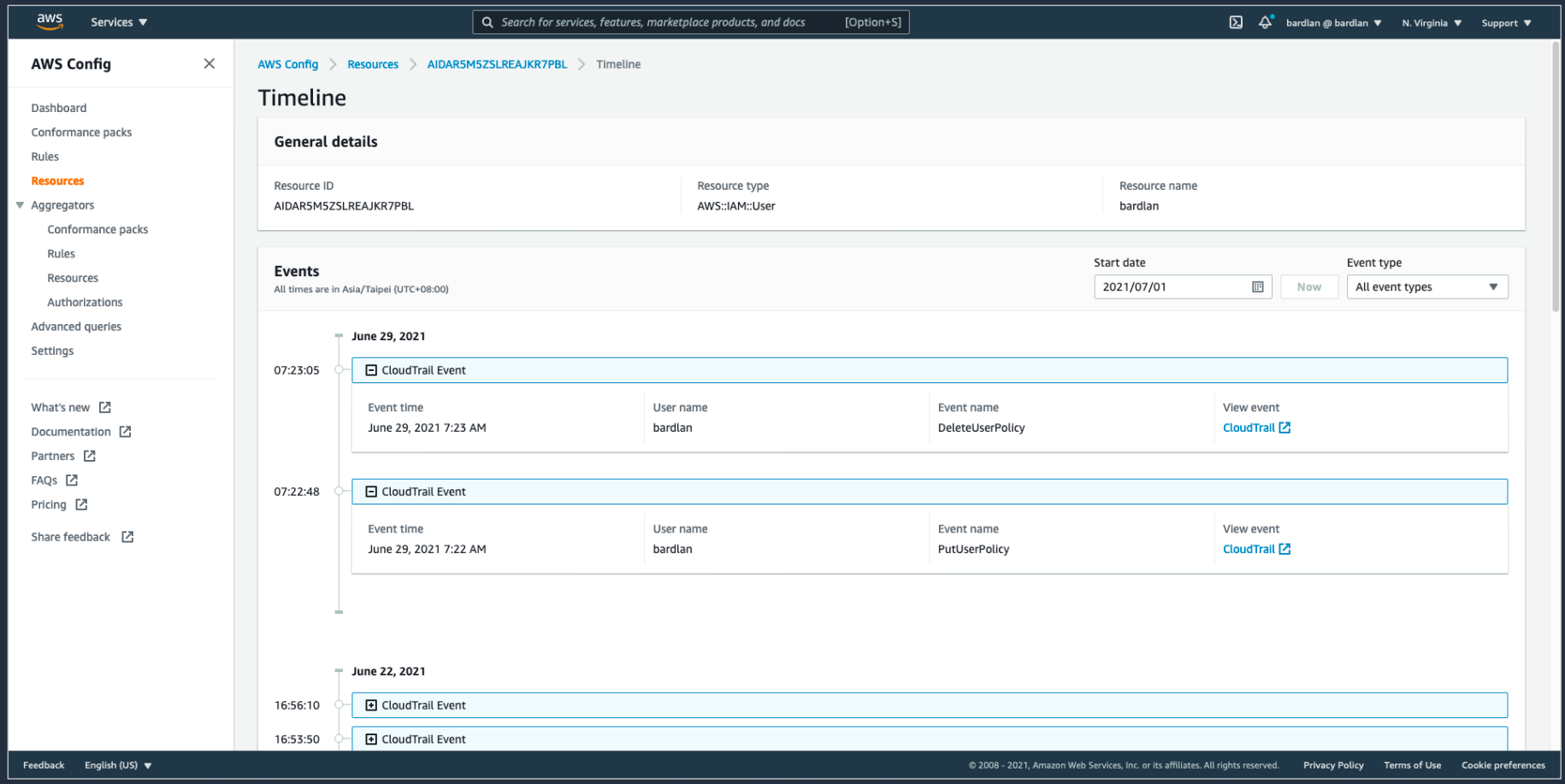
CreateBucket

UpdateSecurityGroup

物 (Which)

