



## 架構 Virtual Desktop Service

NetApp  
May 03, 2022

# 目錄

架構 .....	1
重新導向儲存平台 .....	1
資料移轉考量 .....	5
萬用字元SSL憑證續約程序 .....	7
AVD接地指南 .....	10

# 架構

## 重新導向儲存平台

### 總覽

虛擬桌面服務部署技術可根據基礎架構提供各種儲存選項、本指南將說明如何在部署後進行變更。

虛擬桌面效能取決於各種關鍵資源、儲存效能是其中一項主要變數。隨著需求的變化和工作負載的演進、改變儲存基礎架構的需求是一項常見的工作。在幾乎所有情況Azure NetApp Files 下、這都涉及從檔案伺服器平台移轉至NetApp儲存技術（例如：VMware的VMware、Cloud Volumes Service Google的NetApp支援、Cloud Volumes ONTAP 或AWS的NetApp支援）、因為這些技術通常可為終端使用者運算環境提供最佳效能設定檔。

### 建立新的儲存層

由於各種雲端與HCI基礎架構供應商的潛在儲存服務種類繁多、因此本指南假設已建立新的儲存服務、並採用已知的SMB路徑。

### 建立儲存資料夾

1. 在新的儲存服務中、建立三個資料夾：

- /資料
- /首頁
- /Pro

□

2. 設定資料夾權限

- a. 在「資料夾內容」中、選取「安全性」、>「進階」>「停用繼承」

□

- b. 調整其餘設定、使其符合原先由部署自動化所建立的原始儲存層設定。

### 移動資料

目錄、資料、檔案和安全性設定可透過多種方式移動。下列Robocopy語法將會達成必要的變更。路徑必須變更以符合您的環境。

```
robocopy c:\data\zucd \\uyy-1c37.deskapps.mobi\zucd-data /xd ~snapshot  
/MIR /CopyAll /R:1 /W:1 /tee /log:C:\temp\roboitD.txt
```

### 在轉換時重新導向SMB路徑

當轉換時間到時、有幾項變更會將所有的儲存功能重新導向至VDSI環境。

## 更新GPO

1. 使用者GPO（名稱為\_、公司代碼>-user\_）必須以新的共用路徑進行更新。選取「使用者組態」>「Windows設定」>「偏好設定」>「磁碟機地圖」

□

2. 在\_H:\_上按一下滑鼠右鍵、然後選取「內容」>「編輯」>「動作：取代」、然後輸入新的路徑

□

3. 使用傳統或混合式AD更新公司OU中ADUC中定義的共用區。這反映在VDS資料夾管理中。

□

## 更新FSLogix設定檔路徑

1. 在原始檔案伺服器和其他任何已配置的工作階段主機上開啟RegEdit。



如有需要、也可透過GPO原則設定。

2. 使用新值編輯\_VHDLocations值。這應該是新的SMB路徑加上\_profilecontainers\_、如下面的快照所示。

□

## 更新主目錄的資料夾重新導向設定

1. 開啟群組原則管理、選取使用者GPO連結至DC=domain,DC=obi/Cloud Workspace/Cloud Workspace Companies /////<公司代碼>/<公司代碼>-桌面使用者。
2. 在「使用者組態」>「原則」>「Windows設定」>「資料夾重新導向」下編輯資料夾重新導向路徑。
3. 只有桌面和文件需要更新、而且路徑應符合主磁碟區的新SMB路徑掛載點。

□

## 使用Command Center更新VDS SQL資料庫

WMGR1包含名為Command Center的輔助程式公用程式應用程式、可大量更新VDS資料庫。

若要進行最終資料庫更新：

1. 連線至CWMGR1、瀏覽並執行CommandCenter.exe

□

2. 瀏覽至「Operations」（作業）索引標籤、按一下「\_Load Data」（載入資料）以填入「公司代碼」下拉式清單、選取公司代碼、然後輸入儲存層的新儲存路徑、再按一下「Execute Command」（執行命令）。

