概觀

目錄

產品概觀

「產品概觀」主題說明了 IBM Security Key Lifecycle Manager 產品（早期稱爲 IBM Tivoli Key Lifecycle Manager）及其商業和技術環境。

它們包括以下相關資訊：

- 產品特性及功能
- 產品所基於的技術及架構
- 基於產品特性的使用者模型及角色
- 支援各種使用者角色的圖形介面和工具

此版本的新增功能

IBM Security Key Lifecycle Manager 2.6.0 版提供數個安裝、配置、移轉 IBM Security Key Lifecycle Manager基礎架構和處理程序的使用性及交互作業能力改進項目，來本端建立和管理 KMIP 物件的生命週期。

作業系統獨立的使用者介面型抄寫配置

提供圖形使用者介面來進行自動化抄寫配置。您可以配置抄寫程式，以在將新金鑰新增至主要伺服器時，在複製伺服器之間抄寫重要的 IBM Security Key Lifecycle Manager 資料。

自動化抄寫處理程序能夠以獨立於伺服器作業系統及目錄結構的方式，將 IBM Security Key Lifecycle Manager 環境複製至多個伺服器。例如，您可以將 Windows 系統上主要伺服器中的資料抄寫到 Linux 系統上的複製伺服器。您可以複製主要 IBM Security Key Lifecycle Manager 伺服器，最多可達 20 個副本。如需相關資訊，請參閱複製和主要伺服器的抄寫設定。

作業系統自備份及還原作業

支援跨平台備份及還原功能，以保護重要的 IBM Security Key Lifecycle Manager 資訊。 您可以建立跨平台相容的備份並在作業系統之間還原相同的備份。例如，Linux 系統上的備份可以在 Windows 系統上還原，反之亦然。

您可以使用跨平台備份公用程式，在舊版 IBM Security Key Lifecycle Manager 上執行備份作業以備份重要資料。 您可以在現行版本的 IBM Security Key Lifecycle Manager 上，將這些備份檔還原到與從中進行備份之作業系統不同的作業系統。

您還可以配置 IBM Security Key Lifecycle Manager 以排程自動備份作業。 您必須僅爲主要伺服器配置內容，以定期備份資料。 如需相關資訊，請參閱備份及還原。

NSA 套組 B 合規

支援遵守 US National Security Agency (NSA) 套組 B 加密法準則之安全通訊端通訊，以提供加強的安全等級。如需相關資訊，請參閱第 10 頁的『IBM Security Key Lifecycle Manager 中 NSA 套組 B 加密法的合規』。

透過圖形使用者介面進行除錯記載設定

支援使用圖形使用者介面來配置除錯記載設定以收集除錯資訊。 除錯日誌檔提

供其他資訊來對 IBM Security Key Lifecycle Manager 問題進行分析及疑難排解。如需相關資訊，請參閱指定除錯資訊的設定。

設定透過圖形使用者介面來匯出 SSL/KMIP 伺服器憑證

支援使用圖形使用者介面以編碼格式將 SSL/KMIP 伺服器憑證匯出至檔案。 匯出的檔案可協助更快速地部署憑證，以與伺服器進行安全通訊。 如需相關資訊，請參閱匯出 SSL/KMIP 伺服器憑證。

用來配置 IBM Security Key Lifecycle Manager 以進行 SSL/TLS 信號交換的「伺服器配置精靈」。

包括「伺服器配置精靈」以配置 IBM Security Key Lifecycle Manager 伺服器和用戶端裝置以進行 SSL/TLS 信號交換。 SSL 信號交換可讓伺服器和用戶端裝置能夠建立用於安全通訊的連線。 精靈會提供一個引導式方法來設定 SSL/TLS 信號交換程序。 如需相關資訊，請參閱實務範例：IBM Security Key Lifecycle Manager 伺服器與用戶端裝置之間的 SSL 信號交換設定。

遵守 KIMP 1.2 及 Storage Networking Industry Association Secure Storage Industry Forum (SNIA-SSIF) 憑證

符合 Key Management Interoperability Protocol (KMIP) 的測試程式及其他儲存體行業相關的安全標準。

更便捷地配置 KMIP 相容的用戶端，以進行金鑰管理作業

IBM Security Key Lifecycle Manager 提供圖形使用者介面來建立、配置及搜尋加密物件。這些物件用於將加密金鑰提供給 KMIP 相容的用戶端裝置。如需 KMIP 物件管理的相關資訊，請參閱KMIP 物件管理。

安裝改進項目

對安裝程式進行了數項改良，以在安裝程序期間透過執行環境驗證及必備項目檢查來向使用者提供更多意見。

自動產生 AES 256 位元主要金鑰以進行資料加密

在成功安裝 IBM Security Key Lifecycle Manager 之後，會自動產生 AES 256 位元主要金鑰以進行資料加密。 如果要符合 PCI DSS 標準及提高資料安全，請使用 256 位元長度主要索引鍵來加密 IBM Security Key Lifecycle Manager 機密資料，例如金鑰資料。

註：

- 從 IBM Security Key Lifecycle Manager 2.6 版開始，不支援 Solaris 作業系統。
- 將在 IBM Security Key Lifecycle Manager 的後續版本中，淘汰 IBM Security Key Lifecycle Manager 指令行介面指令。請改用 REST 介面。
- 將在 IBM Security Key Lifecycle Manager 的更高版本中，淘汰對圖形使用者介面、指令行介面及 REST 介面內加密金鑰和憑證 **alias** 內容的所有參照。

支援的語言

IBM Security Key Lifecycle Manager 支援各種語言。 使用者介面標籤、訊息及值都能以英文語言及非英文語言顯示。 然而，IBM Security Key Lifecycle Manager 僅支援單一語言環境的本地化系統。

IBM Security Key Lifecycle Manager 支援下列語言：

- 英文
- 法文

- 德文
- 義大利文
- 日文
- 韓文
- 簡體中文
- 西班牙文
- 繁體中文

特性概觀

使用 IBM Security Key Lifecycle Manager 來管理金鑰的生命週期及企業的憑證。 可以管理對稱金鑰、秘密金鑰、非對稱金鑰組及憑證。

IBM Security Key Lifecycle Manager 具有下列重要特性：

- 角色型存取控制，用於爲特定裝置群組提供執行諸如建立、修改及刪除等作業的許可權。 大部分許可權都與特定的裝置群組相關聯。
- 透過將業界標準的金鑰管理交互作業能力通訊協定 (KMIP) 用於已儲存資料的加密及對應的加密金鑰管理，來延伸裝置支援。

  您可以使用 IBM Security Key Lifecycle Manager 圖形使用者介面來建立、配置及搜尋加密物件。這些物件用於將加密金鑰提供給 KMIP 相容的用戶端裝置。
- 提供對稱金鑰給 DS5000 儲存體伺服器

  對提供給 DS5000 儲存體伺服器 的金鑰進行管理及日常維護。 限制可與某個裝置（例如磁碟機）相關聯的機器集。 您可以將裝置與 IBM Security Key Lifecycle Manager 資料庫中的現有機器相關聯。
- IBM Security Key Lifecycle Manager 伺服器所連接一個以上裝置的加密金鑰。
- 將您所產生自簽憑證的金鑰資料、私密金鑰及金鑰 meta 資料儲存在資料庫中。
- 跨平台備份及還原，用於保護重要資料及其他 IBM Security Key Lifecycle Manager 資料，例如配置檔及現行資料庫資訊。
- 跨平台備份公用程式，用於在舊版 IBM Security Key Lifecycle Manager（1.0、2.0、2.0.1、2.5）及 IBM Encryption Key Manager 2.1 版上執行備份作業。您可以跨作業系統在現行版本的 IBM Security Key Lifecycle Manager 上還原這些備份檔。
- 安裝期間移轉舊版 IBM Security Key Lifecycle Manager（1.0、2.0、2.0.1、2.5）及 IBM Encryption Key Manager 2.1 版元件。
- 審核記錄，以作業成功及/或作業不成功引發的所選事件爲基礎。 安裝或啓動 IBM Security Key Lifecycle Manager 會將建置層次寫入審核日誌中。
- 支援已啓用加密的 3592 磁帶機、LTO 磁帶機、DS5000 儲存體伺服器、DS8000 Turbo 磁帶機及其他裝置。
- 支援使用「硬體安全模組 (HSM)」來儲存用來保護所有密碼的主要索引鍵，及資料庫中所儲存的金鑰。
- 一組作業，用於跨作業系統自動抄寫現行作用中檔案及資料。 此抄寫能夠以獨立於伺服器作業系統及目錄結構的方式，在多個伺服器上複製 IBM Security Key Lifecycle Manager 環境。

- 支援對使用者鑑別使用 LDAP（輕量型目錄存取通訊協定）伺服器。 您可以配置任何 LDAP 儲存庫（例如 IBM Security Directory Server 或 Microsoft Active Directory）中的 IBM Security Key Lifecycle Manager 使用者。
- 用來配置 IBM Security Key Lifecycle Manager 以進行 SSL/TLS 信號交換的「伺服器配置精靈」。 SSL 信號交換可讓伺服器和用戶端裝置能夠建立用於安全通訊的連線。

金鑰提供

IBM Security Key Lifecycle Manager 支援定義及提供金鑰。 IBM Security Key Lifecycle Manager 也支援定義可以與裝置相關聯的金鑰或金鑰群組。 不同的裝置需要不同的金鑰類型。 配置裝置後，IBM Security Key Lifecycle Manager 會將金鑰部署至要求金鑰的裝置。

金鑰群組

IBM Security Key Lifecycle Manager 金鑰群組包含金鑰。 一個金鑰只能爲一個金鑰群組的成員。

在分散式系統上，刪除金鑰群組*也會刪除金鑰群組中的所有金鑰*。

金鑰 meta 資料

IBM Security Key Lifecycle Manager 金鑰的 meta 資料包括金鑰別名、演算法及啓動日等資訊。

meta 資料可能也包含金鑰說明、到期日、停用日、毀損日、受損日、金鑰使用情形、備份時間及狀態（例如作用中）。 IBM Security Key Lifecycle Manager 將金鑰的 meta 資料儲存在 IBM Security Key Lifecycle Manager 資料庫中。

金鑰及憑證狀態

加密物件在其生命期限內，會透過數個狀態進行轉移，這些狀態的功能是反映金鑰或憑證的存在時間長度及資料是否受保護。 其他因數也會影響加密物件的狀態，例如金鑰或憑證是否受損。

IBM Security Key Lifecycle Manager 會保留這些加密物件狀態。

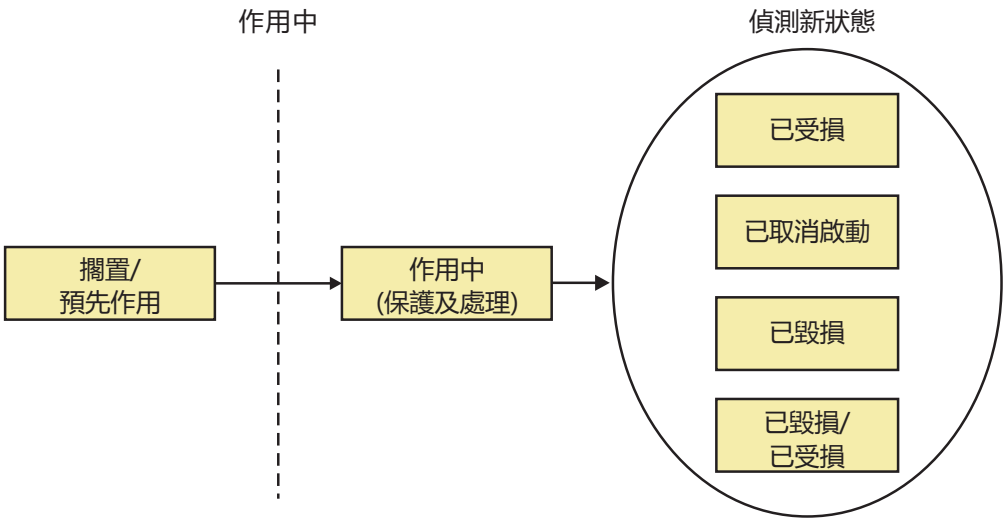

圖 1. 加密物件狀態

金鑰或憑證的狀態定義了容許的使用情形：

擱置
憑證申請項目正在擱置傳回已由憑證管理中心核准及認證的憑證。

前置作用中
物件存在，但尚未可用於任何加密用途，例如具有未來使用時間戳記的已移轉憑證。

作用中
物件正在用於保護及處理可能使用**處理開始日期**和**保護停止日期**屬性的資料。 例如，保護包括加密和簽章發出。 處理包括解密和簽章驗證。

已受損
物件的安全由於某種原因而受到懷疑。 已受損物件永遠不會回到**未受損**狀態，且無法用來保護資料。 僅使用該物件來處理授信用於處理已受損加密物件之用戶端中的受到密碼保護的資訊。

