7-1 NTFS 與 ReFS 權限的種類

使用者必須對磁碟內的檔案或資料夾擁有適當權限後，才可以存取這些資源。權限可分為基本權限與特殊權限，其中基本權限已經可以滿足一般需求，而透過特殊權限可以更精細的來指派權限。

以下權限僅適用於檔案系統為 NTFS 與 ReFS 的磁碟，其他的 exFAT、FAT32 與 FAT 皆不具備權限功能。

基本檔案權限的種類

- **讀取**：它可以讀取檔案內容、檢視檔案屬性與權限等（可透過【開啟**檔案總管**➲對著檔案按右鍵➲內容】的途徑來查看**唯讀**、**隱藏**等檔案屬性）。
- **寫入**：它可以修改檔案內容、在檔案後面增加資料與改變檔案屬性等（使用者至少還需要具備**讀取**權限才可以變更檔案內容）。
- **讀取和執行**：它除了擁有**讀取**的所有權限外，還具備執行應用程式的權限。
- **修改**：它除了擁有前述的所有權限外，還可以刪除檔案。
- **完全控制**：它擁有前述所有權限，再加上**變更權限**與**取得擁有權**的特殊權限。

基本資料夾權限的種類

- **讀取**:它可以檢視資料夾內的檔案與子資料夾名稱、檢視資料夾屬性與權限等。
- **寫入**：它可以在資料夾內新增檔案與子資料夾、改變資料夾屬性等。
- **列出資料夾內容**：它除了擁有**讀取**的所有權限之外，還具備有**周遊資料夾**的特殊權限，也就是可以進出此資料夾。
- **讀取和執行**：它與**列出資料夾內容**相同，不過**列出資料夾內容**權限只會被資料夾繼承，而**讀取和執行**則會同時被資料夾與檔案來繼承。
- **修改**：它除了擁有前述的所有權限之外，還可以刪除此資料夾。
- **完全控制**：它擁有前述所有權限，再加上**變更權限**與**取得擁有權**的特殊權限。

7-2 使用者的有效權限

權限是可以被繼承的

當您針對資料夾設定權限後，這個權限預設會被此資料夾之下的子資料夾與檔案來繼承，例如您設定讓使用者 A 對甲資料夾擁有**讀取**的權限，則使用者 A 對甲資料夾內的檔案也會擁有**讀取**的權限。

設定資料夾權限時，除了可以讓子資料夾與檔案都來繼承權限之外，也可以只單獨讓子資料夾或檔案來繼承，或都不讓它們繼承。

而設定子資料夾或檔案權限時，您可以讓子資料夾或檔案不要繼承父資料夾的權限，如此該子資料夾或檔案的權限將是以您直接針對它們設定的權限為權限。

權限是有累加性的

若使用者同時隸屬於多個群組，且該使用者與這些群組分別對某個檔案擁有個別的權限設定，則該使用者對此檔案的最後有效權限是這些權限的總合，例如若使用者 A 同時屬於**業務部**與**經理**群組，且其權限分別如下表所示，則使用者 A 最後的有效權限為這 3 個權限的總和，也就是**寫入**+**讀取**+**執行**。

使用者或群組	權限
使用者 A	寫入
群組 **業務部**	讀取
群組 **經理**	讀取和執行
使用者 A 最後的有效權限為 **寫入** + **讀取** + **執行**	

「拒絕」權限的優先權較高

雖然使用者對某個檔案的有效權限是其所有權限來源的總合，但只要其中有一個權限來源被設定為**拒絕**的話，則使用者將不會擁有存取權限。例如若使用者 A 同時屬於**業務部**與**經理**群組，且其權限分別如下表所示，則使用者 A 的**讀取**權限會被**拒絕**，也就是無法讀取此檔案。

網域控制站安全性原則的設定

網域控制站安全性原則設定會影響到組織單位 Domain Controllers 內的網域控制站（見圖 9-5-3），但不會影響到位於其他組織單位或容區內的電腦（與使用者）。

圖 9-5-3

您可以到網域控制站上利用系統管理員身分登入，然後【點擊左下角**開始**圖示➡Windows 系統管理工具➡群組原則管理➡如圖 9-5-4 所示對著 Default Domain Controllers Policy(或自建的 GPO)按右鍵➡編輯】來設定網域控制站安全性原則。它的設定方式與**網域安全性原則**、**本機安全性原則**相同，此處不再重複，僅列出注意事項：

