AUTOMATION ANYWHERE

機器人流程自動化的企業級安全性

簡介

營運流程自動化相關技術至今已發展超過了 20 年，爲何目前仍然只有不到 20% 的工作完成自動化？主要的原因是，85% 的企業系統未能明確定義 API。後果就是 IT 待辦的營運端整合需求與日俱增。

機器人流程自動化誕生的遠景，是爲了令企業使用者有能力建立像人類一樣與企業系統互動的軟體機器人。RPA 機器人能夠像人類一樣使用憑證，並自動化執行涉及任何企業應用程式的工作，包括未使用 API 的傳統應用程式。索賠處理、貸款處理、帳戶對帳、發票產生/提交以及報表產生，還都只是少數幾項跨越不同業務領域的自動化潛能範例。

您可以輕易預見到使用 RPA 的各種潛力：節省大量的時間與成本支出、改善客戶滿意度、激勵員工士氣，以及打造競爭對手難以企及的優勢。不過，要完全實現上述效益，必須採用企業級解決方案。

提供強大的可靠性、擴展性和廣泛的功能設置，以達成適用性和可用性最大化，是自動化的部分基本條件。但是上述要素尚未包括營運最重要的要求：端對端安全性。穩健的安全性架構，其具備的功能要完全支援諸如最低權限和職責分離等核心原則，同時也能對關鍵型應用程式和相關敏感資料提供端對端保護，是最關鍵的部分。

本文提供業界企業級安全性最高標準的概觀，市場上領先業界的數位勞動力平台 Automation Anywhere Enterprise 即是最佳典範。

“

您可以輕易預見到使用 RPA 的各種潛力：節省大量的時間與成本支出、改善客戶滿意度、激勵員工士氣，以及打造競爭對手難以企及的優勢。不過，要完全實現上述效益，必須採用企業級解決方案。

架構和營運

要了解企業級 RPA 實施所需安全機制，必須先了解包含解決方案與其運作的元件。

核心元件

如**圖 1** 所示，Automation Anywhere Enterprise 的核心建構元件爲控制室、機器人建立器以及機器人執行器。

控制室

控制室如同自動化環境的大腦。以 Windows 伺服器爲基礎的管理系統，搭配整合式資料庫，爲整體系統管理提供一致的觀點。控制室也是 RPA 操作員協調數位勞動力的地方，也就是說，在這裡排程、部署、執行、監控與管理組織機器人的運作。此外，內建版本的控制功能 (Apache Subversion 伺服器) 促進了多使用者的合作，同時也強制執行變更管理的最佳做法，建立立即可用之機器人的集中存放庫。

機器人建立器

運用機器人建立器打造機器人。機器人建立器是一個在工作站等級電腦或虛擬機上執行的 Windows 桌面應用程式，提供營運流程專家用來建立和測試自動化成果。運用機器人編輯器建立機器人，同時由機器人執行器使用本機非生產用測試資料和應用程式實例，協助機器人測試。成功測試之後 (例如：就效能、資料完整性以及安全性方面)，機器人簽核至控制室存放庫，即可供生產部署使用。

機器人執行器

機器人執行器派遣機器人工作。機器人執行器採用的應用程式程式碼與機器人建立器相同，但使用不同的授權金鑰，在生產環境中執行機器人，也就是，利用目標應用程式和生產資料存放庫的生產實例。事實上，機器人執行器僅能執行機器人，無法提供建立和編輯功能。針對高度可靠、大規模的運作，我們也支援機器人執行器匯集。

