Synology

Synology Directory Server

管理手冊

適用於

DSM 7.1 與 Synology Directory Server 4.10

目錄

第 1 章：簡介

關於 Synology Directory Server

Synology Directory Server 結合 Samba 技術，為您提供帳號及資源的集中管理平台。本套件支援常用的 Windows Active Directory® 功能，包含使用者 / 群組管理、組織單位 (Organizational Unit，OU)、群組規則、Kerberos 驗證、多種用戶端裝置的部署。透過 Synology Directory Server 架設的網域服務，您可以安全地建立目錄資料庫，管理使用者帳號，並根據您的組織架構來部署裝置。

Synology Directory 基本要素

本段落將概述 Synology Directory 服務，讓您在透過 Synology Directory Server 執行管理員任務前，能先清楚掌握其關鍵知識。

目錄服務

目錄為一種檔案庫，用來存放個人、群組、地點等多項資訊。其儲存管理檔案的功能，讓使用者能夠輕鬆查得所需資訊。在資訊科學的領域上，目錄服務則用來集中儲存所有的帳號資訊，亦可統合各類資源，因此適合作為授予存取權限、設定身分、以及管理使用者 / 群組關係的解決方案。

Active Directory® 與 Synology Directory 服務

Active Directory® (AD) 為一種目錄服務，可集中儲存資料，讓 IT 人員安全無虞地管理物件及各類資源，例如帳號、電腦、印表機。Synology Directory Server 運用 AD 的原理來提供 **Synology Directory 服務**，讓使用者在直覺化的介面上儲存、部署資源。

網域名稱系統 (DNS)

Synology Directory 服務採用網域名稱系統 (Domain Name System，DNS) 的技術，將電腦、印表機及其他資源整合至階層式的架構中。

網域是用來新增及管理資源的邏輯性分界，而 DNS 則是一種標準化網路服務，透過網域名稱來規劃資源架構。在網域 (例如：「syno.local」) 中，裝置會利用 DNS 來部署，藉此可將簡單易讀的主機名稱 (例如：「pc1.syno.local」) 解析成透過網路協定搜尋、辨識裝置所需要的 IP 位址。

安裝 Synology Directory Server 的同時必須**架設 DNS 伺服器**，以確保網域能正常運作。

網域控制站

網域控制站 (Domain Controller，DC) 為架設 Synology Directory Server 網域的 Synology NAS。該裝置負責維持網域的功能、儲存目錄檔案，並管理使用者在網域內的各項互動。

在 Synology Directory Server 的機制下，建立網域的 Synology NAS 會自動升級為主要網域控制站 (Primary Domain Controller，PDC)。

網域物件

Synology Directory Server 的網域資料庫是由物件資訊所組成，每個物件都代表資料庫中的單一項目。以下為 Synology Directory Server 內可管理的物件：

- **使用者**：網域內可存取網域資源的使用者帳號。
- **群組**：可將網域物件集結管理的一項單位。群組存取網域內資源 (例如：檔案、裝置) 的權限會套用至所有的群組成員。
- **裝置**：網域使用者可存取的實體資源，包含電腦、印表機、Synology NAS 等裝置。
- **組織單位 (Organizational Unit，OU)**：在網域內可指派管理員權限及群組規則的最小容器。您可以將使用者、群組、電腦放入 OU 內，並為這些物件賦予相同的任務授權及規則。此外，您也可以將 OU 加入另一個 OU，依照真實的組織架構來建立 OU 階層，藉此提升設定 Synology Directory Server 網域物件的效率。

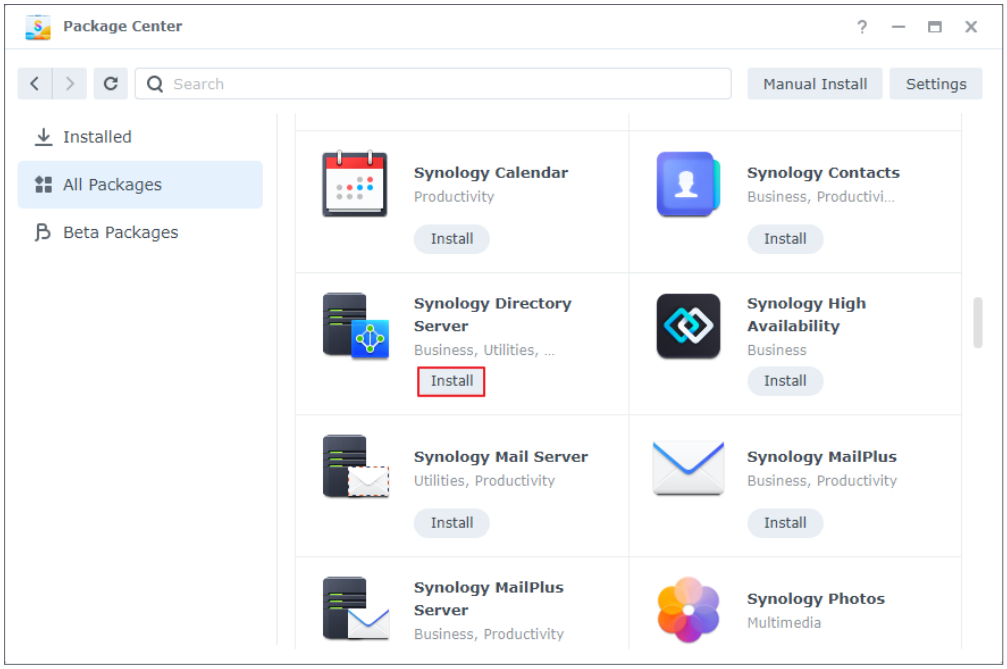
相容性及限制

- DSM 版本需求：DSM 7.1 及以上版本。
- 網域功能等級：等同於 Windows Server 2008 R2。
- Synology Directory Server 須和 **DNS Server** 套件搭配使用。
- Synology Directory Server 與其他網域 / LDAP 服務的設定不相容。
- 支援的網域用戶端：
  - Windows 7 及以上版本
  - macOS
  - Linux
- Synology Directory Server 僅可安裝在**適用的 Synology NAS 機種**上。
- 限制：
  - 僅支援單一網域。
  - Synology Directory Server 啟用後，**Synology NAS (DC) 的主機名稱將無法變更**。
  - 建立網域後，SMB 簽章將隨之自動開啟，**這可能會降低 SMB 檔案傳輸的讀寫效能**。
    - SMB 簽署能在封包層級上，為 SMB 通訊附加數位簽章。若要提升效能，請至**控制台** > **檔案服務** > **SMB** > **進階設定** > **啟用伺服器簽章**，選擇**停用**，並按一下**儲存**。
  - 不支援分散式檔案系統複寫 (Distributed File System Replication，DFSR)。
  - 不支援適用於 Windows PowerShell 的 Active Directory 模組。
  - 次要網域控制站 (Secondary Domain Controller，SDC) 僅能運行於 Synology Directory Server 所建立的網域。

參閱 Synology Directory Server 的**技術規格**以了解更多資訊。

安裝 Synology Directory Server

1. 在 Synology NAS 上安裝 **Synology Directory Server** 之前，請先確認以下事項：
   - Synology NAS 的網路連線正常。
   - Synology NAS 的**儲存空間管理員** > **儲存管理**顯示儲存空間狀態為**良好**。
   - DSM 已更新至 7.1 或以上版本。
   - 您擁有 Synology NAS 的 **DSM** 管理員身分 (即：屬於 **administrators** 群組的使用者)。
   - Synology NAS 使用靜態 IP 位址：請先在區域網路內為 Synology NAS (DC) 設定靜態 IP 位址，以避免因 Synology NAS 的 IP 位址變更而導致用戶端連線中斷。
   - Synology NAS 不是其他網域 / LDAP 目錄的用戶端：若 Synology NAS 已加入網域或 LDAP 目錄，則必須在使用 Synology Directory Server 前先離開該網域 / LDAP 目錄。
   - 確認區域網路內未發生網域名稱衝突：若區域網路內有多個相同的網域名稱，用戶端將無法找到 Synology Directory Server。請用其他名稱命名您的網域，或移除其他相同名稱的網域，以避免此問題。
2. 請以管理員 (即：屬於 **administrators** 群組的使用者) 身分登入 DSM。
3. 前往**套件中心** > **所有套件**。
4. 找到 **Synology Directory Server**，按一下**安裝**，並依螢幕指示完成安裝步驟。



注意：

- 在安裝 Synology Directory Server 前，您可以先**設定 Synology High Availability 叢集來確保不間斷的目錄服務**。

知識中心

請參閱**知識中心**取得更多關於 Synology Directory Server 的說明文章、應用教學、常見問題、技術規格、發行資訊、影片教學等資訊。

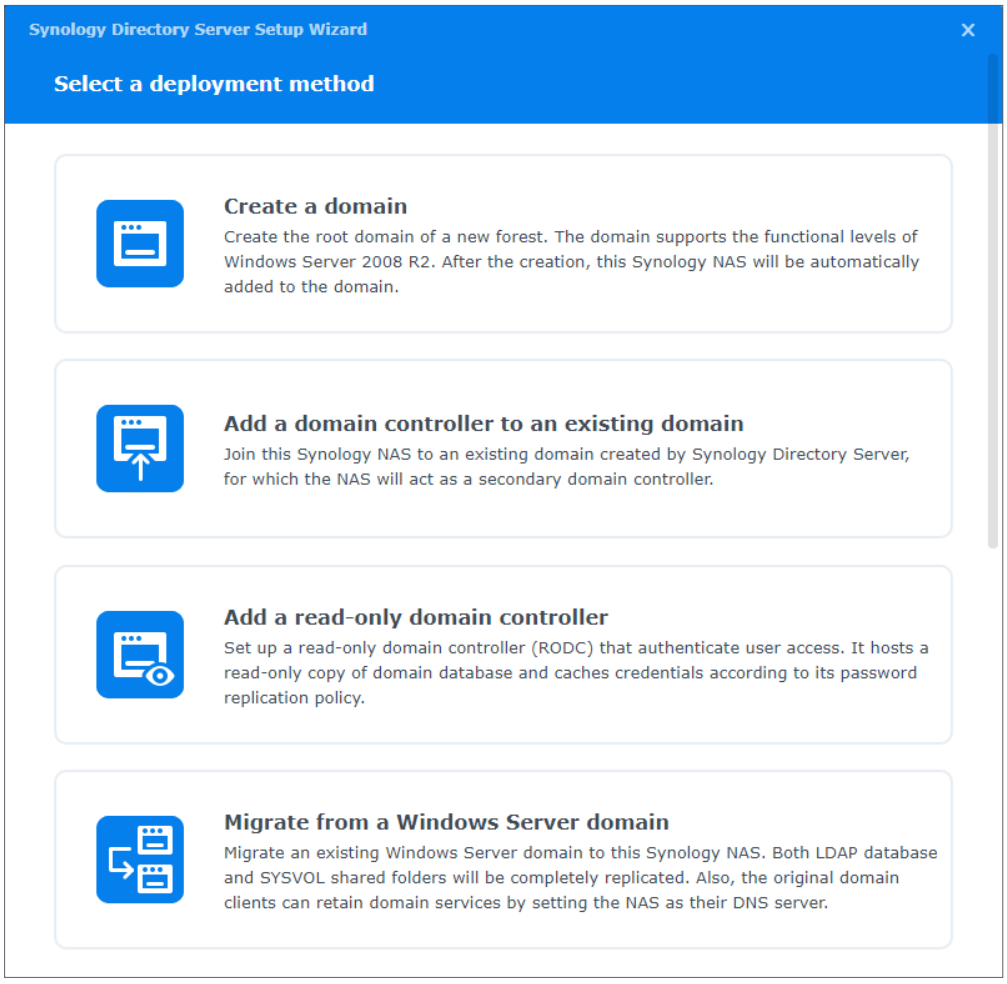
第 2 章：設定網域控制站

您可以將 Synology NAS 設定為主要網域控制站 (PDC) 或次要網域控制站 (SDC)，以管理帳號、部署裝置、設定存取權限、委派管理項目。

- 一個網域只能有一台 PDC，但可以有多台 SDC。
- PDC 是一台讀寫網域控制站 (Read-write Domain Controller，RWDC)。
- SDC 可以是一台 RWDC 或唯讀網域控制站 (Read-only Domain Controller，RODC)，依部署情況而定。

部署方式

請參閱下方圖片以了解 Synology Directory Server 支援的四種部署方式，再搭配下方的表格了解部署方式的更多說明。



DC		部署方式	描述
PDC	RWDC	建立網域	建立新樹系的根網域。 • 此網域支援與 Windows Server 2008 R2 相同的功能等級。 • 建立完成後，您的 Synology NAS 會自動加入至網域。
		從 Windows Server 網域轉移	將既有的 Windows Server 網域轉移至您的 Synology NAS。 • LDAP 資料庫與 SYSVOL 共用資料夾皆會完整複製至您的 Synology NAS。 • 原本的網域用戶端只需要將此 Synology NAS 設為 DNS 伺服器即可維持網域服務。
SDC	RWDC	在現有網域中新增網域控制站	將您的 Synology NAS 加入 Synology Directory Server 所建立之既有網域。
	RODC	新增唯讀網域控制站	將您的 Synology NAS 加入 Synology Directory Server 或 Windows AD 所建立之既有網域，並設定為 RODC。 • 此控制站僅有網域資料庫的讀取權限。 • 此控制站可預先填入使用者帳號的密碼。 • 此控制站可驗證使用者存取。

設定主要網域控制站

當 Synology Directory Server 安裝完成且系統未偵測到其他既有網域時，您即可開始建立網域並將 Synology NAS 升階為 PDC。

1. 開啟 **Synology Directory Server**。
2. 選擇部署方式：
   - **建立網域**
   - **從 Windows Server 網域轉移**
3. 依照網域類別輸入下列資訊。
   - 建立網域：
     - **網域名稱**：輸入網域的完整網域名稱 (Fully Qualified Domain Name，FQDN)，例如：「syno.local」。
     - **工作群組**：工作群組名稱 (或 NetBIOS 網域名稱) 將會自動填入此欄位。舉例來說，若您的網域名稱為「syno.local」，預設的工作群組名稱將為「syno」。
     - **密碼**：為網域管理員帳號設定的密碼。
     - **確認密碼**：再次輸入密碼。
   - 從 Windows Server 網域轉移：
     - **網域名稱**：輸入欲轉移到 Synology Directory Server 的 Windows 網域其 FQDN。

- **DNS 伺服器**：輸入 DNS 伺服器的 IP 位址以解析既有的 Windows DC。
- **帳號**：按照以下格式輸入網域的管理員帳號。

  ```
  NetBIOS 網域名稱 \ 管理員的使用者名稱
  ```

- **密碼**：輸入管理員帳號的密碼。

4. 按**下一步**，精靈將執行環境檢測並提供檢測結果。
   - ：測試項目通過檢測。
   - ：檢測出一個或多個次要問題須解決。這些問題可能會導致網域服務異常。按一下**詳情**，並依照指示解決問題。
   - ：檢測出一個或多個嚴重問題須立即解決。這些問題會造成網域服務異常。按一下**詳情**，並依照指示解決問題。
5. 完成檢查並確認無任何嚴重問題後，按一下**建立網域**或**轉移網域**（視部署方式而定）。轉移資料的所需時間取決於資料大小。

網域命名要求：

- 網域名稱僅可包含拼音字母、數字、減號、小數點（僅用於區隔網域名稱）。
- 網域名稱至少須包含兩個部分，例如：「syno.local」。
- 網域名稱開頭不可為連字號 (-)。
- 網域名稱結尾不可為連字號 (-) 或小數點 (.)。
- 網域名稱不可和 Synology NAS 的主機名稱相同。
- 最多可輸入 64 個字元。

密碼強度要求：

密碼至少須遵守下列規則的其中三項：

- 大寫的拉丁字母（包含 A - Z 及附加符號）、希臘字母、西里爾字母。
- 小寫的拉丁字母（包含 a - z 及附加符號）、希臘字母、西里爾字母。
- 數字 (0 - 9)。
- 特殊符號，包含 #、$、! 等。
- 不分大小寫的 Unicode 字母，包含亞洲語言的字母。

設定次要網域控制站

您可以將 Synology NAS 設定為 SDC（即：RWDC 或 RODC）並將其加入 **Synology Directory Server 已建立的網域**。

1. 開啟 **Synology Directory Server**。
2. 選擇部署方式：
   - **在現有網域中新增網域控制站**：此選項會將 Synology NAS 設定為 RWDC。
   - **新增唯讀網域控制站**：此選項會將 Synology NAS 設定為 RODC。
3. 輸入下列資訊：
   - **網域名稱**：輸入既有 Synology 網域的 FQDN。

- **DNS 伺服器**：輸入 DNS 伺服器的 IP 位址以解析既有的 Synology DC。
- **帳號**：按照以下格式輸入網域的管理員帳號。

  ```
  NetBIOS 網域名稱 \ 管理員的使用者名稱
  ```

- **密碼**：輸入管理員帳號的密碼。

4. 按**下一步**，精靈將執行環境檢測並提供檢測結果。

   - ：測試項目通過檢測。
   - ：檢測出一個或多個次要問題須解決。這些問題可能會導致網域服務異常。按一下**詳情**，並依照指示解決問題。
   - ：檢測出一個或多個嚴重問題須立即解決。這些問題會導致網域服務異常。按一下**詳情**，並依照指示解決問題。

5. 完成檢查並確認無任何嚴重問題後，按一下**加入網域**。

第 3 章：管理網域

檢視網域資訊

您可以在**網域**頁面檢視、編輯、移除網域或 DC。

網域資訊	
網域名稱	網域的完整名稱。
網域 NetBIOS 名稱	此名稱用於識別區域網路。舉例來說，若網域名稱為「syno.local」，NetBIOS 名稱則為「syno」。
DC	
類型	**PDC** • 此伺服器扮演 PDC 模擬器主機及其他彈性單一主機操作 (Flexible Single Master Operation，FSMO) 的角色。 • 當資料發生同步問題時，PDC 將會負責提供資料更新。
	SDC • 此伺服器可扮演 FSMO 角色，但無法扮演 PDC 模擬器主機的角色。
	RODC • 此伺服器僅擁有網域資料庫的讀取權限，可依照密碼複寫原則來複寫使用者帳號的密碼，並驗證使用者的登入。 • RODC 僅會從 RWDC 取得複寫資料。
辨別名稱	辨別名稱 (Distinguished Name，DN) 為網域資料庫中 DC 的物件路徑。舉例來說，若 DC 的 DN 是「CN=SYNOTEST,OU=Domain Controllers,DC=syno,DC=local」，您可以依循以下方式分析其組成： • **CN**=SYNOTEST：此 DC 的主機名稱為「SYNOTEST」。 • **OU**=Domain Controllers：此 DC 屬於 OU 「Domain Controllers」。 • **DC**=syno,**DC**=local：此 DC 部署於網域「syno.local」。
角色	**PDC 模擬器主機** • 扮演 PDC 模擬器主機的 DC 為 Kerberos 認證提供時間同步服務，記錄同網域內其他 DC 的密碼更新。 • 每個網域內只能有一台 RWDC 扮演此角色。