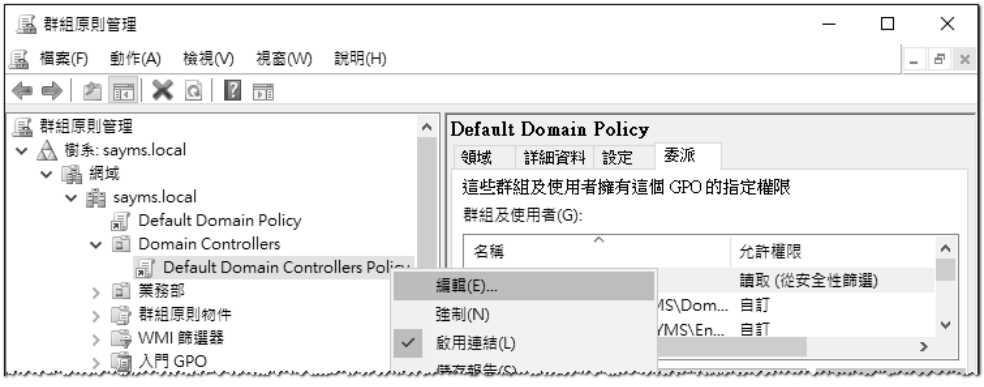

圖 9-5-4

- 位於組織單位 Domain Controllers 內的所有網域控制站，都會受到**網域控制站安全性原則**的影響。

- **網域控制站安全性原則**的設定必須要套用到網域控制站後，這些設定對網域控制站才有作用。套用時機與其他相關說明在前一節內已經介紹過了。
- **網域控制站安全性原則**與**網域安全性原則**的設定有衝突時，對位於 Domain Controllers 內的電腦來說，預設是以**網域控制站安全性原則**的設定優先，也就是**網域安全性原則**自動無效。不過其中的**帳戶原則**例外：網域的帳戶原則只有針對網域來設定才有效，針對組織單位（例如 Domain Controllers） 的設定無效，因此**網域安全性原則**內的**帳戶原則**設定對網域內所有的使用者都有效，而**網域控制站安全性原則**的**帳戶原則**對 Domain Controllers 內的使用者並無作用。

除了**原則設定**之外，還有**喜好設定**功能。**喜好設定**非強制性，用戶端可自行變更設定值，故**喜好設定**適合於用來當作預設值；然而**原則設定**是強制性設定，用戶端套用這些設定後，就無法變更。只有網域群組原則才有**喜好設定**功能，本機電腦原則並無此功能。

9-6 稽核資源的使用

透過稽核（auditing）功能可以讓系統管理員來追蹤是否有使用者存取電腦內的資源、追蹤電腦運作情況等。稽核工作通常需要經過以下兩個步驟：

- **啟用稽核原則**：Administrators 群組內的成員才有權利啟用稽核原則。
- **設定欲稽核的資源**：需具備**管理稽核及安全性記錄**權限的使用者才可以稽核資源，預設是 Administrators 群組內的成員才有此權限。您可以利用**使用者權限指派**原則（參見第 9-19 頁 **使用者權限指派**的說明）來將**管理稽核及安全性記錄**權限賦予其他使用者。

稽核記錄是被儲存在**安全性記錄檔**內，而您可以利用【點擊左下角**開始**圖示➔Windows 系統管理工具➔事件檢視器➔Windows 記錄➔安全性】來查看（或在**伺服器管理員**畫面中點擊右上方的**工具**功能表➔事件檢視器➔...）。

稽核原則的設定

稽核原則的設定可以透過**本機安全性原則**、**網域安全性原則**、**網域控制站安全性原則**或組織單位的群組原則來設定，其相關套用規則已經解釋過了。此處利用本機安全性原則來舉例說明，因此建議到未加入網域的電腦登入後：【點擊左下角**開始**圖示➲Windows 系統管理工具➲本機安全性原則➲如圖 9-6-1 所示展開**本機原則**➲稽核原則】。