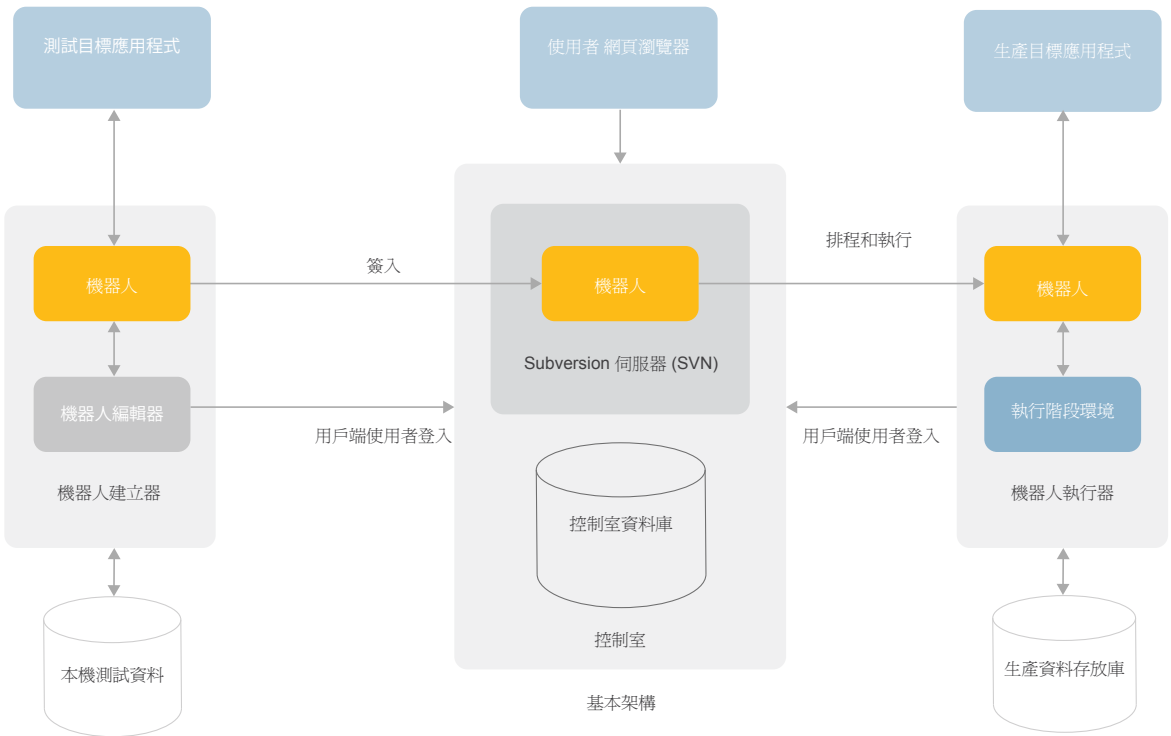

圖 1：基本 Automation Anywhere Enterprise 架構

其他企業級元件

考慮大規模運作時，還有另外兩項與追求企業級部署的組織相關的重要 RPA 解決方案：隨選擴展與 Bot Insight。

隨選擴展

Automation Anywhere Enterprise 運用 Amazon Web Services (AWS) 公有雲，搭配所有伴隨的功能，包括靈活的躍升/急降功能、按用量計算、無限的橫向擴展性以及持續監控和審計記錄機器人執行器基礎架構，有效提供 RPA 即服務。結果就是多節點的高可用性，在自動化工作負載產生的巨大變動中，也能帶來 SLA 推動的績效與業務連續性。

Bot Insight

Bot Insight 是控制室內部完全整合的子系統，爲機器人操作和業務流程資料進行幾近即時的分析。Bot Insight 對每個機器人使用獨一的進階演算法，自動產生可自訂的控制面板。Bot Insight 提供的細節程度，是根據與機器人操作有關的具體事件日誌，得以進行細微差別的提醒、隨意地探索、互動式深入探討、時間序列分析和操作/業務流程的完整洞見。此外，所有資料均可輸出做爲安全性資訊與事件管理 (SIEM) 日誌，供進一步分析、調查和報告之用。

工作中的機器人：兩種自動化類型

最後，在介紹 Automation Anywhere Enterprise 的高端安全性功能之前，必須先澄清兩種基本的自動化類型：半自動和全自動：

半自動流程是指使用者登入機器人執行器，以監視及/或主動支援機器人執行。需要使用者介入的原因，可能是該機器人提供協助使用者工作的工具類功能，或者該機器人所進行的是需要使用者定期輸入或依狀況引導的批次型工作。半自動化也簡稱爲前台自動化。

全自動流程，顧名思義是指無須任何企業使用者或操作員互動，即可自行運作。全自動流程通常是由操作員所執行，而操作員不用深入了解機器人、正在進行自動化的應用程式或是自動化的目的。。操作員與業務單位合作，一同安排在機器人執行器上執行機器人的時程。在執行期間，操作員監控執行中機器人的作業狀況，例如：CPU、記憶體和儲存空間用量，以確保機器人的執行沒有任何錯誤或例外。控制室控制面板顯示機器人執行時的所有作業細節。若是全自動流程因爲錯誤未能完成工作，操作員可能會施行程序以修復自動化，並予以重新啓動；否則，他們會將問題向上呈報給 RPA 團隊或業務單位，以診斷和修復問題。

