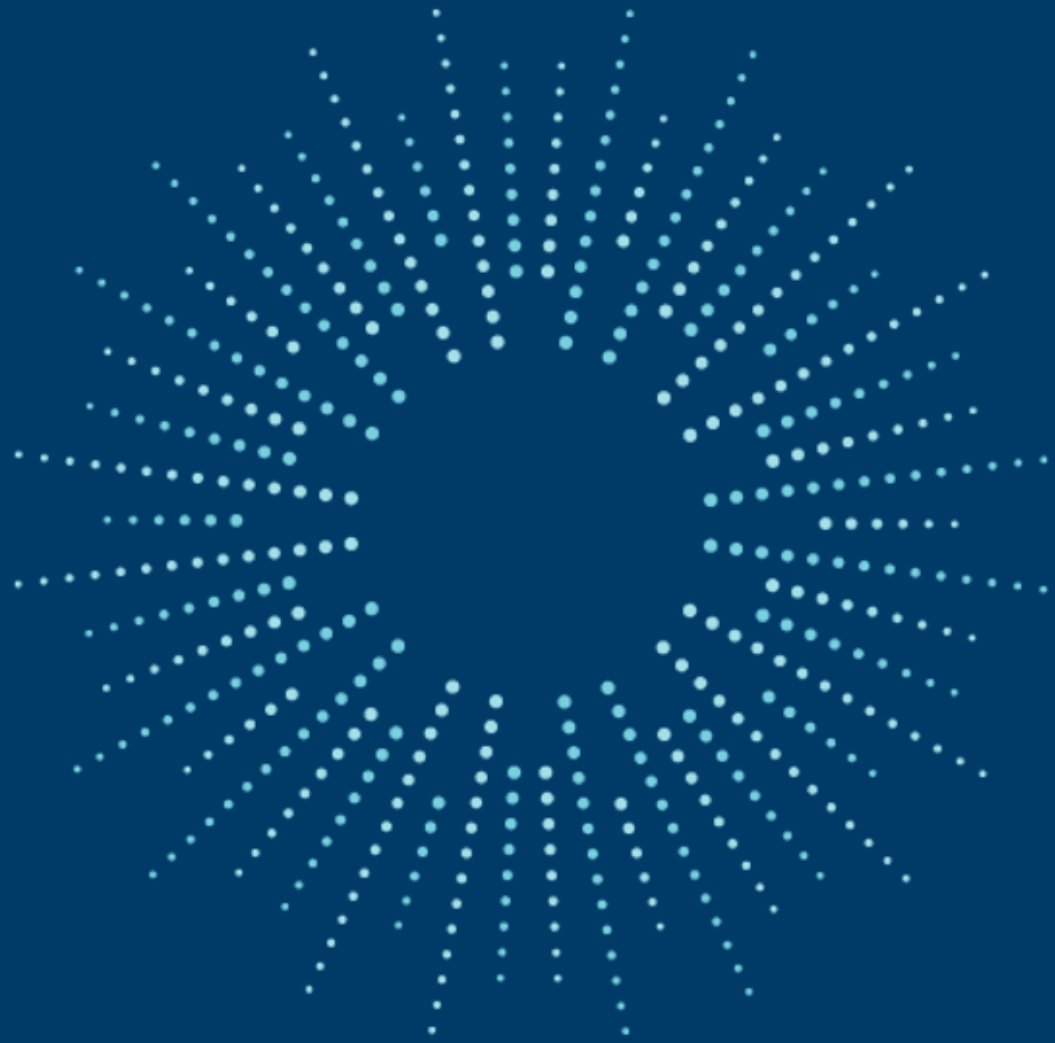
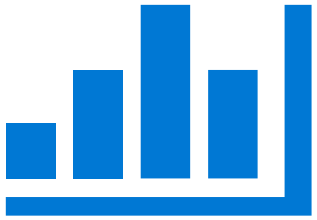
Microsoft Azure
使用 Intel 機密運算
技術之發展現況