角色	**RID 主機** • 扮演相對識別碼 (Relative ID，RID) 主機角色的 DC 回應同網域內所有 DC 的 RID 集區請求，讓 DC 可以新增網域物件。 • 每個網域內只能有一台 RWDC 扮演此角色。
	基礎結構主機 • 扮演基礎結構主機角色的 DC 負責更新跨網域物件的參照。 • 每個網域內只能有一台 RWDC 扮演此角色。
	網域命名主機 • 扮演網域命名主機角色的 DC 負責處理網域名稱空間的變更。 • 每個樹系內只能有一台 RWDC 扮演此角色。
	架構主機 • 扮演架構主機角色的 DC 負責更新目錄架構。 • 每個樹系內只能有一台 RWDC 扮演此角色。

檢視網域權限

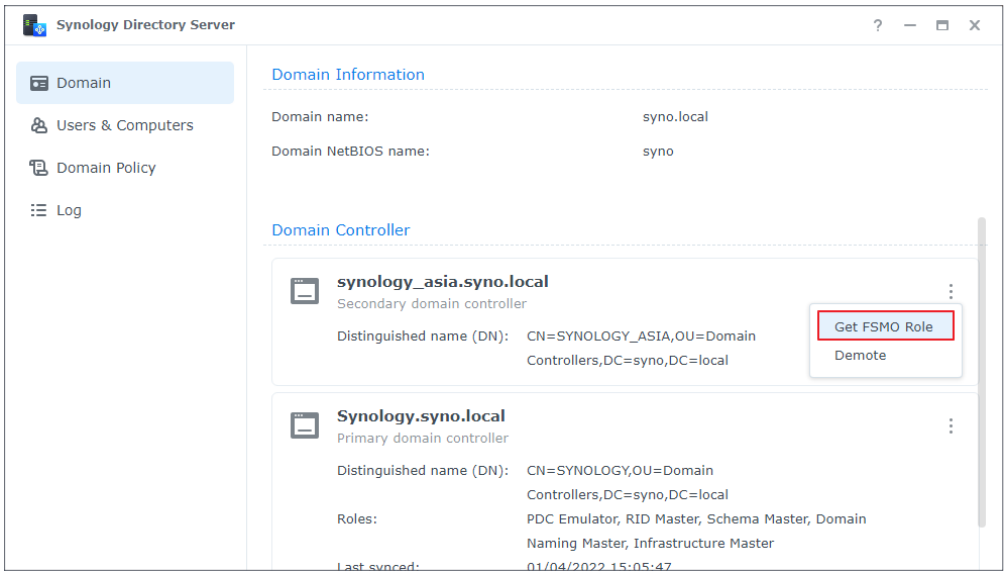
下列表格介紹 DC 可執行的操作。

DC 類型 / 操作	PDC	SDC	
		RWDC	RODC
取得 FSMO 角色	可以	可以	不可以
新增密碼複寫原則	可以	可以	僅可檢視
預覽密碼複寫原則	可以	可以	可以
預先填入密碼	可以	可以	僅可檢視
變更 IP 位址	可以	可以	僅可檢視
將 DC 降階	可以 (可降階所有 DC)	可以 (不可降階 PDC)	僅能降階本身這台 RODC

取得 FSMO 角色

PDC 預設扮演下列 FSMO 角色：PDC 模擬器主機、RID 主機、基礎結構主機、網域命名主機、架構主機。然而，作為 SDC 的 RWDC 可從 PDC 取得 FSMO 角色，PDC 亦可從 SDC 取回 FSMO 角色。

1. 前往 RWDC 的**網域** > **網域控制站**。
2. 在欲取得 FSMO 角色的 RWDC 按一下 ⋮ 並選擇**取得 FSMO 角色**。



3. 從**角色取得方式**的下拉式選單選擇其中一種方式。
   - **傳輸角色**：將其他 RWDC 的角色轉移至目前的 RWDC。
   - **拿取角色**：強制拿取其他 RWDC 的角色。拿取角色可能會造成 RWDC 間的同步問題，因此，除非原本擁有 FSMO 角色的 RWDC 非預期地、永久離線，否則不建議使用此方式。
4. 從**角色**下拉式選單選擇欲取得的角色。
5. 輸入網域的管理員帳號及密碼。
6. 按一下**提交**以從另一個 RWDC 取得角色。

新增密碼複寫原則

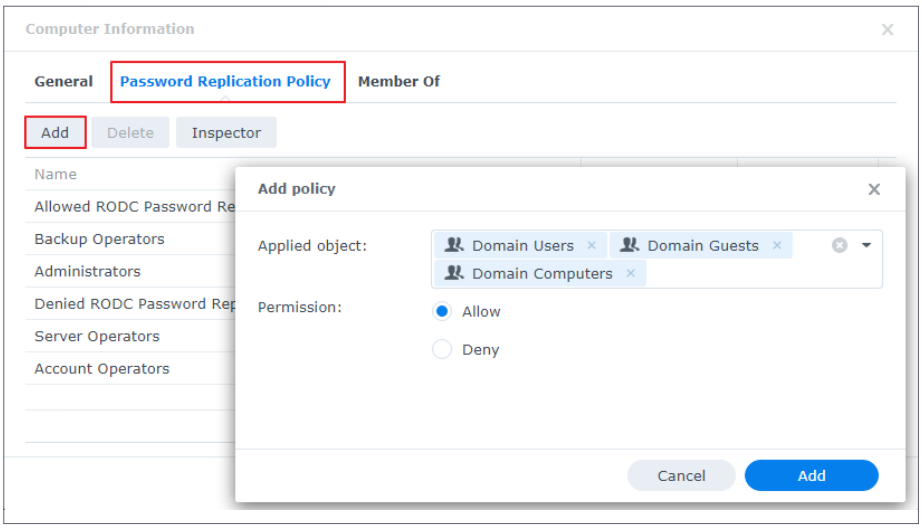
您可以使用密碼複寫原則來決定 RODC 可複寫哪些使用者帳號的密碼。只要新增密碼複寫原則且該使用者帳號被加入允許密碼複寫的清單中，RODC 便會複寫該使用者帳號的密碼。

被允許複寫使用者帳號的 RODC 可針對使用者的登入進行驗證，無需將驗證請求傳送至 RWDC (即：PDC 或 SDC)。不被允許複寫使用者帳號的 RODC 則會將驗證請求傳送至 RWDC。

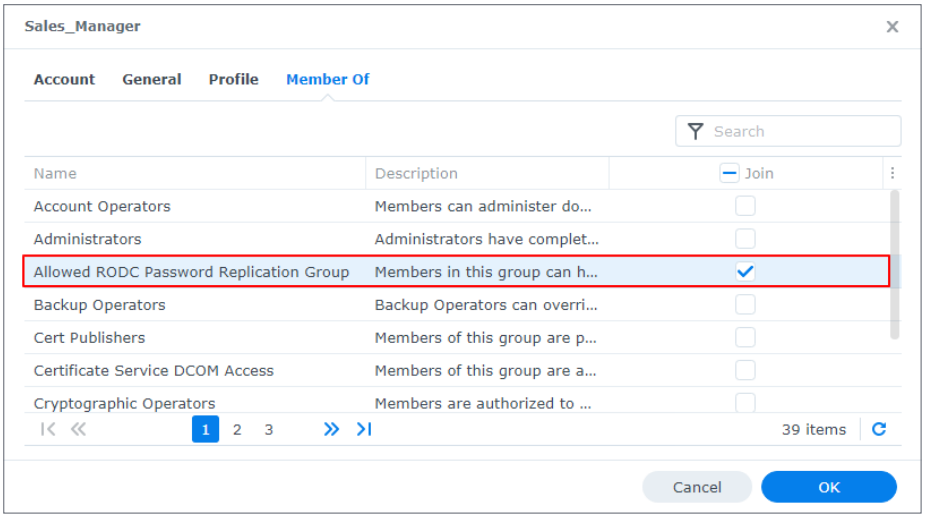
僅 RWDC 可以新增密碼複寫原則；RODC 僅可以檢視已新增的密碼複寫原則。

1. 前往 RWDC 的**使用者 & 電腦**頁面。
2. 按一下 OU 左側的 ▼ 以展開網域物件，並執行下列任一操作：

- 方式一：
  a. 按一下 **Domain Controllers**，在 RODC 欄位按兩下並選擇**密碼複寫原則**。
  b. 按一下**新增**並從**套用至物件**的下拉式選單選擇物件。
  c. 選擇下列其一選項並按一下**新增**：
    - **允許** RODC 複寫所選使用者帳號的密碼。
    - **拒絕** RODC 複寫所選使用者帳號的密碼。
  d. 按一下**新增**。



- 方式二：
  a. 按一下 **Users**，以右鍵按一下物件，並選擇**屬性**。
  b. 按一下**加入群組**並將物件加入 **Allowed RODC Password Replication Group** 或已套用密碼複寫原則的群組。
  c. 按一下**確定**。



3. 使用**檢視器**功能來確認物件已加入您要的允許或拒絕清單。

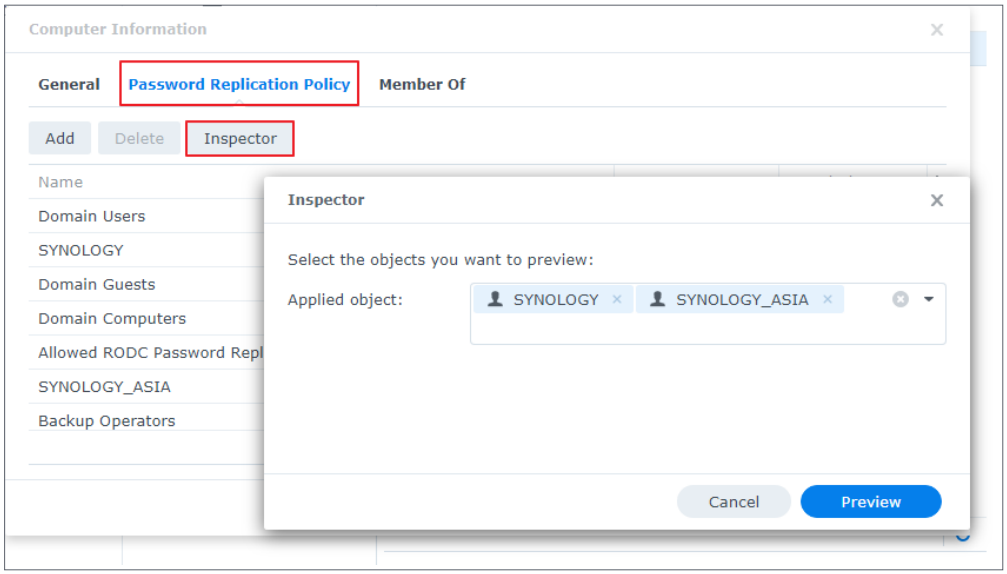
注意：

- 若使用者帳號被同時加入允許與拒絕清單，其密碼便不會被複寫 (即：拒絕清單的優先順序高於允許清單)。

預覽密碼複寫原則

您可以使用**檢視器**功能來預覽哪些使用者帳號被加入密碼複寫原則的允許或拒絕清單。

1. 前往 DC 的**使用者 & 電腦**頁面。
2. 按一下 OU 左側的 ▼ 以展開網域物件，選擇 Domain Controllers。
3. 在 RODC 欄位按兩下並選擇**密碼複寫原則**。
4. 按一下**檢視器**並從**套用至物件**的下拉式選單選擇欲預覽的使用者帳號。
5. 按一下**預覽**。

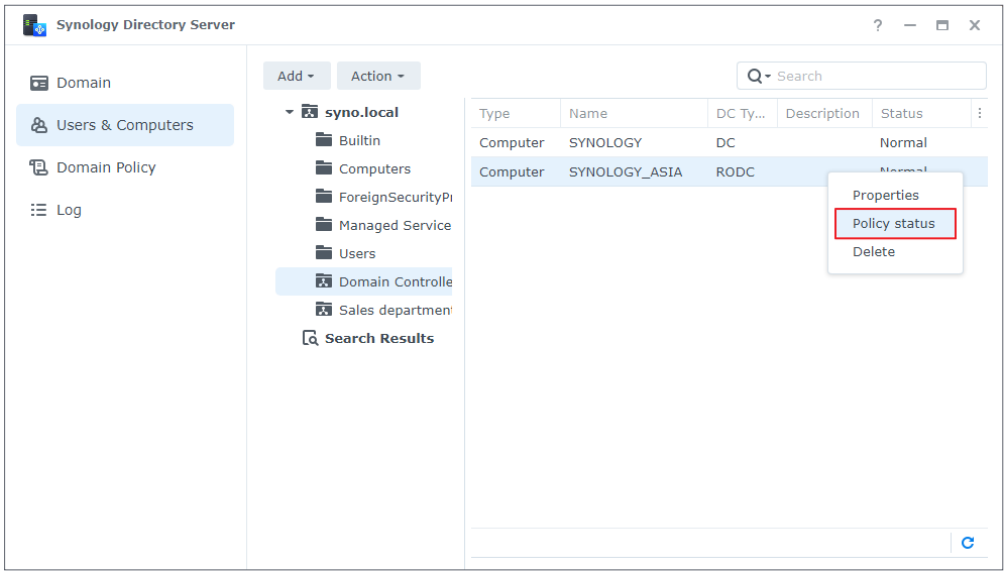


6. 依據您的需求新增、移除、匯出使用者帳號。按住 Ctrl 或 Shift 來選取多個使用者帳號。
   - 按一下**新增**，從**套用至物件**的下拉式選單選擇使用者帳號，按一下**預覽**。
   - 選擇使用者帳號並按一下**移除**。
   - 按一下**匯出**以將使用者帳號匯出成 Excel 檔案。

預先填入密碼

若您已將使用者帳號加入允許套用密碼複寫原則的清單，便可以為 RODC 設定預先填入密碼功能，這可讓 RODC 在使用者首次登入前，就先複寫使用者帳號的密碼。

1. 前往 RWDC 的**使用者 & 電腦**頁面。
2. 按一下 OU 左側的 ▼ 以展開網域物件，選擇 Domain Controllers。
3. 以右鍵按一下 RODC 欄位並選擇**原則狀態**。



4. 前往**檢視帳號類型**並選擇任一選項：

   - **密碼已儲存於此 RODC 的帳號**：此清單顯示密碼已複寫且儲存於 RODC 的使用者帳號。使用者登入由 RODC 驗證。
   - **已受此 RODC 驗證的帳號**：此清單顯示已從 RODC 傳輸至 RWDC 以供驗證的使用者帳號。使用者登入由 RWDC 驗證。RODC 必須加入 Windows AD，此清單才會顯示。

5. 按一下**預先填入密碼**。

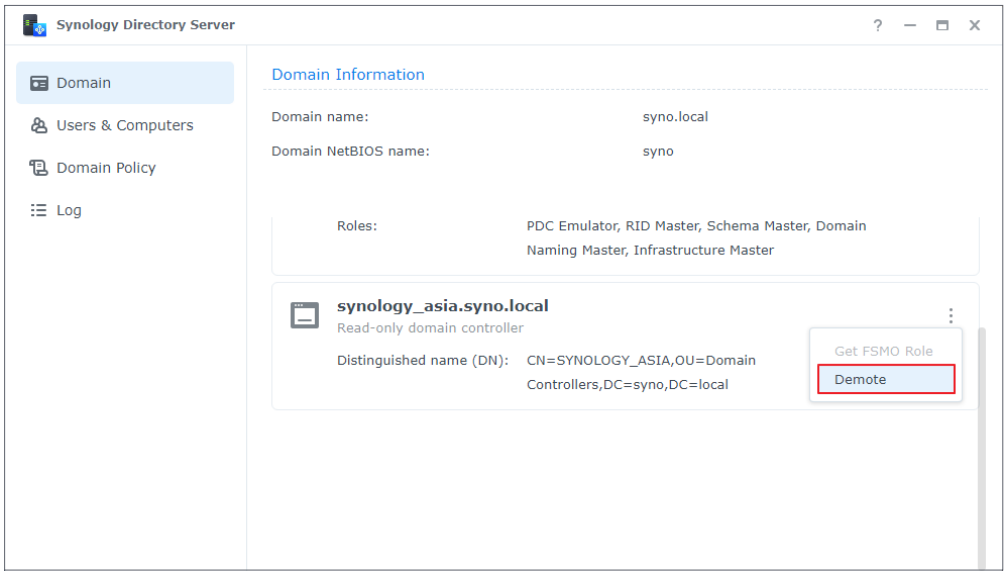
6. 輸入網域管理員的帳號密碼，選擇欲套用的使用者帳號，並按一下**預先填入密碼**。

將 DC 降階

您可透過降階，從目前的網域物件層級中移除裝置的 DC 身分，但仍將該裝置留在網域中。

1. 前往 DC 的**網域** > **網域控制站**。

2. 按一下欲降階 DC 的 ⋮ 並選擇**降階**。



3. 確認此操作並按一下**降階**。DC 一旦被降階，將**無法復原**。
4. 輸入管理員帳號的密碼並按一下**送出**。

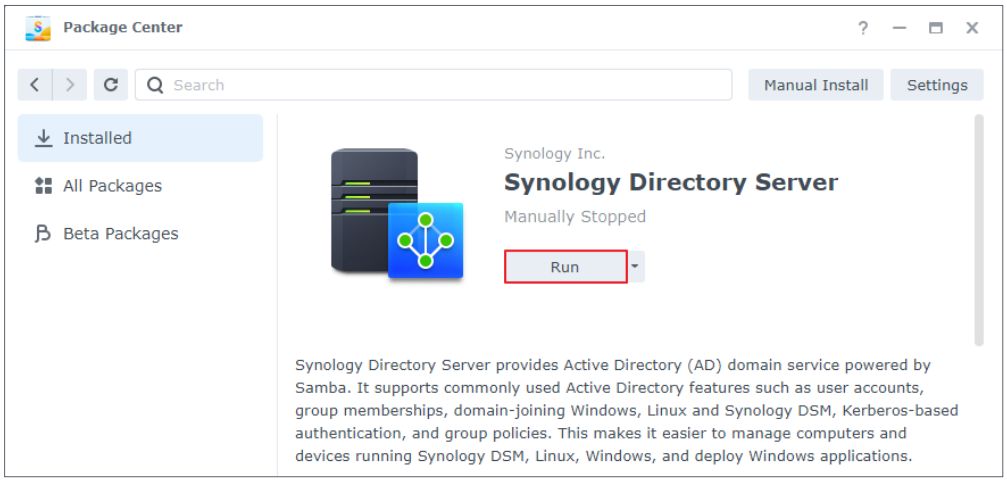
注意：

- 擁有 FSMO 角色的 DC 無法降階。
- 若將網域裡最後一個 DC 降階，整個網域服務將被刪除。
- 若您從 PDC 上降階 SDC，則必須登入該 SDC 以確認要刪除相關資料。

