Dell™ PowerVault™ Encryption Key Manager

LTO Ultrium 4 及 LTO Ultrium 5 快速入門手冊

本手冊將告訴您如何在 LTO Gen 4 和 LTO Gen 5 磁帶機上進行加密的***基本配置***。請造訪 **http://support.dell.com** 以下載最新的程式庫和磁帶機韌體，然後再安裝和配置 Dell PowerVault 加密金鑰管理程式，以確保不會發生問題。

Dell PowerVault Encryption Key Manager（以下稱爲 Encryption Key Manager）是一個 Java™ 軟體程式，可協助已啓用加密的磁帶機來產生、保護、儲存及維護加密金鑰。這些金鑰是用來將寫入 LTO 磁帶媒體的資訊加密，以及將從 LTO 磁帶媒體讀取的資訊解密。Encryption Key Manager 可以在 Linux® 和 Windows® 上運作，而且設計作爲共用資源以部署在企業內部的數個位置中。

本文件說明如何快速地利用圖形使用者介面 (GUI) 或使用指令來安裝和設定 Encryption Key Manager。本文件說明如何使用 JCEKS 金鑰儲存庫類型，因爲 JCEKS 金鑰儲存庫類型是最簡單且最容易傳輸的已支援金鑰儲存庫。如果您要特定步驟或其他已支援金鑰儲存庫類型的相關資訊，請參閱 *Dell Encryption Key Manager 使用手冊*（其位置如下：**http://support.dell.com**）或者您可以在產品所提供的 Dell Encryption Key Manager 媒體中取得。

註: 重要 Encryption Key Manager 主機伺服器配置資訊：建議您讓代管 Dell Encryption Key Manager 程式的機器使用 ECC 記憶體，將資料遺失的風險降低到最小。 Encryption Key Manager 會執行要求產生加密金鑰及將這些金鑰傳給 LTO-4 和 LTO-5 磁帶機的功能。在 Encryption Key Manager 的處理期間，封裝（加密形式）的金鑰資料是在系統記憶體中。請注意，金鑰資料必須無誤地傳送到適當的磁帶機，才能夠回復（解密）寫在卡匣上的資料。如果由於某些原因，造成金鑰資料因系統記憶體位元錯誤而毀損，且該金鑰資料是用來將資料寫入卡匣中，則寫入這個卡匣的資料將無法復原（日後無法解密）。有一些適當的防護措施可確保不會發生這類的資料錯誤。不過，如果代管 Encryption Key Manager 的機器並未使用錯誤更正碼 (ECC) 記憶體，在系統記憶體內的金鑰資料仍有可能毀損，因而造成資料遺失。發生這個情況的機會不大，但對於代管重要應用程式（如 Encryption Key Manager）的機器，一律建議使用 ECC 記憶體。

首要步驟：安裝 Encryption Key Manager 軟體

1. 插入 Dell Encryption Key Manager CD。如果 Windows 的安裝沒有自動啓動，請導覽 CD 內容並按兩下 Install_Windows.bat。

   若爲 Linux，則安裝不會自動啓動。請跳至 CD 根目錄，然後輸入 `Install_Linux.sh`。

   這時會顯示一般使用者授權合約。您必須確認這個授權合約，才能繼續安裝。

   安裝作業會將作業系統適用的所有內容（文件、GUI 檔和配置內容檔），從 CD 複製到您的硬碟中。安裝期間，會檢查系統來找出正確的 IBM Java Runtime Environment。如果找不到，就會自動安裝它。

   安裝好之後，會啓動圖形使用者介面 (GUI)。

方法 1：使用 GUI 來設定 Encryption Key Manager

此程序會建立基本配置。在順利完成時，會啓動 Encryption Key Manager 伺服器。

1. 若 GUI 未啓動，請依下列方式來開啓它：

   在 Windows 上

   導覽至 c:\ekm\gui，再按一下 `LaunchEKMGui.bat`

   在 Linux 平台上

   導覽至 /var/ekm/gui 然後輸入 `. ./LaunchEKMGui.sh`

   附註：指定 . ./ （句點空格句點再加上斜線）之後，再指定 Linux Shell 指令以確保 Shell 能夠找到 Script。

2. 在EKM 伺服器配置頁面 (圖 1)，在所有必要欄位（以星號 * 表示）中輸入資訊。請按一下任何資料欄位右側的問號來取得說明。按 **Next** 來移至 EKM Server Certificate Configuration 頁面。