本機安全性原則的設定只對本機電腦有效，若要利用網域控制站或網域成員電腦做實驗，則請透過網域控制站安全性原則、網域安全性原則或組織單位的群組原則。

由圖 9-6-1 中可知稽核原則內提供了以下的稽核事件：

- **稽核目錄服務存取**：稽核是否有使用者存取 AD DS 內的物件。您必須另外再選擇欲稽核的物件與使用者。此設定只對網域控制站有作用。
- **稽核系統事件**：稽核是否有使用者重新開機、關機或系統發生了任何會影響到系統安全或影響安全性記錄檔正常運作的事件。
- **稽核物件存取**：稽核是否有使用者存取檔案、資料夾或印表機等資源。您必須另外再選擇欲稽核的檔案、資料夾或印表機。
- **稽核原則變更**：稽核**使用者權限指派原則**、**稽核原則**或**信任原則**等是否有異動。
- **稽核特殊權限使用**：稽核使用者是否使用了**使用者權限指派**原則內所賦予的權限，例如變更系統時間（系統不會稽核部分會產生大量記錄的事件，因為這會影響到電腦效能，例如**備份檔案及目錄**、**還原檔案及目錄**等事件，若要稽核它們的話，請透過執行 Regedit，然後啟用 fullprivilegeauditing 登錄值，它位於 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa）。
- **稽核帳戶登入事件**：稽核是否發生了利用本機使用者帳戶來登入的事件。例如此電腦啟用這個原則後，若在此電腦上利用本機使用者帳戶登入的話，則安全性記錄檔內會有記錄，然而若是利用網域使用者帳戶登入的話，就不會有記錄。

會先讀取 GPT，並將控制權交給 GPT 內的程式碼，然後由此程式碼來繼續後續的啟動工作。GPT 磁碟所支援的硬碟可以超過 2.2TB。

您可以利用圖形介面的**磁碟管理**工具或 **Diskpart** 指令將空的 MBR 磁碟轉換成 GPT 磁碟或將空的 GPT 磁碟轉換成 MBR 磁碟。

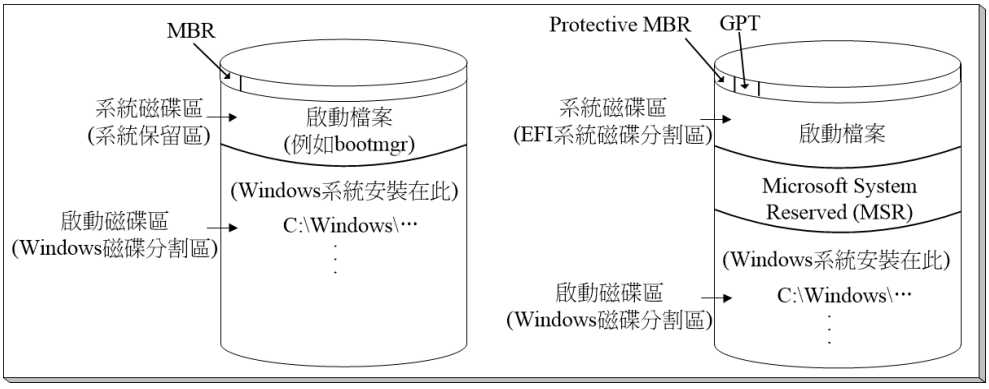

圖 10-1-2

為了相容起見，GPT 磁碟內另外還提供了 Protective MBR，它讓僅支援 MBR 的程式仍然可以正常運作。

基本磁碟與動態磁碟

Windows 系統又將磁碟分為**基本磁碟**與**動態磁碟**兩種類型：

- **基本磁碟**：傳統的磁碟系統，新安裝的硬碟預設是基本磁碟。
- **動態磁碟**：它支援多種特殊的磁碟區，其中有的可以提高系統存取效率、有的可以提供容錯功能、有的可以擴大磁碟的使用空間。

以下先針對基本磁碟來說明，至於動態磁碟則留待後面的章節再介紹。

主要與延伸磁碟分割區

在磁碟可以儲存資料之前，該磁碟必須被分割成一或數個磁碟分割區，而磁碟分割區分為兩種：

14-1 DNS 概觀

當 DNS 用戶端要與某台主機（電腦）溝通時，例如要連接網站 www.sayms.com，該用戶端會向 DNS 伺服器提出查詢 www.sayms.com 的 IP 位址的要求，伺服器收到此要求後，會幫用戶端來找尋 www.sayms.com 的 IP 位址。這台 DNS 伺服器也被稱為**名稱伺服器**（name server）。