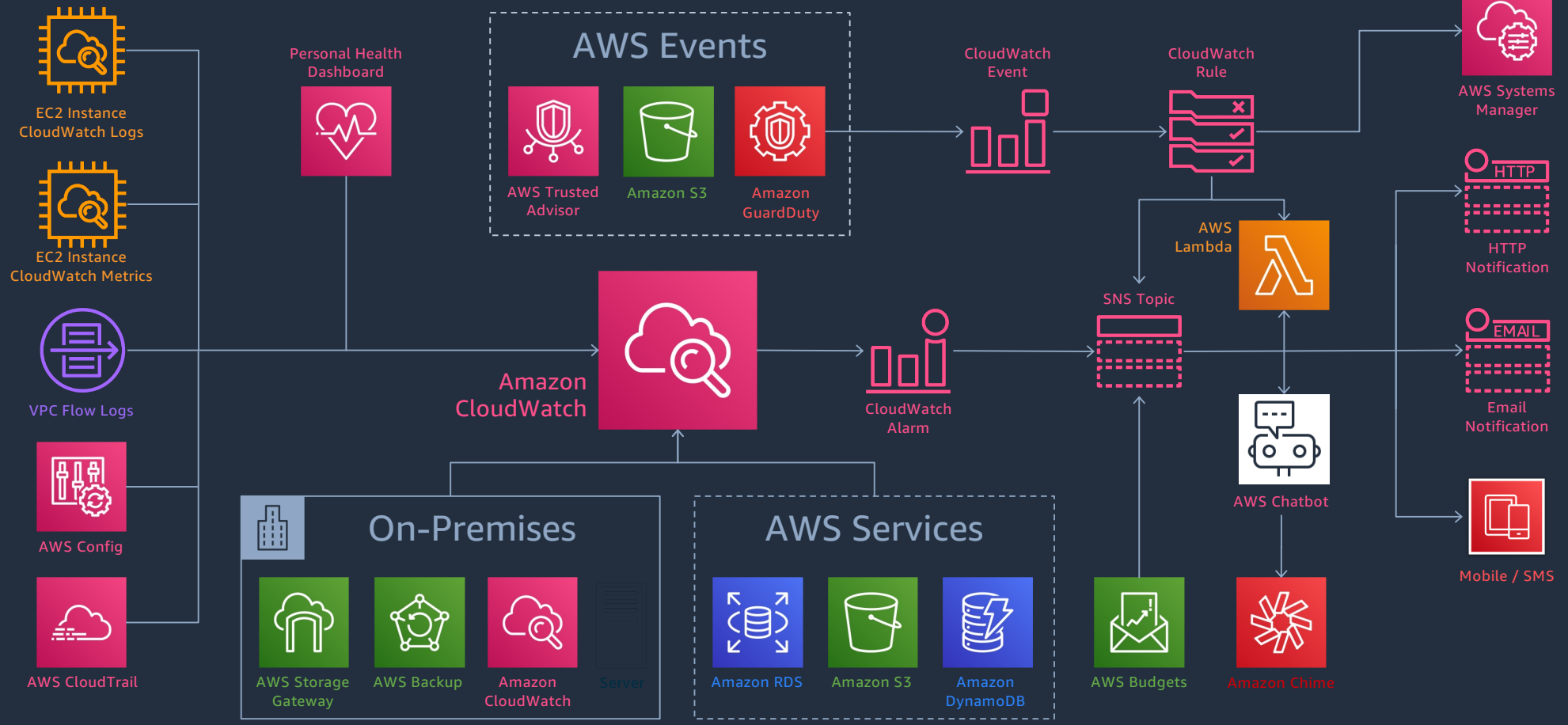
AWS Config - 記錄和評估您的 AWS 資源的配置

Record and evaluate configurations of your AWS resources



Amazon CloudWatch 自動化事件驅動整合架構

Integration architecture of Amazon CloudWatch



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

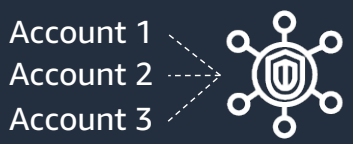
讓人員遠離資料
Keep people away from data

為安全事件做準備
Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

AWS Security Hub - 安全與合規中心