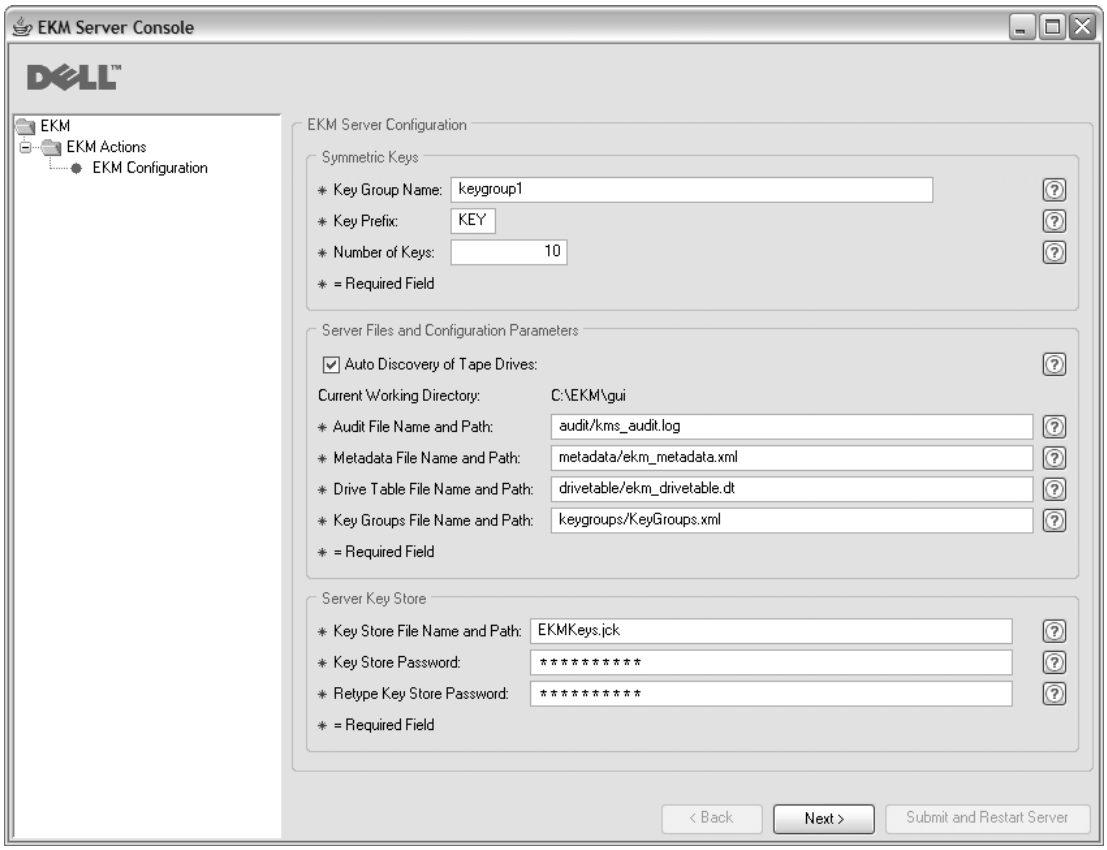

圖 1. EKM Server Configuration 頁面

註:

a. 在透過自動探查來新增磁帶機之後，應該使用 GUI 來重新整理 Encryption Key Manager 伺服器，以確定磁帶機已經儲存在磁帶機表格中。

b. 設定金鑰儲存庫密碼之後，除非安全性有問題，否則**請不要變更**密碼。這些密碼會成爲亂碼，以免出現任何安全漏洞。當變更金鑰儲存庫密碼時，必須利用 **keytool** 指令來個別變更這個金鑰儲存庫中每個金鑰的密碼。請參閱 *Dell Encryption Key Manager 使用手冊*中的『變更金鑰儲存庫密碼』。

3. 在 EKM Server Certificate Configuration 頁面 (圖 2) 中，輸入金鑰儲存庫別名以及填入任何可用來識別憑證及其用途的其他欄位。按一下 **Submit and Start Server**。