2023/3/23

李匡正
雲端解決方案架構師
全球合作夥伴解決方案事業群
台灣微軟

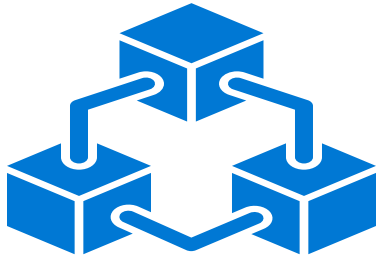


Microsoft Azure 與 Intel 間的合作關係



企業應用

SAP on Azure

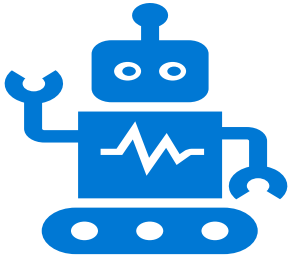


高效能運算

HPC workloads on Azure

機密運算

Confidential Computing

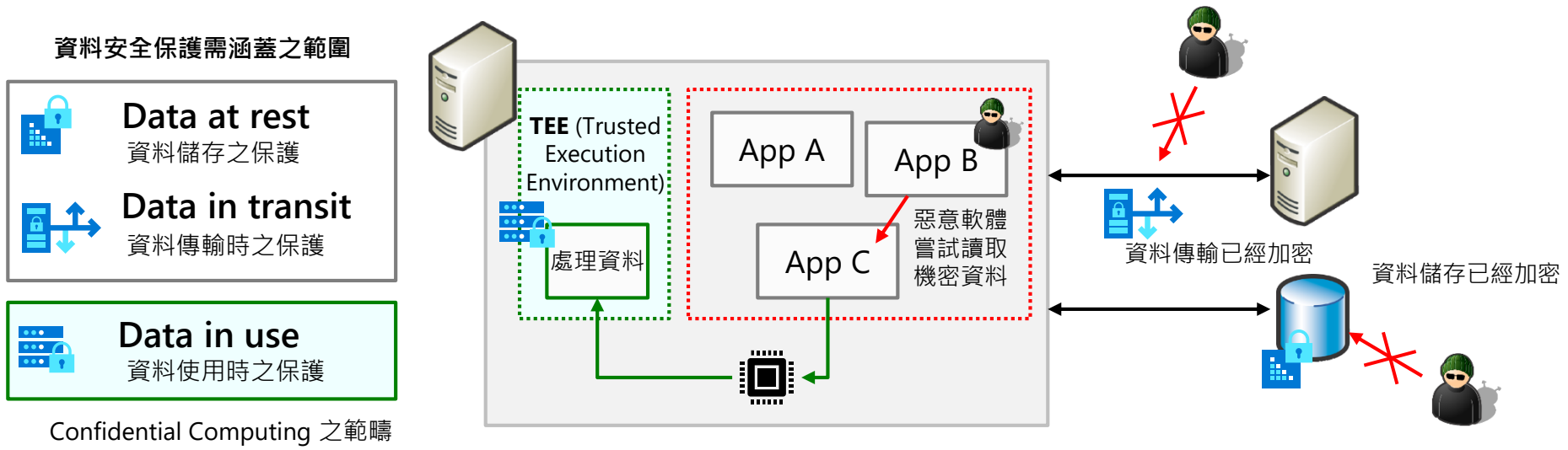


人工智慧

AI on Azure

何謂 Confidential Computing ?

- 簡而言之，是利用硬體保護執行期間記憶體中的資料之技術總稱
  - 儲存與網路傳輸的資料通常已經加密，而記憶體中的資料則未加密，因此可能會受到鄰近被入侵之程式或 VM 之惡意攻擊
  - 透過硬體技術而非軟體技術來確保記憶體中的資料被安全地處理以避免資安風險
  - 利用硬體在記憶體空間中建立可以被信賴，安全處理資料的 TEE 環境，以供 VM、容器、應用程式執行時使用
  - TEE = Trusted Execution Environment 受信賴之隔離執行環境 (記憶體空間)
  - 可防範已被植入 Kernal 層級之惡意軟體來竊取記憶體內資訊，或肇因於虛擬機器 Hypervisor 層級之漏洞，讓惡意軟體能對鄰近 VM 發動攻擊竊取記憶體內資訊