□

## 將儲存平台重新導向至Azure檔案

### 總覽

虛擬桌面服務部署技術可根據基礎架構、提供各種儲存選項。本指南說明如何在部署後變更使用Azure Files。

### 先決條件

- 已安裝並設定AD Connect
- Azure全域管理員帳戶
- AZFilesHybrid PowerShell模組 <https://github.com/Azure-Samples/azure-files-samples/releases>
- AZ PowerShell模組
- ActiveDirectory PowerShell模組

### 建立新的儲存層

1. 使用全域管理員帳戶登入Azure
  2. 在與工作區相同的位置和資源群組中建立新的儲存帳戶
- 
3. 在儲存帳戶下建立資料、主檔案和專業檔案共用

□

### 設定Active Directory

1. 在Cloud Workspace > Cloud Workspace Service Accounts OU下建立名為「儲存帳戶」的新組織單位
- 
2. 啟用AD DS驗證（必須使用PowerShell執行） <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable>
    - a. 網域帳戶類型應為「服務登入帳戶」
    - b. OrganizationalUnitName是上一步建立之OU的辨別名稱（亦即「OID=Storage Account,OID=Cloud Workspace Service Accounts,OID=Cloud Workspace,DC=訓練Krisg,DC=onmicrosoft,DC=com」）

### 設定共用的角色

1. 在Azure入口網站中、為CloudWorkspaceSVC和Level 3技術人員提供「『儲存檔案資料SMB共用提升貢獻者」角色
- 
2. 將「儲存檔案資料SMB共用貢獻者」角色賦予「<公司代碼>-all user」群組

□

## 建立目錄

1. 在每個共用區（資料、主目錄、專業人員）中建立一個目錄、使用公司代碼做為名稱（在此範例中、公司代碼為「Kift」）。

[]

2. 在專業共享區的<公司代碼>目錄中、建立「ProfileContainers」目錄

[]

## 設定NTFS權限

1. 連線至共用區

- a. 瀏覽至Azure入口網站儲存帳戶下的共用區、按一下三個點、然後按一下「Connect（連線）」

[]

- b. 選擇Active Directory做為驗證方法、然後按一下程式碼右下角的複製到剪貼簿圖示

[]

- c. 以屬於Level 3技術人員群組成員的帳戶登入CWMGR1伺服器

- d. 在PowerShell中執行複製的程式碼、以對應磁碟機

- e. 針對每個共用區執行相同的作業、同時為每個共用區選擇不同的磁碟機代號

2. 停用<公司代碼>目錄的繼承

3. 系統和AD群組ClientDHPAccess應擁有對<公司代碼>目錄的完整控制權

4. 網域電腦應擁有對專業共用區中<公司代碼>目錄的完整控制權、以及內部的ProfileContainer目錄

5. 所有使用者AD群組的主共享區和專業共享區中、都應該有「List」（清單）資料夾/「Read」（讀取）資料權限

6. 所有使用者AD群組的資料共用區中的目錄應具有下列特殊權限

[]

7. 「所有使用者AD」群組應擁有ProfileContainer目錄的「修改」權限

## 更新群組原則物件

1. 更新位於Cloud Workspace > Cloud Workspace Companies >><公司代碼>><公司代碼>桌面使用者下的GPO <公司代碼>使用者

- a. 變更主磁碟機對應以指向新的主共用區

[]

- b. 變更「資料夾重新導向」以指向桌面和文件的主共用區

[]



更新**Active Directory**使用者和電腦中的共用區

1. 使用傳統或混合式AD時、公司代碼OU中的共享區必須更新至新位置



更新**VDS**中的資料/主目錄/專業路徑

1. 使用Level 3技術人員群組中的帳戶登入CWMGR1、然後啟動Command Center
2. 在命令下拉式清單中、選取變更資料/主目錄/專業資料夾
3. 按一下「Load Data（載入資料）」按鈕、然後確定從下拉式清單中選取適當的公司代碼
4. 輸入資料、主目錄和專業人員位置的新patsh
5. 取消核取「是Windows伺服器」方塊
6. 按一下「執行命令」按鈕