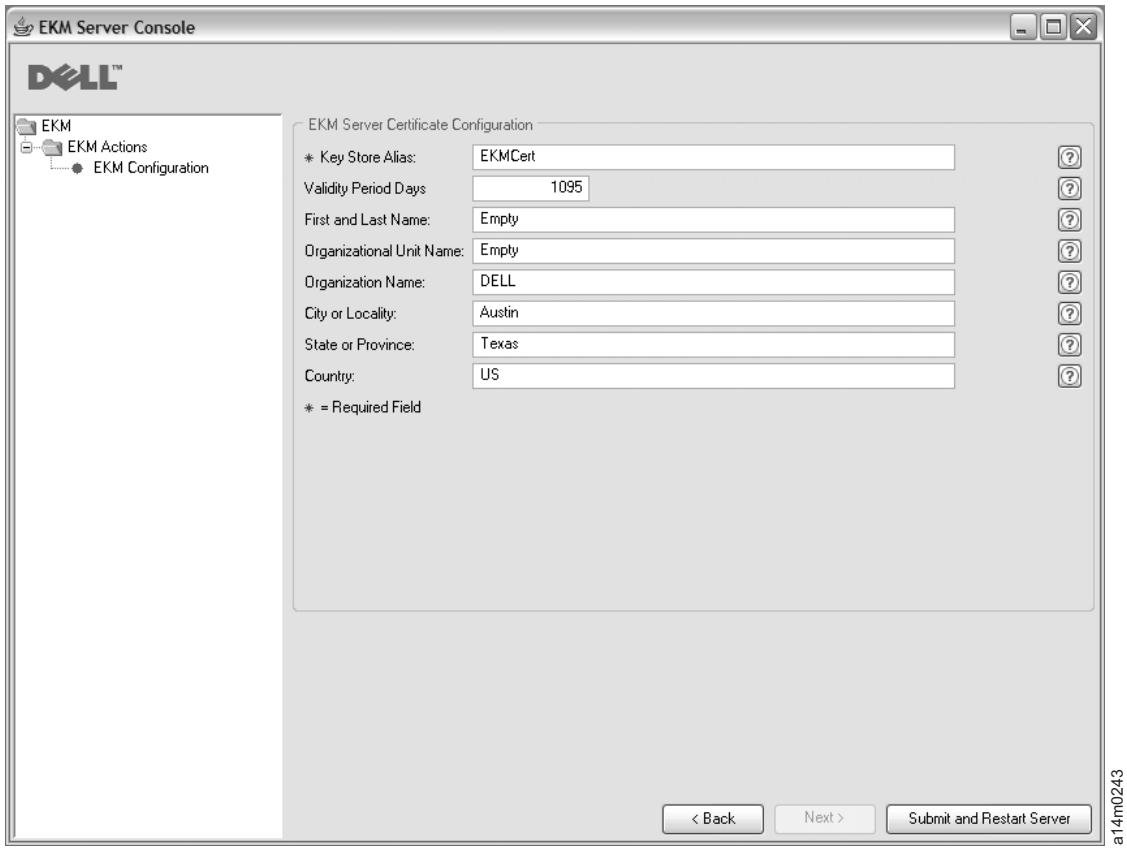

圖 2. EKM Server Certificate Configuration 頁面

註: 在金鑰產生期間岔斷 Encryption Key Manager GUI，需要重新安裝 Encryption Key Manager。

如果您在 Encryption Key Manager 的金鑰產生程序完成之前，停止 Encryption Key Manager，金鑰儲存庫檔案會毀損。如果要從這個事件回復，請遵循下列步驟：

- 如果在起始安裝期間已岔斷 Encryption Key Manager，請導覽至其目錄所在的位置（如 x:\ekm）。刪除目錄，再重新開始安裝。
- 如果在新增新的金鑰群組時岔斷了 Encryption Key Manager，請停止您的 Encryption Key Manager 伺服器，以最新的備份金鑰儲存庫（這個檔案在您的 x:\ekm\gui\backupfiles 資料夾中）來還原您的金鑰儲存庫檔案。請注意，備份檔的檔名含有日期和時間戳記（如 2007_11_19_16_38_31_EKMKeys.jck）。檔案複製到 x:\ekm\gui 目錄之後，必須移除日期和時間戳記。請重新啓動 Encryption Key Manager 伺服器，新增先前岔斷的金鑰群組。