變更 DC 的 IP 位址

Synology Directory Server 在正常情況下會具備一組靜態 IP 位址。但在某些情況下，您可能需要對運行 Synology Directory Server 的 Synology NAS 進行 IP 位址變更。

1. **使用 Hyper Backup 套件來備份 Synology Directory Server**。
2. 變更 Synology NAS 的 IP 位址。
3. **確認並更新 DNS Server 內的資源紀錄**。
4. 重新啟動 **Synology Directory Server** 以更新網路設定：
   1. 前往**套件中心** > **已安裝** > **Synology Directory Server**。
   2. 按一下 ▼ 並選擇**停用**。
   3. 按一下**啟動**。



管理 DNS 資源紀錄

網域名稱系統 (Domain Name System，DNS) 為一種命名系統，有助不同電腦於網際網路或其他網路間交流資料。DNS 可將容易記憶的網域名稱 (例如：「pc1.syno.local」) 轉譯成對應的 IP 位址 (例如：「192.168.1.5」)，是維持 Synology Directory Server 網域服務正常運作的必要功能。

A / AAAA 資源紀錄

A 與 AAAA 皆為用來解析網域名稱 / IP 位址的 DNS 資源紀錄。A 紀錄將網域名稱轉譯成 32 位元的 IPv4 位址，而 AAAA 紀錄則是將網域名稱解析成 128 位元的 IPv6 位址。

DNS 自動註冊

當用戶端成功加入 Synology Directory Server 所建立的網域後，伺服器將自動註冊並更新一筆 A 資源紀錄至 DSM 的 DNS 服務 (若啟用 IPv6，則包括 AAAA 資源紀錄)，記錄該用戶端的主機名稱與 IP 位址的對應關係。

限制：

- DNS 自動註冊無法被停用。
- 網域用戶端之命名規則：只能使用英文字母 (a-z、A-Z)、數字 (0-9) 以及破折號 (-)。
- 針對 Windows 7、10：若主機名稱或 IP 位址曾被改過，則需要重新登入或重新啟動。
- 針對 DSM、SRM：若主機名稱或 IP 位址曾被改過，則不必重新登入或重新啟動，資源紀錄亦不會更新。

調整 A / AAAA 資源紀錄

為了確保 Synology Directory Server 能夠正常運作，依照預設，所有 A / AAAA 資源紀錄指向的 IP 位址皆為建立網域的 Synology NAS。

然而，以下情形可能會導致 A / AAAA 資源紀錄無法正確指向該台 Synology NAS：

- Synology Directory Server 建立網域後，Synology NAS 的 IP 位址又再次變更。
- **從 Hyper Backup 套件的備份任務還原 Synology Directory Server**。

若發生上述情況，請調整 A / AAAA 資源紀錄。

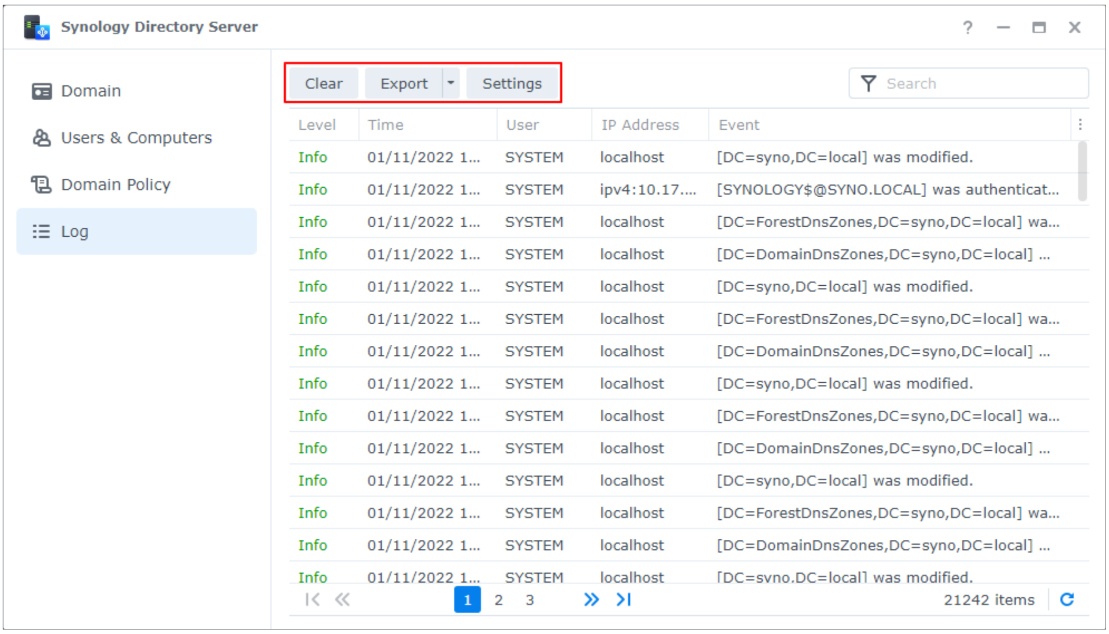
1. 前往 **DNS Server** > **轄區**。
2. 選取相關的 DNS 轄區 (例如：**網域名稱 @Active Directory** 或 **_msdcs. 網域名稱 @Active Directory**)，然後按一下**編輯** > **資源紀錄**。
3. 檢查 A 及 AAAA 類型資源紀錄中設定的 IP 位址。確認所有紀錄皆指向您的 Synology NAS。

注意：

- 若要批量編輯，按住 **Ctrl** 或 **Shift** 來選取多個相同類型但名稱相異的資源紀錄。

檢視並管理事件日誌

在**日誌**頁面中，所有登入事件以及對網域物件所做的更動都會被記錄成日誌。網域管理員可以參考日誌紀錄來監控 Synology Directory Server 的狀態，進而解決可能發生的問題。



啟用稽核日誌

- 按一下**設定**並勾選**啟用稽核日誌 (可能會影響資料庫效能)**。請注意，記錄日誌可能會影響 Synology Directory Server 的資料庫效能。

管理日誌

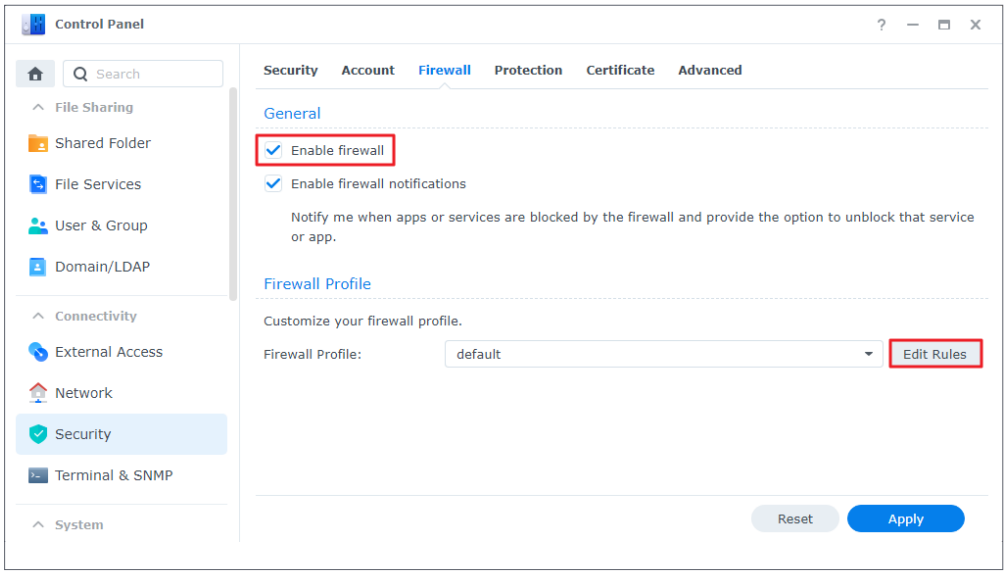
- 在右上方搜尋列 搜尋符合指定條件的日誌。
- 按一下右下角的重新整理圖示 來取得最新的日誌清單。
- 按一下**清除**來刪除所有日誌記錄。刪除的日誌**無法復原**。
- 按一下**匯出**並選擇 **HTML** 或 **CSV** 以將日誌匯出成特定格式。

> **注意：**
> - 當日誌數量到達上限 (200,000 則日誌) 時，最舊的前 5,000 則日誌紀錄將會自動被刪除以節省空間。

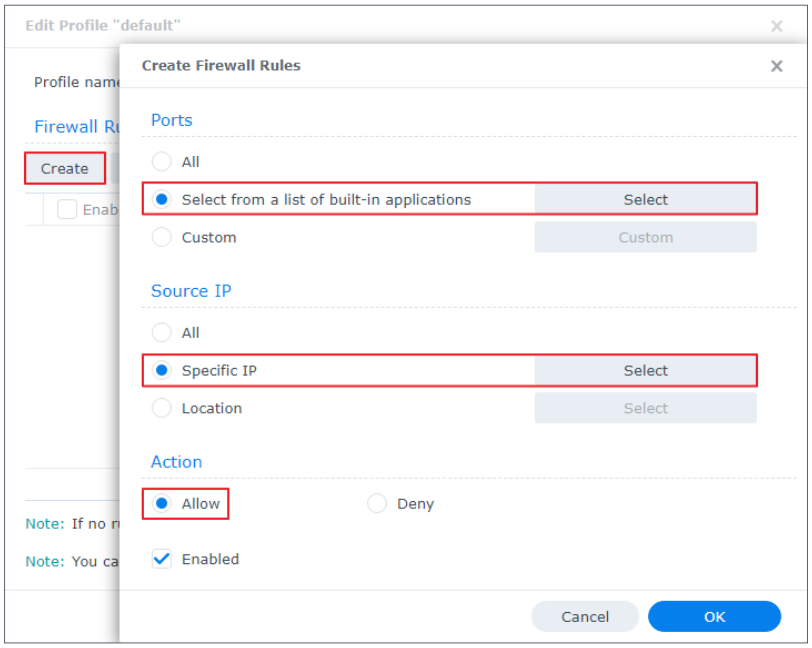
透過防火牆規則提升 Synology Directory 服務的安全性

除了管理效率，安全性亦是 Synology Directory 管理員必須審慎考量的面向。新增防火牆規則可保護您的目錄服務免受未經授權的登入，並允許您控制服務的存取。

1. 前往 RWDC 的**控制台** > **安全性** > **防火牆**。
2. 勾選**啟用防火牆**核取方塊。
3. 在**防火牆設定檔**區塊內，從下拉式選單選擇一個防火牆設定檔，並按一下**編輯規則**。



4. 按一下**新增**。
5. 在**連接埠**區塊內，選擇**從內建服務的清單選取連接埠**，接著按一下**選擇**。
6. 選取 **DNS Server**、**Synology Directory Server**、**Windows 檔案伺服器**。按一下**確定**。
7. 在**來源 IP** 區塊內，選擇**特定 IP**，接著按一下**選擇**。
8. 輸入 IP 位址或 IP 範圍來指定 Synology Directory Server 所在的區域網路。確認資訊無誤後，按一下**確定**。
9. 在**操作**區塊內，選擇**允許**來自指定連接埠及 IP 位址的存取。
10. 按一下**確定**來儲存設定。



注意：

- 若要了解更多 DSM 防火牆的設定，請參閱防火牆的**說明文章**。

第 4 章：管理網域物件

在 Synology Directory Server 網域內，可用的資源皆以物件的形式儲存，包含 OU、群組、使用者、裝置 (例如：電腦、印表機、Synology NAS)。只有 RWDC 可管理網域物件；RODC 僅可檢視網域物件。

檢視網域物件

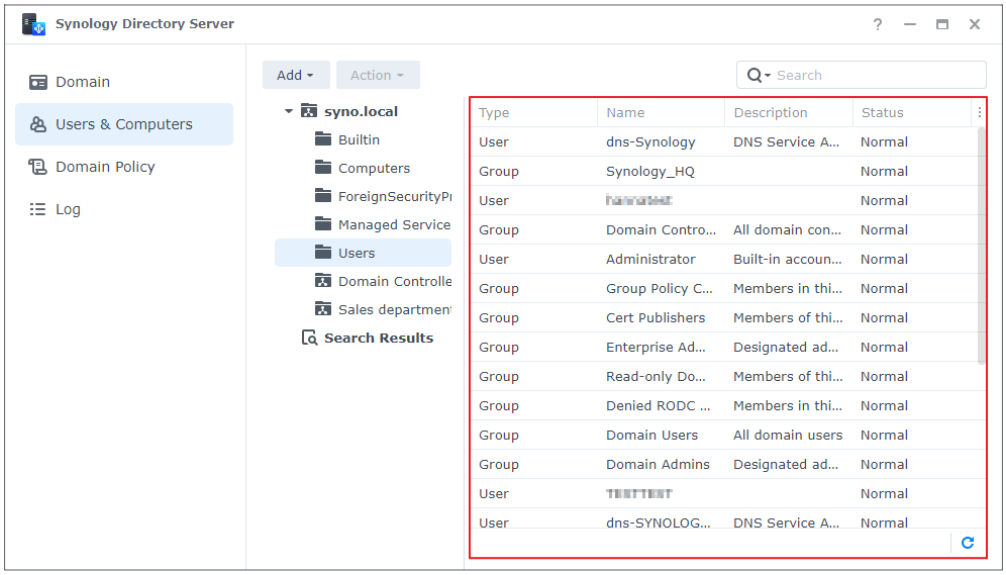
在**使用者 & 電腦**頁面中，您可以在左側面板檢視網域完整的樹狀結構，物件資訊則顯示在右側的面板內：

- **類型**：物件的類型將顯示於此欄位，包含 OU、群組、使用者、電腦。
- **名稱**：物件名稱 (但不包含 OU) 會以下方的格式呈現。

  ```
  NetBIOS 網域名稱 \ 物件名稱
  ```

- **描述**：關於該網域物件的敘述。
- **DN**：辨別名稱 (Distinguished Name，DN) 為網域資料庫內的物件路徑。舉例來說，若使用者的 DN 是「CN=bach,OU=sales,DC=syno,DC=local」，您可依下方介紹分析其組成：
  - **CN**=bach：使用者名稱為「bach」。
  - **OU**=sales：使用者隸屬的 OU 為「sales」。
  - **DC**=syno,**DC**=local：使用者所在的網域為「syno.local」。
- **狀態**：網域物件狀態依停用與否顯示為**正常**或**停用**。

按一下 ⋮ 以選擇並檢視更多物件資訊。

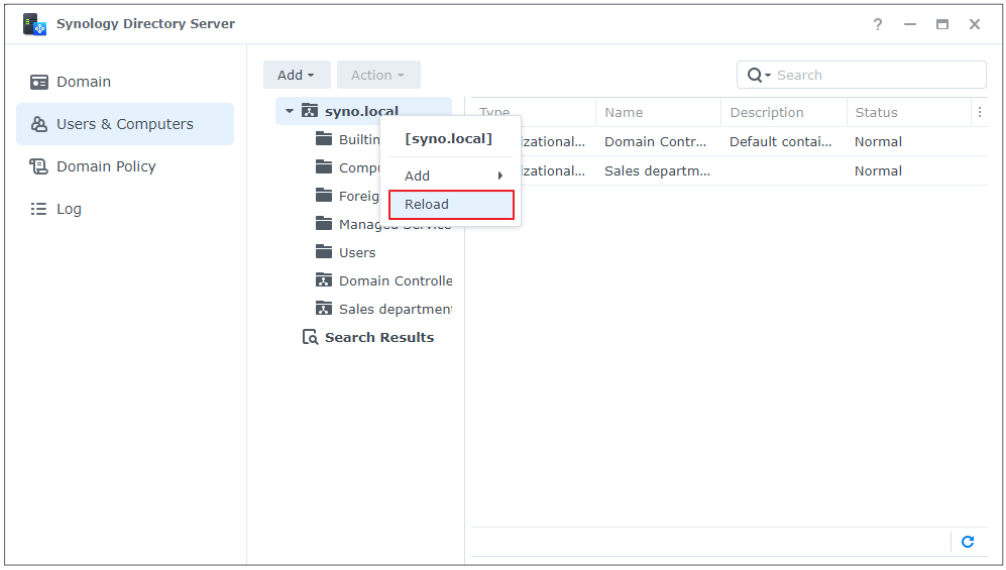


管理 OU

OU 是一種網域內的容器物件，您可新增所有類型的網域物件至 OU，包含使用者、群組、電腦、甚至是其他 OU。OU 可將網域物件進行階層式管理，這對於部署大量使用者、電腦、群組的網域管理很有幫助。設計縝密的 OU 架構可讓您輕鬆連結群組規則、委派管理任務給特定的網域物件。

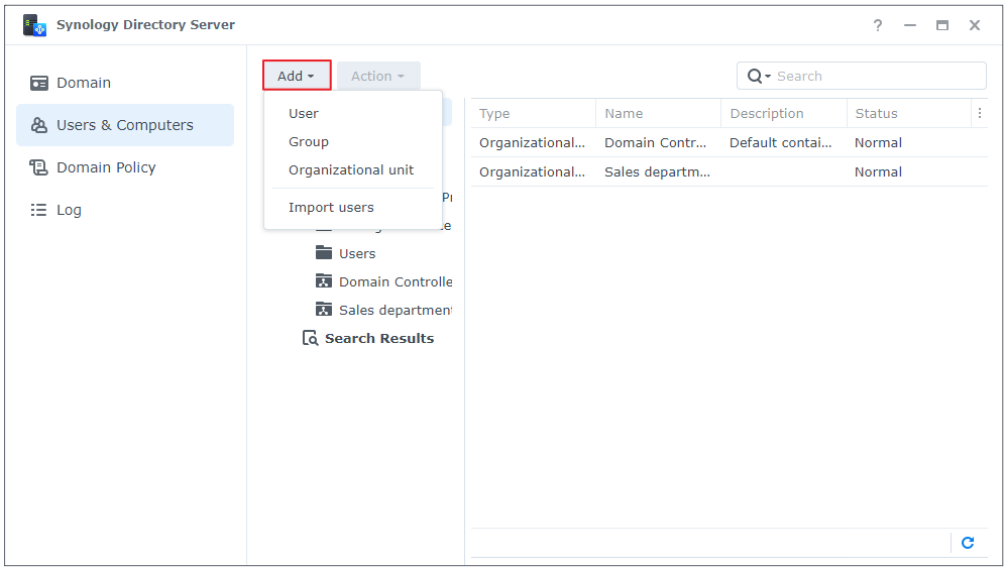
新增 OU

1. 前往 RWDC 的**使用者 & 電腦**頁面，從樹狀清單中選擇網域或一個 OU，並按一下**新增** > **組織單位 (OU)**。
2. 在欄位中為新的 OU 命名，並按一下**確定**。
3. 以右鍵按一下新增 OU 的母容器，並按一下**重新載入**。新增的 OU 將顯示於樹狀清單中。