多層 ENTERPRISE RPA 安全性、多層識別與驗證

Automation Anywhere Enterprise 安全性架構的核心宗旨是：參與實體未經事先驗證，不得進行存取或操作。這同時適用於人類和機器人。結果就是半自動和全自動都有的多層驗證流程。

使用者身分：一般的企業驗證

憑證和人員可以多層。考慮一個簡單的企業驗證情境 (請見**圖 2**)。Alice 是一名企業使用者，向其所屬 Windows 工作站進行驗證。Alice 經由 Windows Domain Active Directory 登入亦或是 Kerberos (視其工作站是否具備有效支援單而定) 驗證後，接著便登入正在遠端執行的應用程式。在此情境中，驗證過程包含一個單一人員與其憑證。

圖 2：一般的企業驗證

現在，我們來考慮一個半自動化情境 (請見**圖 3**)。在這個案例中，使用者 Bob 一般的日常工作是測試機器人，或是執行半自動作業。步驟 1，他先使用個人憑證向機器人執行器工作站進行驗證 (如同上述的 Alice 情境)。步驟 2，他啓動 Automation Anywhere Enterprise 用戶端，輸入他的控制室使用者 ID 和密碼，從而向控制室驗證其用戶端軟體。步驟 3，他執行機器人，而機器人接下來會存取需要憑驗的應用程式。機器人在這個步驟所使用的憑證可能會儲存在企業憑證保存庫，供機器人在執行階段擷取，或使用 Bob 的個人憑證通過 (根據其工作站所提供的演算和相同網域的應用程式伺服器)。無論是哪一種方式，結果都要通過總共三層的識別與驗證。

全自動情境也有三層驗證，如**圖 4** 所示 — 雖然略有不同。在這個案例中，使用者 Charles 從向控制室驗證開始，以便可以選擇一個機器人執行，可能是立即執行，或是排程執行。

步驟 2，當機器人執行開始時，控制室將採用 BotRunnerUser 憑證，啓動程序自動登入機器人執行器工作站。機器人下載至本機 Player 功能之後 (步驟 3)，便開始執行，使用 BotApplicationUser 憑證向目標應用程式驗證 (步驟 4)。如同半自動化情境，BotApplicationUser 憑證可能是擷取自憑證保存庫，或使用 BotRunnerUser 憑證通過。