4. 這時會顯示一個備份視窗 (圖 3)，提醒您備份 Encryption Key Manager 資料檔。請輸入用來儲存備份資料的路徑。按一下 **Backup**。

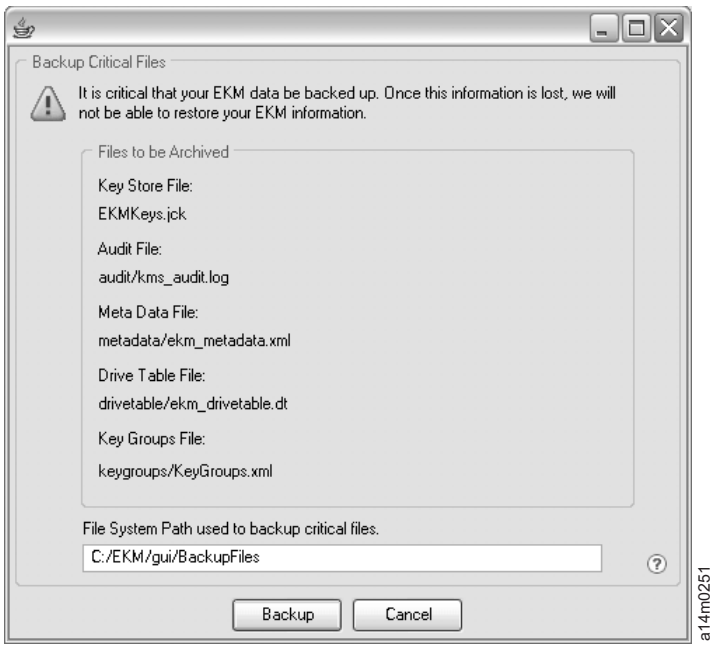

圖 3. Backup Critical Files 視窗

5. 這時會顯示 User Login 頁面。輸入預設使用者名稱 EKMAdmin 及預設密碼 changeME。按一下 **Login**。

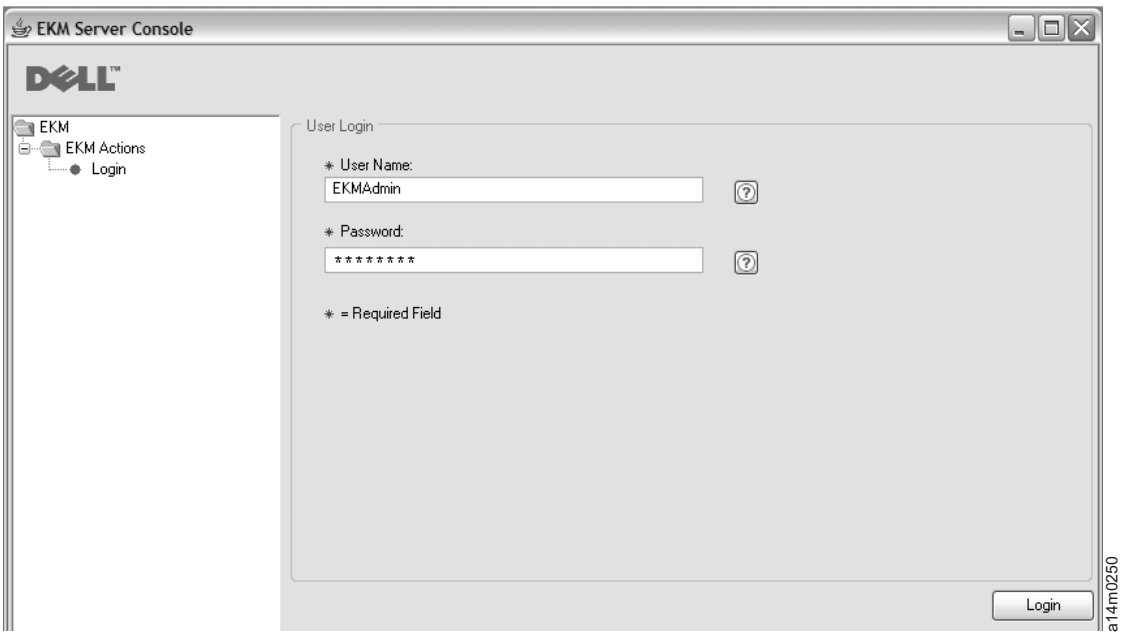

圖 4. User Login 頁面

這時會在背景啓動 Dell Encryption Key Manager 伺服器。

6. 在 GUI 導覽器中，選取 **Server Health Monitor** 來確認 Encryption Key Manager 伺服器已啓動。

如何找到正確的主機 IP 位址：

現行 Encryption Key Manager GUI 的限制，會造成會造成「伺服器性能監視器」無法顯示 Encryption Key Manager 主機 IP 位址：