更新**FSLogix**設定檔路徑

1. 在工作階段主機上開啟登錄暫時功能
2. 編輯HKLM \software\FSLogix\Profiles中的VHDLocations項目、將其做為新ProfileContainer目錄的UNC路徑



設定備份

1. 建議您為新共用區設定備份原則
2. 在相同的資源群組中建立新的恢復服務資料庫
3. 瀏覽至保存庫、然後在「Getting Started（使用入門）」下選取「Backup（備份）」
4. 選擇Azure作為工作負載的執行位置、Azure檔案共用則為您要備份的項目、然後按一下「Backupp」
5. 選取用來建立共用的儲存帳戶
6. 新增要備份的共用
7. 編輯並建立符合您需求的備份原則

## 資料移轉考量

### 總覽

移轉至任何類型的雲端解決方案時、移轉資料幾乎是通用的需求。雖然管理員負責將資料移轉至虛擬桌面、但NetApp的經驗已成為可用的經驗、而且已證實對於無數客戶移轉來說是非常寶貴的經驗。虛擬桌面環境只是託管的Windows環境、因此很可能會採用任何所需的方法。

一般移轉的資料：

- 使用者設定檔（桌面、文件、我的最愛等）
- 檔案伺服器共用
- 資料共用（應用程式資料、資料庫、備份快取）

在虛擬桌面環境中、有兩個主要位置可儲存及組織資料：

- 使用者（通常為H:\）磁碟機：這是每個使用者可見的對應磁碟機。
  - 這會對應回<drive>:\home\CustomerCode\user.name路徑
  - 每個使用者都有自己的H:\磁碟機、而且看不到其他使用者
- 共享磁碟機（通常為I:\）：這是所有使用者都能看到的共享對應磁碟機
  - 這會對應回<drive>:\data\CustomerCode\路徑
  - 所有使用者都可以存取此磁碟機。在VDS的「資料夾」區段中、會管理其對內含資料夾/檔案的存取層級。

## 一般移轉程序

1. 將資料複寫到雲端環境
2. 將資料移至適當的H:\和I:\磁碟機路徑
3. 在虛擬桌面環境中指派適當的權限

## FTPS傳輸與考量

使用FTPS移轉

1. 如果在SWA部署程序期間啟用了FTPS伺服器角色、請登入VDS、瀏覽至「報告」並執行貴組織的主用戶端報告、以收集FTPS認證資料
2. 上傳資料
3. 將資料移至H:\和I:\磁碟機的適當路徑
4. 透過資料夾模組在虛擬桌面環境中指派適當的權限



透過FTPS傳輸資料時、任何中斷都會使資料無法如預期傳輸。由於虛擬桌面服務管理的伺服器每晚都會重新開機、因此標準的夜間傳輸策略可能會中斷。為了避免這種情況、管理員可以啟用移轉模式、以防止VM重新開機1週。

輕鬆啟用移轉模式：瀏覽至組織、然後向下捲動至「Virtual Desktop Settings」（虛擬桌面設定）區段、勾選「Migration Mode」（移轉模式）方塊、然後按一下「Update」（更新）。



NetApp建議系統管理員啟用法規遵循設定、協助組織透過強化部署閘道等來達成PCI、HIPAA及NIST控制。這也會使預設的FTP伺服器角色（若已啟用）不接受透過連接埠21進行的預設未加密傳輸。FileZilla不允許SFTP、這表示應使用FTPS透過連接埠990建立連線。

若要啟用該設定、請連線至CWMGR1並瀏覽至CwVmAutomationService程式、然後啟用PCI v3法規遵循。



## 同步工具與考量

企業檔案同步與共享（通常稱為EFSS或同步工具）在移轉資料時非常實用、因為此工具會在每一端擷取變更、直到轉換為止。Office 365隨附的OneDrive等工具可協助您同步檔案伺服器資料。這也適用於VDI使用者部署、因為使用者與VM之間有1：1關係、只要使用者在共享資料部署一次時（通常為1：1）、不會嘗試將共享內容同步到VDI伺服器。推動整個組織使用。移轉SQL和類似資料（開放式檔案）

