104 年公務人員高等考試三級考試試題

類科：資訊處理

科目：資訊管理與資通安全

一、請敘述美國國家標準與技術局 (NIST) 定義「雲端運算 (Cloud Computing)」的「五大重要特徵 (Five Essential Characteristics)」之意涵。

【擬答】：

(一)

1. 隨需自助服務(On-demand Self-service)

消費者可依據需求狀況自行使用雲端服務，不需透過雲端供應者。

2. 廣泛網路存取(Broad Network Access)

雲端服務可隨時透過網路進行存取，且使用者均可透過標準機制使用網路。

3. 共享資源池(Resource Pooling)

雲端運算資源彙整讓雲端供應者透過多租戶模式(Multi-tenancy)服務消費者，依據消費者要求，來指派或重新指派實體及虛擬資源，消費者通常不必知道所有資源確切位置。其中資源包括儲存、處理、記憶、網路頻寬和虛擬機等。

4. 快速彈性(Rapid Elasticity)

雲端運算具有彈性可以快速重新佈署，即能因應需求彈性且快速調整資源規模大小。

5. 可衡量的服務(Measured Service)

雲端服務各層次均由雲端供應者掌控與監管計算服務量測，確保資源使用可被監測、被控制和被報告，為供應者和消費者雙方提供透明化服務使用資訊。

(二)

1. 財務面雲端優勢

- (1) 降低資本支出
- (2) 降低管理負擔與成本
- (3) 產業經濟資源的最佳配置與使用率
- (4) 組織內部MIS人員需求減少

2. 技術面雲端優勢

- (1) 可擴充性
- (2) 品質可靠性與安全性
- (3) 可隨著雲端服務提供者持續提升技術

3. 維運面雲端優勢

- (1) 快速提供性
- (2) 彈性
- (3) 設備與地點的取得性
- (4) IT嵌入各單位內提供服務支援

二、何謂「政府資料開放 (Open Government Data)」？根據資料的「使用」、「散布」與「分享」說明其特性。政府資料開放有何種重要性？請舉例說明之。

【擬答】：

(一) 依照行政院及所屬各級機關政府資料開放作業原則，政府資料開放是指政府資料以開放格式於網路公開，提供個人、學校、團體、企業或政府機關等使用者，依其需求連結下載及

利用。

(二)政府資料開放的特性

- 1.各機關依作業原則規定，於政府資料開放平臺集中公開列式之資料，以無償及非專屬授權方式授權使用者得不限時間及地域，重製、改作、編輯、公開傳輸或為其他利用方式，開發各種產品或服務（以下簡稱加值衍生物），提供公眾使用，無須取得各資料提供機關之書面或其他方式授權，但授權範圍不包含商標權及專利權。
- 2.各機關開放之資料集，不得任意分割，以確保其完整性，並應強化資料品質，力求資料之正確性及時效性。資料集應採開放格式提供，逐步達成機器對機器識別讀取及利用。
- 3.以允許使用者自由加值應用為原則；資料內容有限制使用之必要時，應於使用規範中定明其使用限制。
- 4.以無償提供為原則。但有特殊業務需求者，得約定收費方式及金額，並定期檢討該約定；其收費，並得依資料使用目的或使用模式約定不同費率。

(三)政府資料開放的重要性

- 1.滿足民眾資料使用需求，以促使跨機關資料流通，增進施政效能，提升民眾生活品質，強化民眾監督政府的力量。
- 2.結合民間無限創意，活化政府資料應用，進一步提升政府資料品質及價值。
- 3.創新政府服務，並透過開放授權民間應用，創造資訊服務產業發展契機。

三、

(一)在「網路鑑識 (Network Forensics)」中，蒐集「網路數位證據 (Network Digital Evidence)」是重要的一環。詳細分析存在於客戶端、伺服器端以及網路設備的網路數位證據，並舉例說明。

(二)分析「瀏覽器」與「網路數位證據」之關係。

【擬答】：

(一)

1.客戶端的電腦紀錄

- (1)系統稽核紀錄：包括System log、Error log、Access log等
- (2)Internet Cookies：Cookies是儲存於客戶端，供瀏覽器與Web伺服器互通資料用的純文字檔 (.txt)。
- (3)快取 (Internet Cache)：儲存網頁瀏覽紀錄。
- (4)防毒軟體：包括病毒掃描結果與Logs。
- (5)入侵偵測軟體：包括軟體式入侵偵測系統之Logs。
- (6)電子郵件軟體：包括電子信箱帳號、電子郵件 (電子郵件資訊與收、發信件內容)、通訊錄等。
- (7)網路連線紀錄：包括查看網路連線資料，包括連結之IP位址、埠號、服務與封包傳輸流量等。

2.網站伺服器端的電腦紀錄

例如Web logs，這是伺服器網站稽核日誌。

3.各種網路設備：例如稽核日誌，包括 Hub、Gateway、Proxy Server、防火牆、入侵偵測系統等設備之 Logs 等紀錄。

(二)瀏覽器會將之前瀏覽的網頁，儲存在快取 (cache) 裡，當再次瀏覽相同網頁時，將瀏覽到儲存在快取裡的舊網頁 (離線可觀賞網頁)，例如在微軟IE瀏覽器必須按下的「重新整理」按鈕才能重新取得最新頁面。微軟Windows作業系統將快取存在「Temporary Internet

Files」資料夾中。

四、

- (一)何謂「數位憑證 (Digital Certificate)」？數位憑證有哪些種類？分別說明其用途。
- (二)試說明數位憑證在設計「Diffie-Hellman 金鑰交換協定 (Diffie-Hellman Key Exchange Protocol)」的用處。

【擬答】：

- (一)數位憑證 (digital certificate) 是一個存在電腦內用來辨識您身分的一個檔案。一般包含了持有人的公開金鑰、持有人的姓名及電子郵件地址、公開金鑰的有效期限、發行者名稱、數位憑證的序號、發行者的數位簽章。
- (二)有四種在網際網路上使用的數位認證：
1. 個人憑證：用來識別個人，以驗證使用者與一個伺服器，或者若要啟用安全的電子郵件使用 S Mime。
 2. 伺服器憑證：識別參與與其他電腦使用的通訊協定，例如 SSL 的安全通訊的伺服器。這些憑證允許伺服器以驗證其用戶端的身分。伺服器憑證依照定義公開金鑰密碼編譯標準(PKCS) 的 X.509 憑證格式。
 3. 軟體發行者的憑證:用來簽署軟體透過網際網路散發。
 4. 憑證授權單位憑證：驗證 CA，分成根憑證授權單位及中繼憑證授權單位的兩種類別。根憑證是自我簽署，表示憑證的主體也憑證的簽署人。根憑證授權單位有能力為中繼憑證授權單位指派憑證。一個中繼憑證授權單位有能力的其他中繼憑證授權單位發出伺服器憑證、個人憑證、發行者憑證。
- (三) Diffie-Hellman 金鑰交換協定是一種安全協定。它可以讓雙方在完全沒有對方任何預先資訊的條件下通過不安全訊息通道建立起一個金鑰。這個金鑰可以在後續的通訊中作為對稱金鑰來加密通訊內容。這是最早提出公開金鑰密碼系統的概念，但沒有真正地利用公開金鑰去對訊息做加解密，而是利用公開金鑰的概念來幫助通訊雙方可以安全地協議出一把共同的交談金鑰(Session Key)，真正的加解密工作是利用所協議出來的這把交談金鑰(本題中所指的數位憑證)，透過 DES 或 AES 等對稱式的密碼系統來完成。