規劃

IBM

目錄

規劃

規劃是您的決策會影響一項以上後續活動的活動。

規劃活動包含的作業有金鑰大小和資料庫、預計是否需要移轉現有資料，以及判定場所需要的進行中工作實務等。

場所需求

在安裝 IBM Security Key Lifecycle Manager 之前，請考量場所問題，例如金鑰大小需求，是使用 IBM Security Key Lifecycle Manager 提供的 DB2® 還是使用已安裝在系統上的現有副本。 您還可能要考量 Encryption Key Manager 移轉需要。

金鑰大小需求

在安裝及配置 IBM Security Key Lifecycle Manager 之前，您必須考量金鑰大小需求。

支援的金鑰大小及匯入和匯出限制

IBM Security Key Lifecycle Manager 可以向裝置提供 2048 或 1024 位元金鑰。 作爲 1024 位元金鑰產生的較舊金鑰可以繼續使用。

表 1 列出 IBM Security Key Lifecycle Manager 支援的受支援金鑰大小。

表 1. 支援的金鑰大小

匯入 PKCS#12 檔案	匯出 PKCS#12 檔案	金鑰產生大小（位元）
是	是	2048

DB2 規劃

您必須考量是使用 DB2 Workgroup Server Edition 的現有副本，還是使用 DB2 版及 IBM Security Key Lifecycle Manager 安裝程式提供給分散式系統的修正套件。 現有 DB2 必須安裝在本端系統上而不是網路或共用磁碟機上。

使用 IBM Security Key Lifecycle Manager 來管理 DB2。

- 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。

如需資料庫需求的相關資訊，請參閱 IBM Knowledge Center for IBM Security Key Lifecycle Manager 上的「安裝與配置」小節。

移轉規劃

在此版本中安裝 IBM Security Key Lifecycle Manager 之前，判定您是從 Java 平台的 Encryption Key Manager 元件移轉舊版 IBM Security Key Lifecycle Manager 還是移轉先前配置資料。

您還可以使用跨平台備份公用程式於 IBM Security Key Lifecycle Manager 的舊版 1.0、2.0、2.0.1、2.5 及 Encryption Key Manager 2.1 版上執行備份作業，以備份重要資料。您可以將 IBM Security Key Lifecycle Manager 2.6 版上的這些備份檔還原至與備份來源不同的作業系統。如需相關資訊，請參閱IBM Security Key Lifecycle Manager 舊版的備份及還原作業。

註：Encryption Key Manager 元件僅支援英文語言環境。 因此，您必須在英文語言環境中執行從 Encryption Key Manager 至 IBM Security Key Lifecycle Manager 的移轉。

- IBM Security Key Lifecycle Manager 2.5 版 Fix Pack 3 或更新版本。

  安裝 IBM Security Key Lifecycle Manager 2.6 版會偵測舊版 IBM Security Key Lifecycle Manager。 安裝會自動移轉其資料。

  IBM Security Key Lifecycle Manager 2.5 版的失敗移轉會保留成功移轉步驟的記錄。會在發生錯誤的移轉處理程序點中開始執行移轉回復 Script。

  註：當您從 IBM Security Key Lifecycle Manager 2.5 版移轉至 2.6 版時，必須將 IBM Security Key Lifecycle Manager 伺服器埠號從 `9080` 變更爲其他可用的埠，例如，`9180`。您還必須變更 WebSphere® Application Server 的安裝目錄名稱，例如，`WebSphere26`。
- IBM Security Key Lifecycle Manager 2.0.1 版或更新版本修正套件。

  安裝 IBM Security Key Lifecycle Manager 2.6 版會偵測舊版 IBM Security Key Lifecycle Manager。 安裝會自動移轉其資料。

  IBM Security Key Lifecycle Manager 2.0.1 版的失敗移轉會保留成功移轉步驟的記錄。會在發生錯誤的移轉處理程序點中開始執行移轉回復 Script。
- IBM Security Key Lifecycle Manager 第 2 版（處於 Fix Pack 4 或更新版本。）

  安裝 IBM Security Key Lifecycle Manager 2.6 版會偵測舊版 IBM Security Key Lifecycle Manager。 安裝會自動移轉其資料。