當用戶端向 DNS 伺服器提出查詢 IP 位址的要求後，伺服器會先從自己的 DNS 資料庫內來尋找，若資料庫內沒有所需資料，此 DNS 伺服器會轉向其他 DNS 伺服器來詢問。

DNS 網域名稱空間

整個 DNS 架構是一個類似圖 14-1-1 所示的階層式樹狀結構，這個樹狀結構被稱為**DNS 網域名稱空間**（DNS domain namespace）。

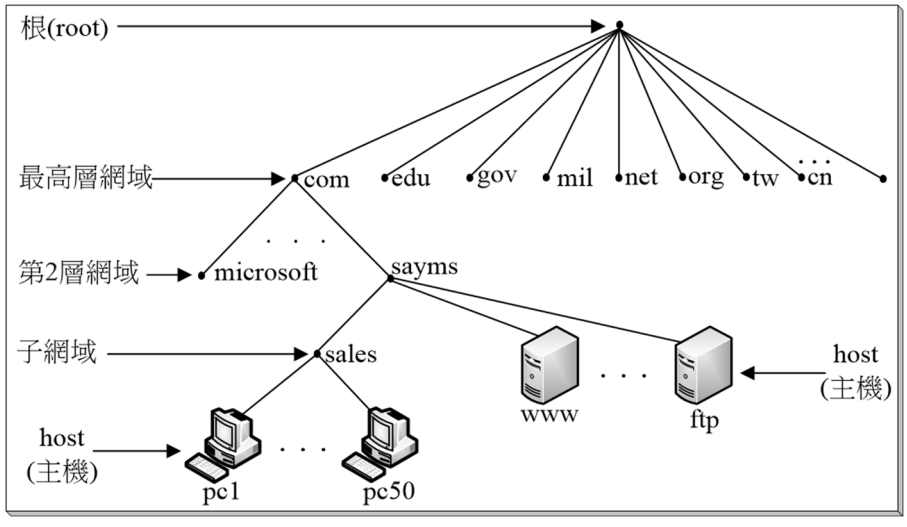

圖 14-1-1

圖中位於樹狀結構最上層的是 DNS 網域名稱空間的**根**（root），一般是用句點（.）來代表**根**，**根**內有多台 DNS 伺服器，分別由不同機構來負責管理。**根**之下為**最高層網域**（top-level domain），每一個最高層網域內都有數台的 DNS 伺服器。最高層網域用來將組織分類。表 14-1-1 為部分的最高層網域名稱。