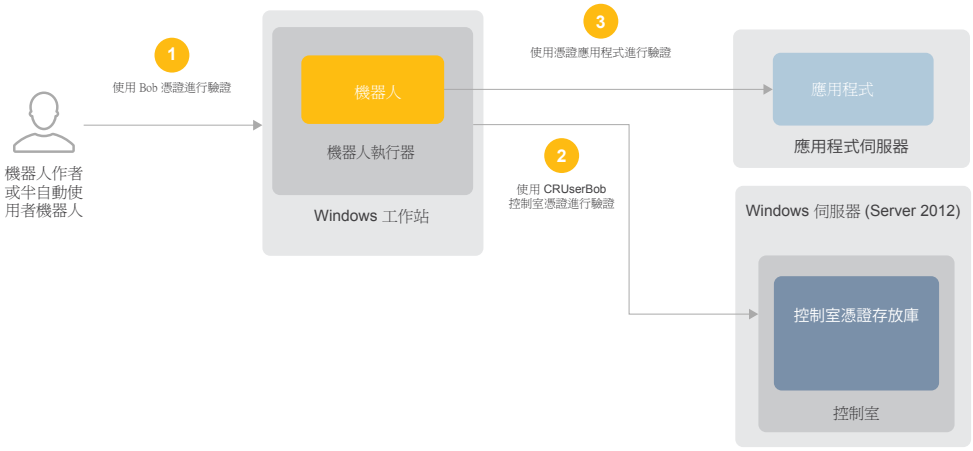

圖 3：半自動化情境的驗證流程

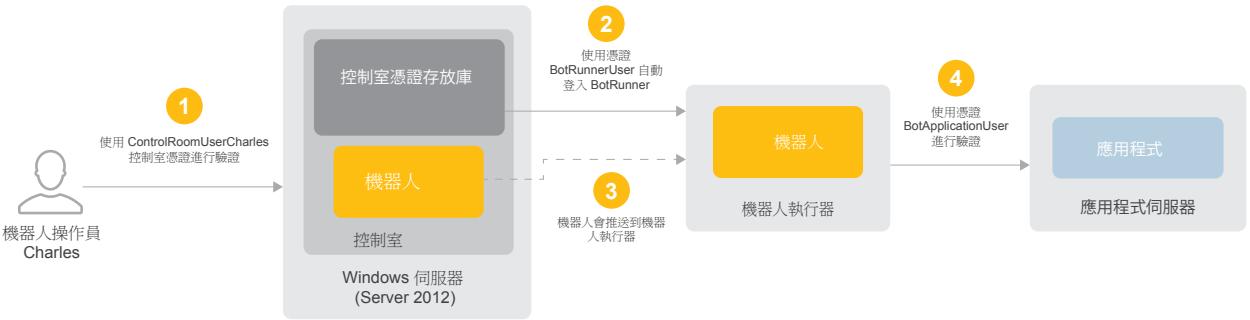

圖 4：全自動情境的驗證流程

驗證選項與 IAM 整合

控制室驗證的支援選項包括使用 LDAP 的 Active Directory、使用 Kerberos 的 Active Directory 以及使用內嵌式憑證保存庫的本機驗證 (詳述於後續章節)。

可供企業部署使用的其他身分與存取管理選項包括：

+ 支援 SAML 2.0 型單一登入
+ 與第三方權限存取/憑證管理解決方案 (例如：CyberArk、One Identity 和 Thycotic) 整合

全方位角色型存取控制

成功驗證僅是 Automation Anywhere Enterprise 安全架構提供強制存取控制管制的第一層。同樣重要的還有支援精密的角色型存取控制，或稱 RBAC，尤其是當我們在遵循最低權限與職責分離的核心原則之時。

RPA 平台的基本架構與主要功能當中，提供 5 種不同的角色 (請見**表 1**) 選擇使用。BotBuilder 利用機器人建立器擷取商業邏輯並建立相應的自動化。BotBuilder 與測試應用程式和資料集搭配運作，以確保生產系統在開發階段不受影響。個別機器人通常會經歷許多不同的反覆運算和版本，不僅是在初始的開發階段，同時也在相關的業務流程及/或目標應用程式更新之際。BotTesters 也與機器人建立器搭配運作，以測試機器人的效能、資料完整性和安全性，確保每個機器人以安全的方式執行其任務。機器人在開始使用生產資料和應用程式執行之前，由 BotTesters 提供第二階段驗證。

機器人一經測試並完成安全性檢查後，BotPromoter 偕同 BotBuilder/BotTester 運作，指定將用於生產的機器人版本。這是 BotOperator 唯一可以看見的機器人版本，BotOperator 與業務單位協調以排程與執行機器人，同時也負責在控制室內監控機器人效能，包括疑難排解所出現的任何執行階段問題。最後，RPA 管理員負責平台的整體管理 – 包括設定元件、介面和所有角色/權限。

進階職責分離

此核心角色集展現了 RBAC 的基本出發點，但是 Automation Anywhere Enterprise 平台內部仍有可能進行更多的職責分攤。管理者可運用內嵌式角色建立精靈，輕鬆界定自訂的角色，設定負責控制室完整物件和功能的權限，包括使用者管理、授權、憑證保存庫、機器人執行器集合、機器人排程、機器人操作/控制面板和稽核日誌。各項權限一經選擇，精靈便會爲附隨/衍生的權限動態新增步驟。

例如：當您選擇 [機器人] (BOTS) > [查看我的機器人] (View my bots) > [執行我的機器人] (Run My bots) 權限 (請見**圖 5**)，工作流程將新增一個步驟，顯示可獲得存取權的特定機器人資料夾 (例如：機器人集合)。最終結果便是得以建立高擬真角色，並兼具精細的存取控制，能充分滿足最嚴謹、最安全和合規監管環境的需求。