IBM Security Key Lifecycle Manager 會在物件受損之前立即保留物件狀態。 爲了處理先前受保護的資料，可能會繼續使用已受損物件。

取消啓動
物件將不用於套用加密保護（例如加密或簽署）。 但是，如果發生特別情況，則物件可與特殊許可權搭配使用以處理受密碼保護的資訊。 例如，處理包括解密或驗證。

已毀損
物件不再可用於任何用途。 此狀態會導致將物件從產品中移除。

已毀損-已受損
物件不再可用於任何用途。 此狀態會導致將物件從產品中移除。

不再處於作用中狀態的物件可以變更狀態，如下所示：

- 從已取消啓動狀態變更爲已毀損狀態。
- 從已取消啓動狀態變更爲已受損狀態。

- 從已受損狀態變更爲已毀損-已受損狀態。
- 從已毀損狀態變更爲已毀損-已受損狀態。

IBM Security Key Lifecycle Manager 金鑰儲存庫

IBM Security Key Lifecycle Manager 可以儲存對稱金鑰、公開金鑰、私密金鑰、它們的關聯憑證鏈及授信憑證。

當 IBM Security Key Lifecycle Manager 產生新金鑰時，金鑰及金鑰的 meta 資料會儲存在 IBM Security Key Lifecycle Manager 資料庫的金鑰表中。使用主要金鑰來保護金鑰資料。 建立憑證申請時，IBM Security Key Lifecycle Manager 會建立處於擱置中狀態的金鑰項目。

使用指令行介面，可以變更金鑰的資訊屬性。

已啓用加密的 3592 磁帶機及 LTO 磁帶機

IBM Security Key Lifecycle Manager 支援已啓用加密的 3592 磁帶機及 LTO 磁帶機。不支援未啓用加密的磁碟機。

IBM Security Key Lifecycle Manager 支援下列磁碟機類型：

- 3592 磁帶機

  已啓用資料加密功能的 TS1120 及 TS1130 磁帶機。
- LTO 磁帶機

  已啓用資料加密功能的 LTO Ultrium 4 磁帶機及 LTO Ultrium 5 磁帶機。

壓縮後，在磁帶機中以全線路速度執行加密。

如需 IBM Security Key Lifecycle Manager 所支援裝置的相關資訊，請參閱「儲存體硬體」小節，網址爲 http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html。

1. 輸入 IBM Security Key Lifecycle Manager。
2. 選取產品版本。 例如，2.6。
3. 選取作業系統。
4. 按一下**提交**。
5. 在「軟體產品相容性報告」頁面上，按一下**硬體**。

企業儲存體：DS8000® 儲存體控制器（2107 及 242x）

IBM Security Key Lifecycle Manager 支援 DS8000 儲存體控制器（IBM System Storage DS8000 Turbo 磁帶機）。

此支援要求 DS8000 儲存體控制器 Licensed Internal Code 層次 64.20.xxx.0 或更高層次上具有適當的微碼組合版本。

IBM System Storage®：DS5000 儲存體控制器（1818-51A、1818-53A 及 1814-20A）

IBM Security Key Lifecycle Manager 支援 DS5000 儲存體伺服器 (IBM System Storage DS5000)。

此支援適用於含有「自行加密光纖通道磁碟機（FDE/SED 磁碟機）」的 DS5000 系列儲存體系統（DS5100、DS5300 及 DS5020）。此外，必須購買選用的「全磁碟加密優質特性」，而且在儲存體子系統中啓用。 系統包括下列儲存體控制器：

- 1818-51A、1818-53A、FC 7358 DS5000 磁碟加密啓動
- 1814-20A、FC 7410 DS5020 磁碟加密啓動

如需設定 DS5000 儲存體子系統以支援 IBM Security Key Lifecycle Manager 的相關資訊，請參閱《IBM® DS Storage Manager 10.70 安裝與主機支援手冊》。

備份及還原

IBM Security Key Lifecycle Manager 提供跨平台備份及還原功能來保護重要的 IBM Security Key Lifecycle Manager 資訊。 您可以建立跨平台相容的備份並在作業系統之間還原相同的備份。 例如，Linux 系統上的備份可以在 Windows 系統上還原，反之亦然。

將 IBM Security Key Lifecycle Manager 與下列功能一起使用來保護資料：

備份 備份是作用中生產資訊的次要副本，可以在需要回復副本以讓使用者重新工作時使用。 發生災禍時，備份可讓業務再次啓動並執行。 由於備份著重於不斷變更的商業資訊，因此它們是短期的，通常會加以改寫。 可以在地理位置上分隔開的安全電腦上保留備份檔的副本。

視網站需求而定，可以保留抄本電腦來提供另一個 IBM Security Key Lifecycle Manager 伺服器，其中包括重要資料備份。 在主要 IBM Security Key Lifecycle Manager 伺服器無法使用時，抄本電腦會啓用快速回復。

還原 還原是使用備份的正式作業資料（例如 IBM Security Key Lifecycle Manager 金鑰儲存庫及其他重要資訊），使 IBM Security Key Lifecycle Manager 伺服器回復爲已知狀態。

審核

IBM Security Key Lifecycle Manager 以「共用基本事件 (CBE)」格式提供分散式系統上的審核記錄。審核記錄以純文字檔形式儲存在審核日誌中。

IBM Security Key Lifecycle Manager 自動化複製抄寫

IBM Security Key Lifecycle Manager 自動化複製抄寫使用程式來複製主要 IBM Security Key Lifecycle Manager 伺服器，最多可達 20 個副本。

您可以配置程式以抄寫金鑰，也可以抄寫其他配置資訊，例如新金鑰的輪替時間。此程式會自動化全部所需內容的抄寫作業。自動化複製抄寫可確保加密裝置可持續使用金鑰及憑證。

IBM Security Key Lifecycle Manager 提供一組作業，用來跨系統抄寫現行作用中的檔案及資料。 此抄寫能夠以獨立於伺服器作業系統及目錄結構的方式，將 IBM Security Key Lifecycle Manager 環境複製至多個伺服器。 例如，您可以將 Windows 系統上主要伺服器中的資料抄寫到 Linux 系統上的複製伺服器。 執行自動化抄寫程式時，會抄寫下列 IBM Security Key Lifecycle Manager 資料：

- IBM Security Key Lifecycle Manager 資料庫表格中的資料。
- IBM Security Key Lifecycle Manager 資料庫中的所有金鑰資料。

- IBM Security Key Lifecycle Manager 配置檔（除了抄寫配置檔以外）。

註：取得此資料作爲 IBM Security Key Lifecycle Manager 備份的一部分。在抄寫期間，抄寫配置檔不會備份並傳遞至複本。

IBM Security Key Lifecycle Manager 抄寫配置參數是在 `ReplicationSKLMConfig.properties` 配置檔中定義的。您可以使用圖形使用者介面、指令行介面或 REST 介面來變更抄寫配置檔的內容。 必須在屬於抄寫處理程序的所有系統上配置抄寫配置檔。 每一個 IBM Security Key Lifecycle Manager 實例皆定義爲*主要系統*（也就是要複製的系統）或者*複製系統*（也就是正在其中抄寫資料的系統）。

硬體安全模組中的主要金鑰

IBM Security Key Lifecycle Manager 支援「硬體安全模組 (HSM)」儲存主要金鑰，以保護資料庫中所儲存的所有密碼。

HSM 會給主要金鑰的儲存及使用新增額外保護。 主要金鑰會保護產品資料庫中所儲存的通行詞組。 主要通行詞組是金鑰儲存庫的密碼，客戶在產品中配置通行詞組以儲存 IBM Security Key Lifecycle Manager 中所建立的金鑰。

LDAP 與 IBM Security Key Lifecycle Manager 伺服器整合

LDAP（輕量型目錄存取通訊協定）支援在企業層級管理使用者 ID 和密碼，而不是在個別系統上管理此資料。 您可以將 IBM Security Key Lifecycle Manager 與 LDAP 使用者儲存庫整合。

您可以配置任何 LDAP 儲存庫（例如 IBM Security Directory Server 或 Microsoft Active Directory）中的 IBM Security Key Lifecycle Manager 使用者來存取 IBM Security Key Lifecycle Manager 伺服器，並呼叫伺服器 API 和 CLI。 您必須將 LDAP 使用者儲存庫新增至 WebSphere® Application Server 的聯合儲存庫並進行配置。 如需 LDAP 配置的相關資訊，請參閱LDAP 配置

伺服器配置精靈

您可以使用「伺服器配置精靈」來配置伺服器和用戶端裝置以進行 SSL/TLS 信號交換。SSL/TLS 信號交換可讓 IBM Security Key Lifecycle Manager 伺服器和用戶端裝置能夠建立用於安全通訊的連線。

在安裝 IBM Security Key Lifecycle Manager 之後，即會提供一個唯一可用的選項，用於利用「伺服器配置精靈」來配置 IBM Security Key Lifecycle Manager 以進行 SSL/TLS 信號交換。 若要開啓，請按一下**檢查配置參數及/或建立 SSL 伺服器憑證**鏈結。精靈會提供一個引導式方法來設定 SSL 信號交換程序。 如需 SSL/TLS 信號交換的相關資訊，請參閱實務範例：IBM Security Key Lifecycle Manager 伺服器與用戶端裝置之間的 SSL 信號交換設定。

技術概觀

可以使用 IBM Security Key Lifecycle Manager 來建立、備份及管理企業所使用的金鑰及憑證生命週期。 可以管理對稱金鑰、非對稱金鑰組及憑證的加密。 IBM Security Key Lifecycle Manager 也提供圖形使用者介面、指令行介面及 REST 介面來管理金鑰和憑證。

IBM Security Key Lifecycle Manager 會等待並回應透過 TCP/IP 通訊抵達的金鑰產生或金鑰擷取要求。 此通訊可以來自磁帶庫、磁帶控制器、磁帶子系統、裝置磁碟機或磁帶機。

主要 IBM Security Key Lifecycle Manager 提供了下列特性：

- 管理對稱金鑰、非對稱金鑰組及 X.509 第 3 版憑證。
- 管理金鑰的建立作業及生命週期，這些金鑰包含關於其預期使用情形的 meta 資料。
- 對於災難回復，提供受保護的重要資料備份。 例如，在分散式系統上，備份包括加密金鑰資料（受管理的實際金鑰及憑證）、關於金鑰的 meta 資料，及配置檔。
- 如需加密裝置的連續金鑰及憑證可用性，您可以提供自動抄寫程式以抄寫金鑰，也可以抄寫其他配置資訊，例如新金鑰的輪替時間。
- 檔案型審核日誌會隨著作業系統而有所不同。在分散式系統上，審核日誌以純文字檔形式包含基於「共用基本事件 (CBE)」安全事件規格的資料。您也可以配置 IBM Security Key Lifecycle Manager，以 syslog 格式來產生審核記錄，並將其傳送給 syslog 伺服器。

金鑰概觀

加密金鑰通常是專門產生用來編碼及解碼資料的隨機位元串。 加密金鑰是使用演算法來建立，這些演算法設計成確保每個金鑰都是唯一的且無法預期。 依照這個方式建構的金鑰越長，加密編碼的破解也就越難。

IBM Security Key Lifecycle Manager 使用兩種類型的加密演算法：對稱演算法及非對稱演算法。 對稱或秘密金鑰加密的加密和解密都使用單一金鑰。 對稱金鑰加密用來有效地加密大量資料。

「進階加密標準 (AES)」金鑰是對稱金鑰，可以具有三種不同的金鑰長度（128、192 或 256 位元）。 AES 是由美國政府認可及建議的加密標準。 256 位元金鑰是 AES 所容許的最長長度。 依預設，IBM Security Key Lifecycle Manager 會產生 256 位元 AES 金鑰。

非對稱或公開/私密加密使用金鑰組。使用一個金鑰加密的資料只能使用公開/私密金鑰組中的另一個金鑰進行解密。 產生非對稱金鑰組時，公開金鑰通常用來加密，而私密金鑰通常用來解密。

IBM Security Key Lifecycle Manager 使用對稱金鑰及非對稱金鑰。 對稱加密支援高速加密使用者或主機資料。 非對稱加密可以保護對稱金鑰，加密速度慢一些，但這是必要的。

美國聯邦資訊處理標準

聯邦政府要求其所有加密提供者必須經過 FIPS 140 認證。 不斷增長的私有社群也會採用此標準。 由協力廠商提供且符合政府標準的加密功能憑證，其價值在這個安全意識非常強的世界裡也不斷增加。

如果您將私密金鑰匯出至 PKCS#12 檔，請確保在該檔案離開電腦之前，使用 FIPS 核准的方法來包裝含有金鑰的該檔案。

IBM Security Key Lifecycle Manager 本身並不提供加密功能，因此不需要或取得 FIPS 140-2 憑證。 然而，IBM Security Key Lifecycle Manager 在 IBM Java Cryptographic

Extension 元件中，利用了 IBM JVM 的加密功能。 這些功能容許選取及使用 IBMJCEFIPS 加密提供者，此提供者具有 FIPS 140-2 層次 1 憑證。

如需 IBMJCEFIPS 提供者及其選項和使用的相關資訊，請參閱 IBM Java 安全資訊說明文件 (http://www-01.ibm.com/support/knowledgecenter/SSYKE2_6.0.0/com.ibm.java.security.component.60.doc/security-component/fips.html)。