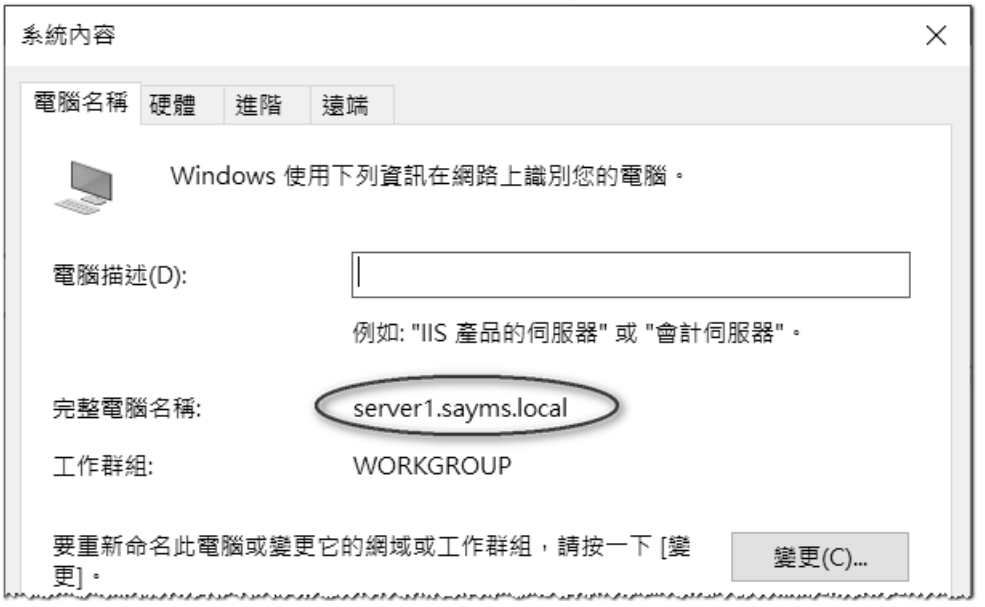

圖 14-1-2

DNS 區域

DNS **區域**（zone）是網域名稱空間樹狀結構的一部分，透過它來將網域名稱空間分割為比較容易管理的小區域。在這個 DNS 區域內的主機資料，是被儲存在 DNS 伺服器內的**區域檔案**（zone file）或 Active Directory 資料庫內。一台 DNS 伺服器內可以儲存一個或多個區域的資料，同時一個區域的資料也可以被儲存到多台 DNS 伺服器內。在區域檔案內的資料被稱為**資源記錄**（resource record，RR）。

將一個 DNS 網域劃分為數個區域，可分散網路管理的工作負荷，例如圖 14-1-3 中將網域 sayms.com 分為**區域 1**（涵蓋子網域 sales.sayms.com）與**區域 2**（涵蓋網域 sayms.com 與子網域 mkt.sayms.com），每一個區域各有一個區域檔案。區域 1 的區域檔案（或 Active Directory 資料庫）內儲存著所涵蓋網域內所有主機（pc1 - pc50）的記錄，區域 2 的區域檔案（或 Active Directory 資料庫）內儲存著所涵蓋網域內所有主機（pc51 - pc100、www 與 ftp）的記錄。這兩個區域檔案可以存放在同一台 DNS 伺服器內，也可以分別存放在不同 DNS 伺服器內。

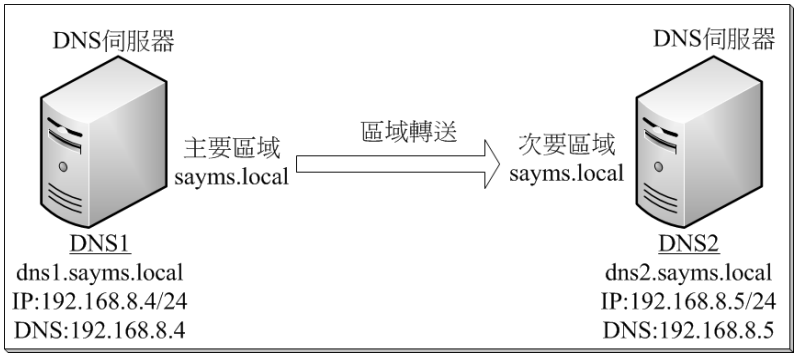

圖 14-3-18

我們將在圖中 DNS2 建立一個次要區域 sayms.local，此區域內的記錄是從其**主機伺服器** DNS1 透過**區域轉送**複寫過來。圖中 DNS1 仍沿用前一節的 DNS 伺服器，不過請先在其 sayms.local 區域內替 DNS2 建立一筆 A 資源記錄（FQDN 為 dns2.sayms.local、IP 位址為 192.68.8.5），然後另外架設第 2 台 DNS 伺服器、將電腦名稱設定為 DNS2、IP 位址設定為 192.168.8.5、完整電腦名稱（FQDN）設定為 dns2.sayms.local，然後重新啟動電腦、新增 DNS 伺服器角色。

確認是否允許區域轉送

若 DNS1 不允許將區域記錄轉送給 DNS2 的話，則 DNS2 向 DNS1 提出**區域轉送**要求時會被拒絕。以下我們先設定讓 DNS1 可以區域轉送給 DSN2。

STEP 1 到 DNS1 伺服器上點擊左下角開始圖示⊞➲Windows 系統管理工具➲DNS➲如圖 14-3-19 所示點擊區域 sayms.local➲點擊上方的**內容**圖示。

圖 14-3-19

STEP 2 如圖 14-3-20 所示勾選**區域轉送**標籤下的**允許區域轉送**➲點選**只到下列伺服器**➲按編輯鈕以便來選擇 DNS2 的 IP 位址。

安裝 Docker

我們要將一台 Windows Server 2022 電腦當作是容器主機（container host）。首先在這台電腦上安裝 Docker，我們可以透過 Docker 來管理容器、管理映像檔（image）、執行容器內的應用程式等。