AWS Security Hub - Security and compliance center



可啟用到企業
所有的 AWS 帳號
Enable AWS Security Hub for all your accounts

持續彙總安全服務
的資安事件並確定
其優先等級
Continuously aggregate and prioritize findings

制定自動化合規掃描
與檢查
Conduct automated compliance scans and checks

根據安全事件發現
採取行動
Take action based on findings

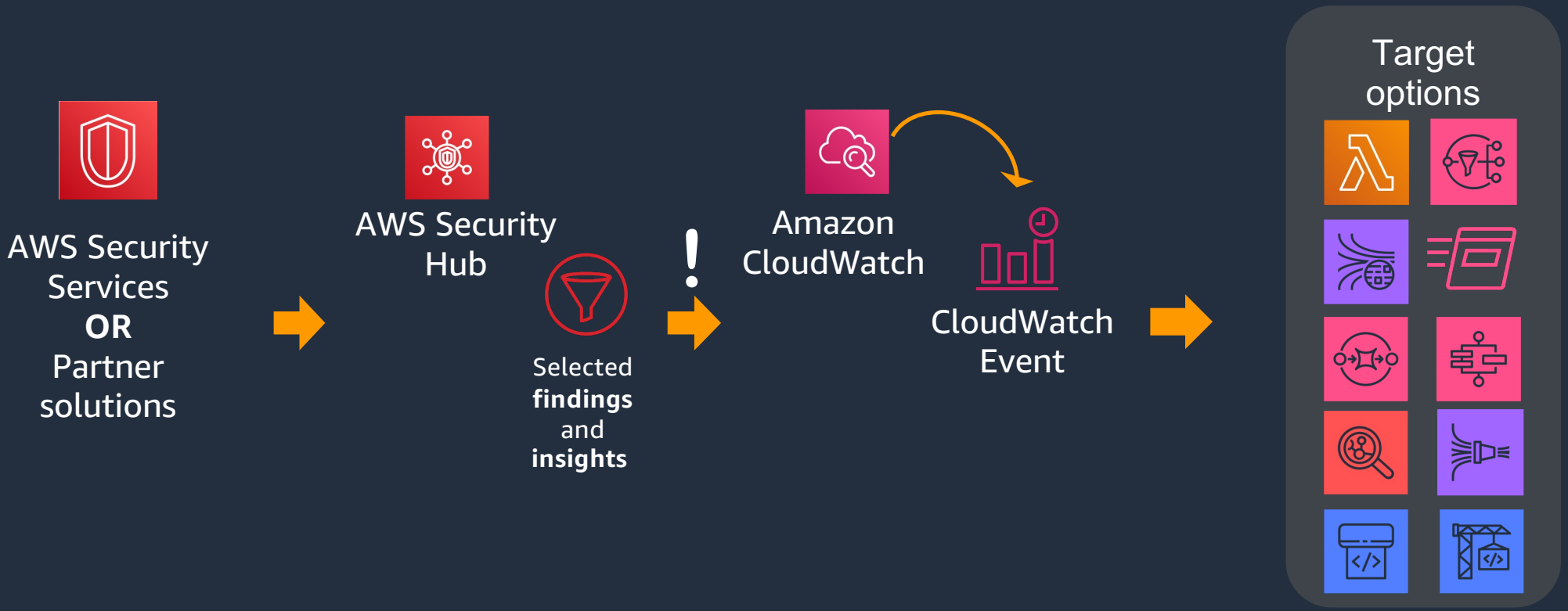
Better visibility into **security issues**. Easier to stay in **compliance**.