如需如何配置 FIPS 的程序，請參閱下列 Technote：http://www-01.ibm.com/support/docview.wss?uid=swg21395541

請參閱特定軟硬體加密提供者的說明文件，以取得其產品是否已經過 FIPS 140-2 認證的資訊。

註：將 **fips** 配置內容設爲 on 會導致 IBM Security Key Lifecycle Manager 對所有加密函數都使用 IBMJCEFIPS 提供者。

IBM Security Key Lifecycle Manager 中 NSA 套組 B 加密法的合規

您可以配置 IBM Security Key Lifecycle Manager，使其符合 US National Security Agency (NSA) 所指定的定義加密安全需求的標準。

NSA 套組 B 需要 TLS 1.2 通訊協定及密碼組合，並使用 ECDSA-256 及 ECDSA-384 配置爲 128 位元最低安全等級，以用於用戶端或伺服器鑑別。爲了支援套組 B 設定檔，已提供下列 Java 系統內容：

```
com.ibm.jsse2.suiteB=128|192|false
```

當您設定 **com.ibm.jsse2.suiteB** 系統內容時，IBMJSSE2 確保遵守指定的安全層次。IBMJSSE2 可驗證通訊協定、金鑰和憑證是否符合所要求的設定檔。如需相關資訊，請參閱https://www-01.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/suiteb.html。

若要在 IBM Security Key Lifecycle Manager 中啓用套組 B 合規，您必須使用下列選項來配置 SKLMConfig.properties 內容檔：

```
suiteB=128|192
```

當您將 **suiteB** 配置爲值 128 或 192 時，會將下列內容新增至內容檔，或當已存在這些內容時更新其值：

```
TransportListener.ssl.protocols=SSL_TLSv2
requireSHA2Signatures=true
autoScaleSignatureHash=true
useThisECKeySize=256(if suiteB is 128)|384(if suiteB is 192)
```

針對套組 B 合規配置 IBM Security Key Lifecycle Manager

1. 停止 IBM Security Key Lifecycle Manager 伺服器。如需指示，請參閱在分散式系統上啓動和停止 IBM Security Key Lifecycle Manager 伺服器。
2. 編輯 *SKLM_HOME*/config/SKLMConfig.properties 檔中的下列內容，並儲存檔案：

   ```
   suiteB=128|192
   ```

   - 值 128 指定了 128 位元的最低安全等級。
   - 值 192 指定了 192 位元的最低安全等級。

您還可以使用 tklmConfigUpdateEntry CLI 指令或 更新配置內容 REST 服務來更新 SKLMConfig.properties 檔。

3. 重新啓動伺服器。

使用金鑰管理交互作業能力通訊協定進行金鑰管理

IBM Security Key Lifecycle Manager 伺服器支援與用戶端進行「金鑰管理交互作業能力通訊協定 (KMIP)」通訊，以對加密資料執行金鑰管理作業。 此資料包括對稱金鑰、非對稱金鑰、憑證及用來建立與控制其用途的範本。

「金鑰管理交互作業能力通訊協定」屬於「Organization for the Advancement of Structured Information Standards (OASIS)」標準化專案，用來加密所儲存資料及進行加密金鑰管理。

如需相關資訊，請參閱「金鑰管理交互作業能力通訊協定」說明文件 (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip)。

您可以使用 IBM Security Key Lifecycle Manager 圖形使用者介面，來管理及控制伺服器支援的加密資料（物件）。如需管理 KMIP 物件的相關資訊，請參閱KMIP 物件管理。

IBM Security Key Lifecycle Manager 支援的 KMIP 設定檔

IBM Security Key Lifecycle Manager 支援用於 KMIP 伺服器與用戶端互動的下列設定檔：

- 基本探索版本伺服器設定檔
- 基本基準線伺服器 KMIP 設定檔
- 基本密碼資料伺服器 KMIP 設定檔
- 基本對稱金鑰儲存庫及伺服器 KMIP 設定檔
- 基本對稱金鑰晶圓代工及伺服器 KMIP 設定檔
- 基本非對稱金鑰儲存庫伺服器 KMIP 設定檔
- 基本非對稱金鑰及憑證庫伺服器 KMIP 設定檔
- 基本非對稱金鑰晶圓代工及伺服器 KMIP 設定檔
- 基本憑證伺服器 KMIP 設定檔（PEM 憑證格式除外）
- 基本非對稱金鑰晶圓代工及憑證伺服器 KMIP 設定檔（PEM 憑證格式除外）
- 探索版本 TLS 1.2 鑑別伺服器設定檔
- 基準線伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 密碼資料伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 對稱金鑰儲存庫及伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 對稱金鑰晶圓代工及伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 非對稱金鑰儲存庫伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 非對稱金鑰及憑證庫伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 非對稱金鑰晶圓代工及伺服器 TLS 1.2 鑑別 KMIP 設定檔
- 憑證伺服器 TLS 1.2 鑑別 KMIP 設定檔（PEM 憑證格式除外）
- 非對稱金鑰晶圓代工及憑證伺服器 TLS 1.2 鑑別 KMIP 設定檔（PEM 憑證格式除外）

如需設定檔的相關資訊，請參閱「KMIP 設定檔 1.2」說明文件 (http://docs.oasis-open.org/kmip/profiles/v1.2/kmip-profiles-v1.2.pdf)。

金鑰及憑證的 KMIP 屬性

IBM Security Key Lifecycle Manager 支援下列作業：

- 追蹤關於圖形使用者介面資訊的 KMIP 資訊：
  - 是否配置了 KMIP 埠及逾時設定。
  - 現行 KMIP 憑證，指出正在將哪個憑證用於安全伺服器或伺服器/用戶端通訊。
  - 指定 SSL/KMIP 還是 SSL 用於安全通訊。
- 可以更新金鑰及憑證的 KMIP 屬性。

  例如，可以使用 **tklmKeyAttributeUpdate** 指令來更新：

  name
  指定用來識別或尋找物件的名稱。此屬性是一個金鑰管理交互作業能力通訊協定屬性。

  applicationSpecificInformation
  將應用程式名稱空間資訊指定爲金鑰管理交互作業能力通訊協定屬性。

  contactInformation
  將聯絡資訊指定爲金鑰管理交互作業能力通訊協定屬性。

  cryptoParams *cryptoparameter1, cryptoparameterN*
  指定用於透過利用物件進行加密作業的加密參數。 此屬性是一個金鑰管理交互作業能力通訊協定屬性。

  customAttribute
  以字串格式將自訂屬性指定爲金鑰管理交互作業能力通訊協定屬性。用戶端特定屬性必須以字元 ″x-″（x 連字號）開頭，而伺服器特定屬性必須以 ″y-″（y 連字號）開頭。

  link
  指定從一個受管理加密物件到另一個緊密相關之目標受管理加密物件的鏈結。 此屬性是一個金鑰管理交互作業能力通訊協定屬性。

  objectGroup
  指定此物件可能隸屬於的一個以上物件群組名稱。 此屬性是一個金鑰管理交互作業能力通訊協定屬性。

  processStartDate
  指定可以將對稱金鑰物件用於處理用途的日期。 在該日期之後無法變更值。如果您指定早於現行日期的日期，則值會設爲現行日期。 此屬性是一個金鑰管理交互作業能力通訊協定屬性。

  protectStopDate
  指定無法將物件用於處理用途的日期。 在該日期之後無法變更值。 如果您指定早於現行日期的日期，則值會設爲現行日期。 此屬性是一個金鑰管理交互作業能力通訊協定屬性。

usageLimits
將位元組數總計 (BYTE) 或物件數總計 (OBJECT) 指定爲金鑰管理交互作業能力通訊協定屬性。一旦使用此物件之後，就無法修改此值。 例如，**GetUsageAllocation** 會呼叫此物件。

- 列出及刪除用戶端登錄的 KMIP 範本。

用戶端使用範本，以標準化或便利方式來指定新物件的加密屬性。 範本是受管理物件，含有作業中由用戶端設定給加密物件的屬性。 例如，用戶端可以設定應用程式特定資訊。

tklmKMIPTemplateList
列出 IBM Security Key Lifecycle Manager 所提供的 KMIP 範本。例如，可列出所有範本。

tklmKMIPTemplateDelete
刪除用戶端向 IBM Security Key Lifecycle Manager 登錄的 KMIP 範本。

- 列出及刪除密碼資料（例如密碼，或用來產生金鑰的種子值）。

tklmSecretDataDelete
刪除 KMIP 用戶端傳送至 IBM Security Key Lifecycle Manager 的密碼資料。

tklmSecretDataList
列出 KMIP 用戶端傳送至 IBM Security Key Lifecycle Manager 的密碼資料。

- 設定預設埠及逾時內容

KMIPListener.ssl.port
指定 IBM Security Key Lifecycle Manager 伺服器上用來接聽來自磁帶庫之要求的埠。 伺服器使用「金鑰管理交互作業能力通訊協定」，透過 SSL Socket 進行通訊。

TransportListener.ssl.port
指定 IBM Security Key Lifecycle Manager 伺服器上用來接聽來自磁帶庫（使用 SSL 通訊協定進行通訊）之要求的埠。

TransportListener.ssl.timeout
指定 Socket 在關閉之前等待 read() 的時間長度。此內容用於 SSL Socket。

- 啓用或停用對來自 KMIP 用戶端之要求進行刪除的作業。

已鑑別的用戶端可以要求刪除作業，但這些作業可能會嚴重影響金鑰可用性、伺服器效能及金鑰安全性。 使用 **tklmDeviceGroupAttributeUpdate** 或 **tklmDeviceGroupCreate** 指令來指定 enableKMIPDelete 屬性，以判斷 IBM Security Key Lifecycle Manager 是否處理這些要求。

金鑰提供管理

IBM Security Key Lifecycle Manager 解決方案可以協助已啓用 IBM 加密的裝置，來產生、保護、儲存及保留加密金鑰。 可以使用金鑰來加密寫入裝置的資訊，及解密從裝置讀取的資訊。

IBM Security Key Lifecycle Manager 用來作爲背景處理程序，等待透過它本身與磁帶庫、磁帶控制器、磁帶子系統、裝置驅動程式或磁帶機之間的 TCP/IP 通訊路徑傳送給它的金鑰產生或金鑰擷取要求。 當磁碟機寫入加密資料時，會先從 IBM Security Key Lifecycle Manager 要求加密金鑰。

AES 金鑰及 3592 磁帶機：

當 3592 磁帶機寫入加密資料時，會先從 IBM Security Key Lifecycle Manager 要求加密金鑰。

收到要求時，IBM Security Key Lifecycle Manager 便會產生「進階加密標準 (AES)」金鑰。 此金鑰會以兩種受保護形式提供給磁帶機：

- 使用 Rivest-Shamir-Adleman (RSA) 金鑰組進行加密或包裝。 3592 磁帶機將此金鑰副本寫入卡匣記憶體，以及卡匣中磁帶媒體上的額外位置作爲備援。
- 單獨包裝以安全傳送至磁帶機，到達磁帶機後便解除包裝。 使用內部金鑰來加密寫入磁帶的資料。

當 3592 磁帶機讀取加密磁帶匣時，磁帶上的受保護 AES 金鑰會傳送至 IBM Security Key Lifecycle Manager，然後在其中解除包裝已包裝的 AES 金鑰。 AES 金鑰隨後會使用不同的金鑰進行包裝，以安全傳回至磁帶機。 此金鑰會解除包裝，並且用來解密儲存在磁帶上的資料。 IBM Security Key Lifecycle Manager 還容許使用不同於寫入磁帶時所使用原始金鑰的 RSA 金鑰，來重新包裝或重新加密受保護的 AES 金鑰。如果出現非預期的需要，必須將磁區匯出給未包括其公開金鑰的事業夥伴，則重新加密就非常有用。 有了重新加密功能，就不需要重新寫入整個磁帶，並且讓磁帶匣的資料金鑰可以使用事業夥伴的公開金鑰進行重新加密。

非對稱金鑰及 3592 磁帶機：

除了 256 位元 AES 對稱資料金鑰之外，IBM Security Key Lifecycle Manager 還使用公開/私密（非對稱）金鑰加密法來保護對稱資料加密金鑰。 系統會產生這些金鑰，並且當這些金鑰在 IBM Security Key Lifecycle Manager 與 3592 磁帶機之間傳遞時會加以擷取。

公開/私密金鑰加密法也用來驗證 IBM Security Key Lifecycle Manager 向其提供金鑰的磁帶機身分。

當 3592 磁帶機要求金鑰時，IBM Security Key Lifecycle Manager 會產生隨機對稱資料加密金鑰。 利用公開/私密金鑰加密法，透過使用金鑰加密金鑰（爲非對稱金鑰組的公開金鑰）來包裝資料加密金鑰。