角色	說明
RPA 管理員	管理系統 (設定元件、角色、介面)
BotBuilder	業務流程專家負責運用 Task Editor 建立機器人並執行基本的功能測試
BotTester	品質管制測試員負責審查機器人的功能準確性、效能和安全性
BotPromoter	系統管理員負責核准機器人並將它們移動到開發、測試及生產階段
RPAOperator	操作員負責排程、執行和監控機器人效能

表 1：Automation Anywhere Enterprise 的主要 RPA 角色

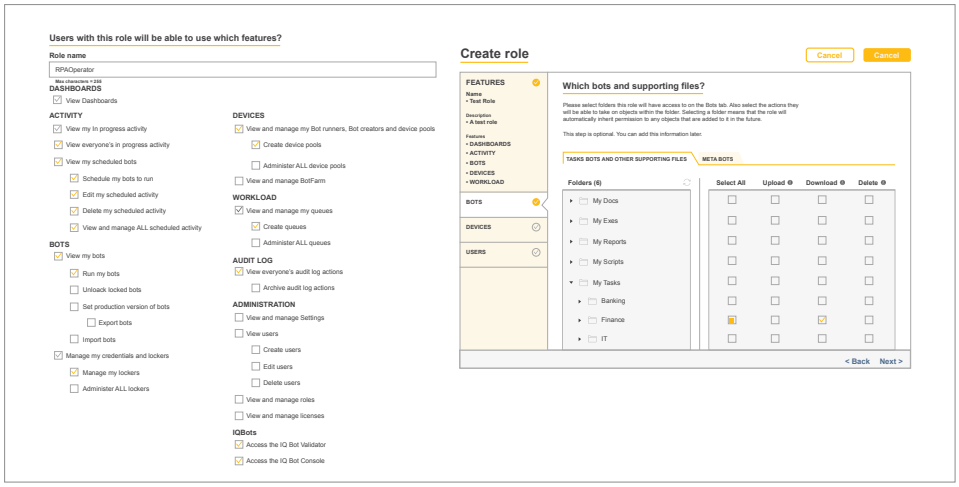

圖 5：使用精密驗證建立角色

獨立控制平面

不只是廣泛的 RBAC 功能，Automation Anywhere Enterprise 向來採用能夠徹底分離機器人開發與機器人執行任務的架構，提供合理的職責分離。

機器人建立器僅能在控制室內部的版本控制系統上傳和下載機器人。同時，機器人執行器僅能執行機器人，不具備機器人建立和測試功能的存取權。這種在架構上強制執行職責分離而構成的雙重授權，符合美國國家標準與技術中心 (NIST) 的最佳做法，因爲這需要 (至少) 開發人員和企業使用者雙方授權，達成最終的業務流程自動化。

獨立處理領域

平台 RBAC 功能其中一項強大的使用案例 (尤其是針對大型企業)，是建立獨立的處理領域 (請見圖 6)。只要將每個所需領域的機器人，嚴格地組織/儲存在控制室內部相應的資料夾中，即可達成此點。

最佳案例：與財務應用程式相關的機器人，將會被存放在財務資料夾中，而與人力資源相關的機器人，則會被存放在人力資源資料夾中。接著將權限分派給財務部門的機器人操作員，且此權限僅限財務機器人和機器人執行器；將權限分派給人力資源部門的機器人操作員，且此權限僅限人力資源機器人和機器人執行器，依此類推其他處理/自動化領域 (請見圖 6)。