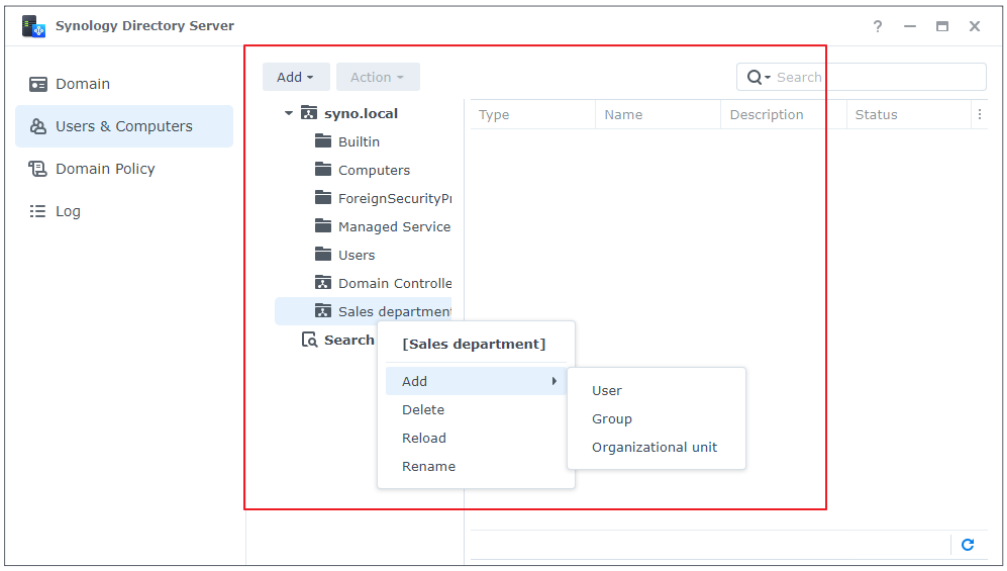


新增物件至 OU

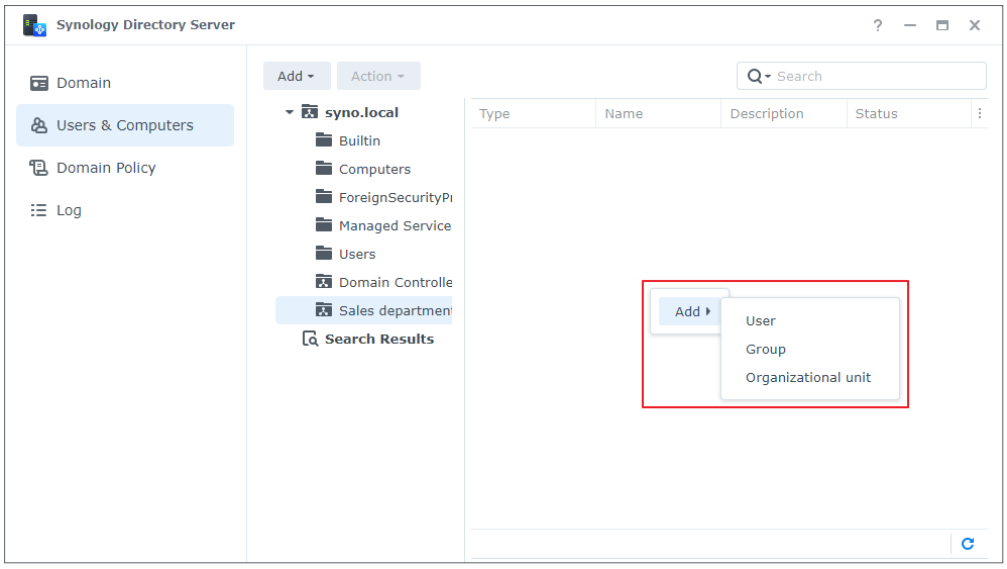
1. 前往 RWDC 的**使用者 & 電腦**頁面，從樹狀清單中選擇一個 OU，選擇下列其中一種方法來啟動建立精靈：
   - **方法一**：按一下**新增**並從下拉式選單中選擇一種網域物件。



- **方法二**：以右鍵按一下樹狀清單中特定的 OU，選擇**新增**，再選擇物件類型。



- **方法三**：以右鍵按一下特定 OU 的空白區域，並選擇您需要的物件類型來新增。



2. 依照精靈的指示來新增物件。請參考**新增 OU**、**新增群組**、**新增使用者**等段落，以了解詳細操作步驟。

注意：

- 您可藉由拖拉的方式，將一或多個物件加到樹狀清單中的 OU。
- 預設的目錄檢視模式僅顯示不屬於任何 OU 的物件。若要檢視所有使用者、群組、電腦、OU：
  1. 從樹狀清單中選取根目錄 (以您的網域命名) 並按一下右上角的放大鏡圖示。
  2. 在搜尋列中，請勾選**所有子項目**並按一下**確認**。

刪除 OU

1. 在 RWDC 以右鍵按一下欲從樹狀清單中刪除的 OU，並按一下**刪除**。
2. 再按一下**刪除**來確認此操作。刪除的 OU **無法復原**。

管理群組

您可將網域使用者放入群組，再為該群組套用針對特定服務的**存取控制清單** (Access Control List，ACL)，以讓網域使用者存取網域內的裝置、應用程式、其他服務。

預設群組

建立網域後，Synology Directory Server 會預設建立以下群組，協助您管理網域及設定存取權限。

群組名稱	描述
Allow RODC Password Replication Group	此群組成員的密碼可被複寫至網域內所有的 RODC。
Cert Publishers	此群組的成員具備發行憑證的權限。
Denied RODC Password Replication Group	此群組成員的密碼不可被複寫至網域內所有的 RODC。
DnsAdmins	此群組的成員可存取網域內的網域名稱系統 (DNS)。
DnsUpdateProxy	此群組的成員可代替部分用戶端 (例如：DHCP 伺服器) 執行 DNS 動態更新。
Domain Admins	此群組的成員具備控制網域內所有物件的管理員權限。
Domain Computers	所有工作站及伺服器皆預設放入此群組。
Domain Controllers	所有 DC 皆預設放入此群組。
Domain Guests	所有網域訪客帳號皆預設放入此群組。
Domain Users	所有網域使用者帳號皆預設放入此群組。
Enterprise Admins	此群組的成員具備控制整個企業網域結構內所有物件的管理員權限。
Enterprise Read-Only Domain Controllers	所有在企業網域結構內的 RODC 皆預設放入此群組。
Group Policy Creator Owners	此群組的成員可變更網域的群組規則。
RAS and IAS Servers	此群組的成員可使用遠端存取服務。
Read-Only Domain Controllers	所有 RODC 皆預設放入此群組。
Schema Admins	此群組的成員可修改網域架構 (Domain Schema)。

注意：

- Synology Directory Server 的功能層級和 Windows Server 2008 R2 一致。請參閱**此篇文章**以取得預設網域群組的更多資訊。

新增群組

1. 前往 RWDC 的**使用者 & 電腦**頁面並按一下**新增** > **群組**。
2. 輸入群組資訊並按**下一步**：
   - **群組領域**
     - **網域本機**：網域本機群組的用途為指派權限給網域內的物件資源。其可容納相同網域內的其他網域本機群組，以及來自任何網域或樹系的使用者帳號、全域群組、萬用群組。
     - **全域**：全域群組的用途為使用者帳號的管理。其可容納相同網域內的使用者帳號及其他全域群組。在實作上，建議將全域群組放入擁有特定權限的網域本機群組，而非直接指派權限給全域群組。
     - **萬用**：萬用群組的主要用途為容納各網域的全域群組。此類群組可收納其所在樹系內任何網域的使用者帳號、全域群組、以及其他萬用群組。在實作上，建議將萬用群組放入擁有特定權限的網域本機群組，而非直接指派權限給萬用群組。
   - **群組類型**
     - **安全性**：安全性群組的用途為建立群組權限，以在網域內執行系統任務。
     - **通訊**：通訊群組的用途為傳送電子郵件給一群使用者，相當於郵件別名。
3. 確認群組資訊後，按一下**完成**。

編輯群組屬性

1. 前往 RWDC 的**使用者 & 電腦**頁面，選擇欲編輯的群組，並執行下列任一操作：
   - 按一下**動作** > **屬性**。
   - 以右鍵按一下群組並選擇**屬性**。
   - 在群組按兩下。
2. 在**一般**與**群組成員**頁籤編輯群組屬性。
   - **一般**：群組名稱、描述、電子郵件、群組領域、群組類型。
   - **群組成員**：將成員加入或移除群組。
3. 按一下**確定**以儲存設定。

刪除群組

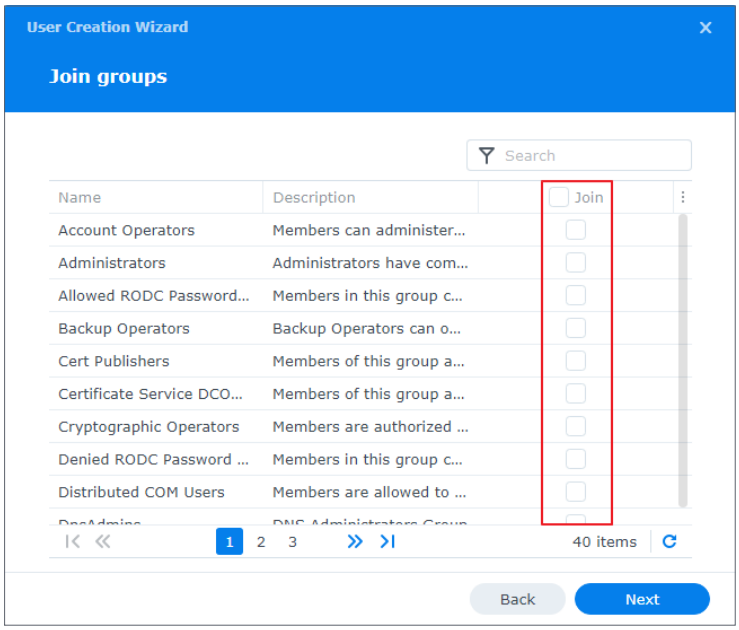
1. 前往 RWDC 的**使用者 & 電腦**頁面，選擇欲刪除的群組。按住 **Ctrl** 或 **Shift** 鍵來選取多個群組。
2. 執行下列任一操作：
   - 按一下**動作** > **刪除**。
   - 以右鍵按一下群組並選擇**刪除**。
3. 按一下**刪除**來確認操作。刪除的群組無法復原。

新增成員至群組

下列三種方式可將使用者加入群組。

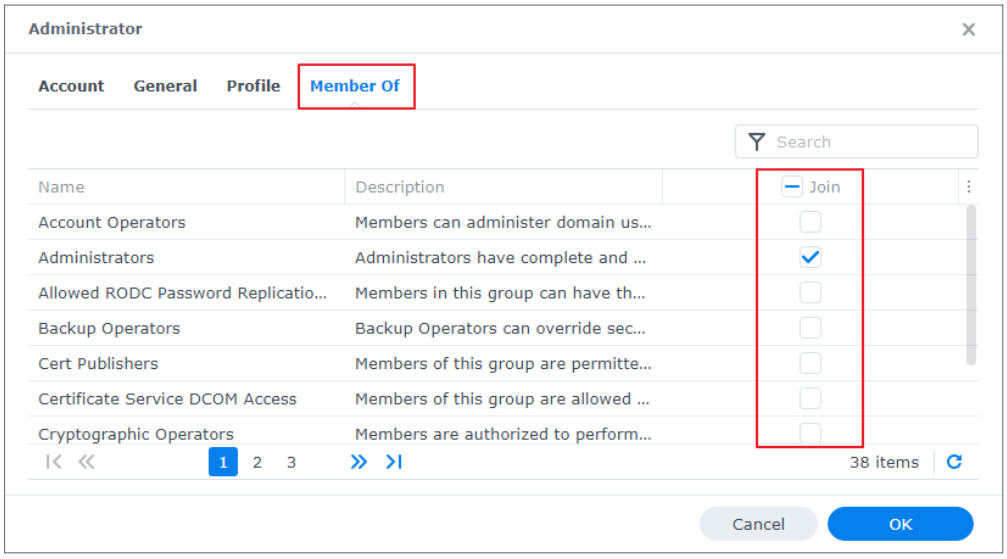
方式一：於新增使用者時加入群組

1. 依照**新增使用者**的步驟操作。
2. 在**新增使用者精靈**的第二步驟，勾選欲讓使用者加入的群組，再按**下一步**。依照精靈指示來完成新增使用者的流程。



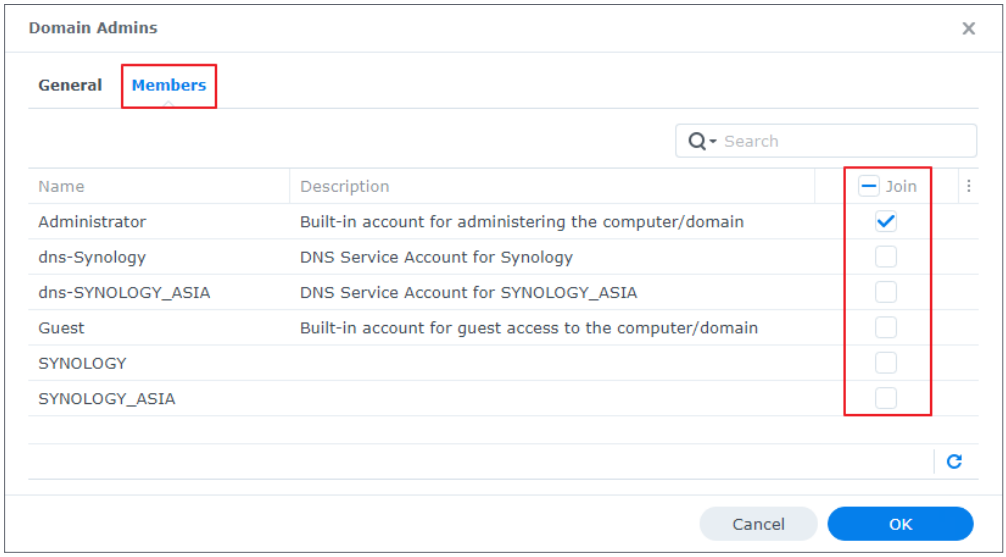
方式二：於編輯使用者檔案時加入群組

1. 前往 RWDC 的**使用者 & 電腦**頁面，選擇欲編輯的使用者，並執行下列任一操作：
   - 按一下**動作** > **屬性**。
   - 以右鍵按一下使用者並選擇**屬性**。
2. 前往**加入群組**頁籤，勾選欲讓使用者加入的群組，再按一下**確定**。



方式三：於編輯群組屬性時加入群組

1. 前往 RWDC 的**使用者 & 電腦**頁面，選擇欲編輯的群組，並執行下列任一操作：
   - 按一下**動作** > **屬性**。
   - 以右鍵按一下群組並選擇**屬性**。
2. 前往**群組成員**頁籤，勾選欲讓使用者加入的群組，再按一下**確定**。



管理使用者

網域內的使用者為可依照相應的權限，存取網域資源的使用者帳號。

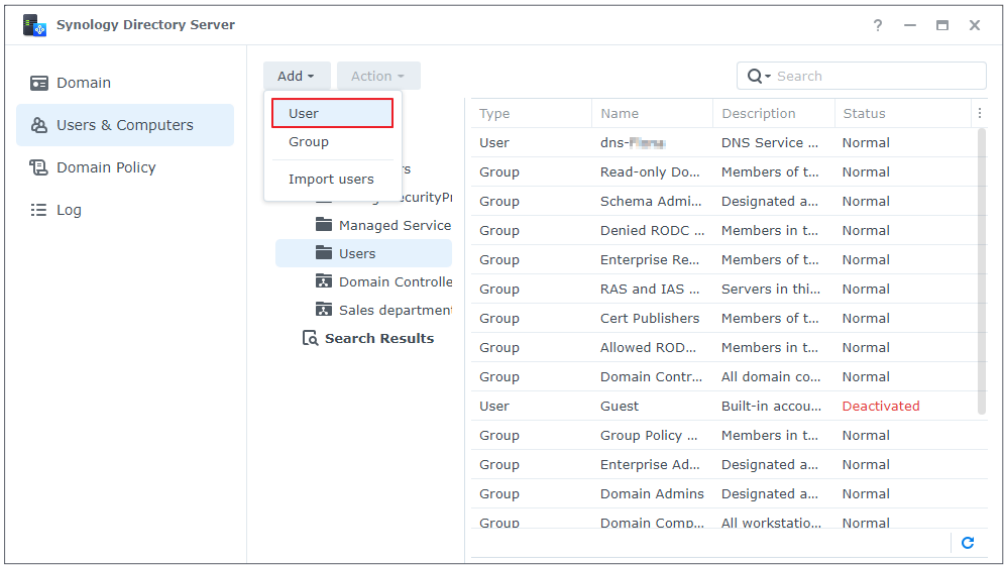
預設使用者

建立網域後，Synology Directory Server 會預設建立以下使用者帳號，協助您管理網域。

使用者名稱	描述
Administrator	擁有 Synology Directory Server 完整控制權的管理員帳號，用來管理網域及 DC。
dns-NAS 的主機名稱	處理 Synology NAS 內 DNS 服務的帳號。此帳號名稱以 DC 的主機名稱命名，例如：「dns-MyNAS」。
Guest	用於存取網域及網域內裝置的訪客帳號。
krbtgt	DC 內執行 Kerberos 金鑰發佈中心 (Key Distribution Center，KDC) 服務的帳號。

新增使用者

1. 前往 RWDC 的**使用者 & 電腦**頁面，從樹狀清單中按一下欲用來放置使用者的容器。該容器可以是以網域所命名的容器 (例如：「SYNO.LOCAL」)、**Users** 容器、OU。
2. 執行下列任一操作：
   - 按一下**新增** > **使用者帳號**。
   - 以右鍵按一下容器並選擇**新增** > **使用者帳號**。
   - 以右鍵按一下特定 OU 的空白區域，並選擇**新增** > **使用者帳號**。