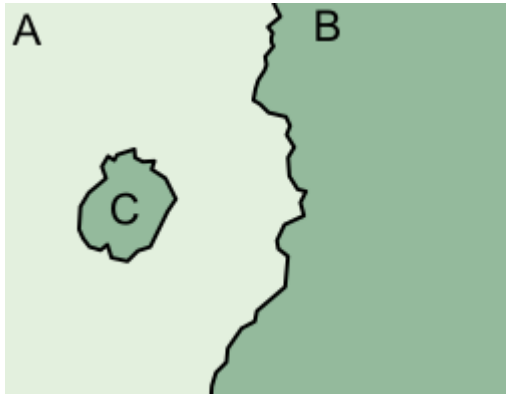
Confidential Computing 常見之技術分類

技術分類	概要	必要之硬體	Azure Virtual Machine 型號或服務	需要應用程式配合 TEE 環境調整
Enclaves 記憶體保護區	在作業系統行程 (Process) 層級建立機密執行環境	**Intel SGX**	• DCsv2 • DCsv3, DCdsv3	需要
Confidential VMs 機密運算虛擬機器	VM 層級建立機密執行環境	**Intel TDX**	• 即將推出	不需要
Confidential Container 機密運算容器	使用了 Enclaves 的容器	**Intel SGX**	• DCsv2 • DCsv3, DCdsv3	需要
	在 Enclaves 內運行的容器			不需要
Confidential Services 機密運算之平台即服務	機密運算之資料庫服務	平台即服務業者可讓用戶選用機密運算之硬體，微軟提供 **Intel SGX** 強化安全	Azure SQL Database Always Encrypted with enclaves	需要
	機密運算之區塊鏈帳本服務		Azure Confidential Ledger	需要

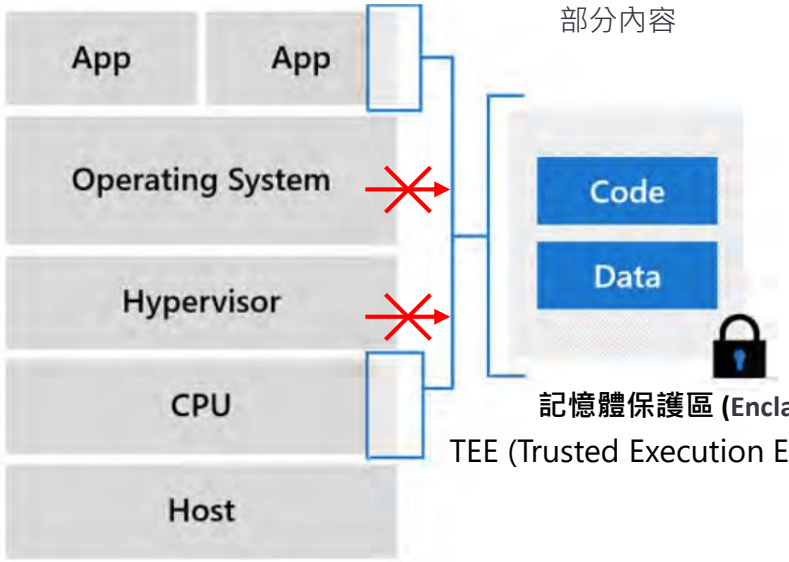
Enclaves 記憶體保護區

- 將應用程式一部分在加密的執行環境 (Enclave) 中執行
- 應用系統需要搭配 Intel SGX (Software Guard Extensions) SDK 改寫

- C 地區的主權屬於母國 B，因此 C 地是 B 國的外飛地 (Enclave)



- 使用 Intel SGX SDK 送出命令給微處理器，以建立一個記憶體保護區，在其中執行應用程式部分內容



- CPU 指令集與應用程式可以存取此一記憶體保護區，但作業系統，虛擬化軟體或其他應用程式無法存取此記憶體保護區

Azure Confidential Computing on 4th Gen Intel Xeon Scalable Processors with Intel TDX