最後結果便是，因爲個別操作員無法查看或操作指定領域以外的機器人，從而進一步將職責分離並區隔相關的應用程式與資料，而且此時是針對 OU/領域層。

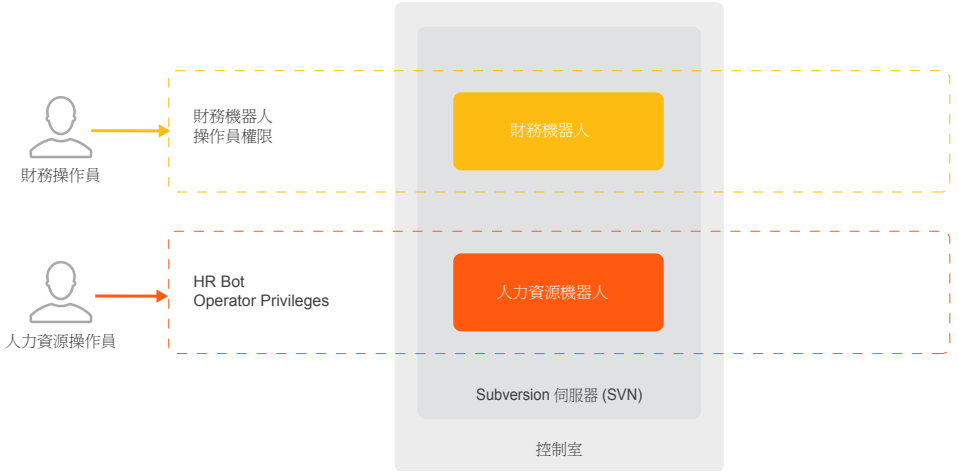

圖 6：支援獨立處理領域

端對端資料保護。

對嚴格控管的環境而言，多層驗證和精密存取控制至關重要。端對端資料保護亦然，對於維護關鍵業務流程、敏感資料和相關機密 (例如：憑證) 的保密性和完整性而言，它也不可或缺。

Automation Anywhere Enterprise 平台使用內嵌式憑證保存庫滿足這項需求，並提供廣泛的保障措施，不但保護靜態以及傳輸中的資料，同時也保護個別系統中所使用的資料。

加密金鑰和憑證保存庫

圖 7 顯示平台所使用的主要加密金鑰，以及這些金鑰與憑證保存庫的關係。所有加密均採用 FIPS 140-2 等級 1 驗證過的加密模組進行。

在安裝期間 (**圖 7**的左半部)，系統產生一對 RSA 2048 位元的公開/私密金鑰和一個 AES 256 位元金鑰。RSA 2048 金鑰對中的私密金鑰是指主金鑰，而 AES 256 金鑰則是指資料金鑰。主金鑰將會顯示給進行安裝的系統管理員，保管於系統外安全的實體地點。公開金鑰用來加密資料金鑰。接著公開金鑰和已加密的資料金鑰都將會儲存至資料庫。使用過程中，所有的金鑰和已加密的資料均會採用 Microsoft 資料保護 API (DPAPI) 存放於已加密的安全記憶體中。

在控制室啓動或重新啓動期間 (**圖 7**的右半部)，系統管理員收到提示要提供主金鑰。從資料庫中擷取已加密的資料金鑰，並使用主金鑰予以解密。此時資料金鑰已就緒可供使用。當系統自憑證保存庫儲存和擷取資料時，會使用資料金鑰對該筆資料進行加密和解密。

憑證保存庫用來儲存所有經系統管理的憑證與重要的系統設定資料。它更可以用來儲存任何組織自動化過程中所使用的其他敏感資料 (例如：名稱/值對)。因此，BotBuilder 可在自動化過程中，直接避免寫入程式碼憑證與其他敏感資料/參數的不安全作法。

保護靜態資料

除了爲本機憑證加密以及選擇機器人所使用的執行階段資料之外，憑證保存庫還可爲敏感的設定參數與關於整合式版本控制和電子郵件服務的詳細資料，提供安全儲存。

保護傳輸中的資料

用戶端與控制室所有的網路服務採用傳輸層安全性協定 (TLS) 1.2 版，以確保資料在元件之間傳輸時的安全性和完整性。

機器人建立器/執行器用來通過控制室驗證的憑證，會先加密再透過 TLS 安全連線提交。這層額外的加密不僅可防範網路堆疊問題 (例如：Heartbleed 漏洞)，還可在外層 TLS 連線於前端負載平衡器終止時，預防實作中的憑證曝光。