- 如果主機配置了 IPv6 位址，Encryption Key Manager 應用程式將無法顯示 IP 位址。
- 如果 Encryption Key Manager 應用程式是安裝在 Linux 系統中，Encryption Key Manager 應用程式會顯示本端主機位址，而不是實際作用中的 IP 埠。

a. 如果要擷取主機系統的實際 IP 位址，請存取網路配置來尋找 IP 埠位址。
   - 在 Windows 系統中，開啓一個指令視窗，輸入 `ipconfig`。
   - 如果是 Linux，請輸入 `isconfig`。

如何識別 EKM SSL 埠

a. 利用指令行啓動 Encryption Key Manager 伺服器。
   - 在 Windows 上，導覽至 cd `c:\ekm`，並按一下 **startServer.bat**
   - 在 Linux 平台上，導覽至 `/var/ekm`，並輸入 `startServer.sh`
   - 請參閱 *Dell Encryption Key Manager 使用手冊*中的「啓動、重新整理和停止金鑰管理程式伺服器」，以取得詳細資訊。

b. 利用指令行來啓動 CLI 用戶端。
   - 在 Windows 上，導覽至 cd `c:\ekm`，並按一下 **startClient.bat**
   - 在 Linux 平台上，導覽至 `/var/ekm`，並輸入 `startClient.sh`
   - 請參閱 *Dell Encryption Key Manager 使用手冊*中的「啓動指令行介面用戶端」，以取得詳細資訊。

c. 在 Encryption Key Manager 伺服器上，利用下列指令來登入 CLI 用戶端：

   ```
   login -ekmuser userID -ekmpassword password
   ```

   其中*使用者 ID* = EKMAdmin 與*密碼* = changeME （這是預設密碼。如果您先前變更了預設密碼，請使用您的新密碼。）

   成功登入之後，畫面上會顯示使用者已順利登入。

d. 輸入下列指令來識別 SSL 埠：

   ```
   status
   ```

   顯示的回應如下：伺服器在執行中。TCP 埠：3801，SSL 埠：443。

   請記下 SSL 配置埠，以確定它是用來配置磁帶庫管理加密設定的埠。

e. 從指令行登出。輸入下列指令：

   ```
   exit
   ```

   關閉指令視窗。

方法 2：使用指令來設定 Encryption Key Manager

步驟 1. 建立 JCEKS 金鑰儲存庫

警告：強烈建議您定期製作 Encryption Key Manager 及所有相關檔案的副本。如果 Encryption Key Manager 加密金鑰遺失或毀損，將無法回復已加密的資料。

建立金鑰儲存庫並且移入憑證和私密金鑰。 憑證是用來保護 Encryption Key Manager 伺服器與 Encryption Key Manager CLI 用戶端之間的通訊。此 **keytool** 指令會建立一個新的 JCEKS 金鑰儲存庫（名稱爲 EKMKeys.jck）

並且使用 ekmcert 的別名來移入憑證和私密金鑰。此憑證的有效期是 5 年。當憑證過期時，「Encryption Key Manager 伺服器」之間的通訊以及「Encryption Key Manager CLI 用戶端」和「Encryption Key Manager 伺服器」之間的通訊將無法運作。請移除舊的失效憑證，然後根據這個步驟來建立新的憑證。

```
keytool -keystore EKMKeys.jck -storetype jceks -genkey -alias ekmcert -keyAlg RSA -keysize 2048 -validity 1825
```

keytool 指令會提示您輸入用來建立憑證的資訊（此憑證可接受您的 Encryption Key Manager 識別）。以下是類似的提示和範例回應：

```
您的姓氏和名字？[不明]：ekmcert
您所屬的組織單位名稱？[不明]：EKM
您所屬的組織名稱？[不明]：Dell
您所在的城市或地區名稱？[不明]：Austin
您所在的州/省（縣/市）名稱？[不明]：TX
此單位的國碼（兩個字母）為何？[不明]：US
CN=ekmcert, OU=EKM, O=Dell, L=Austin, ST=TX, C=US 是否正確？（請輸入 "yes" 或 "no"）：
```