包裝的資料金鑰，以及解除包裝對稱金鑰時所需私密金鑰的相關金鑰標籤資訊，組成了稱爲外部加密資料金鑰結構的數位信封。 此結構儲存在用於存放使用此方法進行加密之資料的任何磁帶匣中的磁帶標頭區域內。 用來解密資料的金鑰與資料一起儲存在磁帶本身，以非對稱方式進行保護，且進行了公開/私密金鑰包裝。 從下列兩個來源之一取得用來包裝資料金鑰的公開金鑰：

- 儲存在金鑰儲存庫中的公開金鑰（內部產生公開/私密金鑰組的一部分）。
- 儲存在金鑰儲存庫中的憑證（例如，來自事業夥伴）。

儲存在金鑰儲存庫中的憑證及金鑰，是容許磁帶機或磁帶庫解密磁帶上資料的控制點。 如果金鑰儲存庫中沒有此資訊，則無法讀取磁帶。 請務必防止未獲授權的使用者從金鑰儲存庫中取得私密金鑰。 必須一律使金鑰儲存庫可供您用來讀取磁帶。

資料加密金鑰只以受保護的包裝形式儲存在磁帶上。 如果加密的磁帶將由 3592 磁帶機讀取，則磁帶機會將外部加密的資料金鑰傳送至 IBM Security Key Lifecycle Man-

ager。 IBM Security Key Lifecycle Manager 會從別名或金鑰標籤判定，使用其金鑰儲存庫中的哪個私密金鑰加密金鑰，來解除包裝外部加密的資料金鑰及回復資料加密金鑰。

資料加密金鑰在回復後，便會使用不同的金鑰進行包裝，而此金鑰可由磁帶機進行解密。 此金鑰隨後會傳回給磁帶機，讓磁帶機可以解密資料。

IBM Security Key Lifecycle Manager 使用別名（也稱爲金鑰標籤）來識別公開/私密金鑰；當您使用 3592 磁帶機進行加密時，這些公開/私密金鑰用來包裝外部加密資料金鑰。 可以使用 IBM Security Key Lifecycle Manager 圖形使用者介面或指令行介面，給每個磁帶機定義特定別名。

IBM Security Key Lifecycle Manager 容許給每個加密磁帶機至少定義兩個別名（憑證或金鑰標籤）。 這些別名容許存取組織內部或外部其他位置的加密資料。 其中一個別名的私密金鑰必須是已知的。 如果不想指定兩個不同的金鑰標籤或別名，則可以定義兩個具有相同值的別名。

AES 金鑰及 LTO 磁帶機：

當 LTO 磁帶機寫入加密資料時，會先從 IBM Security Key Lifecycle Manager 要求加密金鑰。

收到要求後，IBM Security Key Lifecycle Manager 會從金鑰儲存庫中取得現有 AES 金鑰。 此金鑰隨後會包裝，以安全傳送至磁帶機。 此金鑰隨後會解除包裝，並且用來加密已寫入磁帶的資料。

當 LTO 磁帶機讀取加密的磁帶時，IBM Security Key Lifecycle Manager 會從金鑰儲存庫中取得所需金鑰。 此金鑰基於磁帶上金鑰 ID 中的資訊，且會將它進行包裝提供給磁帶機以便安全傳送。

對稱金鑰及 LTO 磁帶機：

IBM Security Key Lifecycle Manager 僅使用對稱資料金鑰來處理 LTO 磁帶機上的加密作業。

當 LTO 磁帶機要求金鑰時，IBM Security Key Lifecycle Manager 會使用指定給磁帶機的別名。 如果未給磁帶機指定別名，則 IBM Security Key Lifecycle Manager 會使用金鑰群組、金鑰別名清單或金鑰別名範圍中的別名。

金鑰群組中的金鑰是以循環方式使用，有助於更加平衡地使用金鑰。

所選別名與金鑰儲存庫中預先安裝的對稱資料金鑰相關聯。 IBM Security Key Lifecycle Manager 會將資料金鑰傳送至 LTO 磁帶機以加密資料。 所選別名也會轉換成稱爲資料金鑰 ID 的實體，其會與加密資料一起寫入磁帶。 IBM Security Key Lifecycle Manager 可以使用資料金鑰 ID 來識別讀取 LTO 磁帶時解密資料所需的正確資料金鑰。

AES 金鑰及 DS8000 Turbo 磁帶機：

當 DS8000 Turbo 磁帶機啓動時，裝置會從 IBM Security Key Lifecycle Manager 要求解除鎖定金鑰。

如果 DS8000 Turbo 磁帶機爲其解除鎖定金鑰要求新金鑰，則 IBM Security Key Lifecycle Manager 會產生「進階加密標準 (AES)」金鑰。 此金鑰隨後會以下列兩種受保護形式提供給磁碟機：

- 使用 Rivest-Shamir-Adleman (RSA) 金鑰組進行加密（包裝）。 DS8000 Turbo 磁帶機會將此金鑰副本儲存在陣列上的未加密分割區中。
- 單獨包裝以安全傳送至磁碟機，到達磁碟機後便解除包裝，並且使用內部金鑰來解除鎖定陣列。

如果 DS8000 Turbo 磁帶機要求現有解除鎖定金鑰，則陣列上的受保護 AES 金鑰會傳送至 IBM Security Key Lifecycle Manager，然後在其中解除包裝已包裝的 AES 金鑰。 AES 金鑰隨後會使用不同的金鑰進行包裝，以安全傳回至 DS8000 Turbo 磁帶機。 此金鑰會解除包裝，並且用來解除鎖定陣列。

非對稱金鑰及 DS8000 Turbo 磁帶機：

IBM Security Key Lifecycle Manager 還使用公開/私密（非對稱）金鑰加密法來保護 IBM Security Key Lifecycle Manager 與 DS8000 Turbo 磁帶機之間傳遞的 256 位元 AES 對稱資料加密金鑰。

公開/私密金鑰加密法也用來驗證 IBM Security Key Lifecycle Manager 向其提供金鑰的磁帶機身分。 當 DS8000 Turbo 磁帶機要求新金鑰時，IBM Security Key Lifecycle Manager 會產生隨機對稱資料加密金鑰。 利用公開/私密金鑰加密法，透過使用金鑰加密金鑰（爲非對稱金鑰組的公開金鑰）來包裝資料加密金鑰。

包裝的資料金鑰，以及解除包裝對稱金鑰時所需私密金鑰的相關金鑰標籤資訊，組成了稱爲外部加密資料金鑰結構的數位信封。此結構儲存在用於存放使用此方法進行加密之資料的任何磁帶匣中的磁帶標頭區域內。 用來解密資料的金鑰與資料一起儲存在磁帶本身，以非對稱方式進行保護，且進行了公開/私密金鑰包裝。 從下列兩個來源之一取得用來包裝資料金鑰的公開金鑰：

- 儲存在金鑰儲存庫中的憑證（例如，來自事業夥伴）。
- 儲存在金鑰儲存庫中的公開金鑰（內部產生公開/私密金鑰組的一部分）。

儲存在金鑰儲存庫中的憑證及金鑰，是容許解除鎖定 DS8000 Turbo 磁帶機的控制點。 如果金鑰儲存庫中沒有此資訊，則無法解除鎖定 DS8000 Turbo 磁帶機。

必須防止未獲授權的使用者從金鑰儲存庫中取得私密金鑰，並且一律使金鑰儲存庫可供您用來解除鎖定陣列。 資料加密金鑰只以受保護的包裝形式儲存在 DS8000 Turbo 磁帶機上。

爲了解除鎖定 DS8000 Turbo 磁帶機，DS8000 Turbo 磁帶機會將外部加密的資料金鑰傳送至 IBM Security Key Lifecycle Manager。 IBM Security Key Lifecycle Manager 會從別名或金鑰標籤判定，使用其金鑰儲存庫中的哪個私密金鑰加密金鑰，來解除包裝外部加密的資料金鑰及回復資料加密金鑰。 資料加密金鑰在回復後，便會使用不同的金鑰進行包裝，而此金鑰可由磁帶機進行解密。 此金鑰會傳回給磁帶機，讓磁帶機可以解密資料。

IBM Security Key Lifecycle Manager 使用別名（也稱爲金鑰標籤）來識別您用來包裝解除鎖定金鑰的公開/私密金鑰。 可以給每個裝置定義特定別名。 IBM Security Key Lifecycle Manager 容許給每個 DS8000 Turbo 磁帶機定義多達兩個別名（憑證或金鑰標籤），以防止出現死鎖狀況。 IBM Security Key Lifecycle Manager 和 DS8000 Turbo

磁帶機必須位在同一個系統上。 必須先解除鎖定 DS8000 Turbo 磁帶機，IBM Security Key Lifecycle Manager 才能啓動。 其中一個別名的私密金鑰必須是已知的。 如果不想指定兩個不同的金鑰標籤或別名，則可以定義兩個具有相同值的別名。

AES 金鑰及 DS5000 儲存體伺服器：

當 DS5000 儲存體伺服器啓動時，裝置會從 IBM Security Key Lifecycle Manager 要求金鑰以解除鎖定磁碟機。

在回應中，IBM Security Key Lifecycle Manager 會從金鑰儲存庫中取得現有 AES 金鑰。 IBM Security Key Lifecycle Manager 會包裝 AES 金鑰以安全傳送至 DS5000 儲存體伺服器，其會解除包裝金鑰並使用金鑰來解除鎖定磁碟機。

對稱金鑰及 DS5000 儲存體伺服器：

IBM Security Key Lifecycle Manager 僅使用對稱資料金鑰作爲 DS5000 儲存體伺服器的解除鎖定金鑰。

當 DS5000 儲存體伺服器要求金鑰時，IBM Security Key Lifecycle Manager 會使用要求所指定的別名來取得金鑰。 如果 DS5000 儲存體伺服器要求沒有指定別名，則 IBM Security Key Lifecycle Manager 會從與發出要求之 DS5000 儲存體伺服器 相關聯的金鑰清單中取得別名。 清單中的金鑰是以循環方式提供，以平衡地使用金鑰。

所選別名與金鑰儲存庫中預先安裝的對稱資料金鑰相關聯。 IBM Security Key Lifecycle Manager 會將對稱資料金鑰傳送至裝置，以解除鎖定此陣列的磁碟機。 所選別名也會轉換成稱爲資料金鑰 ID 的實體，其由 DS5000 儲存體伺服器進行儲存。 必要時，IBM Security Key Lifecycle Manager 可以使用資料金鑰 ID 來識別正確的資料金鑰。

主要元件

分散式系統上的 IBM Security Key Lifecycle Manager 解決方案包括 IBM Security Key Lifecycle Manager 伺服器、WebSphere Application Server 及 DB2®。

在分散式系統上，安裝 IBM Security Key Lifecycle Manager 也會安裝必備項目。

執行時期環境

- 分散式系統

  WebSphere Application Server 執行 Java 虛擬機器 (JVM)，給應用程式碼提供執行時期環境。 應用程式伺服器提供通訊安全、記載、傳訊與 Web 服務。

資料庫伺服器

IBM Security Key Lifecycle Manager 將金鑰資料儲存在 DB2 關聯式資料庫中。使用 IBM Security Key Lifecycle Manager 來管理 DB2。

在 Windows 系統及 Linux 或 AIX 等系統上進行部署

在 Windows 系統及 Linux 或 AIX 等其他系統上，IBM Security Key Lifecycle Manager 安裝程式會將 IBM Security Key Lifecycle Manager 伺服器及必要的中介軟體元件部署在同一部電腦上。 必須確保電腦具有所需記憶體、速度及可用磁碟空間來滿足工作量。

IBM Security Key Lifecycle Manager 可以在網域控制站環境中的成員伺服器上執行，但在主要或備份網域控制站上則不受支援。

圖 2. Windows 系統及 Linux 或 AIX 等系統上的主要元件

部署主要伺服器及抄本伺服器

如果要確保可用性，請部署主要 IBM Security Key Lifecycle Manager 伺服器，然後在個別系統上，部署主要 IBM Security Key Lifecycle Manager 伺服器的抄本。

在 Windows 系統及其他系統（例如 Linux 或 AIX）上，兩部電腦都必須具有所需記憶體、速度及可用磁碟空間來符合工作量。 在這兩部電腦上，作業系統及中介軟體元件都必須是相同的。 安裝路徑也必須相同。

圖 3. 主要及抄本 IBM Security Key Lifecycle Manager 伺服器

抄本系統需求

抄本系統必須具有相同的作業系統、資料庫及 IBM Security Key Lifecycle Manager 應用程式，其中包括來自現行 IBM Security Key Lifecycle Manager 伺服器備份檔的重要資料。 安裝路徑也必須相同。

請確保兩個系統符合下列需求且具有相同版本及修正層次：

- 作業系統及修正程式或修補程式。
- DB2 及所需可用磁碟空間。 資料庫必須存在於執行 IBM Security Key Lifecycle Manager 伺服器的同一個系統上。
- IBM Security Key Lifecycle Manager 伺服器.