請【點擊左下角**開始**圖示⊞➲Windows PowerShell】來開啟 PowerShell 視窗，然後執行以下指令後按 Y 鍵，它會從 PowerShell Gallery 來安裝 Docker-Microsoft PackageManagement Provider（參考圖 20-6-3）：

Install-Module -Name DockerMsftProvider –Repository PSGallery -Force

接著執行 PackageManagement PowerShell 模組所提供的以下指令後按 A 鍵，它會安裝最新版的 Docker（參考圖 20-6-3）：

Install-Package -Name docker -ProviderName DockerMsftProvider

安裝完成後，執行 **Restart-Computer** 來重新啟動電腦。

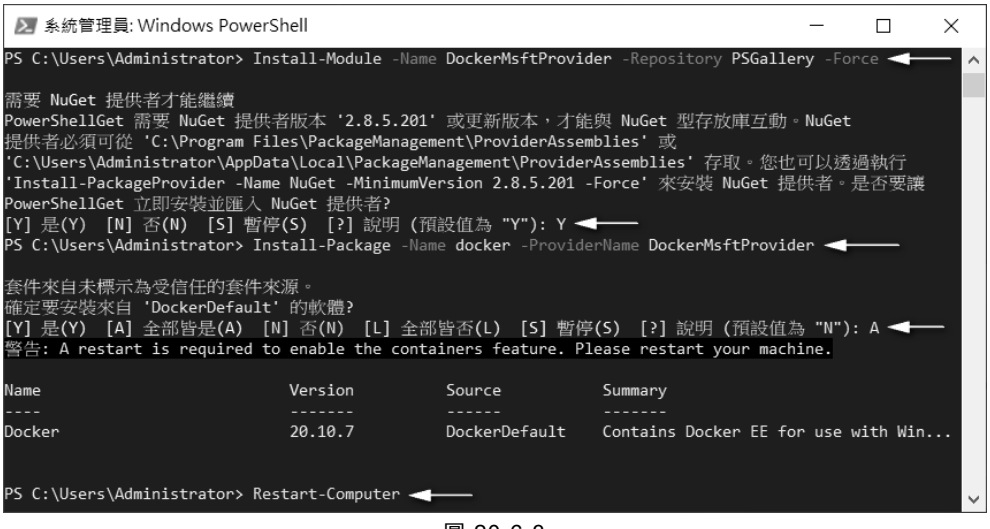

圖 20-6-3

重新啟動電腦後，再開啟 PowerShell 視窗，然後分別利用 docker version 與 docker info 兩個指令，來查看 docker 版本與 docker 的更多資訊，如圖 20-6-4 所示

若要在 Windows 11 內來練習容器的話，請先到以下網址下載與安裝 **Docker Desktop for Windows**：
https://hub.docker.com/editions/community/docker-ce-desktop-windows
安裝完成後，對著右下方的 Docker Desktop 圖示按右鍵，然後點選 **Switch to Windows containers...**，然後接續以下章節的動作。

部署第一個容器

本練習利用以下 docker run 指令，來從 Docker Hub 下載所需的映像檔（image），然後透過部署容器來執行映像檔裡的 Hello World 應用程式（參考圖 20-6-6）：

docker run hello-world

它會先從本機硬碟來找尋是否有此映像檔，若有的話，則直接使用此映像檔，若無的話，則會顯示類似 Unable to find image 'hello-world:latest' locally...的訊息（參考圖 20-6-6 第 2 行的文字），然後改從 Docker Hub 下載，下載完成後，會將其打包到容器內並執行之（另外也會將映像檔儲存一份到本機硬碟，預設是在 C:\ProgramData\Docker\windowsfilter 資料夾內）。