3. 輸入使用者資訊並按**下一步**。為了加強安全性，**強制此帳號須於下次登入時變更密碼**預設為勾選。請留意，密碼強度要求視 **Synology Directory Server** > **網域規則**頁面中設定的密碼規則而定。
4. 選擇欲讓此使用者加入的群組並按**下一步**。
5. 確認設定後，按一下**完成**以新增網域使用者。

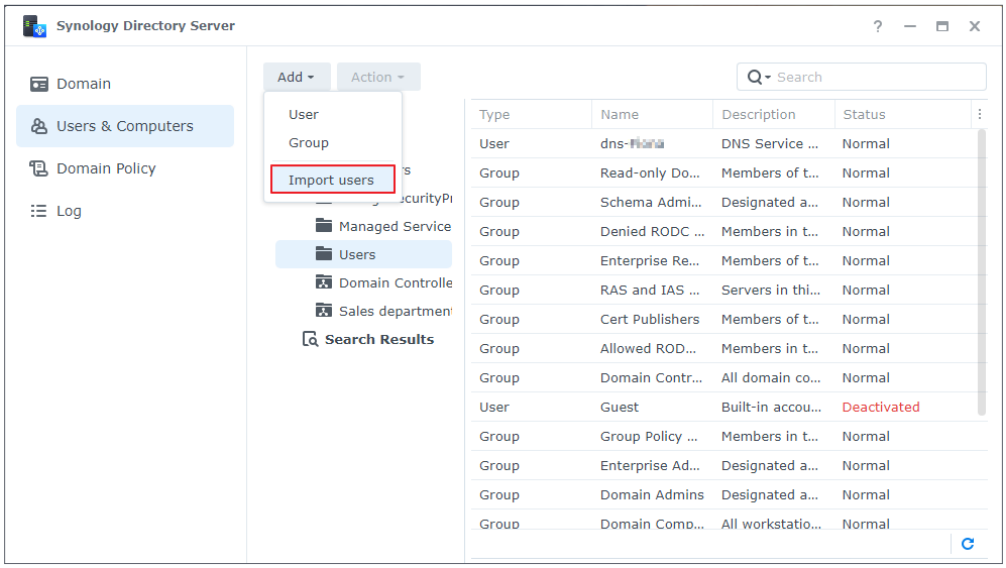
密碼強度要求：

密碼至少須遵守下列規則的其中三項：

- 大寫的拉丁字母 (包含 A - Z 及附加符號)、希臘字母、西里爾字母。
- 小寫的拉丁字母 (包含 a - z 及附加符號)、希臘字母、西里爾字母。
- 數字 (0 - 9)。
- 特殊符號，包含 #、$、! 等。
- 不分大小寫的 Unicode 字母，包含亞洲語言的字母。

匯入多位使用者

1. 前往 RWDC 的**使用者 & 電腦**頁面，從樹狀清單中按一下欲用來放置使用者的容器。該容器可以是以網域所命名的容器 (例如：「SYNO.LOCAL」)、**Users** 容器、OU。
2. 按一下**新增** > **匯入使用者**。



3. 根據您的需求勾選以下選項：

   - **覆寫重複的使用者帳號**：以清單中的使用者帳號來取代名稱重複的現有帳號。
   - **寄通知信給新使用者**：在新帳號建立完成後，寄送訊息通知給該使用者。若要使用此選項，須先前往**控制台** > **通知設定** > **電子郵件**並啟用電子郵件通知功能。
   - **在通知郵件中顯示使用者密碼**：在通知郵件訊息中顯示使用者帳號的密碼。必須先勾選**寄通知信給新使用者**，才可勾選此選項。
   - **匯入的使用者須於第一次登入時變更密碼**：強制匯入的使用者於初次登入時變更密碼。此設定將能為匯入的使用者帳號增加額外防護。

4. 按一下**瀏覽**並上傳 .txt 檔案。

5. 按一下**確定**。

檔案格式：

準備匯入的檔案時，各使用者帳號須輸入至不同的列。每個資訊都必須按照下列順序排列，並且以 Tab 鍵來區隔：

1. 使用者名稱	2. 密碼	3. 描述	4. 電子郵件
5. 名	6. 姓	7. 全名	
8. 設定檔路徑	9. 登入指令碼	10. 家目錄	

匯入的檔案必須符合下列的格式需求：

- 檔案格式必須為 UTF-8。
- 各欄位資訊的順序必須正確 (從左到右排列)。
- 匯入的密碼必須符合**密碼強度要求**。
- 每列資訊都必須包含九個分隔符號。若想要跳過某個資訊，您仍須輸入一個 Tab 鍵來區隔此空白值和下一個值。

編輯使用者屬性

1. 前往 RWDC 的**使用者 & 電腦**頁面並選擇欲編輯的使用者。按住 **Ctrl** 或 **Shift** 鍵來選取多個使用者進行編輯。
2. 執行下列任一操作：
   - 按一下**動作 > 屬性**。
   - 以右鍵按一下使用者並選擇**屬性**。
3. 前往**帳號**頁籤並編輯以下屬性：
   - **使用者登入名稱**：您可在此欄位為使用者重新命名。
   - **登入時段：**選取網格以**拒絕**或**允許**使用者的登入時段。若要選取一整天或每一天的同一個小時，直接點選當天或該小時即可。
   - **可用裝置**：選擇使用者可存取的電腦。
   - **變更密碼**：勾選核取方塊以變更使用者的密碼。
   - **鎖定此帳號**：在**網域規則 > 帳號鎖定規則**設定的帳號鎖定規則被觸發後，此選項便會啟用。您可以停用此選項來解鎖帳號。
   - **強制此帳號須於下次登入時變更密碼**：此帳號會在下次登入 Windows 或 Synology NAS 時被強制要求變更密碼。
   - **不允許使用者變更密碼**：此使用者將無法自行變更密碼。
   - **密碼永遠有效**：此使用者的密碼永遠不會到期。建議僅對管理員帳號啟用此選項。
   - **使用可還原加密方式來儲存密碼**：啟用此選項可能會降低網域安全性。除非網域用戶端服務的需求優先於密碼安全，否則不建議使用此選項。
   - **停用此帳號**：勾選核取方塊以停用使用者的帳號。
   - **須使用智慧卡以進行互動式登入**：使用者必須使用特定的智慧卡才可登入用戶端裝置。
   - **禁止委派此機密帳號**：這是機密帳號，無法委派。啟用此選項代表運行於用戶端裝置上的服務無法以其他使用者身分執行。
   - **此帳號使用 DES 加密**：在 Kerberos 驗證過程中，此帳號的密碼將會透過資料加密標準 (Data Encryption Standard，DES) 來加密。
   - **此帳號不須 Kerberos 預先認證**：若使用者的帳號不需要 Kerberos 預先認證，請勾選此核取方塊。
   - **帳號到期設定**：選擇**帳號永不到期**或指定**帳號到期日**。
4. 前往**一般**頁籤編輯一般資訊。
5. 前往**設定檔**頁籤編輯使用者設定檔，讓使用者在網域內的任何裝置上都能有一致的桌面體驗：
   - **設定檔路徑**：使用者設定檔 (例如：**Desktop**、**Document**、**Picture** 資料夾) 的儲存路徑。
   - **登入指令碼**：使用者登入 Windows 作業系統時，自動執行的程式腳本。您可以按一下**上傳檔案**按鈕，上傳 2 MB (含) 以下的 Windows .bat 檔案。
   - **家目錄**：
     - **本機路徑**：將特定的本地資料夾設為家目錄。

- **連接 ... 至**：將家目錄設定至 Synology NAS 上的特定遠端共用資料夾。若啟用此選項，Windows 作業系統會自動將此遠端共用資料夾**掛載為網路磁碟機**。

6. 前往**加入群組**以將使用者加入或移除群組。
7. 按一下**確定**來儲存設定。

> **注意：**
> - 即便使用者狀態為**停用**，使用者屬性仍可編輯。

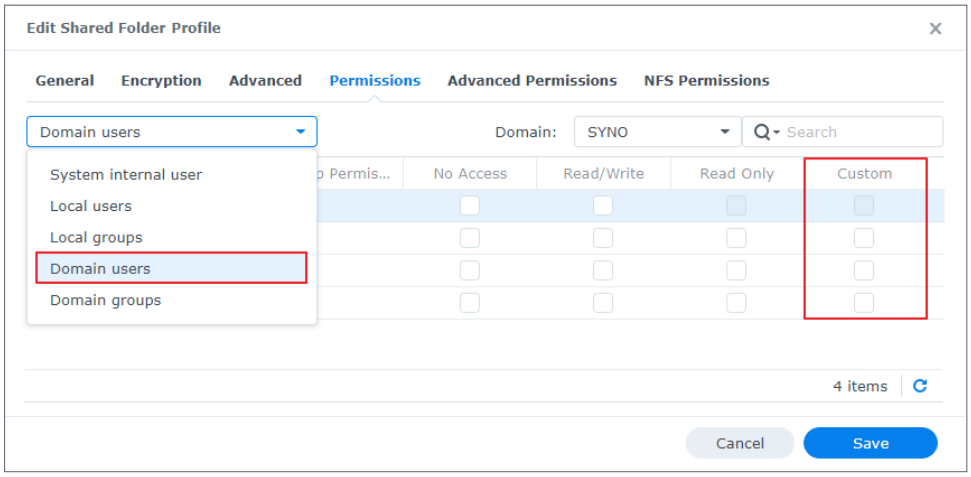
刪除使用者

1. 前往 RWDC 的**使用者 & 電腦**頁面並選擇欲刪除的使用者。按住 **Ctrl** 或 **Shift** 鍵來選取多個使用者進行刪除。
2. 執行下列任一操作：
   - 按一下**動作** > **刪除**。
   - 以右鍵按一下使用者並選擇**刪除**。
3. 按一下**刪除**來確認此操作。刪除的使用者**無法復原**。

指派漫遊設定檔給單一使用者

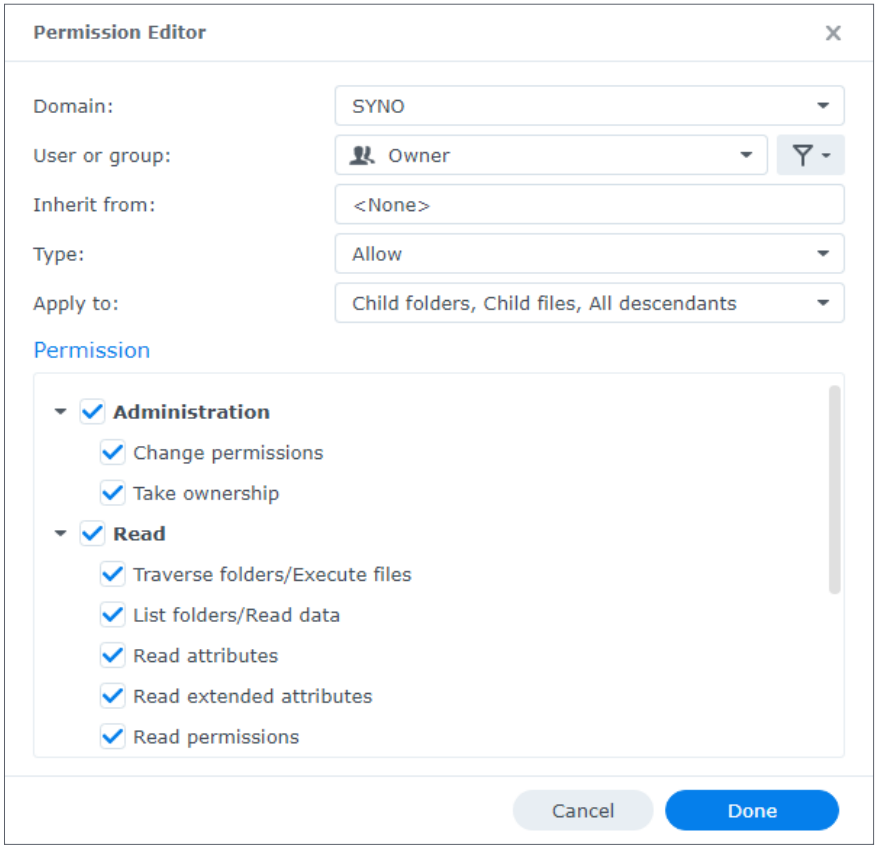
透過漫遊設定檔，可讓網域使用者登入不同電腦時，也能存取自己的檔案。在指派漫遊設定檔給使用者前，您必須先新增一個共用資料夾，並將至少一台電腦加入網域。

1. **將 Windows 電腦加入網域**。
2. 前往 RWDC 的**控制台** > **共用資料夾** > **新增** > **新增共用資料夾**以新增共用資料夾。給單一使用者的共用資料夾與給所有使用者的共用資料夾不可相同。
3. 以右鍵按一下已新增的共用資料夾，再按一下**編輯**。
4. 前往**權限**頁籤並從下拉式選單選擇**網域使用者**。
5. 按一下**自訂**核取方塊，即會顯示**權限編輯器**。



6. 從**使用者或群組**下拉式選單選擇目標，並依照下方表格進行**套用至**及**權限**的設定。下圖將以設定「Owner」群組的權限作為範例。

使用者或群組	套用至	權限
自訂的群組 (例如「Owner」)	勾選**子資料夾**、**子檔案**、**所有子項目**。	勾選**管理**、**讀取**、**寫入**以取得完整的控制權限。
Domain Admins	選擇**全部**。	勾選**管理**、**讀取**、**寫入**以取得完整的控制權限。
Domain Users	選擇**全部**。	• 勾選**讀取**以取得完整的讀取權限。 • 僅勾選**寫入**底下的**建立資料夾 / 附加資料**。



7. 按一下**完成**以儲存設定。

8. 前往 Synology Directory Server > **使用者 & 電腦** > **Users**。

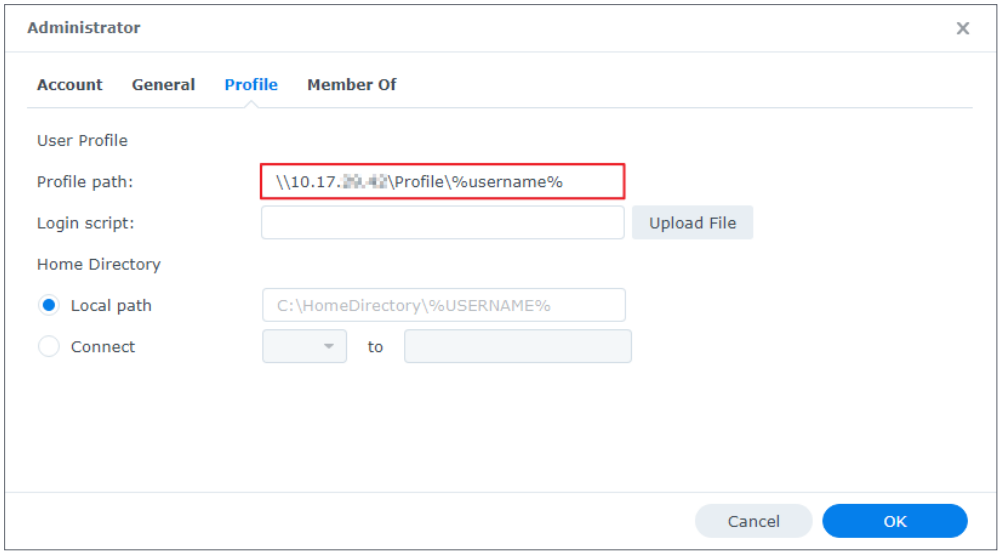
9. 執行下列任一操作：

   - 選擇使用者並按一下**動作** > **屬性**。
   - 以右鍵按一下使用者並選擇**屬性**。

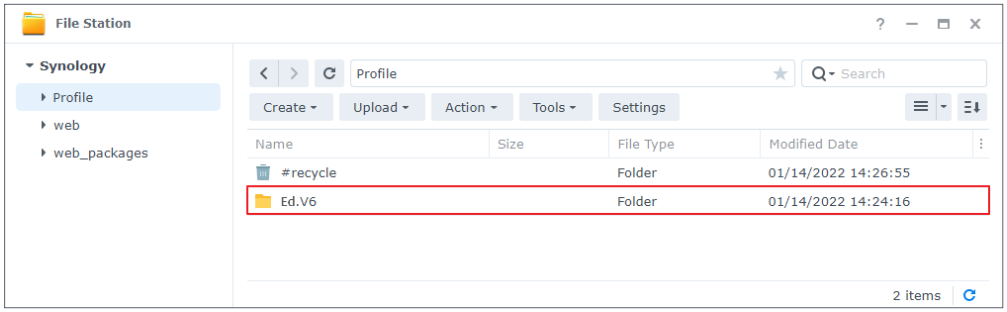
10. 前往**設定檔**頁籤，在**設定檔路徑**欄位內，依照下方的格式輸入使用者漫遊設定檔的共用資料夾路徑。請勿修改環境變數「%username%」，因為此變數可使設定檔資料夾自動指向選定的使用者。

```
\\NAS 的 IP 位址\共用資料夾名稱\%username%
```

11. 按一下**確定**以儲存設定。



12. 當使用者以該網域使用者帳號登入網域內的 Windows 電腦，Windows 電腦會自動在 Synology NAS 的遠端共用資料夾內替該使用者建立一個對應的漫遊設定檔 (資料夾名稱為「使用者名稱 .V6」)。若以此使用者的身分新增或修改資料，在登出電腦後，這些資料將會同步回傳至方才指派的路徑。



注意：

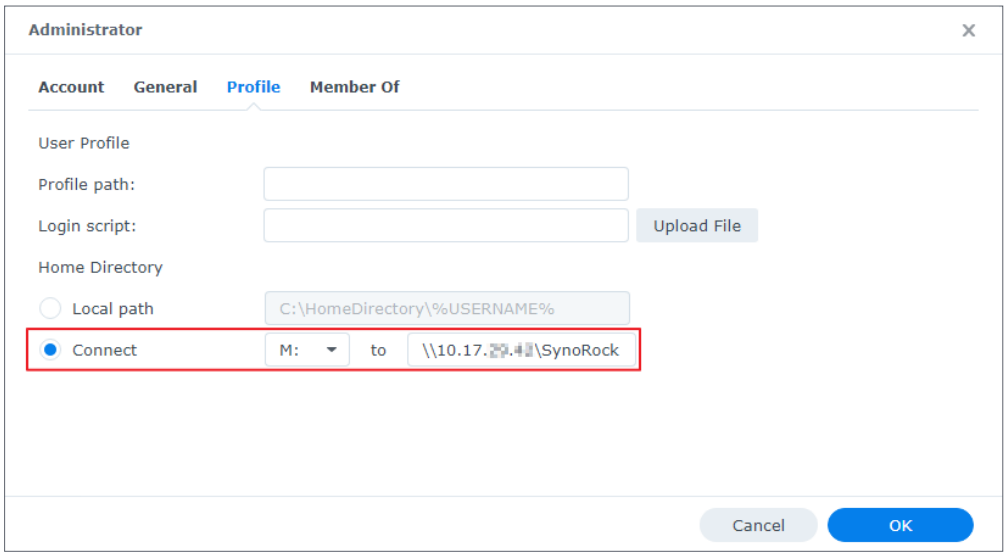
- 您也可以**使用 RSAT 指派漫遊檔給所有使用者**。
- **設定檔**頁籤內的**本機路徑**為指向 Windows 本地資料夾的位置。請確認此路徑已確實建立於您指派的電腦，否則設定將會無效。