IBM Security Key Lifecycle Manager 2.0 版的失敗移轉會保留成功移轉步驟的記錄。會在發生錯誤的移轉處理程序點中開始執行移轉回復 Script。

- IBM Security Key Lifecycle Manager 第 1 版（處於 Fix Pack 3 或更新版本。）

  安裝 IBM Security Key Lifecycle Manager 2.6 版會偵測舊版 IBM Security Key Lifecycle Manager。 安裝會自動移轉其資料。

  IBM Security Key Lifecycle Manager 第 1 版的失敗移轉會保留成功移轉步驟的記錄。會在發生錯誤的移轉處理程序點中開始執行移轉回復 Script。

- Encryption Key Manager 2.1 版

  已對 2.1 版啓用移轉，但未對舊版 Encryption Key Manager 啓用移轉。在您變更 IBM Security Key Lifecycle Manager 配置之前，移轉配置的唯一機會是在安裝 IBM Security Key Lifecycle Manager 期間或緊跟在安裝之後移轉。

  如果 Encryption Key Manager 2.1 版移轉失敗，則沒有資料移轉至 IBM Security Key Lifecycle Manager 資料庫。會撤銷所做的任何變更。

如果從安裝程式進行移轉失敗，則可以在結束安裝之後，從 *SKLM_HOME*\migration\bin 目錄手動執行 IBM Security Key Lifecycle Manager 2.6 版移轉公用程式。

- 執行 **migrate.bat** 或 **migrate.sh**，以將 Encryption Key Manager 2.1 版移轉至 IBM Security Key Lifecycle Manager。 在 Linux 或 AIX 等系統上，確保您以 root 使用者身分登入，然後再執行 **migrate.sh**。
- 在 *SKLM_HOME*\migration 中執行 **migrateToSKLM.bat** 或 **migrateToSKLM.sh**，以將舊版 IBM Security Key Lifecycle Manager 移轉至 2.6 版。 在 Linux 或 AIX 等系統上，確保您以 root 使用者身分登入，然後再執行 **migrateToSKLM.sh**。

請勿執行您可能在此目錄中看到的其他 ***.bat** 公用程式。 這些公用程式僅供自動安裝程序使用。

加密資料的憑證需求

IBM Security Key Lifecycle Manager 至少需要一個 X.509 數位憑證（其中包含公開/私密金鑰組），以在於 3592 磁帶機 或 DS8000 Turbo 磁帶機 上加密資料時保護 IBM Security Key Lifecycle Manager 伺服器所建立的資料加密金鑰。

IBM Security Key Lifecycle Manager 容許對每個寫入要求定義兩個數位憑證別名。在建立磁帶或磁碟時，指定的兩個別名（標籤）之一必須在 IBM Security Key Lifecycle Manager 金鑰儲存資料庫中具有一個私密金鑰。 此金鑰能夠讓建立者讀取磁帶或磁碟。另一個別名（標籤）可以是來自夥伴的公開金鑰，該夥伴可以使用其私密金鑰進行解密。 若要讀取已加密磁帶或磁碟，需要正確的私密金鑰。

有兩種方法可設定數位憑證：

- 建立您自己的公開/私密金鑰組及對應憑證以用來寫入及加密磁帶或磁碟，從而可讓您稍後讀取及解密資料。
- 從夥伴處取得公開金鑰及對應憑證，以用來寫入及加密可由夥伴讀取及解密的磁帶或磁碟。

與其他組織共用磁帶

您可與其他組織共用磁帶，以用於資料傳送、聯合開發、訂立服務合約或其他用途。 共用已加密磁帶的方法對於 3592 磁帶機 和 LTO 磁帶機 來說有所不同。

如果您將金鑰移至您專屬的災難回復位置，請使用金鑰儲存資料庫。 如果您將金鑰移至事業夥伴，請向事業夥伴提供公開金鑰。

驗證從事業夥伴處收到的任何憑證的有效性，方法是往回檢查此類憑證的信任鏈直至最終簽署它的憑證管理中心 (CA)。 如果您信任該 CA，則可以信任該憑證。 或者，可以在傳送期間安全地保護憑證時，驗證憑證的有效性。 若無法以上述其中一種方法來驗證憑證的有效性，則可能會導致發生「中間人」攻擊。