必須將現行 IBM Security Key Lifecycle Manager 伺服器備份檔手動複製到抄本系統。 IBM Security Key Lifecycle Manager 不會自動地在兩個 IBM Security Key Lifecycle Manager 伺服器之間同步化資料。

備份及還原

備份及還原作業會爲重要資料提供保護，並且需要考量網站實務以確保伺服器可用性及執行時期功能。

IBM Security Key Lifecycle Manager 會以獨立於伺服器作業系統及目錄結構的方式來建立備份檔。 備份檔包含 IBM Security Key Lifecycle Manager 伺服器現行狀態的重要資料。 網站實務必須考量如何確保金鑰提供可以使用。

您可以使用跨平台備份公用程式，在舊版 IBM Security Key Lifecycle Manager 上執行備份作業以備份重要資料。 您可以在現行版本的 IBM Security Key Lifecycle Manager 上，將這些備份檔還原到與從中進行備份之作業系統不同的作業系統。

註：從 IBM Security Key Lifecycle Manager 2.6 版開始，不支援 Solaris 作業系統。如果您在 Solaris 系統上使用 IBM Security Key Lifecycle Manager，請使用跨平台備份公用程式來備份資料。 然後可以在部署於任何受支援作業系統（例如 Windows、Linux 或 AIX）中的 IBM Security Key Lifecycle Manager 2.6 版系統上執行還原作業來還原資料。

IBM Security Key Lifecycle Manager 備份及還原作業支援使用 AES 256 位元金鑰長度進行資料加密/解密，以符合 PCI DSS（支付卡產業資料安全標準）標準，來提高資料安全。

只有在使用 AES 256 位元主要金鑰進行資料加密時，備份及還原作業才會使用 AES 256 位元長度金鑰來加密或解密資料。 如果 IBM Security Key Lifecycle Manager 備份作業使用 AES 256 位元金鑰進行資料加密，則必須安裝 Java Cryptography Extension (JCE) 無限制強度適用範圍原則檔。 如需安裝指示，請參閱安裝 Java Cryptography Extension 無限制強度適用範圍原則檔。

註：在現行版本中，安裝 IBM Security Key Lifecycle Manager 之後，依預設會產生 AES 256 位元主要金鑰，且會在伺服器中安裝 JCE 無限制強度適用範圍原則檔案。

備份檔中資料的種類

IBM Security Key Lifecycle Manager 的備份檔包含重要資料。 例如，視配置而定，它可能包含金鑰資料、配置檔及其他資訊。

下列資料種類需要備份保護：

IBM Security Key Lifecycle Manager 配置檔

用來定義所選 IBM Security Key Lifecycle Manager 活動（例如，審核設定及其他您可以針對系統配置進行自訂的值）的內容。

IBM Security Key Lifecycle Manager 資料庫

關於 IBM Security Key Lifecycle Manager 物件（例如，裝置、金鑰群組、憑證、金鑰資料及磁碟機）的資料。

備份檔安全

確保您不會意外地毀損備份檔或放錯其加密密碼。

如果要爲備份檔提供安全，請執行下列作業：

- 將備份檔副本保留到 IBM Security Key Lifecycle Manager 電腦之外的位置，而不是保留到 IBM Security Key Lifecycle Manager 目錄路徑。 如果移除了 IBM Security Key Lifecycle Manager，則個別位置可確保其他程序無法移除審核日誌及備份檔。
- 請勿編輯備份 Jar 檔中的檔案，否則，這些檔案會變成無法讀取。
- 請確保保留用來加密備份檔的密碼。 需要相同的密碼才能解密及還原檔案。

還原

還原是使用備份的正式作業資料（例如 IBM Security Key Lifecycle Manager 金鑰資料及其他重要資訊），使 IBM Security Key Lifecycle Manager 伺服器回復爲已知狀態。

IBM Security Key Lifecycle Manager 支援跨作業系統的還原作業。 您可以在與從中進行備份之作業系統不同的作業系統上，還原 IBM Security Key Lifecycle Manager 備份檔。 例如，您可以將在 Linux 系統上建立的備份還原到 Windows 系統。

從您早先時候指定的位置（不在 IBM Security Key Lifecycle Manager 目錄路徑中）擷取備份檔副本。 您也必須知道用來加密備份檔的密碼。 在主要 IBM Security Key Lifecycle Manager 伺服器上，使用密碼來解密及還原檔案。

還原備份檔之前，請確保備份資訊清單檔列出保存檔中的 IBM Security Key Lifecycle Manager 資料檔案。 當執行備份作業時，會隨備份保存檔一起建立資訊清單檔。

在開始還原作業之前，請先隔離系統以進行維護。 執行現有系統的備份。如果在還原過程中發生任何問題，您可以稍後使用此備份來將系統返回至原始狀態。在執行還原之後，您必須立即重新啓動 IBM Security Key Lifecycle Manager 伺服器。 在將 IBM Security Key Lifecycle Manager 伺服器帶回到正式作業之前，請先驗證環境。

登入 URL 及起始使用者 ID

如果要在安裝 IBM Security Key Lifecycle Manager 後開始使用，請取得登入 URL 及起始 IBM Security Key Lifecycle Manager 管理者使用者 ID 和密碼。

存取需求

以管理者（root 使用者）身分安裝 IBM Security Key Lifecycle Manager。

您也能以非 root 使用者身分安裝 IBM Security Key Lifecycle Manager（僅限於 Linux 作業系統）。

登入 URL

使用登入 URL 來存取 IBM Security Key Lifecycle Manager Web 介面。 IBM Security Key Lifecycle Manager 管理主控台的登入 URL 爲：

`https://ip-address:port/ibm/SKLM/login.jsp`

ip-address 的值爲 IBM Security Key Lifecycle Manager 伺服器的 IP 位址或 DNS 位址。

port 的值是 IBM Security Key Lifecycle Manager 伺服器 在其上接聽要求的埠號。

如果使用 HTTPS 位址，則埠的預設值爲 9080：

`https://ip-address:9080/ibm/SKLM/login.jsp`

請勿使用大於 65520 的埠值。

在 Windows 系統上，此資訊位於開始功能表上。按一下**開始 > 所有程式 > IBM Security Key Lifecycle Manager 2.6**。

WebSphere Application Server 管理主控台的登入 URL 爲：

`https://ip-address:port/ibm/console/logon.jsp`

ip-address 的值爲 WebSphere Application Server的 IP 位址或 DNS 位址。

port 的值是 WebSphere Application Server 在其上接聽要求的埠號。

WebSphere Application Server 資訊畫面上的預設埠爲 9083。 移轉期間，或者如果預設埠由於其他原因而具有衝突，WebSphere Application Server 會自動選取另一個可用的埠。

安裝完成畫面會指出已配置給 WebSphere Application Server 的埠。 Windows 開始功能表包含用來以正確埠號連接 WebSphere Application Server 的項目。

按一下 **IBM WebSphere > IBM WebSphere Application Server 8.5.5 版 > 設定檔 > KLMProfile > 管理主控台**。

管理者使用者 ID 和密碼

安裝 IBM Security Key Lifecycle Manager 會提供預設管理者使用者 ID WASAdmin、SKLMAdmin 及 `sklmdb26`。

表 1. 管理者使用者 ID 和密碼

程式	使用者 ID	密碼
分散式系統 對於分散式作業系統，必須由本端管理 ID 執行安裝，此 ID 是 root 使用者（AIX 或 Linux 系統）或隸屬於 Administrators 群組（Windows 系統）。 請勿使用網域使用者 ID 來安裝 IBM Security Key Lifecycle Manager。 您可能具有其中的一個以上使用者 ID：		

表 1. 管理者使用者 ID 和密碼 (繼續)

程式	使用者 ID	密碼
IBM Security Key Lifecycle Manager 管理者	**SKLMAdmin** 作爲對所有作業皆具有完整存取權的主要管理者，此使用者 ID 在名爲 `klmSecurityOfficerGroup` 的群組中具有 `klmSecurityOfficer` 超級使用者角色。此使用者 ID 不區分大小寫。 或者，使用 **sklmadmin**。使用 SKLMAdmin 使用者 ID 來管理 IBM Security Key Lifecycle Manager。 有了 SKLMAdmin 使用者 ID，您可以執行下列作業： • 檢視及使用 IBM Security Key Lifecycle Manager 介面。 • 變更 IBM Security Key Lifecycle Manager 管理者的密碼。 但不能執行下列作業： • 建立一個以上的額外 IBM Security Key Lifecycle Manager 管理者使用者 ID。 • 執行 WebSphere Application Server 管理者作業，例如建立或指派角色。 • 啓動或停止伺服器。	安裝期間指定及安全地儲存密碼。

表 1. 管理者使用者 ID 和密碼 (繼續)

程式	使用者 ID	密碼
WebSphere Application Server 管理者	**WASAdmin** 此使用者 ID 不區分大小寫。 或者，使用 **wasadmin** 或安裝期間指定的使用者 ID。 請勿執行下列作業： • 使用 SKLMAdmin 使用者 ID 來管理 WebSphere Application Server。 • 使用 WASAdmin 使用者 ID 來管理 IBM Security Key Lifecycle Manager。 WASAdmin 使用者 ID 不具有使用 IBM Security Key Lifecycle Manager 的角色。 此管理者使用者 ID 是 WebSphere Application Server 管理者使用者 ID。 有了 wasadmin 使用者 ID，您可以執行下列作業： • 僅檢視及使用 WebSphere Application Server 介面。 • 建立一個以上的額外 IBM Security Key Lifecycle Manager 管理者使用者 ID、群組和角色。 • 重設任何 IBM Security Key Lifecycle Manager 使用者 ID（包括 SKLMAdmin 管理者）的密碼。 • 啓動和停止伺服器。 但不能執行下列作業： • 使用 IBM Security Key Lifecycle Manager 來完成作業。 例如，無法建立 IBM Security Key Lifecycle Manager 裝置群組。 • 執行其他需要存取 IBM Security Key Lifecycle Manager 資料的作業。 wasadmin 使用者 ID *無法*以超級使用者身分來存取 IBM Security Key Lifecycle Manager 資料。	安裝期間指定及安全地儲存密碼。 以保護 SKLMAdmin 使用者 ID 之使用的相同方式，保護 WASAdmin 使用者 ID。 WASAdmin 使用者 ID 有權重設 SKLMAdmin 密碼，以及建立新的 IBM Security Key Lifecycle Manager 使用者並向其指派權限。
IBM Security Key Lifecycle Manager DB2 資料庫		

表 1. 管理者使用者 ID 和密碼 (繼續)

程式	使用者 ID	密碼
資料庫的實例擁有者	**Windows 系統及 AIX 或 Linux 之類的系統**：預設值爲 sklmdb26。可在安裝期間指定不同的值。 此 ID 是資料庫實例擁有者的安裝預設使用者 ID。 請勿指定長度大於八個字元的使用者 ID。 實例名稱也是 sklmdb26。 如果 DB2 位於 AIX 或 Linux 等系統上，則您的使用者 ID 必須在 bin 或 root 群組中，或在 root 所屬的個別群組中。 如果使用現有使用者 ID 來作爲 IBM Security Key Lifecycle Manager 資料庫的實例擁有者，則此使用者 ID 無法擁有另一個資料庫實例。 **註**： 爲 DB2 現有副本指定使用者 ID 時，請勿使用連字號 (-) 或底線字元 (_)。	安裝期間指定及安全地儲存密碼。 此密碼是作業系統密碼。 如果變更作業系統上的密碼，則必須變更此密碼。 如需相關資訊，請參閱第 29 頁的『在分散式系統上重設密碼』。.
資料庫實例	管理者 ID sklmdb2 擁有名稱爲 sklmdb26 的 DB2 實例。	

HOME 及其他目錄變數的定義

可以爲特定實作自訂 *HOME* 目錄。 針對每個目錄變數的定義進行適當的替代。

本資訊中使用下表所含預設定義來表示各種產品安裝路徑的 *HOME* 目錄層次。

path 的預設值隨這些作業系統（爲方便參考，我們稱之爲*分散式系統*）而有所不同。 術語「分散式系統」是指非大型主機硬體平台，其中包括個人電腦及工作站。

- 對於 Windows 系統，預設路徑爲：
  - DB2

    drive:\Program Files (x86)\IBM
  - DB2 之外的所有應用程式

    drive:\
- 對於 Linux 及 AIX 系統，/opt 是預設路徑。

表 2. HOME 及其他目錄變數

目錄變數	預設定義	說明
DB_HOME	**Windows 系統**： *drive*:\Program Files (x86)\IBM\DB2SKLMV26 **AIX 及 Linux 系統**： /opt/IBM/DB2SKLMV26	此目錄包含用於 IBM Security Key Lifecycle Manager 的 DB2 應用程式。

表 2. HOME 及其他目錄變數 (繼續)