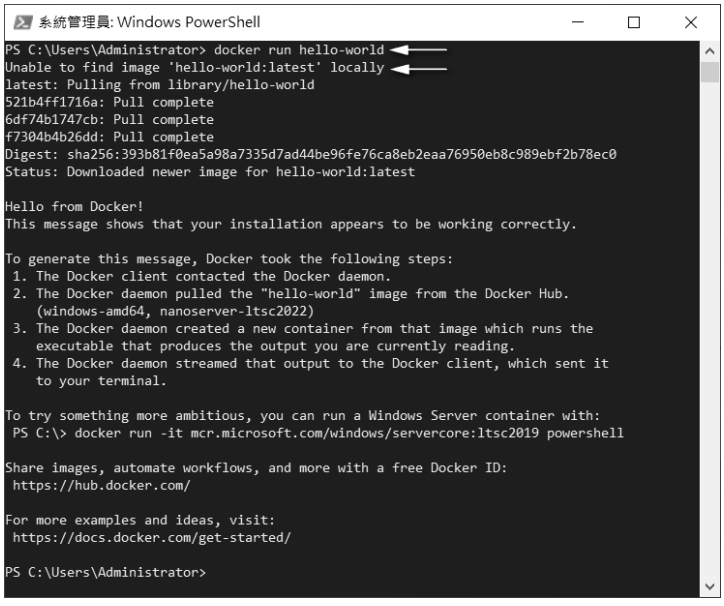

圖 20-6-6

我們可以分別利用 docker images 與 docker ps –a 來查看現存的映像檔與容器，如圖 20-6-7 所示，圖中有一個 hello-world 的映像檔與一個使用此映像檔的容器。

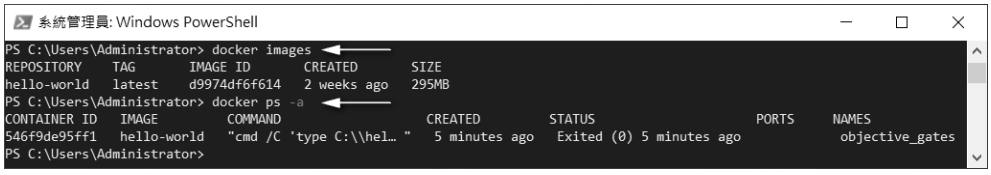

圖 20-6-7

若要刪除容器的話，請使用 docker rm <*容器識別碼*>，以圖 20-6-7 來說，其容器識別碼（CONTAINER ID）為 546f9de95ff1，故可利用以下指令來刪除它：

docker rm 546f9de95ff1

若要刪除映像檔的話，請使用 docker rmi <*映像檔識別碼*>，以圖 20-6-7 來說，其映像檔識別碼（IMAGE ID）為 d9974df6f614，故可利用以下指令來刪除它：

docker rmi d9974df6f614

被容器使用中的映像檔無法刪除，需先刪除容器，再來刪除映像檔。

也可以利用 docker pull hello-world 指令事先將映像檔下載、儲存到本機硬碟，事後再用 docker run hello-world 來執行，參考圖 20-6-8（假設已經將之前練習的容器與映像檔都刪除了，請先用 docker images 與 docker ps -a 來確認已經刪除）：

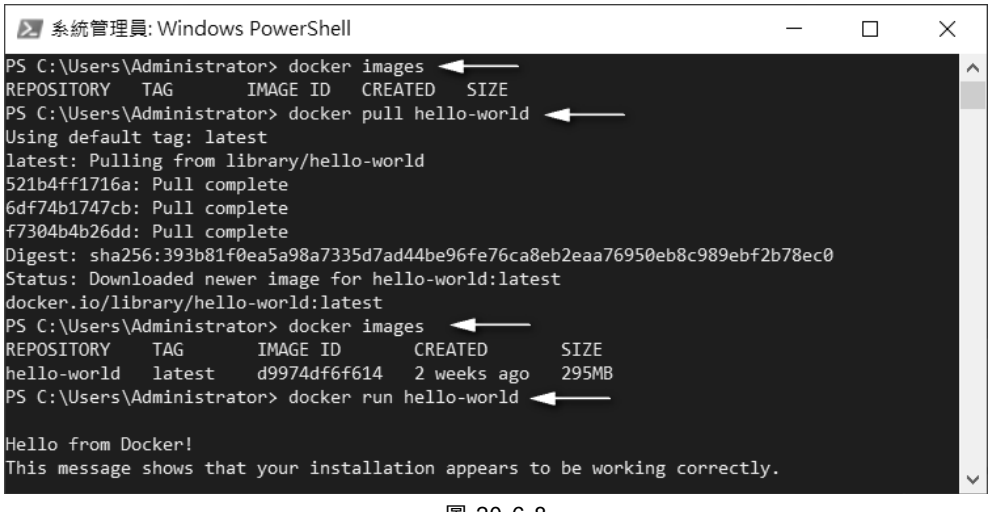

圖 20-6-8