最佳實踐：啟用自動安全與合規檢查

Automated security checks

針對不安全或不符規的設定自動通報及採取行動

Take Action for Non-compliant configurations



偵測 Detect

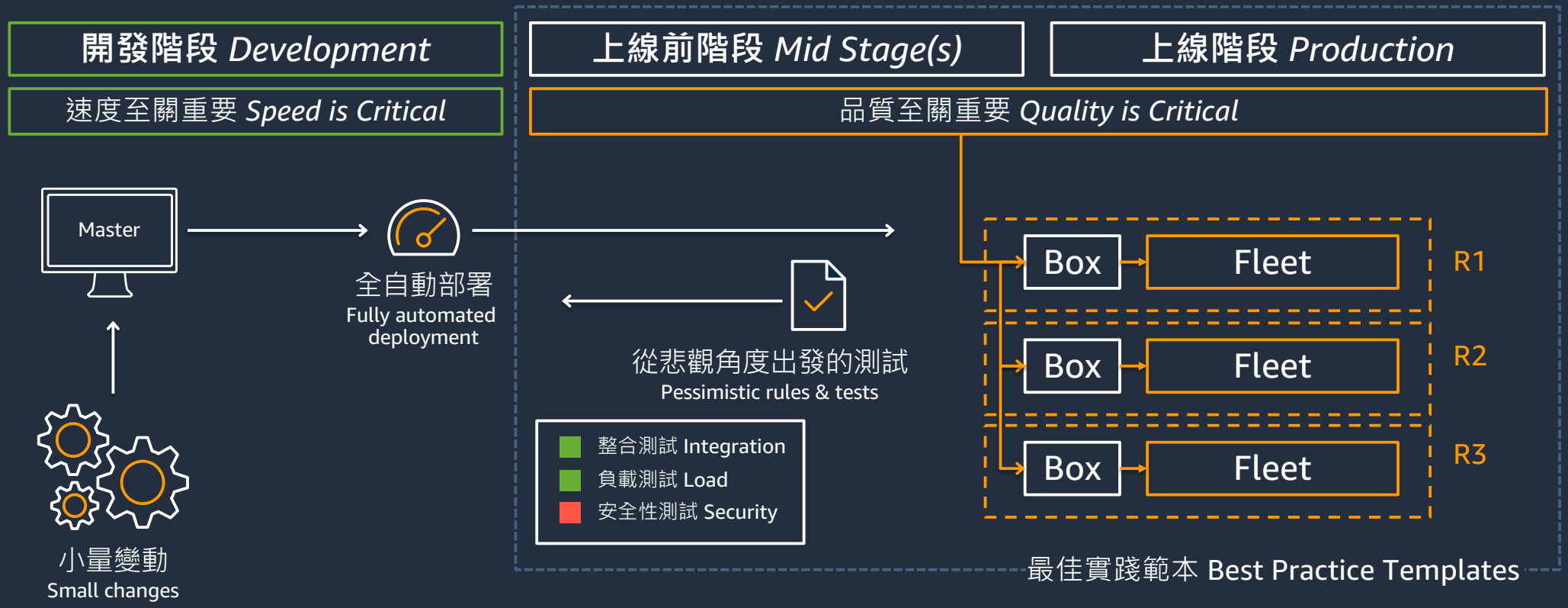
彙整 Aggregate

觸發通報 Report

採取行動 Take Action

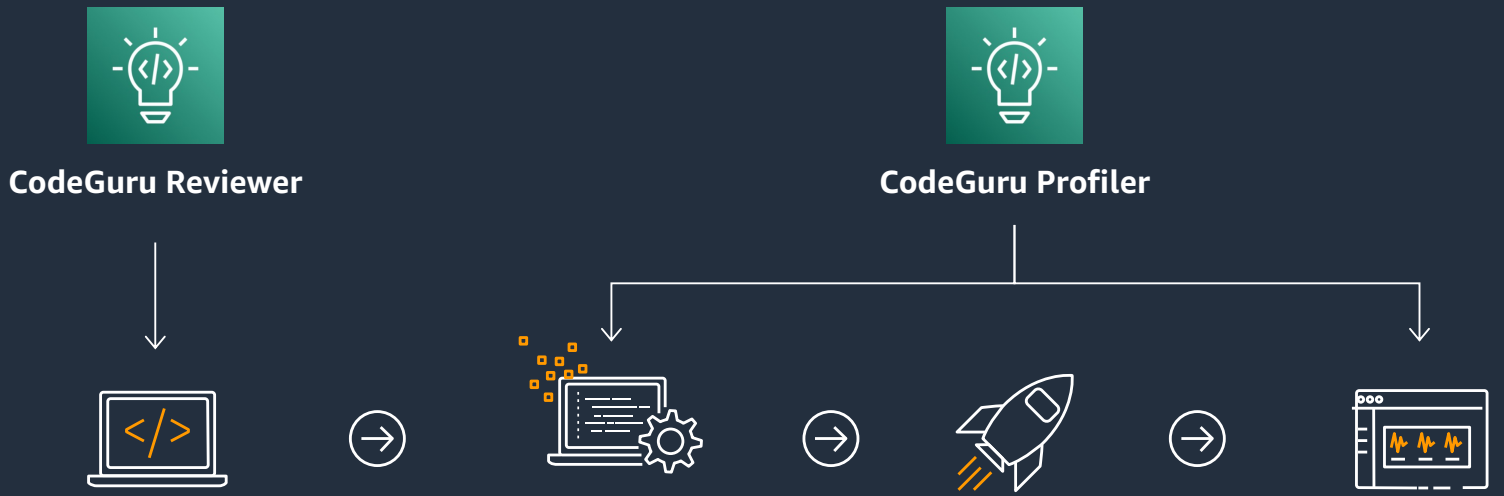
程式碼自動化持續整合、持續交付與部署

CI/CD



可藉助機器學習技術，自動執行程式碼檢測和效能優化

Automate code reviews and optimize application performance with ML-powered recommendations



AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

讓人員遠離資料
Keep people away from data

為安全事件做準備
Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

最佳實踐：啟用伺服器端預設加密

Enable default encryption

AWS Key Management Service (KMS)