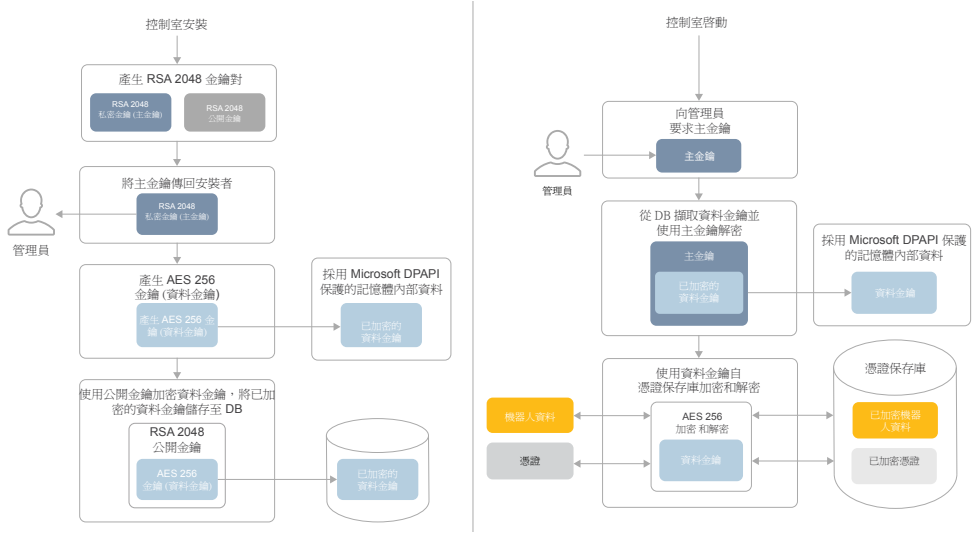

圖 7：Automation Anywhere Enterprise 加密架構

保護使用中的資料

執行階段安全性始於分散式憑證保護。具體而言，機器人執行器的本機憑證儲存並不存在。自動化過程中，從憑證保存庫動態擷取以供使用的憑證和其他資料，只會以加密格式被保留在揮發性記憶體中，而且當相關機器人完成執行後，便會遭到清除。

能夠用來防止未經授權而存取機密資訊 (亦即，資料洩露) 或防止在執行階段竄改機器人的其他功能與設定選項包括：

+ 隱藏模式 – 本機螢幕不會顯示任何程式畫面，且登入使用者可選擇停用機器人建立器和機器人執行器的截圖，從而防範螢幕上所顯示的敏感資訊被儲存至機器人中
+ 輸入鎖定 – 能夠針對正在執行自動化的機器，停用其滑鼠和鍵盤
+ 限時 – 能夠設定時限，在自動化尚未完成執行的情況下，超過此時限即終止自動化
+ 中央控制 – 能夠從控制室內部集中控制 (亦即，暫停、恢復、停止) 遠端執行自動化的作業

軟體開發生命週期 (SDLC) 安全支援

爲促進自動化環境相關控制與安全防護措施的最大化，前述的基本部署情境可加以「擴展」，進一步提供安全軟體開發生命週期 (SDLC) 最佳做法，例如 FISMA、FedRamp 和 PCI DSS 所要求的做法。產生的進階部署模型提供三個不同的 RPA 區域 – 各自針對開發、使用者驗收測試 (UAT) 和生產 (請見圖 8)。每個區域使用不同的使用者群組加以邏輯區隔 (隔離)，不同的使用者群組具備不同的角色和權限。垂直虛線代表網路分段以及防火牆。

與基本的部署模型一樣，機器人的生命週期始於開發階段。當 BotBuilder 對機器人感到滿意時，UAT BotPromoter 會將機器人從開發版本存放庫 (SVN) 移轉至 UAT 存放庫。UAT 區域的唯一目的是測試機器人的準確性、效能和安全性。當機器人通過驗收測試時，生產 BotPromoter 便會將其移轉至生產區域。此時，它會達到生產狀態，並可供 RPAOperators 搭配生產應用程式使用。在流程的每個步驟中，都由具備不同角色和權限的不同系統管理員進行檢查和認證。嚴格的職責分離和多層控制在設計時都已內建，以確保數位勞動力的可靠性、可擴展性、高效性、安全性及合規性。