目錄變數	預設定義	說明
DB_INSTANCE_HOME	**Windows** *drive**db2adminID* 例如，如果 *drive* 的值爲 C: 且預設 DB2 管理者是 sklmdb26，則 *DB_INSTANCE_HOME* 爲 C:\SKLMDB26。 **Linux 及 AIX®** /home/*db2adminID*	此目錄包含用於 IBM Security Key Lifecycle Manager 的 DB2 資料庫實例。
WAS_HOME	**Windows** *drive*:\Program Files (x86)\IBM\WebSphere\AppServer **Linux 及 AIX** *path*/IBM/WebSphere/AppServer 例如：/opt/IBM/WebSphere/AppServer	WebSphere Application Server 起始目錄。
SKLM_HOME	**Windows** *WAS_HOME*\products\sklm **Linux 及 AIX** *WAS_HOME*/products/sklm	IBM Security Key Lifecycle Manager 起始目錄。
SKLM_INSTALL_HOME	**Windows** *drive*:\Program Files (x86)\IBM\SKLMV26 **Linux 及 AIX** *path*/IBM/SKLMV26	此目錄包含 IBM Security Key Lifecycle Manager 授權檔及移轉檔案。
IM_INSTALL_DIR	**Windows** *drive*:\ProgramData\IBM\Installation Manager **Linux 及 UNIX** /var/ibm/InstallationManager	IBM Installation Manager 的安裝目錄。

共用瀏覽器階段作業的問題

必須避免那些使用 WebSphere Application Server 及 IBM Security Key Lifecycle Manager 的共用瀏覽器階段作業，以防止伺服器上出現無法預期的結果。 如果在同一個用戶端上使用多個瀏覽器視窗，則階段作業可能是共用的。

例如，使用 Firefox 瀏覽器時，一律共用階段作業。 視登錄設定或者開啓瀏覽器視窗的方式而定，階段作業在 Internet Explorer 中也可能是共用的。

必須避免：

- 多個使用者登入同一個階段作業。
- 同一個用戶端上的多個瀏覽器視窗存取同一個 WebSphere Application Server。

IBM Security Key Lifecycle Manager 使用者的密碼原則

適用於新 IBM Security Key Lifecycle Manager 使用者密碼的密碼原則，是透過 *SKLM_HOME*/config/TKLMPasswordPolicy.xml 檔來指定。

此原則不適用於爲預設使用者（例如 SKLMAdmin）建立的起始密碼。 這些預設使用者是在安裝 IBM Security Key Lifecycle Manager 期間建立的。

密碼原則的確適用於對預設使用者密碼進行的變更，以及新使用者的新密碼和變更密碼。只有在建立或變更使用者設定檔時，才進行原則檢查。 必須爲新使用者指派角色，該使用者然後才能嘗試登入 IBM Security Key Lifecycle Manager。

依預設，會啓用密碼原則。 可以使用 XML 或 ASCII 編輯器來變更此檔案。 如果要停用原則，請將原則檔中 **enabled** 參數的值變更爲 false：

```
PasswordPolicy enabled="true"
```

IBM Security Key Lifecycle Manager 支援下列密碼規則：

表 3. 密碼規則

規則	預設值
長度下限	6
長度上限	20
數值字元數目下限	2
英文字母數目下限	3
同一個字元的連續出現次數上限	2
禁止密碼中存在使用者 ID*	啓用
禁止密碼中存在使用者名稱*	啓用

* 偵測此值時區分大小寫。

註：如果要指定此值不區分大小寫，請編輯預設密碼原則並爲使用者 ID 和使用者名稱指定 CaseInsensitive：

```
<?xml version="1.0" encoding="UTF-8"?>
<PasswordPolicy version="1.0" uuid="" name="Password policy for TKLM"
enabled="true">
    <Description/>
    <PasswordRules><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
 <PasswordRuleSet version="1.0">
     <MinLengthConstraint Min="6"/>
     <MaxLengthConstraint Max="20"/>
     <MaxSequentialChars Max="2"/>
     <MinAlphabeticCharacters Min="3"/>
     <MinDigitCharacters Min="2"/>
     <NotUserIDCaseInsensitive/>
     <NotUserNameCaseInsensitive/>
 </PasswordRuleSet>
]]></PasswordRules>
</PasswordPolicy>
```

變更密碼原則

使用編輯器來手動地變更 IBM Security Key Lifecycle Manager 提供的密碼原則。

關於這項作業

請確保僅變更密碼原則中的元素值及屬性值，而不要變更元素名稱及屬性名稱本身。 密碼原則適用於對預設使用者密碼進行的變更，以及新使用者的新密碼和變更密碼。 只有在建立或變更使用者設定檔時，才進行原則檢查。

程序

1. 開始之前，請在安全位置建立 *SKLM_HOME*/config/TKLMPasswordPolicy.xml 檔的備份副本。位置。 如果所變更的密碼原則有問題，則可以回復爲備份副本。
2. 在文字編輯器中編輯 TKLMPasswordPolicy.xml 檔，僅變更密碼原則中 XML 元素及屬性的值。
3. 儲存所變更的檔案。

   原則變更會立即生效。 不需重新啓動 IBM Security Key Lifecycle Manager 伺服器。
4. 如果要測試變更，請以 WASAdmin 身分登入 WebSphere Application Server，然後爲新使用者建立使用者設定檔。

   確認系統接受符合原則的密碼，而拒絕違反原則的密碼。 完成後，必要的話，請刪除測試使用者設定檔。

變更使用者密碼

變更的使用者密碼必須符合 IBM Security Key Lifecycle Manager 提供的密碼原則。

關於這項作業

此作業使用 WebSphere Integrated Solutions Console 上的 WASAdmin 使用者 ID 來變更使用者密碼，其中包括 SKLMAdmin 使用者 ID 的密碼。

如需用於建立群組和使用者之指令的相關資訊，請參閱 IBM WebSphere Application Server 說明文件 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml_atwimmgt.html)。

程序

1. 登入 WebSphere Integrated Solutions Console。
   - 圖形使用者介面：
     a. 在瀏覽器的「歡迎使用」頁面上，輸入 WASAdmin 的使用者 ID 及密碼值，例如 wasadminpw。
     b. 在導覽樹狀結構中，按一下**使用者和群組 > 管理使用者**。
   - 指令行介面：

     在 *WAS_HOME*/bin 目錄中，使用 Jython 來啓動 **wsadmin** 階段作業。 使用授權使用者 ID（如 WASAdmin 使用者 ID）來登入 **wsadmin**。例如，在 Windows 系統上，導覽至 *drive*:\Program Files (x86)\IBM\WebSphere\AppServer\bin 目錄並鍵入：
     – Windows 系統：

       ```
       wsadmin -username WASAdmin -password wasadminpw -lang jython
       ```
     – AIX 或 Linux 等系統：

       ```
       ./wsadmin.sh -username WASAdmin -password wasadminpw -lang jython
       ```

2. 變更使用者的密碼。
   - 圖形使用者介面：
     a. 在**管理使用者 > 搜尋使用者**對話框上，按一下**搜尋**。
     b. 在搜尋準則表格中，按兩下所選使用者 ID。例如，按兩下使用者 ID myAdmin。
     c. 在「使用者內容」對話框上，變更**密碼**及**確認密碼**欄位的值。
     d. 按一下**確定**。
   - 指令行介面：
     a. 輸入 updateUser 並指定必要值。 例如，透過使用 Jython，在一行上輸入：

```
print AdminTask.updateUser('-uniqueName uid=test2,
o=defaultWIMFileBasedRealm -password secret12 -confirmPassword secret12')
```

其中，

-uniqueName
為您想要建立密碼的使用者指定唯一名稱。 （字串，必要項目）

變更密碼前，可使用 **searchUsers** 指令來驗證名稱是否正確地識別使用者。

-password
指定使用者的密碼。 （字串，必要項目）

新密碼必須符合 IBM Security Key Lifecycle Manager 提供的密碼原則。

-confirmPassword
再次指定密碼以驗證是如何爲 password 參數輸入密碼的。 （字串，選用項目）

下一步

接著，驗證使用者是否可以登入。 以 WASAdmin 身分登出。 以使用者身分登入，並確認系統可以接受所變更的密碼。

變更 IBM Security Key Lifecycle Manager 使用者密碼

可以使用 IBM Security Key Lifecycle Manager 應用程式使用者 ID 來變更使用者密碼。所變更密碼必須符合 IBM Security Key Lifecycle Manager 提供的密碼原則。

關於這項作業

如需用來變更密碼之指令的相關資訊，請參閱 IBM WebSphere Application Server 說明文件 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.iseries.doc/ae/rxml_atwimmgt.html)。

程序

1. 導覽至適當的頁面或目錄：
   - 指令行介面：
     – 在 *WAS_HOME*/bin 目錄中，使用 Jython 來啓動 wsadmin 階段作業。 使用授權使用者 ID 來登入 wsadmin。

Windows

導覽至 C:\Program Files (x86)\IBM\WebSphere\AppServer\bin 目錄並輸入：

```
wsadmin.bat -username <SKLM user> -password <SKLM user passwd>
-lang jython
```

AIX 或 Linux

導覽至 /opt/IBM/WebSphere/AppServer/bin 目錄並輸入：

```
./wsadmin.sh -username <SKLM user> -password <SKLM user passwd>
-lang jython
```

- 圖形使用者介面：
  - 登入圖形使用者介面。

2. 變更使用者的密碼。
   - 指令行介面：
     - 執行下列指令：

       ```
       AdminTask.changeMyPassword('[-oldPassword <oldpasswordvalue>
       -newPassword
       <newpasswordvalue> -confirmNewPassword <newpasswordvalue>]')
       ```

       範例：

       ```
       AdminTask.changeMyPassword('[-oldPassword sklmadmin -newPassword
       Ibm12one
       -confirmNewPassword Ibm12One]')
       ```

   - 圖形使用者介面：
     a. 在標頭列上，按一下 **<SKLM 使用者>** 鏈結。
     b. 按一下**變更密碼**。
     c. 在「變更密碼」對話框中，輸入**現行密碼**。
     d. 輸入**新密碼**。
     e. 在**確認新密碼**欄位再次輸入新密碼。
     f. 按一下**變更密碼**。

在分散式系統上重設密碼

必須是管理者才能重設 IBM Security Key Lifecycle Manager 或 WebSphere Application Server 的密碼。

關於這項作業

可以在執行 IBM Security Key Lifecycle Manager 的電腦上重設密碼。只有在遺失了使用者密碼時，才使用這些步驟。 在所有其他情況下，請使用圖形使用者介面來更新密碼。

程序

1. 使用本端管理者使用者 ID 登入。
2. 備份 *WAS_HOME*/profiles/KLMProfile/config/cells/SKLMCell/fileRegistry.xml 檔。變更密碼值會變更此登錄檔。
3. 變更密碼。
   - Windows 系統

a. 使用 Jython 語法來啓動 **wsadmin** 階段作業。 例如，輸入：

```
WAS_HOME/bin/wsadmin -conntype none -profileName KLMProfile -lang jython
```

b. 重設 SKLMAdmin 使用者 ID 的密碼：

```
wsadmin>print AdminTask.changeFileRegistryAccountPassword
 ('-userId SKLMAdmin -password newpassword')
```

註：

– 僅 WASAdmin 使用者 ID 或者其他具有 WebSphere Application Server 管理者權限的使用者 ID，才能使用 **AdminTask.changeFileRegistryAccountPassword** 指令來變更密碼。

– 不會依據 IBM Security Key Lifecycle Manager 提供的已配置密碼原則，來驗證您使用 **AdminTask.changeFileRegistryAccountPassword** 指令建立的密碼。

重設遺失的密碼後，使用者必須使用圖形使用者介面來設定密碼。

c. 儲存變更並結束：

```
wsadmin>print AdminConfig.save()
wsadmin>exit
```

- Linux 或 AIX 等系統

a. 使用 Jython 語法來啓動 **wsadmin** 階段作業。 例如，在一行上輸入：

```
WAS_HOME/bin/wsadmin.sh -conntype none
   -profileName KLMProfile -lang jython
```

b. 重設 SKLMAdmin 使用者 ID 的密碼：

```
wsadmin>print AdminTask.changeFileRegistryAccountPassword
 ('-userId SKLMAdmin -password newpassword')
```

註：

– 僅 WASAdmin 使用者 ID 或者其他具有 IBM Security Key Lifecycle Manager 管理者權限的使用者 ID，才能使用 **AdminTask.changeFileRegistryAccountPassword** 指令來變更密碼。

– 不會依據 IBM Security Key Lifecycle Manager 提供的已配置密碼原則，來驗證您使用 **AdminTask.changeFileRegistryAccountPassword** 指令建立的密碼。

重設遺失的密碼後，使用者必須使用圖形使用者介面來設定密碼。

c. 儲存變更並結束：

```
wsadmin>print AdminConfig.save()
wsadmin>exit
```

4. 停止和啓動伺服器。

- 停止

在 Windows 系統上：

```
stopServer.bat server1
```

在 Linux 或 AIX 等系統上：

```
./stopServer.sh server1
```

- 啓動

在 Windows 系統上：

```
startServer.bat server1
```

在 Linux 或 AIX 等系統上：

```
./startServer.sh server1
```

5. 驗證是否能以所指定管理者的身分及新密碼進行登入。

使用者角色

IBM Security Key Lifecycle Manager 提供了超級使用者（klmSecurityOfficer 及 klmGUICLIAccessGroup）角色及方法（用來指定更多受限制管理角色）以符合組織的需要。依預設，SKLMAdmin 使用者 ID 具有 klmSecurityOfficer 角色。