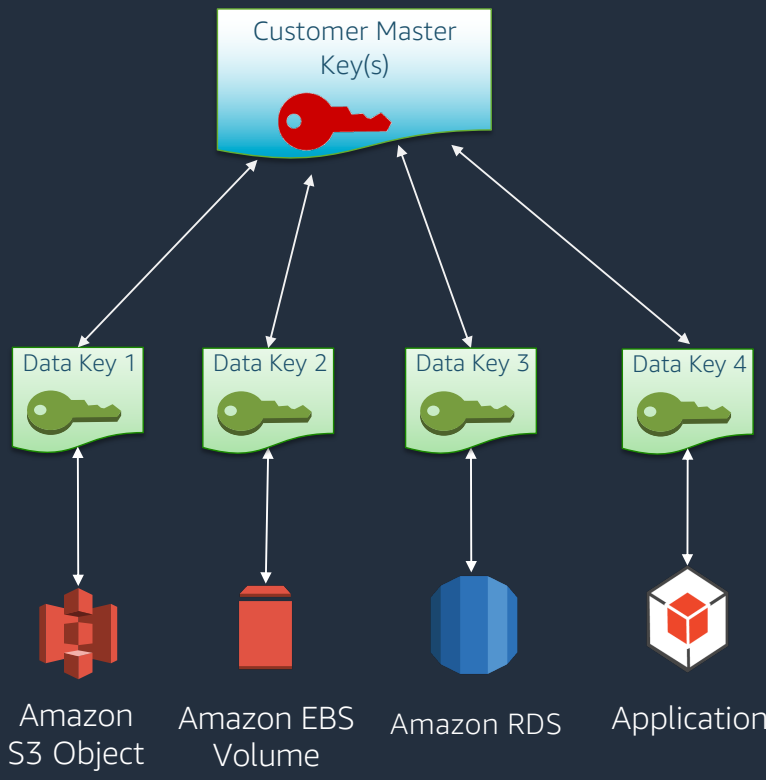
安全地創建、控制、輪換與使用加密金鑰的託管服務

Managed service to securely create, control, rotate, and use encryption keys

EBS | S3 | RDS | AWS SDK

AWS CloudTrail

- 集中式密鑰管理 (創建、刪除、檢視、策略權限設置)
  Centralized key management (create, delete, view, set policies)
- 匯入您自己的密鑰 (Import your own keys)
- 強制且自動的密鑰輪換 (Enforced, automatic key rotation)



LINK: https://aws.amazon.com/kms/

AWS 雲端環境安全設計原則

Design principles for security

建立強大的身份識別基礎
Implement a strong identity foundation

在所有網路層套用安全性
Apply security at all layers

啟用可追溯性
Enable traceability

自動化安全最佳實務
Automate security best practices

保護傳輸中資料和靜態資料
Protect data in transit and at rest

讓人員遠離資料
Keep people away from data

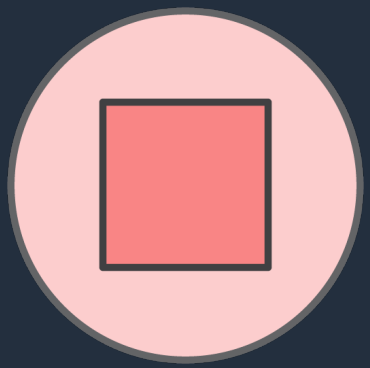
為安全事件做準備
Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

最佳實踐：讓人員遠離對資料的直接操作

keep people away from data

- 不儲存在非安全之處
  - Don't store
- 避免授與過大的權限
  - Don't grant



- 資料分類
  - Data categorization
- 重要資料加密儲存
  - Data encryption
- 機敏資料遮罩
  - Data masking
- 依需要去識別化
  - Tokenize data

- 規劃資料隔離策略
  - Isolate
- 應用工具來操作資料
  - Tooling
- 消除人員的直接操作
  - Eliminate human access

- 作業即程式碼
  - Infrastructure as code
  - Policy as code
- 版本控制
  - Version control

aws

AWS 雲端環境安全設計原則

Design principles for security

- 建立強大的身份識別基礎
  Implement a strong identity foundation
- 在所有網路層套用安全性
  Apply security at all layers
- 啟用可追溯性
  Enable traceability
- 自動化安全最佳實務
  Automate security best practices
- 保護傳輸中資料和靜態資料
  Protect data in transit and at rest
- 讓人員遠離資料
  Keep people away from data
- **為安全事件做準備**
  Prepare for security events