為單一使用者掛載網路磁碟機

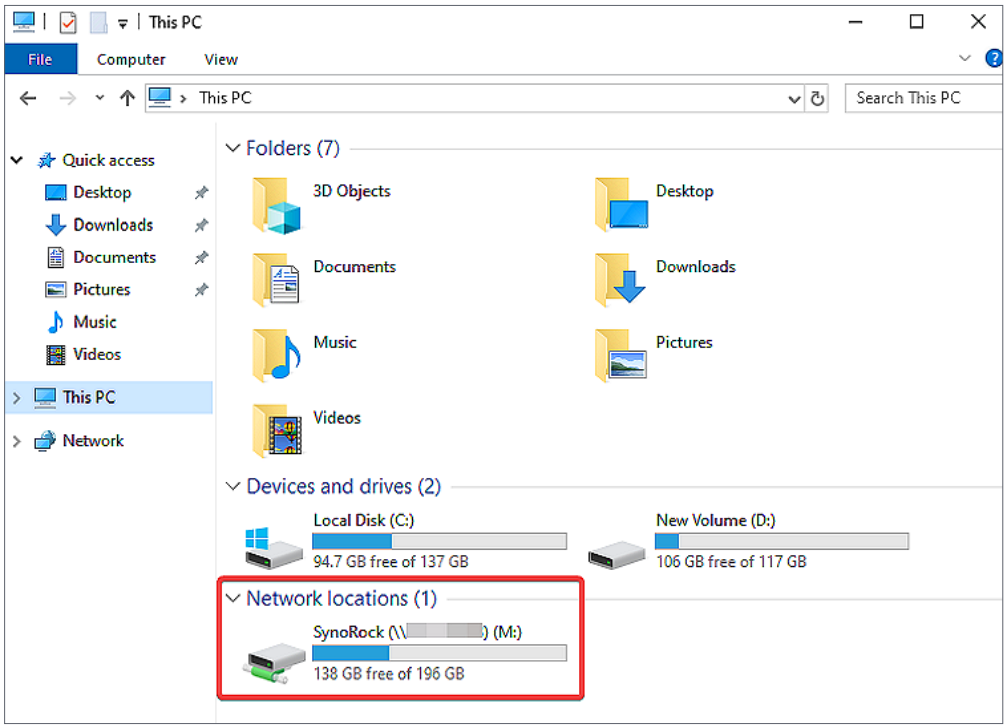
1. **將 Windows 電腦加入網域**。
2. 前往 RWDC 的**控制台** > **共用資料夾** > **新增** > **新增共用資料夾**以新增共用資料夾 (至少具備讀取權限)。給單一使用者的共用資料夾與給所有使用者的共用資料夾不可相同。
3. 依照**指派漫遊設定檔給單一使用者**的步驟三到步驟九進行操作。
4. 前往**設定檔** > **家目錄**的**連接 ... 至**。
5. 為網路磁碟機指派磁碟機代號。
6. 依照下方的格式輸入欲掛載為網路磁碟機的共用資料夾 (或是共用資料夾下的資料夾) 路徑。

```
\\NAS 的 IP 位址\( 共用 ) 資料夾名稱
```

7. 按一下**確定**來儲存設定。



8. 以該網域使用者帳號登入網域內的 Windows 電腦。使用者將會在電腦上看見已掛載的網路磁碟機。



注意：

- 若在磁碟機掛載前，網域使用者已登入指派的 Windows 電腦，該使用者必須重新登入才會看到磁碟機。

管理電腦

加入網域的裝置稱為電腦 (例如：工作站、伺服器、Synology NAS)。此類型的物件可部署於網域內，供使用者存取。

編輯電腦屬性

1. 前往 RWDC 的**使用者 & 電腦**頁面並選擇欲編輯的電腦。
2. 執行下列任一操作：
   - 在電腦按兩下。
   - 按一下**動作** > **屬性**。
   - 以右鍵按一下電腦並選擇**屬性**。
3. 前往**一般**頁籤並編輯電腦的**描述**。
4. 前往**加入群組**頁籤並將電腦加入或移除群組。
5. 按一下**確定**來儲存設定。

刪除電腦

1. 前往 RWDC 的**使用者 & 電腦**頁面並選擇欲刪除的電腦。按住 **Ctrl** 或 **Shift** 鍵來選取多台電腦進行刪除。
2. 執行下列任一操作：
   - 按一下**動作** > **刪除**。
   - 以右鍵按一下電腦並選擇**刪除**。
3. 按一下**刪除**來確認此操作。刪除的電腦**無法復原**。

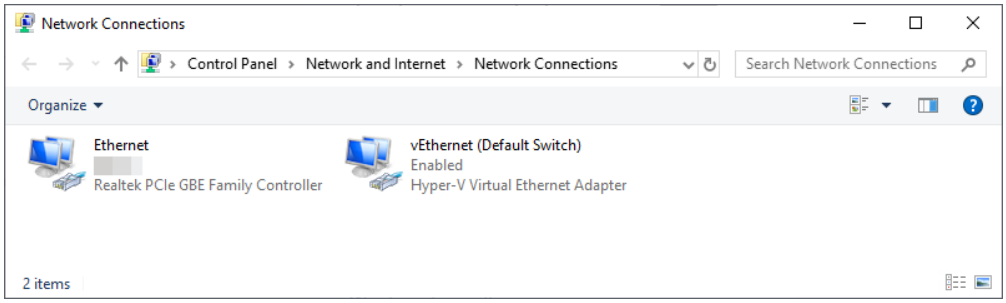
第 5 章：將裝置加入網域

您可將裝置加入網域成為網域用戶端，方便統合管理組織內部的資源，使用者也可透過單一帳號密碼來存取資源。

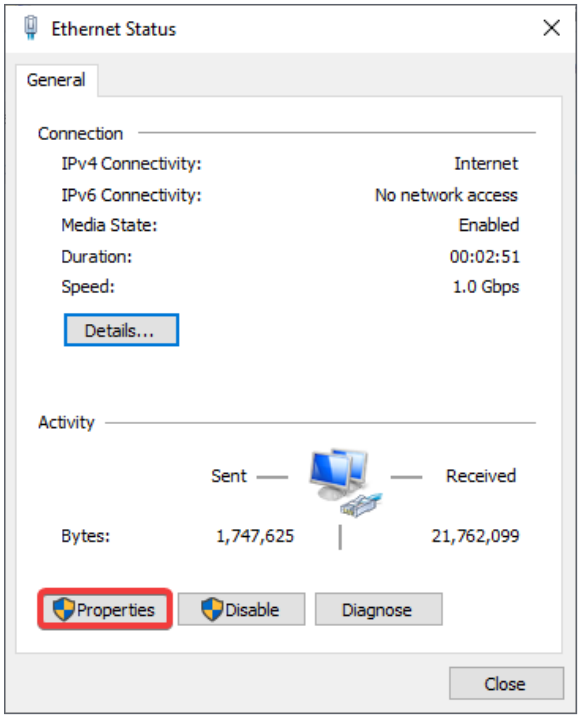
將 Windows 電腦加入網域

運行 Windows 7 及以上版本的電腦可加入 Synology Directory Server 建立的網域。此處以 Windows 10 電腦為範例。

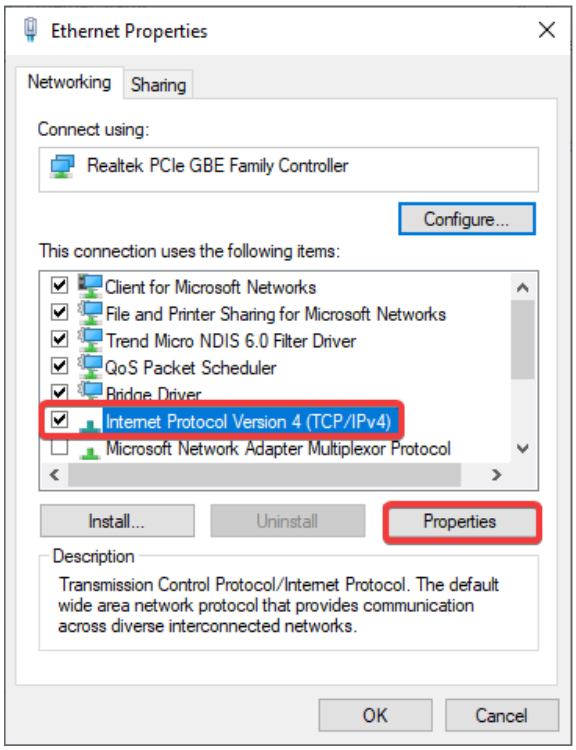
1. 前往 Windows **開始**圖示 > **設定** > **網路和網際網路** > **狀態** > **變更介面卡選項**，按兩下電腦正在使用的網路介面。



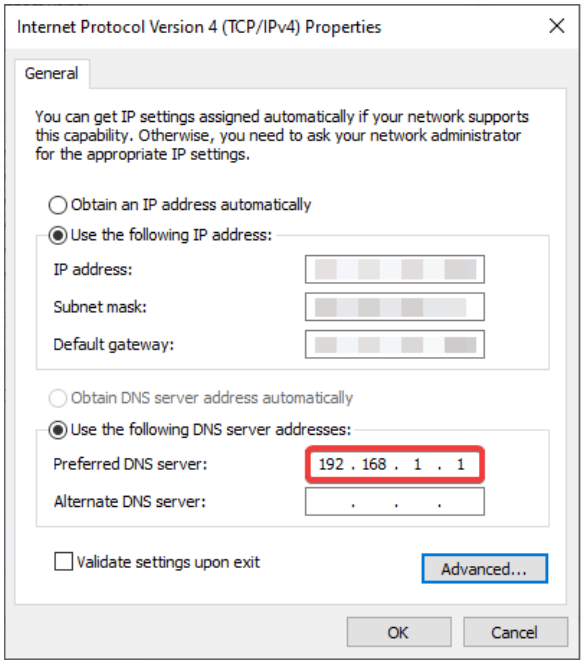
2. 在**狀態**頁面中按一下**內容**。



3. 在**網路功能**頁籤內，選擇**網際網路通訊協定第 4 版 (TCP/IPv4)** 並按一下**內容**。

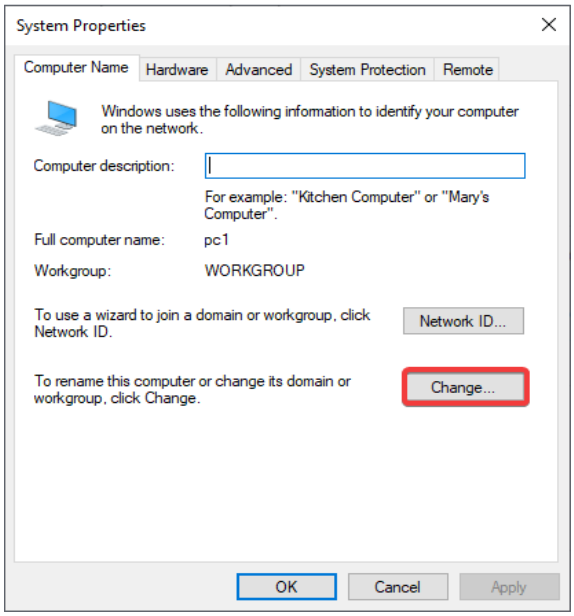


4. 勾選**使用下列的 DNS 伺服器位址**，並在**慣用 DNS 伺服器**欄位內輸入 DC 的 IP 位址。接著，按一下**確定**來儲存設定。

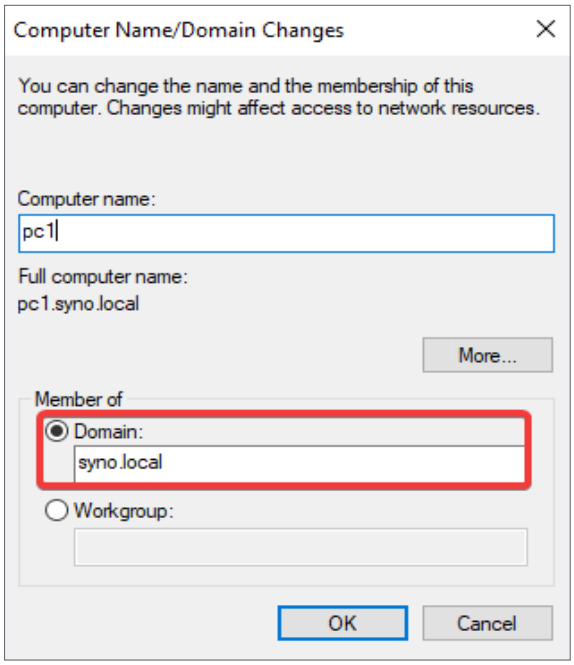


5. 前往 Windows **開始**圖示 > **設定** > **系統** > **關於** > **系統資訊**，再按一下**變更設定**。

6. 在**電腦名稱**頁籤內，按一下**變更 ...**。



7. 在**成員隸屬**區塊內，按一下**網域**並輸入欲將此電腦加入的網域名稱。確認資訊無誤後，按一下**確定**。



8. 依照下方的使用者名稱格式輸入網域管理員的帳號密碼，再按一下**確定**。

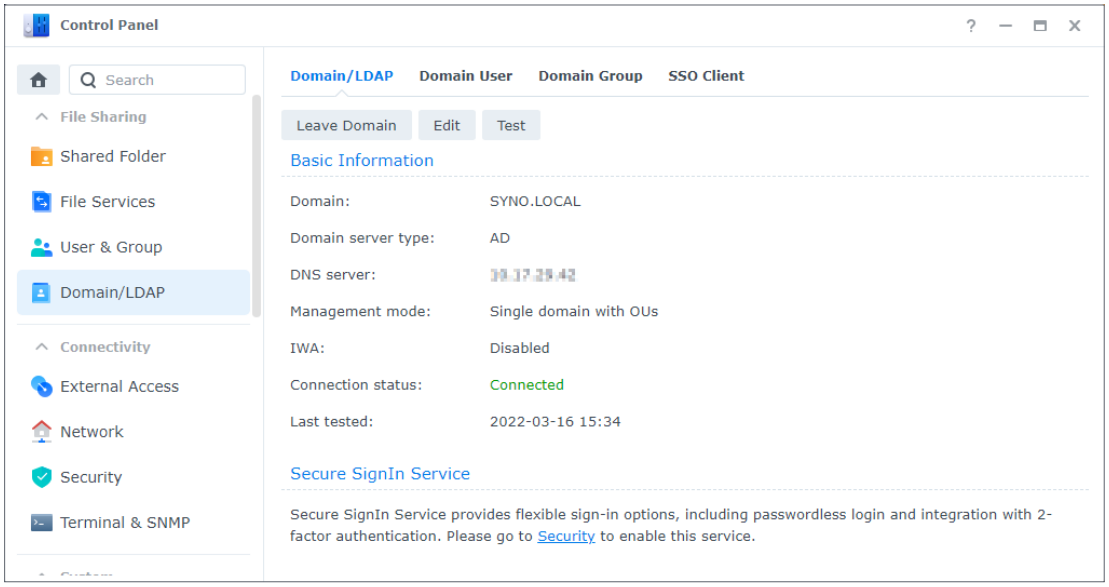
```
網域 NetBIOS 名稱 \ 管理員的使用者名稱
```

9. 重新啟動電腦以完成加入網域。

將 Synology NAS 加入網域

將 Synology NAS 加入網域作為網域用戶端後，網域使用者可透過其網域帳號密碼登入 Synology NAS，以存取檔案及使用 DSM 應用程式，無須額外記住其他帳號密碼。

1. 前往 DSM **控制台** > **網域 / LDAP** > **網域 / LDAP** 並按一下**加入網域**。
2. 輸入伺服器名稱並按**下一步**。
3. 輸入網域資訊並按**下一步**。
4. 精靈將執行環境檢測並提供檢測結果。
   - ：測試項目通過檢測。
   - ：檢測出一個或多個次要問題須解決。這些問題可能會導致網域服務異常。按一下**詳情**，並依照指示解決問題。
   - ：檢測出一個或多個嚴重問題須立即解決。這些問題會導致 Synology NAS 無法加入網域。按一下**詳情**，並依照指示解決問題。
5. 測試項目通過環境檢測並確認無任何嚴重問題後，按一下**確定**以將 Synology NAS 加入網域。
6. 若需要，按一下**編輯**以**進行一般或進階設定**。



注意：

- 請參閱加入網域的**說明文章**以了解更多資訊。

第 6 章：設定群組規則

您可以透過群組規則來管理網域內的使用者。其可用來限制常用操作、部署服務於網域裝置、管理更新、為使用者建構一致性的工作環境。妥善地管理群組規則可減輕網域管理的負擔。

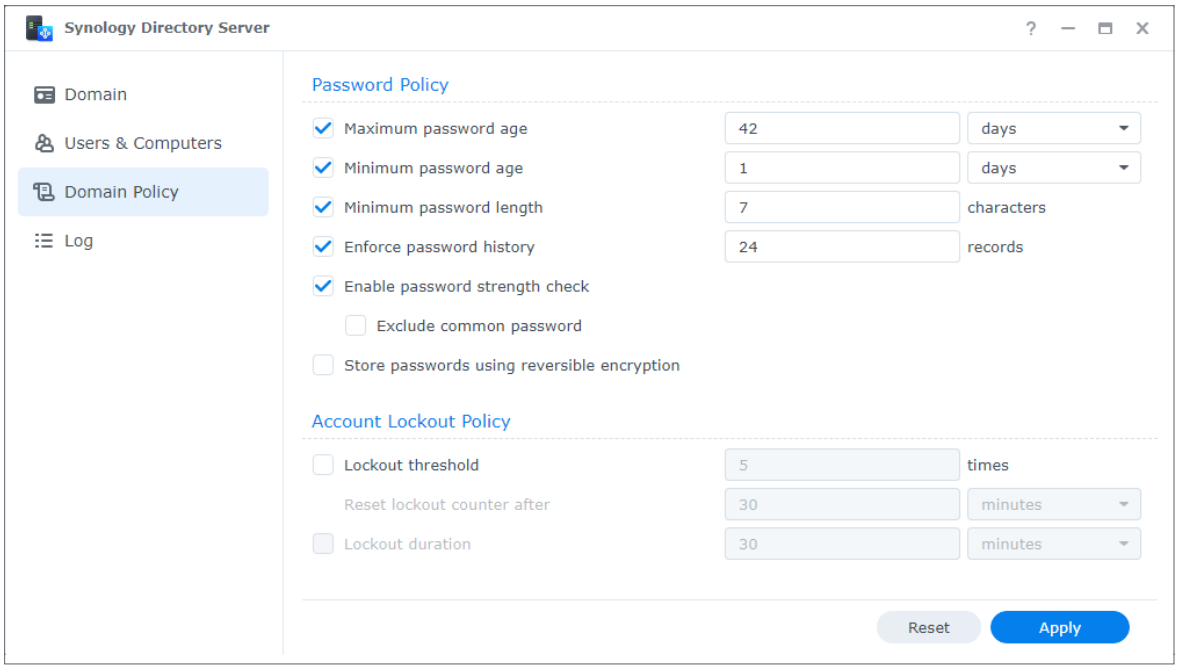
本章節將引導您如何透過 Windows 遠端伺服器管理工具 (Remote Server Administration Tools，RSAT) 來為您的網域設定群組規則。