通用同步和/或移轉解決方案不會傳輸開啟的檔案、包括下列檔案類型：

- 信箱（.ost）檔案
- 快速書籍檔案
- Microsoft Access檔案
- SQL資料庫

這表示如果整個檔案（例如出現1封新電子郵件）或資料庫（在應用程式的系統中輸入1筆新記錄）的單一元素、則整個檔案會有所不同、而且是標準的同步工具（例如Dropbox）。會認為這是全新的檔案、需要重新移動。如有需要、可向第三方供應商購買專用工具。

處理這些移轉的另一種常見方法是提供第三方VAR的存取權限、而第三方VAR通常會簡化匯入/匯出資料庫的作業。

## 運送磁碟機

許多資料中心供應商不再隨附硬碟、也不需要您遵守特定的政策與程序。

Microsoft Azure讓組織能夠使用Azure Data Box、管理員可與Microsoft代表協調、充分發揮Azure Data Box的優勢。

## 萬用字元SSL憑證續約程序

建立憑證簽署要求（CSR）：

1. 連線至CWMGR1
2. 從「管理員工具」開啟「IIS管理員」
3. 選取「CWMGR1」並開啟「伺服器憑證」
4. 按一下「動作」窗格中的「建立憑證要求」

□

5. 在「Request Certificate Wizard」（申請憑證精靈）中填寫「Distinguished Name Properties」（辨別名稱內容）、然後按「
  - a. 一般名稱：FQDN of Wildcard \*.domain.com
  - b. 組織：貴公司合法註冊的名稱
  - c. 組織單位：「IT」運作正常
  - d. 城市：公司所在的城市
  - e. 州/省：公司所在的州/省

f. 國家/地區：公司所在的國家/地區

□

6. 在「Cryptographic Service Provider Properties（密碼編譯服務提供者內容）」頁面上、確認下列項目出現、然後按「Next（下一步）」

□

7. 指定檔案名稱、然後瀏覽至您要儲存CSR的位置。如果您未指定位置、CSR將位於C:\Windows\System32..

□

8. 完成後按一下「Finish（完成）」您將使用此文字檔將訂單提交給憑證註冊機構
9. 請聯絡登錄支援部門、以購買新的萬用字元SSL作為您的憑證：\*.domain.com
10. 收到SSL憑證後、請將SSL憑證.cer檔案儲存在CWMGR1上的某個位置、然後依照下列步驟進行。

## 安裝及設定**CSR**：

1. 連線至CWMGR1
2. 從「管理員工具」開啟「IIS管理員」
3. 選取「CWMGR1」並開啟「伺服器憑證」
4. 按一下「動作」窗格中的「完成憑證要求」

□

5. 完成「完整憑證要求」中的下列欄位、然後按一下「確定」：

□

- a. 檔案名稱：選取先前儲存的.cer檔案
- b. 易記名稱：\*.domain.com
- c. 憑證存放區：選取「Web託管」或「個人」

## 指派**SSL**憑證：

1. 確認「移轉模式」未啟用。您可以在VDS的「安全性設定」下的「工作區總覽」頁面上找到這項功能。

□

2. 連線至CWMGR1
3. 從「管理員工具」開啟「IIS管理員」
4. 選取「CWMGR1」並開啟「伺服器憑證」
5. 按一下「動作」窗格中的「匯出」
6. 以.pfx格式匯出憑證

7. 建立密碼。儲存密碼以供日後匯入或重新使用.pfx檔案所需
8. 將.pfx檔案儲存至C:\installs\RDPcert目錄
9. 按一下「確定」並關閉「IIS管理員」

