適用於 IT 人員的 Adobe Creative Cloud 安全性常見問答集

在 Adobe 收到有關 Creative Cloud 的問題中，安全性、隱私權和規範政策就是部分最常見問題的領域。使用 Creative Cloud 的組織會擔心資料的安全以及資料的存取權是否可靠。本文件旨在解答 IT 安全性人員在考慮使用 Creative Cloud 時針對這些主題提出的許多常見問題。

1 Creative Cloud 架設在哪裡？

Creative Cloud 是由 Amazon Web Services (AWS) 代管，包括 Amazon Elastic Compute Cloud (Amazon EC2) 和 Amazon Simple Storage Service (Amazon S3)，主機架設於美國、歐洲和亞太地區。AWS 為全世界數千家企業所使用的軟體服務提供了一套可靠的平台。AWS 會根據安全性最佳作法提供服務，並且通過業界公認的認證與稽核 (aws.amazon.com/security/)。這表示，Creative Cloud 會員將可享有 Amazon 致力於保障儲存資產安全的一貫承諾。

2 客戶資料位於何處？

客戶資料儲存在 Amazon S3 中，而且 Adobe 會指定個別客戶資料與伺服器所在的實際地區。Amazon S3 資料物件的資料複寫作業是在地區叢集內部完成，不會複寫到其他地區的資料中心叢集。Adobe 營運 Creative Cloud 的地區有三個：美國、歐洲和亞太地區。

範例：根據預設，歐洲 Creative Cloud 客戶的所有資料會將其雲端資料儲存在歐洲的 AWS 資料中心，而且這些資料不會傳送到歐洲以外的資料中心。

3 誰能控制 Creative Cloud 資料中心？

對於 AWS 中部署的 Creative Cloud 部分，Amazon 控制了實體元件。為了協助客戶深入了解 AWS 擁有哪些控制措施以及這些控制措施的實際運作方式，AWS 發行了一份 Service Organization Controls 1 (SOC 1), Type 2 報告 (aws.amazon.com/security/)，其中定義關於 Amazon EC2、Amazon S3 和 Virtual Private Cloud (VPC) 的控制，以及詳細的實體安全性與環境控制。這些控制的定義相當明確，應該能夠符合大多數客戶的需求。

4 Amazon 是否允許客戶參觀 AWS 資料中心？

不允許。鑑於 AWS 資料中心代管了多位客戶的資料，所以 AWS 不允許客戶參觀資料中心，因為此舉會導致第三方實際接觸眾多客戶。為了符合這項客戶需求，獨立的主管稽核員會驗證 SOC 1 Type 2 報告中的控制是否存在且正常運作。在控制措施的成效方面，這種廣為接受的第三方驗證為客戶提供了超然的觀點。Adobe 已經與 AWS 簽署了一份非公開合約，而且能夠取得 SOC 1 Type 2 報告的副本 (aws.amazon.com/security/)。資料中心實體安全性的獨立審核也屬於 AWS ISO 27001 稽核、PCI 評估以及 ITAR 稽核程序的一部分。

5 是否允許第三方存取 AWS 資料中心？

AWS 嚴格控制資料中心的存取權，即使是內部員工也一樣。除非適當的 AWS 資料中心管理員依據 AWS 存取政策明確核准，否則第三方無法獲得 AWS 資料中心的存取權。請參閱 SOC 1 Type 2 報告 (aws.amazon.com/security/) 以了解與實體存取有關的特定控制、資料中心存取授權和其他相關控制。

6 誰負責修補？

Adobe 負責修補我們在 AWS 中執行的客體作業系統 (OS)、軟體和應用程式。AWS 負責修補支援 AWS 服務傳遞的系統，例如 Hypervisor 和網路服務。這種修補作業的進行方式是 AWS 政策的要求，而且符合 ISO 27001、NIST 和 PCI 規定。

7 授權動作是否受到監視和控制？

控制措施限制了系統和資料的存取權，而資料也受到限制和監視。此外，客戶資料和伺服器實例預設以邏輯方式與其他客戶隔離。在 AWS SOC 1、ISO 27001、PCI、ITAR 和 FISMA 稽核期間，獨立稽核員會審核 AWS 基礎結構的授權使用者存取控制。

8 雲端提供者是否能解決內部人員不當存取客戶資料和應用程式的威脅？

AWS 提供了特定的 SOC 1 (涵蓋在 SOC 1 Type 2 報告中) (aws.amazon.com/security/)。此外，Adobe 也會針對內部人員存取的控制和監視方式執行定期的風險評估。