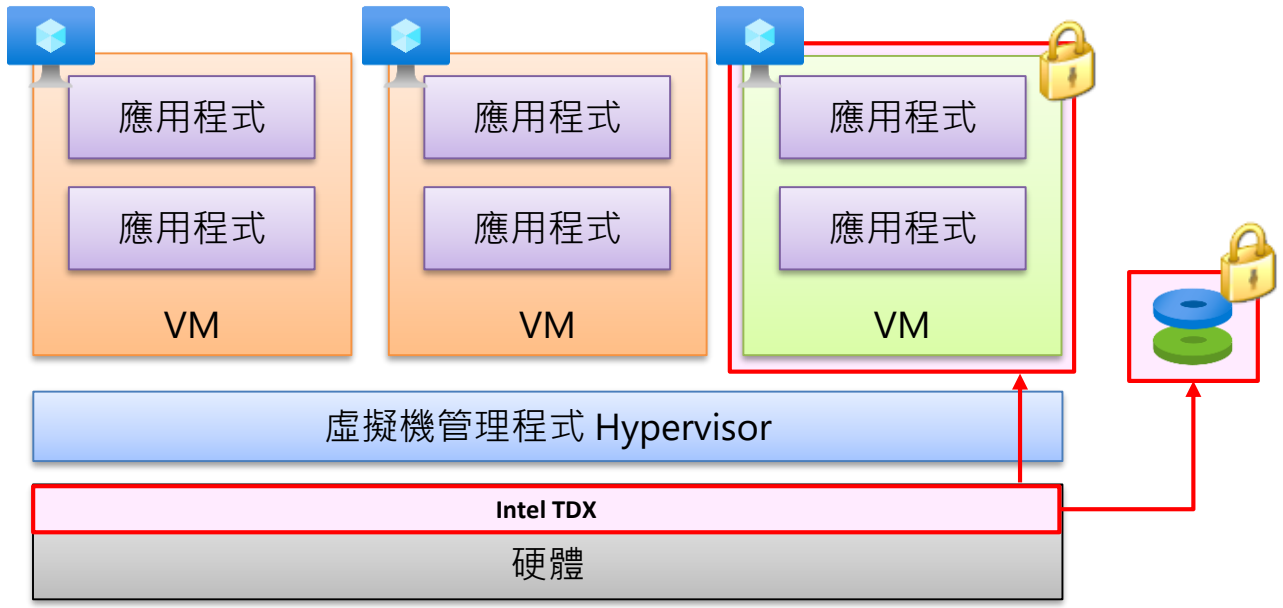
Posted on January 10, 2023

Mark Russinovich, Chief Technology Officer and Technical Fellow, Microsoft Azure

Microsoft continues to be the cloud leader in confidential computing, and the Azure team is excited to continue our leadership by partnering with Intel to offer confidential computing on 4th Gen Intel Xeon Scalable processors with Intel Trusted Domain Extensions (Intel TDX) later this year, enabling organizations in highly regulated industries to lift and shift their workloads that handle sensitive data to scale in the cloud. Intel TDX meets the Confidential Computing Consortium (CCC) standard for hardware-enforced memory protection not controlled by the cloud provider, all while delivering minimal performance impact with no code changes.

Confidential VM 機密運算虛擬機器

- 2023 年 1 月 Intel 發表最新的第四代 Xeon Scalable 微處理器與 TDX (Trusted Domain Extensions) 技術的同時，微軟也宣布 Microsoft Azure 將支援 TDX 機密運算技術
- 用戶現有應用程式無須任何修改，直接移植到符合機密運算環境之虛擬機器
- 2023 年稍晚即會於 Azure Virtual Machine 上提供支援 TDX 機密運算環境之虛擬機器



Confidential Container 機密運算容器

- (廣義) 機密運算容器可分三類

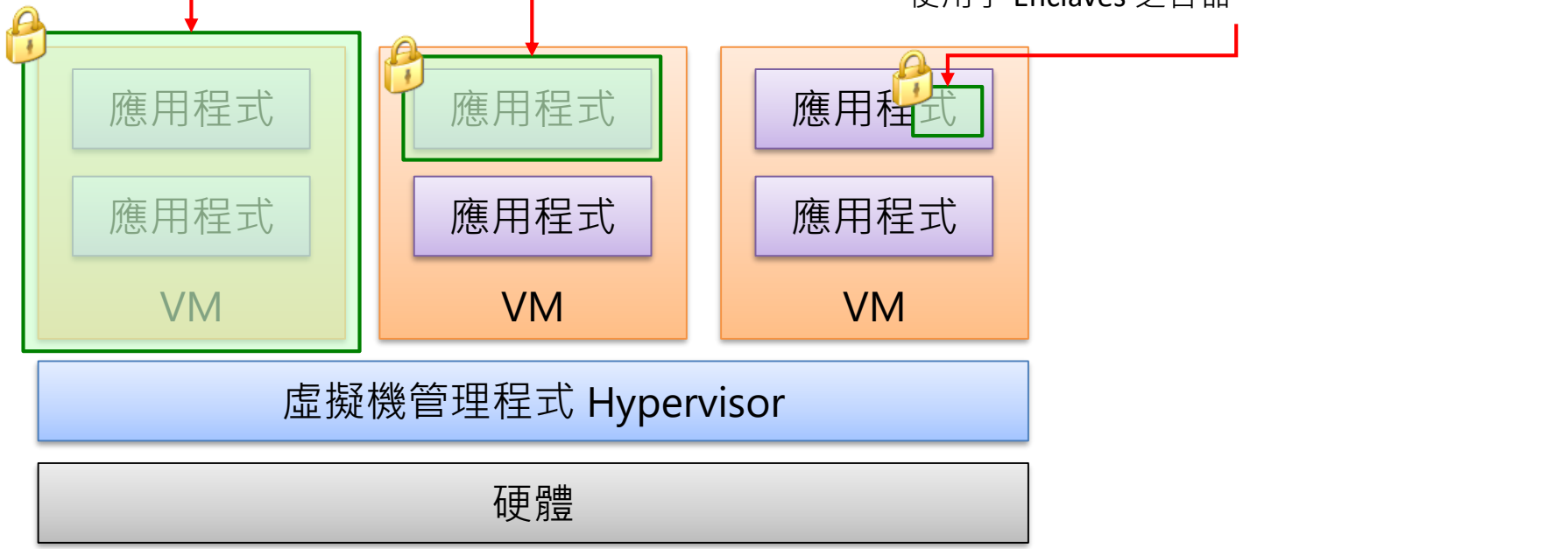
Azure Kubernetes Service (AKS) with Intel SGX confidential computing VM nodes