對於備份及還原作業，IBM Security Key Lifecycle Manager 也會安裝 klmBackupRestoreGroup（任何使用者 ID 最初皆不屬於此群組）。 安裝 IBM Security Key Lifecycle Manager 會建立預先定義的管理者、操作員及審核員群組以管理 LTO 磁帶機。

WASAdmin 使用者 ID 有權建立並指派這些角色，及變更任何 IBM Security Key Lifecycle Manager 管理者的密碼。如果要給 IBM Security Key Lifecycle Manager 設定管理限制，請使用 WebSphere Integrated Solutions Console 上的 WASAdmin 使用者 ID 來建立角色、使用者和群組。 將角色和使用者指派給群組。 例如，可建立群組並指派使用者及角色，此角色將使用者活動限制爲僅管理 LTO 磁帶機。 必須給新使用者指派角色，該使用者然後才能嘗試登入 IBM Security Key Lifecycle Manager。

在開始之前，請完成下列作業：

- 決定裝置管理上組織所需的限制。

  例如，可決定特定裝置群組具有專屬管理。
- 估計在一個時間間隔內可能需要的管理使用者數目。 爲了方便使用，請考量指定群組及一個用來指定群組使用者作業的角色。

  例如，可指定一個群組，其具有僅管理 3592 磁帶機的受限權限範圍。

使用者、群組、角色及受保護物件之間的關係

如果要對受保護物件進行有用的處理，則 IBM Security Key Lifecycle Manager 使用者必須具有一個以上的角色。 角色必須對 LTO 裝置系列中的裝置啓用動作，例如建立物件。

使用者可以是群組成員。 一個群組可具有一個以上的角色。角色給受保護物件指定作業權限。例如，受保護物件包括裝置、裝置群組、加密物件（憑證、金鑰、金鑰組及金鑰群組），及憑證和金鑰群組的輪替設定。

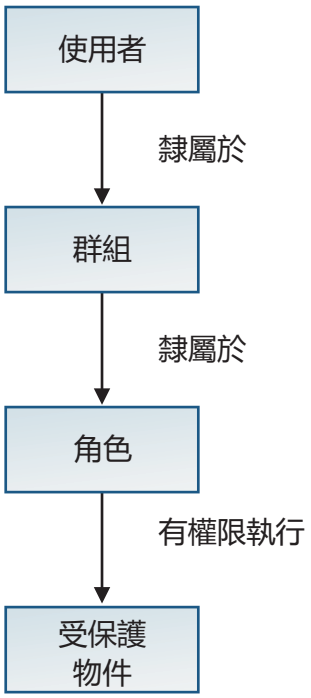

圖 4. 使用者、群組、角色及受保護物件之間的關係

您可以使用 WebSphere Integrated Solutions Console 來在上層群組內建立具有不同許可權的子群組。但是，IBM Security Key Lifecycle Manager 只會辨識上層群組的許可權，而不會辨識其子群組的許可權。

可用的權限

安裝 IBM Security Key Lifecycle Manager 會建立 SKLMAdmin 使用者 ID，此 ID 以 `klmSecurityOfficer` 角色作爲預設超級使用者。 安裝程序也會將預先定義的權限部署至 WebSphere Application Server 管理角色清單。

IBM Security Key Lifecycle Manager 中的*權限*可啓用動作或裝置群組。 IBM Security Key Lifecycle Manager 中的*角色*是一種以上的權限。 然而，在 WebSphere Application Server 圖形使用者介面中，術語*角色*包括 IBM Security Key Lifecycle Manager 權限及角色。

註：安裝會建立下列預設群組：

klmSecurityOfficerGroup

安裝會指派 `klmSecurityOfficer` 角色給此群組。 `klmSecurityOfficer` 角色會取代 `klmGroup` 群組中先前的 `klmApplicationRole` 角色。 `klmSecurityOfficerGroup` 會取代 `klmGroup`。

`klmSecurityOfficer` 角色具有：

- 權限及裝置群組（如第 33 頁的表 4 及第 34 頁的表 5 中所述）之完整集合的 root 存取權。
- 可建立之任何角色或裝置群組的權限。
- `suppressmonitor` 角色。

WebSphere Application Server 提供了 suppressmonitor 角色來隱藏 WebSphere Integrated Solutions Console 左窗格中 IBM Security Key Lifecycle Manager 管理者不使用的作業。 隱藏的項目與應用程式伺服器相關聯，其中包括 Security、Troubleshooting 及 Users and Groups 資料夾中的 WebSphere Application Server 管理作業。

klmBackupRestoreGroup

備份及還原 IBM Security Key Lifecycle Manager。

LTOAdmin

使用包括建立、檢視、修改、刪除、取得（匯出）、備份及配置在內的動作來管理 LTO 裝置系列中的裝置。

LTOOperator

使用包括建立、檢視、修改及備份在內的動作來操作 LTO 裝置系列中的裝置。

LTOAuditor

使用包括檢視及審核在內的動作來審核 LTO 裝置系列中的裝置。

klmGUICLIAccessGroup

將 IBM Security Key Lifecycle Manager 圖形使用者介面及指令行介面存取權提供給使用者。 每個產品使用者都必須屬於此群組。

註：必須將這種對群組的存取權及其他存取權提供給使用者，使用者才能成爲功能產品使用者。

具有表 4 中任何一種權限的使用者都可以檢視：

- SKLMConfig.properties 檔中所定義的 IBM Security Key Lifecycle Manager 廣域配置參數。
- 金鑰伺服器狀態及前次備份日期。

表 4. 動作權限

權限	啓用這些動作	與裝置群組無關	與裝置群組相關聯
klmCreate	建立而不是檢視、修改或刪除物件。		✓
klmDelete	刪除物件，而不是檢視、修改或建立物件。		✓
klmGet	匯出用戶端裝置的金鑰或憑證。		✓
klmModify	修改物件，而不是檢視、建立或刪除物件。		✓
klmView	檢視物件，而不是建立、刪除或修改物件。 例如，必須具有此權限，才能查看您想要在圖形使用者介面上執行的作業。		✓
klmAdminDeviceGroup	管理。 建立裝置群組，設定預設參數，檢視，刪除空的裝置群組。 此權限並不提供裝置、金鑰或憑證的存取權。	✓	

表 4. 動作權限 (繼續)

權限	啓用這些動作	與裝置群組無關	與裝置群組相關聯
klmAudit	使用 **tklmServedDataList** 指令來檢視審核資料。	✓	
klmBackup	建立及刪除 IBM Security Key Lifecycle Manager 資料備份。	✓	
klmConfigure	讀取及變更 IBM Security Key Lifecycle Manager 配置內容，或者處理 SSL 憑證。 新增、檢視、更新或刪除金鑰儲存庫。	✓	
klmRestore	還原先前的 IBM Security Key Lifecycle Manager 資料備份副本。	✓	

klmSecurityOfficer 角色也具有所有裝置群組權限的 root 存取權。

表 5. 裝置群組

權限	容許對這些物件採取動作
LTO	LTO 裝置系列
TS3592	3592 裝置系列
DS5000	DS5000 裝置系列
DS8000	DS8000 裝置系列
BRCD_ENCRYPTOR	BRCD_ENCRYPTOR 裝置群組
ONESECURE	ONESECURE 裝置群組
ETERNUS_DX	ETERNUS_DX 裝置群組
XIV	XIV 裝置群組
IBM_SYSTEM_X_SED	IBM_SYSTEM_X_SED 裝置群組
IBM Spectrum Scale（以前叫作 GPFS）	IBM Spectrum Scale 裝置群組
GENERIC	GENERIC 裝置系列中的物件。
userdevicegroup	使用者定義的實例，例如，您根據預先定義的裝置系列（例如 LTO）手動建立的 myLTO。

多種權限

如果要使用裝置，則使用者必須具有一個以上動作及一個以上裝置群組的權限。

如果出現下列情況，則會發生錯誤：

使用者具有動作權限，但沒有裝置群組權限

例如，使用者具有包括檢視、建立、修改及刪除在內的動作權限集。 但是，使用者沒有裝置群組權限來接收動作。

裝置群組權限，但沒有動作權限

例如，使用者具有包括 LTO 及 3592 的裝置群組權限。然而，使用者不具有針對裝置群組執行的動作權限。

新裝置群組的新角色，但沒有動作權限

例如，使用者具有新角色 myLTO，此角色是給名爲 myLTO 的新裝置群組建立。然而，使用者沒有其他動作權限。

權限可能是：

- 直接指派。

  例如，作爲使用者的角色可能具有特定裝置群組的檢視及修改權限。

- 透過群組成員資格取得。

  權限特定於裝置群組。 您可能是兩個使用者群組的成員。 例如，一個使用者群組中的成員資格可將檢視及修改權限授與 LTO 裝置群組使用。第二個使用者群組可將檢視、建立及修改權限授與 3592 裝置群組使用。可以檢視及修改任一裝置群組中的裝置。 然而，只能針對 3592 裝置群組中的裝置完成建立動作。

金鑰及憑證等資料與裝置群組相關聯。 此類資料僅在與資料相關聯之裝置群組的圖形使用者介面頁面中可見。 具有數個裝置群組權限的使用者，可以將資料關聯從一個裝置群組變更爲使用者擁有其適當權限的另一個裝置群組。

IBM Security Key Lifecycle Manager 資料庫中的部分內容或屬性與裝置群組相關聯。例如，IBM Security Key Lifecycle Manager 資料庫中的 **symmetricKeySet** 屬性，與預先定義的 LTO 裝置群組相關聯。 如果要變更屬性，則角色必須具有該修改動作的權限，及 LTO 裝置群組的權限。

用來管理 LTO 磁帶機 的預先定義群組

安裝 IBM Security Key Lifecycle Manager 會建立預先定義的管理群組來管理 LTO 磁帶機。 可以使用這些群組作爲模型，給其他裝置群組定義類似的管理群組。

LTOAdmin 群組：

可以使用 LTOAdmin 群組中的成員資格，透過包括建立、檢視、修改、刪除、取得（匯出）、備份及配置在內的動作來管理 LTO 裝置系列中的裝置。

此群組包括下列權限：

表 6. 動作權限

權限	啓用這些動作
LTO	LTO 裝置系列
klmCreate	建立而不是檢視、修改或刪除物件。
klmDelete	刪除物件，而不是檢視、修改或建立物件。
klmGet	匯出用戶端裝置的金鑰或憑證。
klmModify	修改物件，而不是檢視、建立或刪除物件。
klmView	檢視物件，而不是建立、刪除或修改物件。
klmAudit	使用 **tklmServedDataList** 指令來檢視審核資料。
klmBackup	建立及刪除 IBM Security Key Lifecycle Manager 資料備份。
klmConfigure	讀取及變更 IBM Security Key Lifecycle Manager 配置內容，或者處理 SSL 憑證。

表 6. 動作權限 (繼續)

權限	啓用這些動作
suppressmonitor	隱藏 WebSphere Integrated Solutions Console 左窗格中 IBM Security Key Lifecycle Manager 管理者不需要使用的作業。

LTOOperator 群組：

可以使用 LTOOperator 群組中的成員資格，透過包括建立、檢視、修改及備份在內的動作，來操作 LTO 裝置系列中的裝置。

此群組包括下列權限：

表 7. 動作權限

權限	啓用這些動作
LTO	LTO 裝置系列.
klmCreate	建立而不是檢視、修改或刪除物件。
klmModify	修改物件，而不是檢視、建立或刪除物件。
klmView	檢視物件，而不是建立、刪除或修改物件。
klmBackup	建立及刪除 IBM Security Key Lifecycle Manager 資料備份。
suppressmonitor	隱藏 WebSphere Integrated Solutions Console 左窗格中 IBM Security Key Lifecycle Manager 管理者不需要使用的作業。

LTOAuditor 群組：

可以使用 LTOAuditor 群組中的成員資格，透過包括檢視及審核在內的動作，來審核 LTO 裝置系列中的裝置。

此群組包括下列權限：

表 8. 動作權限

權限	啓用這些動作
LTO	LTO 裝置系列.
klmView	檢視物件，而不是建立、刪除或修改物件。
klmAudit	使用 **tklmServedDataList** 指令來檢視審核資料。
suppressmonitor	隱藏 WebSphere Integrated Solutions Console 左窗格中 IBM Security Key Lifecycle Manager 管理者不需要使用的作業。

WebSphere Application Server 角色

WebSphere Application Server 提供了您可能需要使用的角色。 例如，您可能需要檢視或變更 WebSphere Application Server 配置。可將使用者和群組指派給管理使用者角色及管理群組角色。

角色包括監視員、配置者、操作員、管理者、安全管理員及其他角色。

如需相關資訊，請在 WebSphere Application Server 說明文件 (http://www-01.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.home.doc_wasinfo_v8r5/welcome_ic_home.html) 中搜尋*管理角色*。

版本資訊

「版本資訊」主題說明本版 IBM Security Key Lifecycle Manager 的特定資訊。

系統需求

環境必須符合最低系統需求才能安裝 IBM Security Key Lifecycle Manager。

如需軟硬體需求的相關資訊，請參閱 IBM Knowledge Center for IBM Security Key Lifecycle Manager 上的「安裝與配置手冊」小節。 所發佈軟硬體需求在發佈時非常準確。