LINK: https://wa.aws.amazon.com/wat.pillar.security.zh_TW.html

持續追蹤最新安全威脅與補救建議

Keep up to date with security threats & recommendations

CVEs
Social media
Forums

Subscribe

Blogs

AWS Marketplace

https://aws.amazon.com/blogs/
https://aws.amazon.com/security/
https://cve.mitre.org/

定期舉辦災防演練

Run a gameday

各式雲端安全服務，協助客戶控管「雲中」的安全與合規

Aligning to the NIST Cybersecurity Framework (CSF) in the AWS Cloud (NIST 800-53)

廣泛安全合作夥伴與解決方案生態系上架在 AWS Marketplace

Largest ecosystem of security partners & solutions

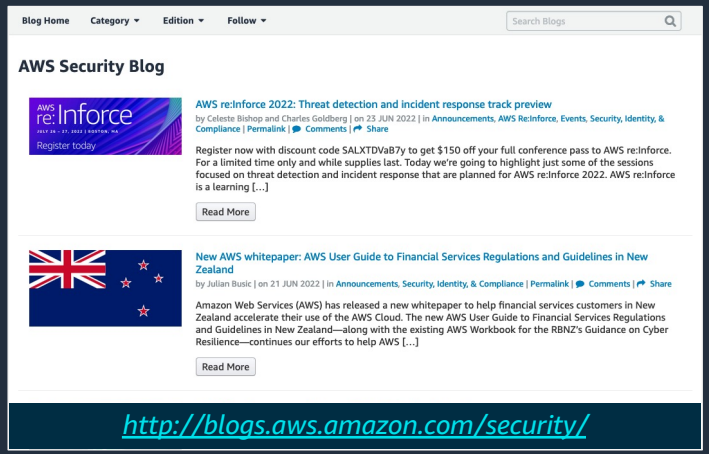
LINK: https://aws.amazon.com/marketplace/solutions/security

AWS 雲端安全學習資源

AWS Cloud Security Resources

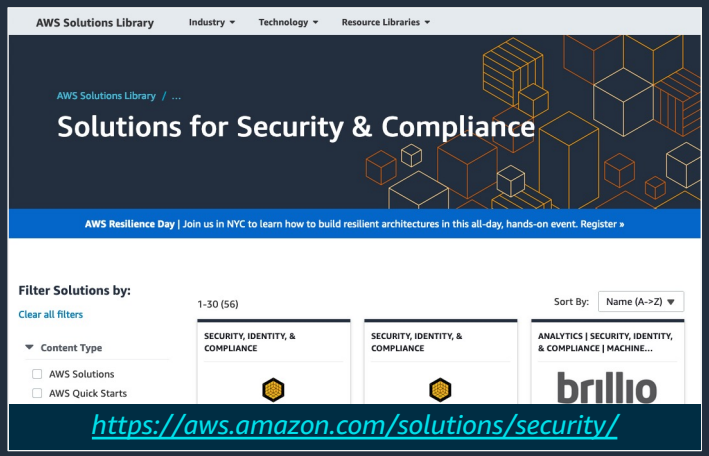
https://aws.amazon.com/security/

https://aws.amazon.com/security/security-bulletins/

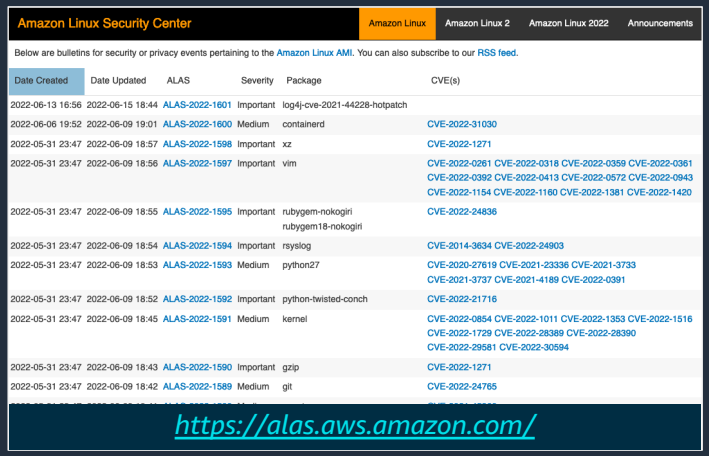


http://blogs.aws.amazon.com/security/

http://aws.amazon.com/security/security-resources/



https://aws.amazon.com/solutions/security/



https://alas.aws.amazon.com/

Thank you!