9 Creative Cloud 如何隔離客戶資料？
Adobe 代表客戶儲存的所有資料都具有強大的租用戶隔離安全性與控制功能。Creative Cloud 儲存空間所運用的 Amazon S3 提供了先進的資料存取控制。

10 客戶隔離的實作方式是否安全？
AWS 環境是一種虛擬化的多租用戶環境。AWS 已經實作了安全性管理程序、PCI 控制以及其他專為隔離客戶所設計的安全性控制。AWS 系統的設計可以防止客戶通過虛擬化軟體存取未受指派的實體主機或實例。這種架構已經由獨立的 PCI Qualified Security Assessor (QSA) 驗證，而且證實符合 PCI DSS 2.0 的所有規定 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/)。

11 AWS 是否解決了已知的 Hypervisor 弱點？
Amazon EC2 目前採用 Xen Hypervisor 的高度自訂版本。在評估與稽核期間，獨立稽核員會定期評估 AWS Xen Hypervisor 安全性。請參閱 AWS 安全性白皮書 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) 以取得有關 Xen Hypervisor 和實例隔離的詳細資訊。

12 提供的服務是否支援加密？
Creative Cloud 會使用 SSL 來加密傳送中的資料。

13 雲端提供者對於客戶資料擁有哪些權限？
Creative Cloud 客戶保有資料的控制和所有權。請檢閱 Adobe 的使用條款 (www.adobe.com/go/gffooter_terms_of_use) 和隱私權政策 (www.adobe.com/privacy/policy.html) 以了解詳細資訊。

14 AWS 是否發行其實體與環境控制？
是。實體與環境控制已明確概述於 SOC 1 Type 2 報告中 (aws.amazon.com/security/)。此外，AWS 也支援 ISO 27001 和 FISMA 認證，這些認證要求最佳作法的實體與環境控制。

15 客戶是否能從電腦和行動裝置等用戶端保護及管理 Creative Cloud 的存取權？
是。Creative Cloud 可讓客戶依照自己的需求管理用戶端與行動裝置存取權。

16 AWS 是否允許客戶保護其虛擬伺服器？
是。Adobe 已經根據業界最佳作法，在 AWS 之上實作自己的安全性架構，包括 SANS Top 20 Controls for Internet Security、Consensus Audit Guidelines、NIST 方針以及網際網路標準。

17 AWS 是否包含身分識別與存取管理 (IAM) 功能？
AWS 具有一套身分識別與存取管理方案，讓 Adobe 能夠集中管理使用者身分識別、指派安全性認證、組織使用者群組以及管理使用者權限。

18 Adobe 是否會讓 Creative Cloud 系統停機以進行維護？
Creative Cloud 採用的實作方式讓系統幾乎不需要停機。因為使用了 A/B 環境以及其他允許即時切換的機制，在系統外部察覺不到停機，所以新增部署期間仍然可以存取和連接服務。

19 AWS 如何抵禦分散式阻斷服務 (DDoS) 攻擊？
AWS 網路所提供的保護機制能有效抵禦傳統的網路安全性威脅。請參閱 AWS 安全性白皮書 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) 以取得有關本主題的詳細資訊，包括 DDoS 的討論。

20 Adobe 是否針對 Creative Cloud 提供業務續航力方案？
AWS 提供了業務續航力計畫 (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) 而且 Creative Cloud 的設計能夠充分運用多個地區與多個可用區域或資料中心。Adobe 設計、建構和實作的 Creative Cloud 採用資料備援複寫，以及多地區/可用區域部署架構。

21 AWS 是否指定資料耐用性？
Creative Cloud 將資料儲存在 Amazon S3 中，這項服務提供了耐用的儲存基礎結構。物件是以備援方式儲存在 Amazon S3 地區中多個設施間的多部裝置上。一旦儲存資料之後，Amazon S3 就會快速偵測並修復任何遺失的備援性，藉以維持物件的耐用性。Amazon S3 也會定期使用總和檢查碼來驗證儲存資料的完整性。如果偵測到損毀，系統就會使用備援的資料進行修復。

22 Adobe 是否計畫取得 Federal Information Security Management Act (FISMA) 規範？
Adobe 目前沒有針對 Creative Cloud 取得聯邦資訊安全管理法 (FISMA) 規範的立即計畫。

23 Creative Cloud 是否符合 HIPAA？

Adobe 無意證明 Creative Cloud 符合 1996 年的健康保險隱私及責任法案 (HIPAA)，因為 Creative Cloud 並非用於處理醫療記錄。

參考資料

《Overview of AWS Security Practices Whitepaper》，2013 年 3 月
(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

《AWS Risk and Compliance Whitepaper》，2013 年 1 月
(media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com