AWS Security Essentials (Traditional Chinese)

AWS Classroom Training

描述

本課程涵蓋基礎的 AWS 雲端安全概念，包含 AWS 存取控制、資料加密方法，以及如何保護 AWS 基礎設施的網路存取安全。根據 AWS 共同安全模型，您瞭解您在 AWS Cloud 中應負責落實安全性的位置、您可以使用的安全導向服務，以及安全服務有助於滿足貴組織安全需求的原因和方式。

目標對象

本課程適用於：

- 想了解雲端安全實務的安全性 IT 商業級專業人員
- 幾乎或完全不了解 AWS 的安全專業人員

課程目標

在本課程中，您將了解如何執行以下事項：

- 識別使用 AWS Cloud 的安全優勢和責任。
- 描述 AWS 的存取控制與管理功能。
- 說明在 AWS 中儲存資料時，為傳輸中資料和靜態資料加密的可用方法。
- 描述如何保護 AWS 資源的網路存取權。
- 判斷哪些 AWS 服務可監控運作情形及回應事件。

先決條件

建議參加本課程的學員具備以下條件：

- 具有 IT 安全實務與基礎設施概念的應用知識，並熟悉雲端運算概念

授課方式

本課程將結合以下方式授課：

- 課堂培訓
- 實作實驗室

aws training and certification

AWS Security Essentials (Traditional Chinese)

AWS Classroom Training

實作活動

本課程可讓您透過各種實作練習測試新技能，並將學到的知識應用到您的工作環境。

授課時長

1 天

課程大綱

本課程涵蓋下列概念：

單元 1：探索安全性支柱

- Well-Architected 架構：安全性支柱

單元 2：雲端安全性

- 共同責任模型
- AWS 全球基礎設施
- 合規與管控

單元 3：身分與存取權管理

- 身分與存取權管理
- 資料保護基本要點
- 實驗室 01 – 安全政策簡介

單元 4：保護基礎設施

- 保護網路基礎設施
- 節點安全性
- 保護運算資源
- 實驗室 02 – 使用安全群組保護 VPC 資源

單元 5：偵測及回應

- 監控和偵測控制
- 事件回應基本要點

單元 6：課程總結

- 課程總結和回顧

aws training and certification