或者，請參閱詳細系統需求文件，網址爲 http://pic.dhe.ibm.com/infocenter/prodguid/v1r0/clarity/softwareReqsForProduct.html。

1. 輸入 `IBM Security Key Lifecycle Manager`。
2. 選取產品版本。 例如，`2.6`。
3. 選取作業系統。
4. 按一下**提交**。

軟體需求

IBM Security Key Lifecycle Manager 具有下列軟體需求：

Java 執行時期環境 (JRE) 需求

IBM Security Key Lifecycle Manager 是否需要某一版本的 Java 執行時期環境，取決於所使用的作業系統。

在分散式系統上：

隨附於 WebSphere Application Server 的 IBM Java 執行時期環境。

在所有系統上，都不支援使用用於 Java™ 的獨立安裝開發套件，不論是來自 IBM，還是其他供應商。

執行時期環境需求

執行時期環境的 IBM Security Key Lifecycle Manager 需求相依於所使用的作業系統。

在分散式系統上：

WebSphere Application Server 8.5.5.7 及任何適用的修正套件或 APAR 需求。

IBM Security Key Lifecycle Manager 包括且安裝 WebSphere Application Server。安裝期間，IBM Security Key Lifecycle Manager 會修改 WebSphere Application Server。 此修改可能會造成在解除安裝 IBM Security Key Lifecycle Manager 後，使用同一個伺服器的產品發生問題。如果要避免這些問題，請注意下列事項：

- 切勿在另一個產品所提供的 WebSphere Application Server 實例中安裝 IBM Security Key Lifecycle Manager。
- 切勿將另一個產品安裝在 IBM Security Key Lifecycle Manager 所提供的 WebSphere Application Server 實例中。

資料庫權限及需求

資料庫的 IBM Security Key Lifecycle Manager 需求相依於所使用的作業系統。

- 分散式系統：

  位於 IBM Security Key Lifecycle Manager 伺服器執行所在之相同電腦上的 DB2 Workgroup Server Edition：

  – 10.5.0.6 版及未來修正套件，位於 IBM Security Key Lifecycle Manager 支援的其他分散式作業系統上。

    註：

    - 您必須使用 IBM Security Key Lifecycle Manager 來管理資料庫。 若要避免資料同步化問題，請勿使用資料庫應用程式可能提供的工具。
    - 爲了改進 AIX 系統上 DB2 10.5.0.6 版的效能，請確保您已安裝及配置 DB2 說明文件 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.perf.doc/doc/t0054518.html) 中所述的 I/O 完成埠 (IOCP) 套件。
    - 如果已經以 root 使用者身分在適合作業系統的正確版本層次安裝 DB2 Workgroup Server Edition 的現有副本，則您可以使用這個現有的 DB2 Workgroup Server Edition。 IBM Security Key Lifecycle Manager 安裝程式不會偵測是否存在 DB2。 您必須指定 DB2 安裝路徑。

如需 DB2 必要條件的相關資訊，請參閱 DB2 文件 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.cmd.doc/doc/r0059710.html)。

DB2 核心設定

確保核心設定適合於那些需要更新的作業系統，例如 Linux 作業系統。

在安裝應用程式之前，請參閱下列網站上的 DB2 文件，以取得下列其他核心設定：

AIX 系統

不需要。

Linux 系統

如需在其他受支援 Linux 系統上修改 DB2 Workgroup Server Edition 10.5.0.6 版核心參數的相關資訊，請參閱 DB2 文件 (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.qb.server.doc/doc/t0008238.html)。

Windows 系統

不需要。

針對大規模環境進行 DB2 緩衝池調整

可能需要針對大規模環境調整 DB2 緩衝池設定。

使用下列設定：

```
db2 alter bufferpool TKLMBP_LG immediate size 1000 automatic
#---
#--- Use one of the following two statements:
#--- If you migrate from IBM Security Key Lifecycle Manager Version 1,
#--- specify the next statement:
db2 alter bufferpool TKLMBP_4K_IDX immediate size 1000 automatic
#--- Otherwise, omit the statement.
```

```
#--- However, if NO migration occurs, specify the next statement:
db2 alter bufferpool TKLMBP_4K_LG_IDX immediate size 1000 automatic
#--- Otherwise, omit the statement.

#---
db2 alter bufferpool TKLMBP_8K_LG immediate size 1000 automatic
db2 alter bufferpool TKLMBP_32K_LG immediate size 1000 automatic
db2 alter bufferpool TKLMBP_SM immediate size 1000 automatic
db2 alter bufferpool TKLMBP_IDX immediate size 1000 automatic
db2 alter bufferpool TKLMBP_32K_IDX immediate size 1000 automatic
db2 alter bufferpool TKLMBP_SCH immediate size 1000 automatic
```

安裝映像檔及修正套件

對於分散式系統，使用 IBM Passport Advantage® 網站來取得 IBM Security Key Lifecycle Manager 安裝檔及修正套件。 您也可以透過其他方式（例如 IBM 業務代表所提供的 DVD）來取得這些檔案。

Passport Advantage 網站爲各種 IBM 產品提供套件，稱爲 eAssembly。

「修正程式中心」網站爲系統的軟體、硬體及作業系統提供修正程式和更新項目。 在「修正程式中心」網站上發佈 IBM Security Key Lifecycle Manager 修正套件。

IBM Knowledge Center for IBM Security Key Lifecycle Manager 上的「安裝與配置」小節提供 IBM Security Key Lifecycle Manager 及必要中介軟體產品的安裝與配置指示。

注意事項

本資訊係針對 IBM 在美國所提供之產品與服務所開發。 在其他國家，IBM 不見得有提供本文件所提及之各項產品、服務或功能。 請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。 本書在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。 只要未侵犯 IBM 的智慧財產權，任何功能相當的產品、程式或服務都可以取代 IBM 的產品、程式或服務。 不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

本書或文件可能包含 IBM 所有之專利或專利申請案。 本書使用者並不享有前述專利之任何授權。 您可以書面提出授權查詢，來函請寄到：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

如果是有關雙位元組字集 (DBCS) 資訊的授權查詢，請洽詢所在國的 IBM 智慧財產部門，或書面提出授權查詢，來函請寄到：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

下列段落不適用於英國，若與任何其他國家之法律條款抵觸，亦不適用於該國：

International Business Machines Corporation 只依「現況」提供本出版品，不提供任何明示或默示之保證，其中包括且不限於不侵權、可商用性或特定目的之適用性的隱含保證。

有些地區在某些交易上並不接受明示或默示保證的排除，因此，這項聲明對 貴客戶不見得適用。

本資訊中可能會有技術上或排版印刷上的訛誤。 因此，IBM 會定期修訂；並將修訂後的內容納入新版中。 IBM 隨時會改進及/或變更本出版品所提及的產品及/或程式，將不另行通知。

本資訊中任何對非 IBM 網站的敘述僅供參考，IBM 對該網站並不提供任何保證。 該等網站所提供的資料不是 IBM 本產品的資料內容，如果要使用這些網站的資料， 貴客戶必須自行承擔風險。

IBM 得以各種 IBM 認爲適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。

如果本程式之獲授權人爲了 (i) 在個別建立的程式和其他程式（包括本程式）之間交換資訊，以及 (ii) 相互使用所交換的資訊，因而需要相關的資訊，請洽詢：

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於雙方之 IBM 客戶合約、IBM 國際程式授權合約或任何同等合約之條款，提供本文件所提及的授權程式與其所有適用的授權資料。

這裡包含的效能資料是在控制環境下得出的。 因此，在其他作業環境下取得的結果可能大不相同。 有些測定已在開發階段系統上做過，不過這並不保證在一般系統上會出現相同結果。 再者，有些測定可能已透過推測方式評估過。 但實際結果可能並非如此。 本文件的使用者應依自己的特定環境，查證適用的資料。

本文件所提及之非 IBM 產品資訊，取自產品的供應商，或其發佈的聲明或其他公開管道。 IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性、或任何對產品的其他主張是否完全無誤。 有關非 IBM 產品的性能問題應直接洽詢該產品供應商。

所有關於 IBM 未來方針或目的之聲明，隨時可能更改或撤銷，不必另行通知，且僅代表目標與主旨。

所有顯示的 IBM 價格皆爲 IBM 所建議之現行零售價，在價格調整時不須另行通知。經銷商價格可能會有所不同。

此資訊僅供規劃之用。 在所說明的產品上市之前，這裡的資訊有可能會改變。

本資訊含有日常商業運作所用之資料和報告範例。 爲了盡可能地加以完整說明，範例中含有個人、公司、品牌及產品的名稱。 所有這些名稱全爲虛構，如有任何類似實際企業所用的名稱及地址之處，純屬巧合。

著作權：

本資訊含有原始語言之範例應用程式，用以說明各作業平台中之程式設計技術。 貴客戶得爲開發、使用、行銷或散佈運用範例程式之作業平台的應用程式程式介面所撰寫的應用程式之目的，免費複製、修改並散佈這些範例程式。 這些範例並未在所有情況下完整測試。 因此，IBM 無法保證或默示這些程式的可靠性、服務功能或功能性。貴客戶得爲開發、使用、銷售或散佈運用範例程式之 IBM 應用程式設計介面之目的，免費複製、修改並散佈這些範例程式。

在這些程式範例或任何衍生作品的每一個複本或任何部分中，必須包含下列版權聲明：

©（您的公司名稱）（年份）。 本程式的若干部分係衍生自 IBM Corp. 範例程式。 © Copyright IBM Corp. _輸入年份_. All rights reserved.

若 貴客戶正在以電子檔格式閱讀本資訊，則可能不會顯示照片和彩色說明。

產品說明文件的條款

這些出版品的使用，其許可權的授與需遵循下列條款。

適用性 這些條款附加於 IBM 網站所適用的任何條款。

個人用途

貴客戶可以爲了非商務性的私人用途而複製這些出版品， 但必須保留所有專利注意事項。如果未經 IBM 明文同意， 貴客戶不能散布、 顯示或衍生這些出版品或其中的任何部分。

商業用途

貴客戶可以在企業內複製、散布和顯示這些出版品，但必須保留所有專利注意事項。未經 IBM 的明文同意， 貴客戶不能在您的企業外衍生這些出版品，或複製、散布或顯示這些出版品或其中的任何部分。

權利 除了在此明確授予的許可權之外，並未授予（明確或隱含）出版品或其包含的任何資訊、資料、軟體或其他智慧財產的任何其他許可權、軟體授權或權利。

IBM 保留在判定出版品的使用將損害其利益或判定未適當遵守上述指示時，撤銷此處所授予之許可權的權利。

貴客戶必須完全遵守所有適用的法律及規則 (包括所有美國的出口法律及規則)，才能下載、出口或再出口此資訊。

IBM 不提供這些出版品內容的任何保證。出版品依「現狀」提供，不含任何明示或默示保證，包括且不限於適售性、無侵權行爲或符合特定效用之默示保證。

商標

IBM、IBM 標誌和 ibm.com 是 International Business Machines Corp. 在全球適用範圍內註冊的商標或註冊商標。 其他產品與服務名稱可能是 IBM 或其他公司的商標。 如需查看 IBM 商標的最新清單，請造訪以下網站：http://www.ibm.com/legal/copytrade.shtml。

Adobe、Acrobat、PostScript 及所有 Adobe 型商標是 Adobe Systems Incorporated 在美國及/或其他國家或地區的註冊商標或商標。

IT Infrastructure Library 是 Central Computer and Telecommunications Agency（現在是 Office of Government Commerce 的一部分）的註冊商標。

Intel、Intel 標誌、Intel Inside、Intel Inside 標誌、Intel Centrino、Intel Centrino 標誌、Celeron、Intel Xeon、Intel SpeedStep、Itanium 及 Pentium 是 Intel Corporation 或其子公司在美國及其他國家或地區的商標或註冊商標。

Linux 是 Linus Torvalds 在美國及/或其他國家或地區的商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其他國家或地區的商標。

ITIL 是 Office of Government Commerce 在美國 Patent and Trademark Office 註冊的註冊商標及註冊社群商標。

UNIX 是 The Open Group 在美國及其他國家或地區的註冊商標。

Java 和所有以 Java 爲基礎的商標及標誌是 Oracle 及（或）其子公司的商標或註冊商標。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美國及/或其他國家或地區的商標，並獲其授權使用。

Linear Tape-Open、LTO、LTO 標誌、Ultrium 和 Ultrium 標誌皆爲 HP、IBM Corp. 和 Quantum 於美國和其他國家的商標。

索引

索引順序以中文字，英文字，及特殊符號之次序排列。

〔三劃〕

〔四劃〕

〔五劃〕

〔六劃〕

〔七劃〕

〔八劃〕

〔九劃〕

〔十劃〕

〔十一劃〕

〔十二劃〕

〔十三劃〕

〔十四劃〕

〔十五劃〕

〔十七劃〕

〔二十二劃〕

〔二十三劃〕

〔數字〕

A

B

D

E

F

H

I

J

K