輸入 yes，然後按 Enter 鍵。

步驟 2. 產生加密金鑰

註: 在任何階段作業中，在初次使用 keytool 指令之前，請執行 **updatePath** Script 來設定正確的環境。

在 Windows 上

導覽至 cd c:\ekm，再按一下 updatePath.bat

在 Linux 平台上

導覽至 /var/ekm 然後輸入 . ./updatePath.sh

附註：指定 . ./ （句點空格句點再加上斜線）之後，再指定 Linux Shell 指令以確保 Shell 能夠找到 Script。

若使用 LTO 加密，Encryption Key Manager 需要預先產生許多對稱金鑰，並且它們必須儲存在金鑰儲存庫中。**keytool** 指令會產生 32 個 256 位元的 AES 金鑰，並且將它們儲存在步驟 3 所建立的金鑰儲存庫中。請在 Encryption Key Manager 目錄中執行這個指令，以便在該目錄中建立金鑰儲存庫檔。產生的金鑰將使用 key0000000000000000000 到 key0000000000000001f 的名稱。

```
keytool -keystore EKMKeys.jck -storetype jceks -genseckey -keyAlg aes -keysize 256 -aliasrange key00-1f
```

這個指令會提示您輸入用來存取金鑰儲存庫的金鑰儲存庫密碼。請輸入想要的密碼，然後按 Enter 鍵。 在提示您輸入金鑰密碼時，請再按一次 Enter 鍵，因爲這項資訊是不需要的。 請不要輸入不同或新的密碼。這樣會使金鑰密碼與金鑰儲存庫密碼相同。 請注意，稍後在啓動 Encryption Key Manager 時，會需要使用在這裡所輸入的金鑰儲存庫密碼。

註: 設定金鑰儲存庫密碼之後，除非安全性有問題，否則請不要變更密碼。變更金鑰儲存庫密碼時，需要一併變更配置檔中的所有密碼內容。這些密碼會成爲亂碼，以免出現任何安全漏洞。

步驟 3. 啓動 Encryption Key Manager 伺服器

若要在不使用 GUI 的情況下啓動 Encryption Key Manager 伺服器，請啓動 startServer Script：

在 Windows 上

導覽至 cd c:\ekm\ekmserver，再按一下 startServer.bat

在 Linux 平台上

導覽至 /var/ekm/ekmserver，輸入 . ./startServer.sh

附註：指定 . ./ （句點空格句點再加上斜線）之後，再指定 Linux Shell 指令以確保 Shell 能夠找到 Script。

警告：強烈建議您定期製作 Encryption Key Manager 及所有相關檔案的副本。如果 Encryption Key Manager 加密金鑰遺失或毀損，將無法回復已加密的資料。

步驟 4. 啓動 Encryption Key Manager 指令行介面用戶端

若要啓動「Encryption Key Manager CLI 用戶端」，請啓動 startClient Script：

在 Windows 上

導覽至 `cd c:\ekm\ekmclient`，再按一下 startClient.bat

在 Linux 平台上

導覽至 /var/ekm\ekmclient，輸入 `. ./startClient.sh`

附註：指定 . ./ （句點空格句點再加上斜線）之後，再指定 Linux Shell 指令以確保 Shell 能夠找到 Script。

CLI 用戶端順利登入金鑰管理程式伺服器之後，您便可以執行任何 CLI 指令。完成時，請使用 quit 指令 來關閉 CLI 用戶端。若超過 10 分鐘沒有使用，用戶端將會自動關閉。如需 CLI 指令資訊，請參閱 *Dell Encryption Key Manager 使用手冊*（其位置如下：**http://support.dell.com**），或者您可以在產品所提供的 Dell Encryption Key Manager 媒體中取得。

其他資訊

如需相關資訊，請參閱下列出版品。

- *Dell Encryption Key Manager 使用手冊*（包含於 Dell Encryption Key Manager CD 中，也可從 **http://support.dell.com** 下載)。
- The *Library Managed Encryption for Tape* 白皮書：提供 LTO 磁帶加密的最佳實務建議（可從 **http://www.dell.com** 取得）。