3592 磁帶共用

IBM Security Key Lifecycle Manager 可以在 3592 磁帶上儲存兩組已包裝的加密金鑰。此實務可讓其他組織讀取該特定磁帶，而不必向他們提供任何共用密碼資訊或損害憑證和金鑰的安全。

使用第二個別名（或金鑰標籤），將另一個組織之公開/私密憑證的公開部分新增至 IBM Security Key Lifecycle Manager 的金鑰儲存資料庫。 寫入磁帶時，加密金鑰儲存在磁帶上，該磁帶由兩組公開/私密金鑰保護，這些金鑰是您的集合且是屬於另一個組織的集合。 另一個組織必須具有已啓用加密的 3592 磁帶機。 另一個組織可以使用其 IBM Security Key Lifecycle Manager 及其私密金鑰來解除包裝容許讀取該特定磁帶的資料金鑰。

IBM Security Key Lifecycle Manager 必須具有夥伴組織的憑證。 另一個組織必須在金鑰儲存庫中具有另一個組織所執行之 IBM Security Key Lifecycle Manager 使用的相關聯私密金鑰。 此彈性會提供可由這兩個組織讀取的磁帶。 如果您要利用此功能，您必須將包含公開金鑰之另一個組織的憑證新增至金鑰儲存資料庫。

LTO 磁帶共用

若要共用 LTO 磁帶上的已加密資料，用來在磁帶上加密資料之對稱金鑰的副本必須可供另一個組織使用。 此金鑰可讓他們讀取磁帶。 若要共用對稱金鑰，另一個組織必須與您共用其公開金鑰。

此公開金鑰用來在從 IBM Security Key Lifecycle Manager 金鑰儲存庫匯出對稱金鑰時對其進行包裝。當另一個組織將該對稱金鑰匯入至其 IBM Security Key Lifecycle Manager 金鑰儲存庫時，會使用其對應的私密金鑰對其解除包裝。

此實務可以確保對稱金鑰能夠安全轉移，因爲只有私密金鑰的持有者才能解除私密金鑰包裝。 當 IBM Security Key Lifecycle Manager 金鑰儲存庫中有了用來加密資料的對稱金鑰之後，另一個組織便可讀取磁帶上的資料。

建議的場所實務

規劃加密金鑰伺服器（例如 IBM Security Key Lifecycle Manager）必須考量場所實務，範圍可以是從第一次實作到完善的實務。

表 2是您的場所可能考量的最佳作法清單。

表 2. 建議的場所實務

主題	建議的實務
自簽憑證	將自簽憑證用於公司內的內部正式作業及測試用途。
CA 發出的憑證	對於正式作業環境，使用 CA 發出的憑證。
憑證更換頻率	每個季度更換一次用來建立新卡匣的憑證。
CA 發出的憑證數目下限	最少一個憑證，且假設該憑證同時用作預設及夥伴憑證。
測試及正式作業環境中的磁帶機正常數量	裝置數量範圍從數個到數百個，裝置數量中位數爲 100+ 範圍。
遠端場所	存在一個以上遠端場所，IBM Security Key Lifecycle Manager 會向遠端場所提供金鑰。
每年發生的已受損憑證數目	沒有已受損憑證。
必要失效接手需求	許多場所都要求備份加密金鑰伺服器必須一律在其他場所中處於執行中狀態。 每當資料變更時，主要場所都會備份金鑰資料。 此外，所備份資料會可靠地還原至離站抄本 IBM Security Key Lifecycle Manager 伺服器，以在發生失效接手時使用。
選擇性地加密或加密所有資料	您必須考量是選擇性地加密還是加密除金鑰儲存資料庫以外的所有資料，以及可能發生的回復問題。 大部分場所會加密除 IBM Security Key Lifecycle Manager 資料及其備份資料以外的所有資料。
備份檔	如需相關資訊，請參閱有關備份及還原的管理主題。