設定預設網域規則

預設網域規則可讓您設定密碼及帳號鎖定規則，以維護在網域層級上的帳號安全。您可以在**網域規則**頁面管理這兩種類型的預設網域規則。

注意：

- 本頁面的網域規則亦可透過 Windows RSAT 的 **Default Domain Policy** (預設網域規則) 進行設定。



密碼規則

- **密碼最長有效期限**：指定密碼要在多久之後到期。若停用此選項，密碼將永遠不會到期。
- **密碼最短有效期限**：指定密碼從最後一次變更日算起，要多久之後才能進行變更。若停用此選項，密碼將可隨時變更。
- **密碼最短長度**：指定新密碼的最短長度。
- **強制執行密碼歷史紀錄**：新密碼不可與之前設定的密碼相同。指定密碼須相異的次數。
- **啟用密碼強度檢查**：密碼強度至少須符合下列規則的其中三項：
  - 大寫的拉丁字母 (包含 A - Z 及附加符號)、希臘字母、西里爾字母。
  - 小寫的拉丁字母 (包含 a - z 及附加符號)、希臘字母、西里爾字母。
  - 數字 (0 - 9)。
  - 特殊符號，包含 #、$、! 等。
  - 不分大小寫的 Unicode 字母，包含亞洲語言的字母。
- **排除常用密碼**：禁止使用者設定常見密碼，例如：「123456」、「password」、「qwerty」。
- **使用可還原加密方式來儲存密碼**：啟用此選項可能會降低網域安全性。除非網域用戶端服務的需求優先於密碼安全，否則不建議使用此選項。

帳戶鎖定規則

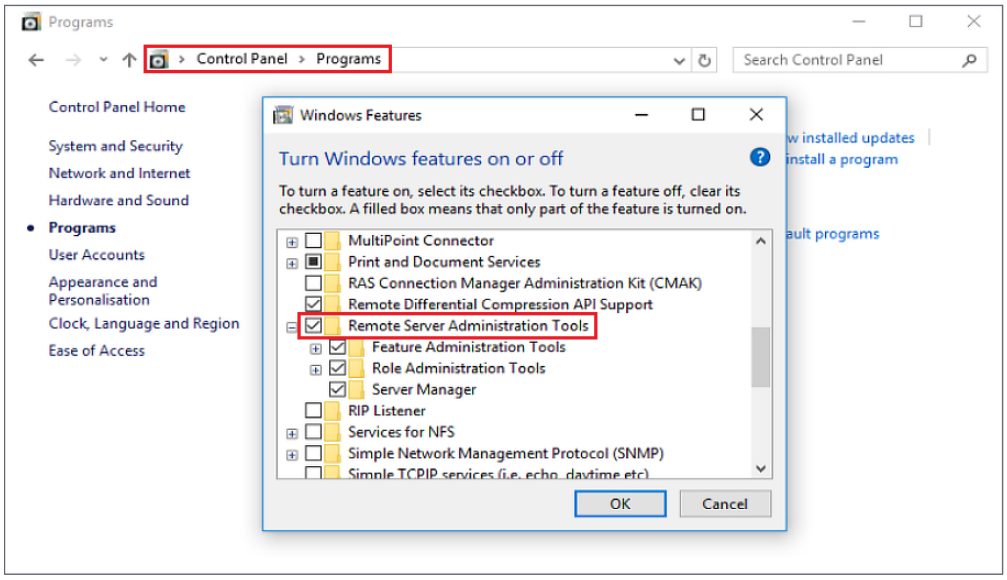
- **帳號鎖定條件**：當登入失敗次數超過指定的鎖定門檻時，該使用者帳號將會被鎖定。
- **鎖定計數器於指定時間後歸零**：登入失敗的次數將會在指定時間後重新計算。
- **鎖定期間**：在指定的期間過後，系統才會解除對使用者帳號的鎖定。

使用 RSAT 管理群組規則

您可以在**已加入網域的 Windows 電腦**上操作遠端伺服器管理工具 (Remote Server Administration Tools，RSAT) 來設定密碼及帳號鎖定規則以外的群組規則。

在 Windows 電腦安裝 RSAT

1. 從 Microsoft 下載中心將 **Windows RSAT** 下載至一台 Windows 電腦。每個 Windows 作業系統版本皆有獨立的 RSAT 安裝檔。
2. 執行下載的檔案，並依螢幕指示完成 RSAT 的安裝步驟。
3. 前往 Windows **控制台** > **程式集** > **開啟或關閉 Windows 功能**，並勾選**遠端伺服器管理工具**核取方塊。



4. 確認您已將使用中的電腦加入網域，並且以網域管理員的身分登入。您即可在**控制台** > **系統管理工具**找到 RSAT。

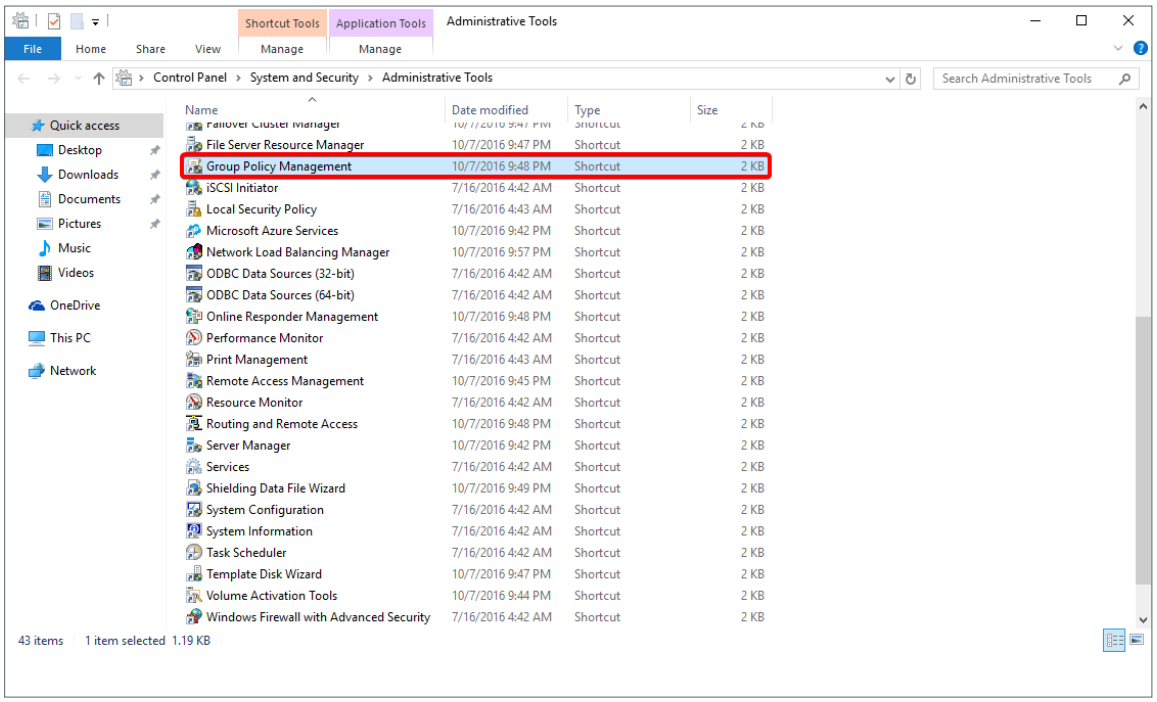
注意：

- RSAT 可設定的選項取決於安裝該軟體的 Windows 電腦版本。舉例來說，Windows 8 版的 RSAT 可能未完全包含 Windows 10 版的 RSAT 功能。

指派漫遊設定檔給所有使用者

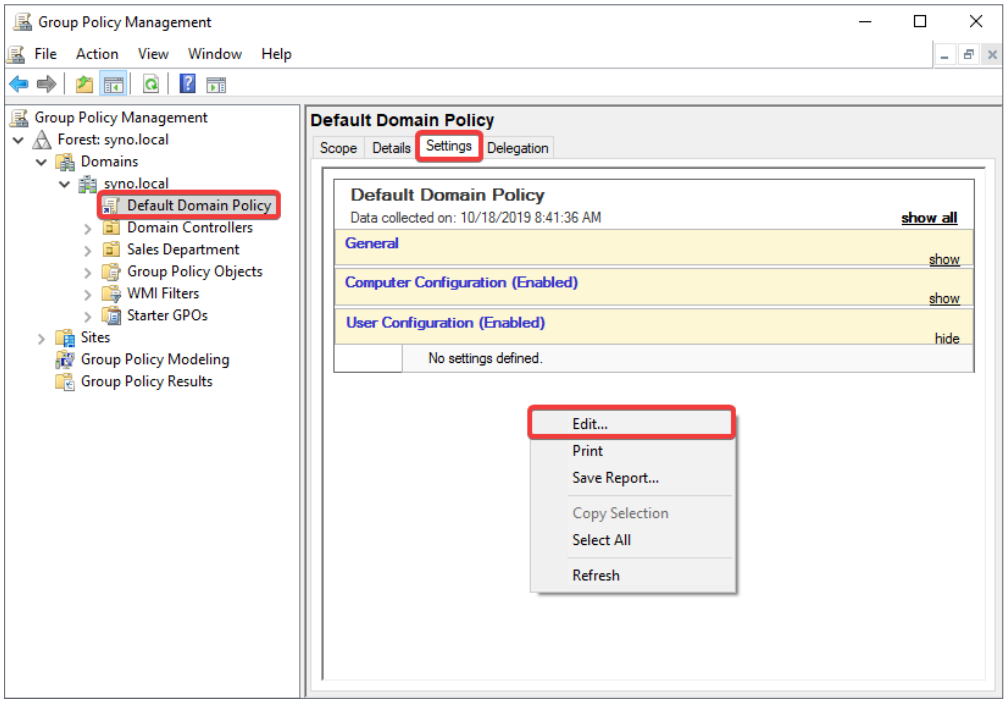
漫遊設定檔讓網域使用者登入已加入網域的不同 Windows 電腦時，也能存取自己的檔案。

1. 確認您已在作為 RWDC 的 Synology NAS 上新增一個共用資料夾，並給予所有網域使用者足夠的權限。詳細步驟請參閱**指派漫遊設定檔給單一使用者**的步驟一至步驟七。
2. 以網域管理員身分登入一台已加入網域的 Windows 電腦。
3. 前往 Windows **控制台** > **系統及安全性** > **系統管理工具** > **群組原則管理**。



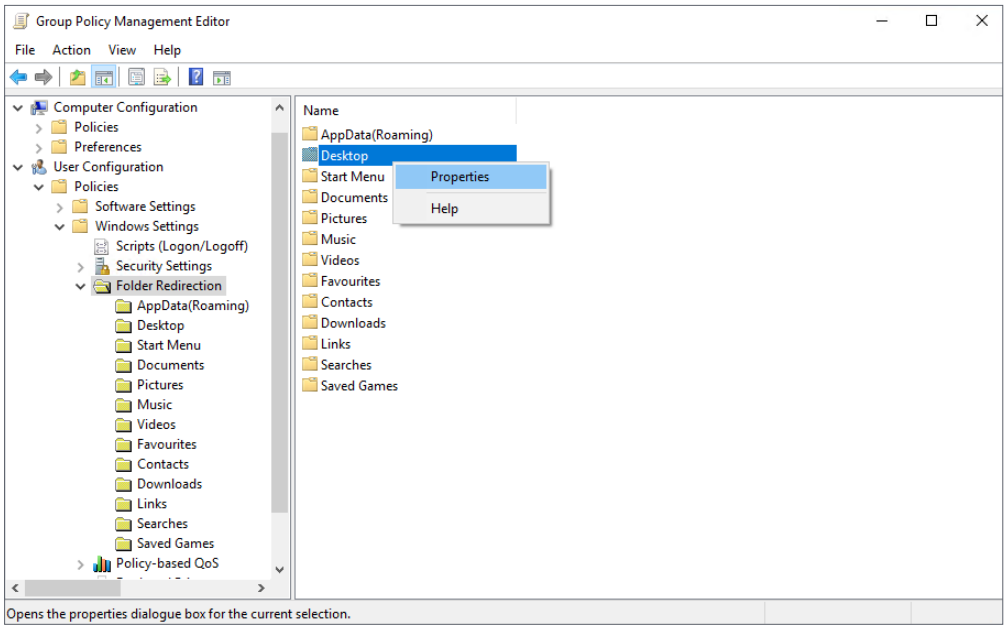
4. 前往**樹系：網域名稱** > **網域** > **網域名稱** > Default Domain Policy。

5. 在**設定**頁籤內的空白處按一下右鍵，再按一下**編輯**。



6. 前往**使用者設定** > **原則** > **Windows 設定** > **資料夾重新導向**。

7. 以右鍵按一下欲重新導向的資料夾，再按一下**內容**。



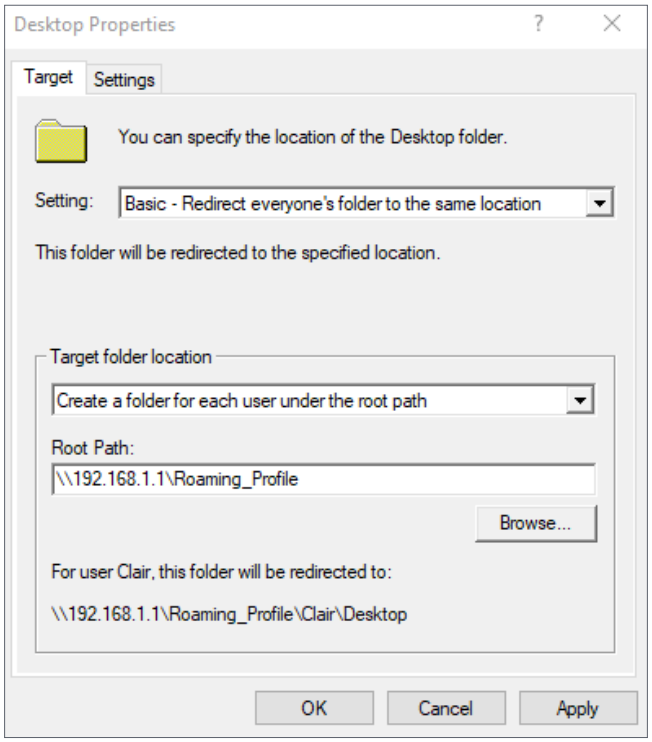
8. 設定下方選項：

   a. 切換至**目標**分頁。

   b. 選擇**基本 - 將每個人的資料夾重新導向至同一位置**。

   c. 在**目標資料夾位置**和**根路徑**中輸入需要的資訊。

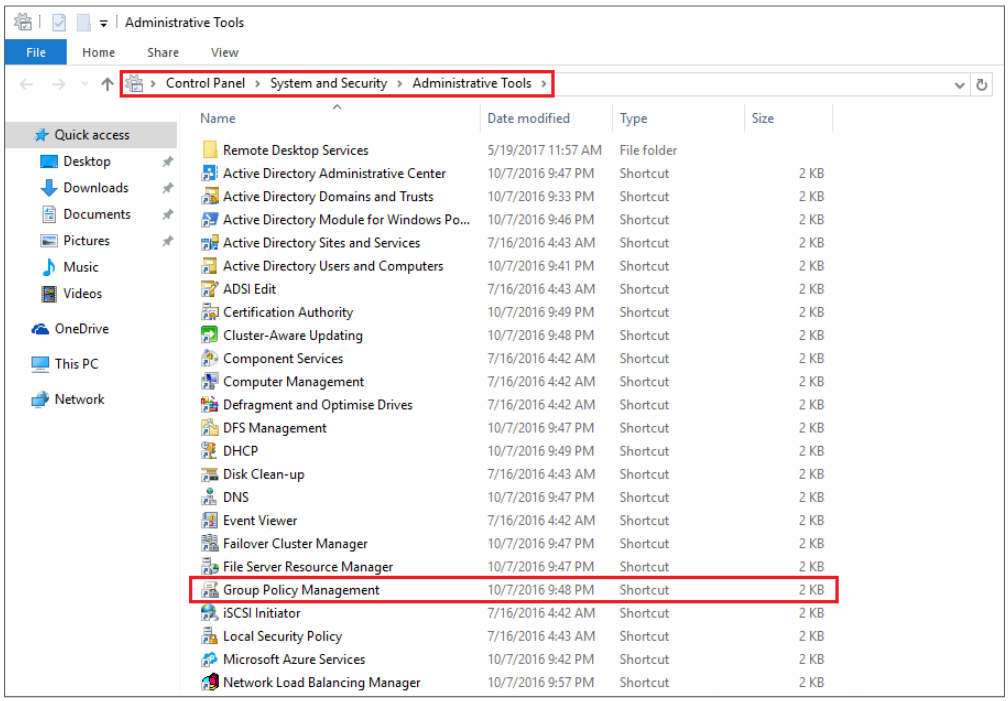
   d. 按一下**確定**。



9. 網域使用者的漫遊設定檔將導向您所指派的路徑。

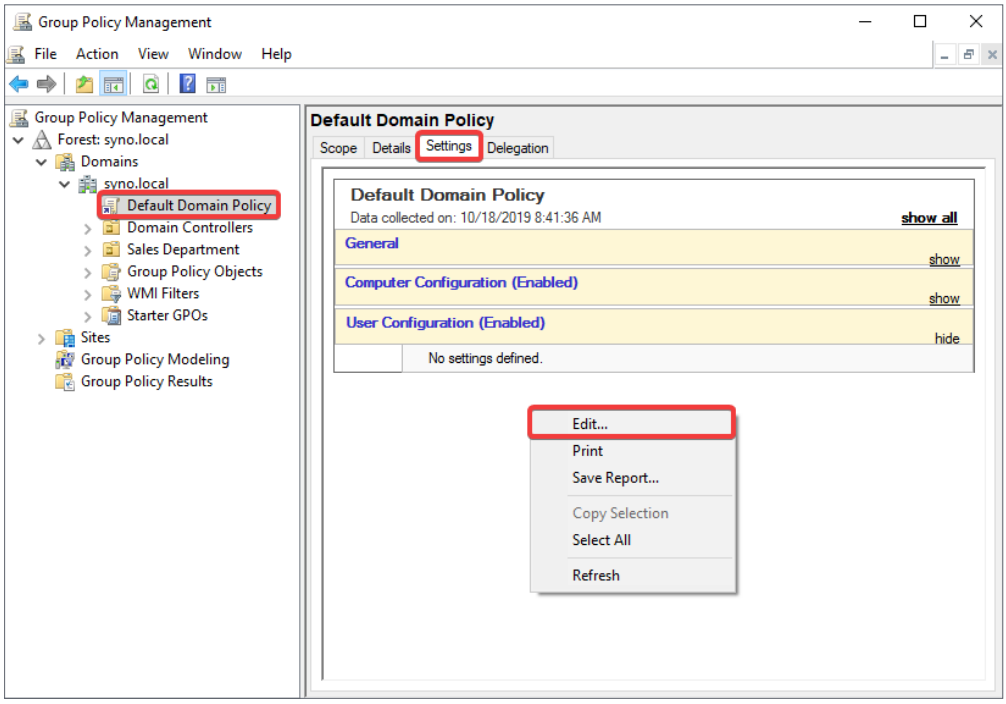
為所有使用者掛載網路磁碟機

1. 確認您已在作為 RWDC 的 Synology NAS 上新增一個共用資料夾，並給予所有網域使用者足夠的權限 (至少具備讀取權限)。詳細步驟請參閱**指派漫遊設定檔給單一使用者**的步驟一至步驟七。
2. 以網域管理員身分登入一台已加入網域的 Windows 電腦。
3. 前往 Windows **控制台** > **系統及安全性** > **系統管理工具** > **群組原則管理**。