Confidential Container (狹義)
搭配合作夥伴或開放源碼方案，在 Enclaves 內運行的容器

Azure Kubernetes Service (AKS) 未來搭配支援 Intel TDX 之虛擬機器
Confidential VM (Node)

Azure Kubernetes Service (AKS) with Intel SGX confidential computing VM nodes

使用 Intel SGX SDK 之應用程式包裝成容器形式
透過 Intel SGX AKS Addon confcom
使用了 Enclaves 之容器



Confidential Services 機密運算之平台即服務

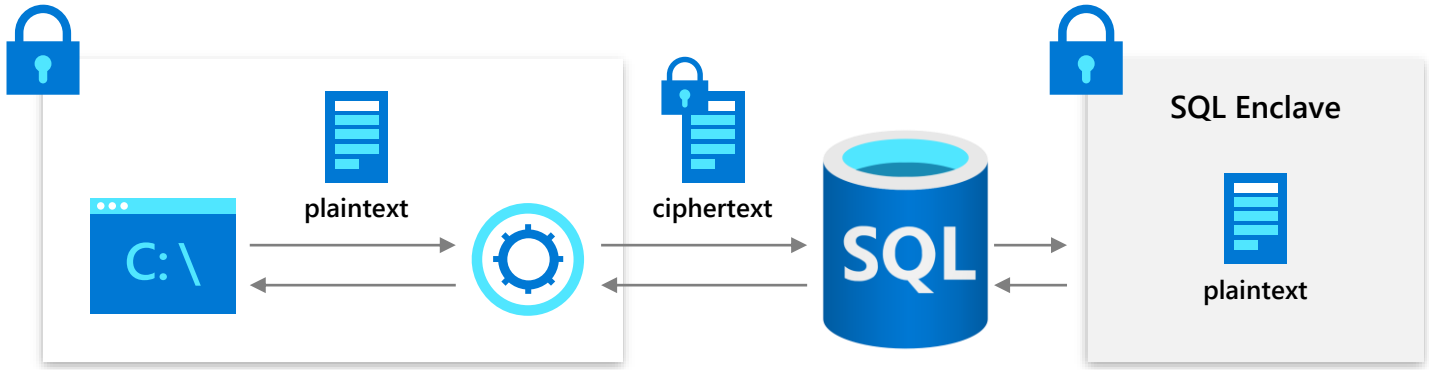
- Azure SQL Database Always Encrypted with Secure Enclaves 用戶可以選用 DC 系列虛擬機器， 以 Intel SGX 記憶體保護區來實作 Secure Enclaves ，以硬體實現機密運算要求

保護敏感資料

兼顧豐富之查詢語法與就地加密 (in-place encryption) 確保安全

在 SQL Enclave 內安全的進行運算

SQL Server 引擎面對的都是經過加密的資料，運算僅在安全的 SQL Enclave 內解密處理



支援複雜之 SQL 查詢

可使用 SQL LIKE 查詢 , 範圍查詢 (<, >, etc.), 排序, 索引等

就地加密 (In-place encryption)

SQL Enclave 可進行資料初始化資料加密與 key 輪換，無須將資料搬離資料庫

Microsoft Azure 使用 Intel 機密運算技術案例

加拿大皇家銀行

[Microsoft Customer Story-RBC creates relevant personalized offers while protecting data privacy with Azure confidential computing]


Microsoft