自簽憑證

您必須考量如何根據企業的安全需要來平衡自簽憑證的可用性。

判定您的組織在使用自簽憑證及由憑證管理中心 (CA) 發出之憑證上的原則。 您可能需要爲專案的測試階段建立自簽憑證。您還可以事先爲正式作業階段從憑證管理中心處要求憑證。

機密性資訊的安全

您必須確保只有授權人員才能存取 IBM Security Key Lifecycle Manager 資料庫中 IBM Security Key Lifecycle Manager 金鑰資料的機密性資訊。

場所的權責區分各有不同，且可能沒有權責區分。 但是，場所可以執行下列步驟來提高安全：

- 一個人員提供 IBM Security Key Lifecycle Manager 伺服器的執行時期系統管理者支援。 場所具有一個系統管理者來執行 IBM Security Key Lifecycle Manager 伺服器。
- 另一個人員充當資料庫管理者，具有 DB2 使用者 ID 及 IBM Security Key Lifecycle Manager 所用資料庫實例的受限存取權。

安全配置

您必須最大化環境、安裝、管理及作業中的安全，以確保只有授權人員才能存取 IBM Security Key Lifecycle Manager 的機密性資訊。

環境

您可以配置下列環境元素以最大化安全：

- 限制系統的實體存取權以防止對伺服器硬體進行未獲授權的存取，只容許已授權管理者存取系統主控台。
- 確保通訊網路沒有偷聽及盜用風險。
- 使用防火牆並維護防火牆後的所有埠。 僅開啓 IBM Security Key Lifecycle Manager 需要的埠。
- 指定用來在 IBM Security Key Lifecycle Manager 系統上保護機密檔的檔案系統控制項。控制項必須保護檔案安全並限制只能供需要存取權的那些使用者存取。
- 保護金鑰伺服器、配置檔、日誌檔、審核日誌檔、資料庫實例及 IBM Security Key Lifecycle Manager 備份檔的安全。
- 確保系統具有足夠的磁碟空間來儲存審核日誌。
- 如果您在 IBM Security Key Lifecycle Manager上使用任何類型的除錯公用程式，則必須確保輸出是安全的。 僅從您瞭解其所有已安裝應用程式的安全系統中存取 IBM Security Key Lifecycle Manager。
- 雖然 IBM Security Key Lifecycle Manager 備份 JAR 檔中的機密性資訊有密碼保護，但並非 JAR 檔的所有內容都有密碼保護，這使得檔案容易遭到毀損或損壞。 請保持 JAR 檔安全。
- 請勿編輯備份 JAR 檔中包含的檔案。這些檔案變成無法讀取。 請將備份檔保留在您可以控制密碼的安全位置中。 將備份檔副本保留在不是位於 IBM Security Key Lifecycle Manager 電腦及 IBM Security Key Lifecycle Manager 目錄路徑上的安全位置中。
- 當您使用瀏覽器，利用部分 IBM Security Key Lifecycle Manager 畫面來管理 IBM Security Key Lifecycle Manager 時，您可以瀏覽伺服器系統上的目錄佈置。 IBM Security Key Lifecycle Manager 產品以 root 身分執行，當您瀏覽檔案系統時，會使用這些 root 許可權。

安裝

- 請勿在網域控制站上安裝。
- 請勿在共用檔案系統上安裝。

管理和使用者假設

安全地對管理者進行管理：

- 僅將管理者權限授與給管理 IBM Security Key Lifecycle Manager 及符合場所需求（針對信任及維護 IBM Security Key Lifecycle Manager 安全的競爭力）的人員。
- 管理者必須遵循系統說明文件及 IBM Security Key Lifecycle Manager 說明文件所提供的指引進行工作。
- SKLMAdmin 是特許使用者，具有 IBM Security Key Lifecycle Manager 的不受限存取權。 僅當需要專用權時，使用者才必須以 SKLMAdmin 身分登入。