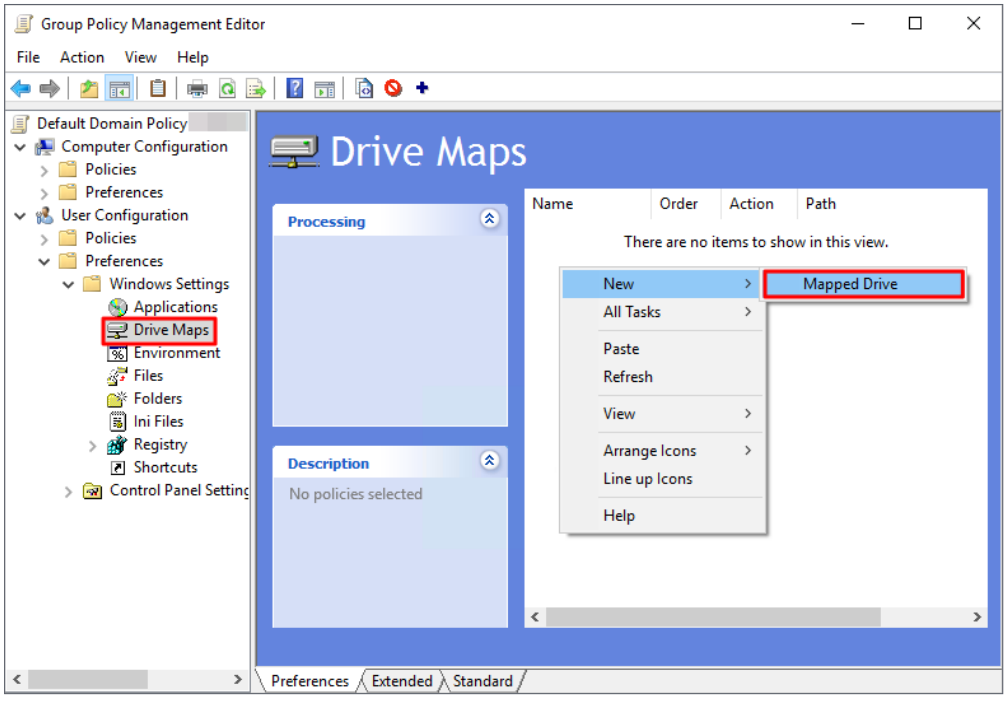


4. 前往**樹系：網域名稱** > **網域** > **網域名稱** > Default Domain Policy。

5. 在**設定**頁籤內的空白處按一下右鍵，再按一下**編輯**。

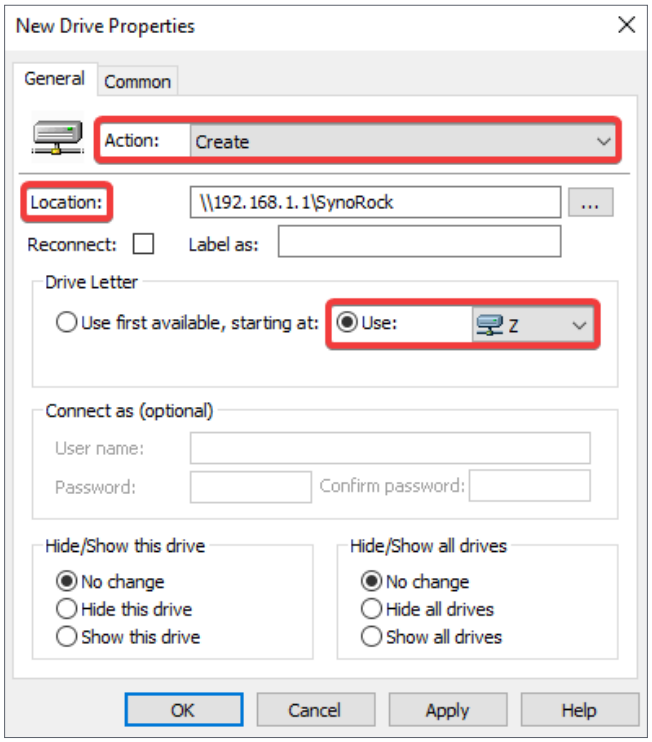


6. 前往左側目錄中的**使用者設定** > **喜好** > **Windows 設定** > **磁碟機對應**。在右側窗格內按一下右鍵，並按一下**新增** > **對應磁碟機**。



7. 進行以下設定，並按一下**確定**：

   - **動作**：從下拉式選單中選擇**建立**。
   - **位置**：輸入網路磁碟機的位置，例如：「\\192.168.1.1\SynoRock」。
   - **磁碟機代號**：在此區塊內，選擇**使用**並選擇一個磁碟機代號。



8. 設定完成後，當使用者以網域使用者帳號登入此電腦時，就能看見此網路磁碟機。

注意：

- 網域使用者登入時，Windows 會自動將網路磁碟機掛載於該使用者的帳號，因此您無須輸入**連線身分 (選擇性)** 區塊內的**使用者名稱**及**密碼**。
- 若要使網路磁碟機正常運作，請確認磁碟機目的地真實存在，且使用者擁有存取的權限。

第 7 章：維護及還原目錄服務

使用 Synology Directory Server 時，您必須確保目錄服務已獲得妥善的維護及備份。定期維護及備份讓您的目錄服務獲得保障，免於系統異常或檔案誤刪所造成的資料遺失。本章節將引導您使用 Synology High Availability 建立高可用叢集及使用 Hyper Backup 備份目錄服務。

透過 Synology High Availability 確保不間斷的目錄服務

透過 **Synology High Availability** 來保護目錄服務及確保 Synology Directory Server 的高可用性。

Synology High Availability 使用兩台伺服器來組成「高可用叢集」，一台伺服器擔任「主伺服器」，另一台則擔任「副伺服器」。使用此伺服器配置解決方案，能降低因伺服器異常所造成的服務中斷。請參閱 **Synology High Availability 的指南**以了解高可用叢集的核心觀念。

系統需求

若要透過 Synology High Availability 建立叢集，需要兩台同款的 Synology NAS，且系統設定皆須相同。在開始之前，請先了解 Synology High Availability 的**限制與系統需求**及**技術規格**，並請注意以下資訊。

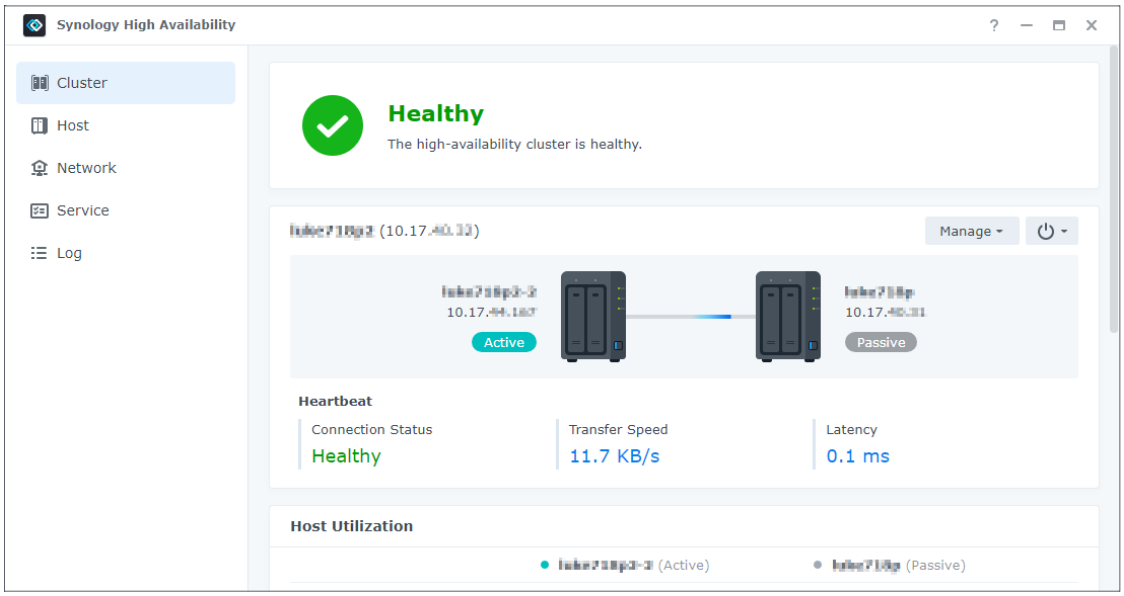
- **適用機種**：主伺服器與副伺服器的機種必須相同。
- **DSM 及套件版本**：主伺服器與副伺服器皆須安裝相同版本的 DSM 及 Synology High Availability。
  - **Synology Directory Server** 必須為 4.10.18-0363 及以上版本。
  - **Synology High Availability** 必須為 2.1.1-1279 及以上版本。
- **相同的儲存空間及網路設定**：
  - 主伺服器與副伺服器的硬碟插槽數量以及所安裝的硬碟數量、容量必須相同。
  - 主伺服器與副伺服器的網路介面數及網路設定必須相同。
  - 兩台伺服器皆至少有一組相同子網路內的靜態 IP 位址。
  - 兩台伺服器須相互建立 Heartbeat 連線以進行內部通訊。

建立高可用叢集

為確保 Synology Directory Server 能正常運作，請在啟用 Synology Directory 服務之前架設 Synology High Availability 叢集。

1. 前往**套件中心**並安裝 **Synology High Availability**。
2. 開啟 **Synology High Availability**。

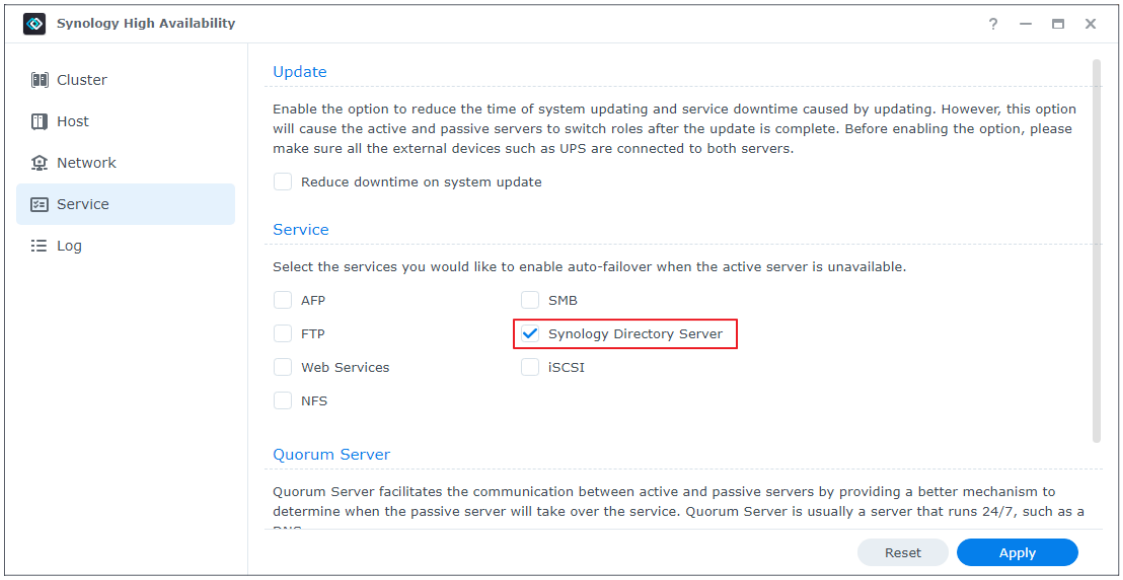
3. 按一下**建立高可用叢集**，再依照精靈的指示完成建立流程 (請參閱**說明文章**以了解詳細步驟)。



4. 安裝 Synology Directory Server 並建立 Synology Directory 服務。

5. 前往 **Synology High Availability** > **服務**。

6. 勾選 **Synology Directory Server**，並按一下**套用**以儲存設定。



透過 Hyper Backup 備份及還原目錄服務

Hyper Backup 提供以下功能，可用來備份、還原 Synology Directory Server 的資料與設定。

- 保留最多 65,535 份資料版本，並且透過跨版本的重覆資料刪除技術，減少儲存空間使用量。
- 存放備份資料至獨立資料庫，透過專屬的多版本瀏覽器 (適用於 DSM、Windows、Linux 平台) 輕鬆進行瀏覽、下載、還原。
- 手動及排程備份各類資料，例如：系統設定、共用資料夾、應用程式、套件。

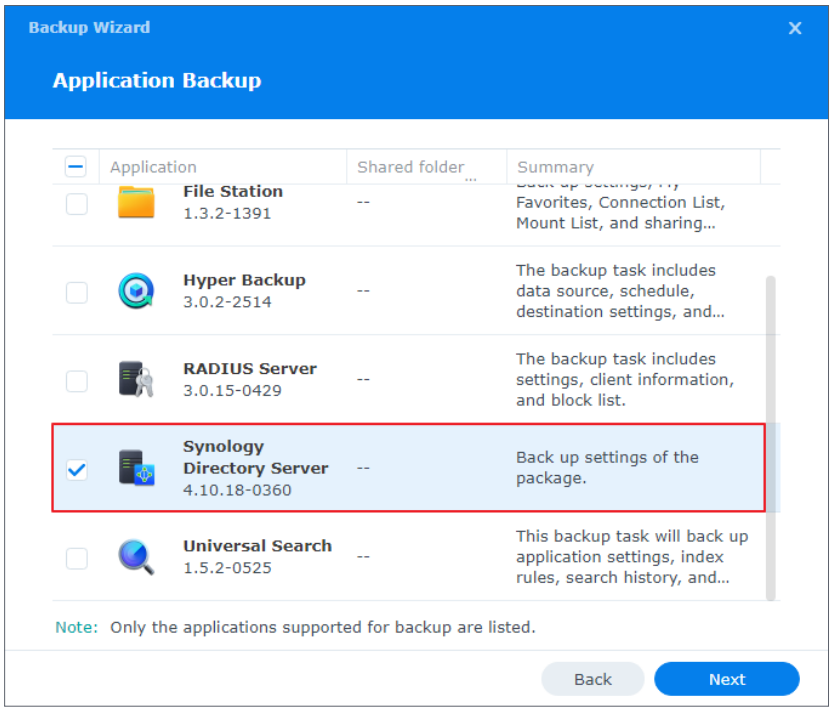
- 將備份資料儲存至本地共用資料夾、遠端伺服器、公有雲。
- 為每項備份任務保留多個備份版本。自動刪除備份版本 (可自行選擇是否啟用) 共包含三種機制：從最早版本開始刪除、Smart Recycle、自訂保留版本。

請參閱 Hyper Backup 的**技術規格**以了解更多資訊。

建立備份任務

Hyper Backup 可讓您建立、管理、監控檔案備份任務。

1. 前往**套件中心**並安裝 **Hyper Backup**。
2. 開啟 **Hyper Backup**。
3. 按一下左上角的 並選擇**資料備份任務**來啟動備份精靈。
4. 選擇備份目的地類型。建議將資料備份至不同的裝置或服務。
5. 選擇**建立備份任務**。
6. 選擇欲備份的資料夾，按**下一步**。
7. 勾選 **Synology Directory Server**，按**下一步**。



8. 依照精靈指示完成設定。

還原備份資料

若 Synology Directory Server 發生錯誤，您可透過 Hyper Backup 來還原目錄資料。此外，您也可透過 Hyper Backup 的服務還原功能，將 Synology Directory 服務轉移至另一台 Synology NAS。

1. 開啟 **Hyper Backup**。
2. 按一下左上角的 並選擇**資料**來啟動備份精靈。
3. 選擇要還原的備份任務。
4. 跳出的視窗會依照您欲還原的備份任務類型，要求您選擇系統設定、備份檔案版本等資訊。
5. 若備份任務已加密，則須輸入密碼或加密金鑰。
6. 依照精靈指示來完成還原。

注意：

- 請參閱 **Hyper Backup 的說明文章**以了解更多資訊。

SYNOLOGY INC.
新北市板橋區
遠東路 1 號 9 樓
台灣
電話：+886 2 2955 1814

SYNOLOGY AMERICA CORP.
3535 Factoria Blvd SE #200,
Bellevue, WA 98006
USA
電話：+1 425 818 1587

SYNOLOGY UK LTD.
Unit 5 Danbury Court, Linford
Wood, Milton Keynes, MK14 6PL
United Kingdom
電話：+44 (0)1908048029

SYNOLOGY FRANCE
102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
電話：+33 147 176288

SYNOLOGY GMBH
Grafenberger Allee 295
40237 Düsseldorf
Deutschland
電話：+49 211 9666 9666

SYNOLOGY SHANGHAI
200070 中國上海市
靜安區天目西路 511 號輔
房 201 室
中國

SYNOLOGY JAPAN CO., LTD.
4F, No. 3-1-2, Higashikanda,
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®

synology.com