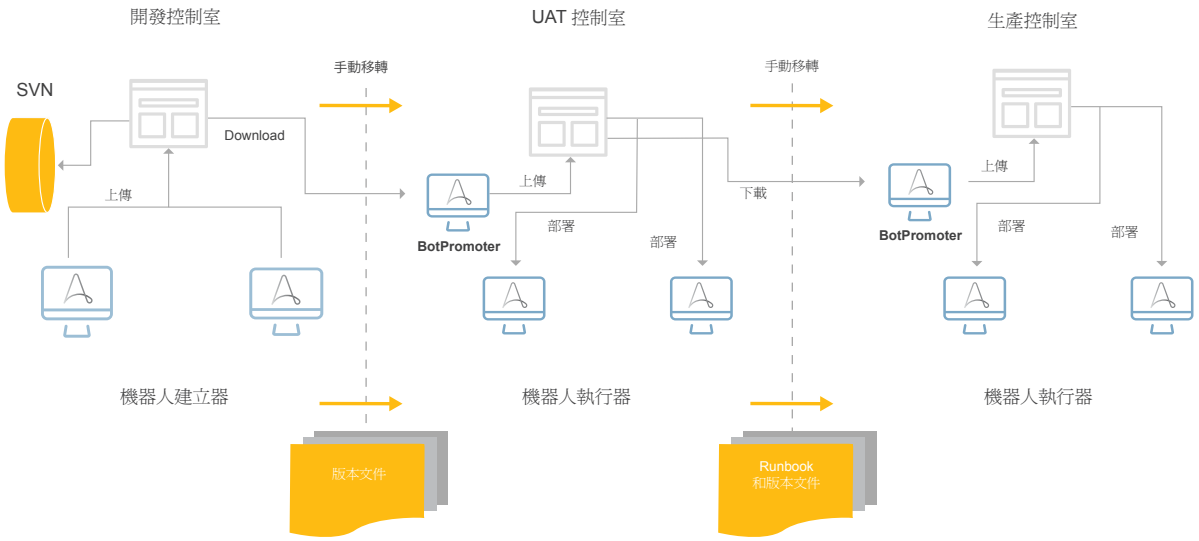

圖 8：完整 SDLC 支援的進階部署模型

登入與監控

完整的稽核記錄、監控和通報功能，對任何備受關注的 IT 解決方案的安全性架構而言，都至關重要。Automation Anywhere Enterprise 也不例外。

跨平台可自動擷取 60 多種使用者/實體動作類型的事件詳細資料 (對象、內容、時間、地點和結果) – 包括使用者、機器人、機器人建立器和機器人執行器的建立、修改、啓動、停用和移除。透過結合自動擷取、將每項活動綁定特定身分及預設唯讀政策，達成不可否認機制。RBAC 還可用來嚴格控制哪些角色可以先看見稽核日誌。

從監控的觀點看來，控制室內的自動控制面板和報告是可以存取的，也可加以客製化，以識別和警示不正常的活動 (或自動化或安全團隊決定要關注的任何其他細節)。此外，輸出記錄的能力可支援運用組織已在使用的其他分析、報告和事件調查/回應基礎架構，例如 SIEM、UEBA 和進階的分析工具。

額外企業安全性與彈性功能

Automation Anywhere Enterprise 使用下列方式進一步支援企業安全性與彈性目標：

+ 能夠和諧「加入」組織現有高可用性/災難復原 (HA/DR) 基礎架構與流程的分散式 (彈性) 元件架構
+ 整合式版本控制系統 (Apache Subversion) 與平台的衍生 RBAC 功能相結合，能夠實施和強制實行非常嚴謹的變更管理政策和流程
+ 在平台開發期間使用諸如 Hibernate 與 ReactJS 架構等工具編寫程式碼，協助消除常見攻擊 (例如 SQL 資料隱碼攻擊和跨網站指令碼攻擊) 容易突破的弱點
+ 程式碼開發安全性計畫/協定要求持續進行多工具、多層掃描，藉此偵測和消除軟體漏洞

若您想要深入了解前述功能及更多其他 Automation Anywhere Enterprise 所包含之控制、安全防護及安全性功能，請參閱：「Automation Anywhere Enterprise：安全性架構」。

機器人流程自動化讓期待降低營運成本、加強客戶滿意度和獲得競爭優勢的現代化企業信心十足。做爲業界領先的智慧型數位勞動力平台，Automation Anywhere Enterprise 不僅提供成功所需要的可靠性、可擴展性和可用性功能，同時也提供爲維護整體自動化環境的機密性、完整性和可用性所需的企業級安全性，協助確保達成前述及其他利益的最大化。

如需進一步了解 Automation Anywhere Enterprise 的相關資訊，請參考網站： https://www.automationanywhere.com/products/enterprise。