- WebSphere Application Server 管理者是特許使用者，具有建立使用者帳戶及授與 IBM Security Key Lifecycle Manager 存取權的權限。 僅向授權人員提供 WASAdmin 使用者 ID 及密碼。
- 僅將系統上的使用者 ID 授與給已獲授權使用系統上資訊的使用者。
- 確保具有 IBM Security Key Lifecycle Manager 存取權的使用者有合作精神且沒有惡意。
- 請勿將作業系統專用權授與給不需要啓動或停止 IBM Security Key Lifecycle Manager 伺服器 的管理者（例如 LTOAuditor）。

作業

安全地管理進行中作業：

- 啓用建議的密碼原則。
- 根據密碼原則選擇及管理使用者和管理者密碼。
- 啓用審核。
- 建立及實作必要程序以保護系統作業安全。
- 確保維護程序包括定期診斷及審核系統，其中包括定期備份及檢閱審核檔案和錯誤日誌。
- 將密碼安全地傳送給系統使用者。
- 指示使用者和管理者不要揭露其密碼。
- 針對反覆輸入不正確密碼的使用者，尚未有鎖定機制。
- 像保護管理者密碼一樣嚴格地保護配置檔免遭揭露，其中包括配置檔內容的所有呈現（如輸出和備份）。

配置內容和屬性

表 3說明一組配置內容和屬性以及最大化安全的設定。 以安全的方式配置內容，但未針對最大化安全進行設定。 提供了下列範例以幫助您瞭解那些決策。

表 3. 安全的配置內容設定

內容	最安全的建議
Audit.event.outcome	指定成功及失敗事件。
Audit.eventQueue.max	設定爲零值。
Audit.event.types	指定值 none 以外的所有其他值。
Audit.handler.file.multithreads	無安全影響。
Audit.handler.file.name	爲檔案指定有效的安全位置。
Audit.handler.file.size	無安全影響。
Audit.handler.file.threadlifespan	無安全影響。
backup.keycert.before.serving	設定爲值 true。
cert.valiDATE	設定爲值 true。
config.keystore.name	請勿變更此值。
config.keystore.ssl.certalias	使用圖形使用者介面或指令行介面來設定通訊協定的有效值。
debug	啓用除錯記載可能會影響 IBM Security Key Lifecycle Manager 的效能。請在 IBM 支援代表的指引下啓用此選項。

表 3. 安全的配置內容設定 (繼續)

內容	最安全的建議
device.AutoPendingAutoDiscovery（IBM Security Key Lifecycle Manager 資料庫中的屬性）	設定爲值 0（零或手動）或 2（自動擱置）。
enableClientCertPush	設定爲值 false。
enableMachineAffinity（IBM Security Key Lifecycle Manager 資料庫中的屬性）	設定爲值 true（已啓用）。
fips	設定爲值 true（已啓用）。
KMIPListener.ssl.port	設定爲有效的埠號。
lock.timeout	使用預設值。
maxPendingClientCerts	使用預設值。
pcache.refresh.interval	使用預設值。
tklm.backup.db2.dir	指定有效的安全目錄。
tklm.backup.dir	指定有效的安全目錄。
tklm.encryption.keysize	使用預設值。
tklm.encryption.password	此內容在內部使用。請勿變更其值。
tklm.encryption.pbe.algorithm	此內容在內部使用。 請勿變更其值。
TransportListener.tcp.port	指定有效的埠號。
TransportListener.tcp.timeout	指定有效的逾時間隔。
TransportListener.ssl.ciphersuites	使用預設值。
TransportListener.ssl.clientauthentication	指定裝置支援的最高值。
TransportListener.ssl.port *	指定有效的埠號。
TransportListener.ssl.protocols	指定值 SSL_TLSv2。
TransportListener.ssl.timeout	指定有效的逾時間隔。
Transport.ssl.vulnerableciphers.patterns	使用預設值。
stopRoundRobinKeyGrps	指定值 true，儘管在某些環境中可以接受 false。 如需更多注意事項，請參閱 **stopRoundRobinKeyGrps** 內容的參考主題。
useSKIDefaultLabels	無安全影響。
zOSCompatibility	無安全影響。

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。

〔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〕

〔十六劃〕

〔十七劃〕

〔二十一劃〕

〔二十二劃〕

〔數字〕

A

B

C

D

E

F

K

L

M

P

S

T

U

Z

〔特殊字元〕