□

10. 開啟DCConfig
11. 在"萬用字元憑證"下、將"憑證路徑"更新為新的.pfx檔案
12. 出現提示時輸入.pfx密碼
13. 按一下儲存

□

14. 如果憑證的有效時間超過30天、請允許自動化在一週內的「每日早上行動」工作期間套用新的憑證
15. 定期檢查平台伺服器、確認新的憑證已傳播。驗證並測試使用者連線能力以確認。
  - a. 在伺服器上、前往管理工具
  - b. 選取「遠端桌面服務」>「遠端桌面閘道管理員」
  - c. 在閘道伺服器名稱上按一下滑鼠右鍵、然後選取「內容」。按一下「SSL憑證」索引標籤以檢閱到期日

□

16. 定期檢查執行連線代理人角色的用戶端VM
  - a. 移至「伺服器管理員」>「遠端桌面服務」
  - b. 在「部署總覽」下、選取「工作」下拉式清單、然後選擇「編輯部署內容」
- c. 按一下「憑證」、選取「憑證」、然後按一下「檢視詳細資料」將會列出到期日。

□

□

17. 如果您想要立即推出新的憑證、請使用TestVdcTools強制更新。這應該在維護期間完成、因為任何登入的使用者都會失去連線、而且您與CWMGR1的連線也會中斷。
  - a. 前往C:\Program Files\CloudWorkspace\TestVdcTools、按一下「Operations（作業）」索引標籤、然後選取「Wildcard Cert Install（萬用字元證書安裝）」命令
  - b. 將伺服器欄位保留空白
  - c. 核取力方塊
  - d. 按一下「執行命令」
  - e. 使用上述步驟驗證憑證傳播

□

# AVD接地指南

## 總覽

本文涵蓋移除 VDS 和 NetApp 控制權、同時維持 AVD 終端使用者存取權。未來的管理將會採用原生的 Azure / Windows 管理工具。完成此程序後、建議聯絡 [support@spotpc.netapp.com](mailto:support@spotpc.netapp.com)、以便 NetApp 清理我們的後端與帳單系統。

## 初始狀態

- AVD部署
- TDS1是FS Logix Fileshare
- TS1是工作階段主機
- 使用者已登入、並在下列位置建立FS Logix磁碟：

```
\\*****TSD1\*****-Pro$\ProfileContainers (***** = Unique Company Code)
```

## 刪除連續波代理程式服務

連續波代理程式會在環境中的每部機器上執行。在環境中的每部VM上、應使用下列命令來解除安裝啟動此程序的服務。可跳過CWMGR1、因為大多數情況下會關閉並最終刪除該VM。理想情況下、此行動將透過指令碼自動化來執行。以下影片顯示手動完成。

```
C:\Program files\CloudWorkspace\CwAgent\CwAgent.exe -u
```

### 刪除連續波代理服務影片

 | <https://img.youtube.com/vi/I9ASmM5aap0/maxresdefault.jpg>

## 刪除連續波代理程式目錄

先前的解除安裝會移除啟動連續波代理程式的服務、但檔案仍會保留。刪除目錄：

```
"C:\Program Files\CloudWorkspace"
```

### 刪除連續波代理目錄影片

 | [https://img.youtube.com/vi/hMM\\_z4K2-il/maxresdefault.jpg](https://img.youtube.com/vi/hMM_z4K2-il/maxresdefault.jpg)

## 移除啟動捷徑

「啟動項目」目錄包含前一個步驟中刪除檔案的兩個捷徑。為了避免終端使用者出現錯誤訊息、應刪除這些檔案。

```
"C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\Pen.lnk"  
"C:\ProgramData\Microsoft\Windows\Start  
Menu\Programs\StartUp\CwRemoteApps.lnk"
```

移除開機捷徑影片

 | <https://img.youtube.com/vi/U0YLZ3Qfu9w/maxresdefault.jpg>

## 取消「使用者」與「公司」 GPO的連結

VDS實作了三個GPO。我們建議您取消連結其中兩個項目、然後檢閱第三個項目的內容。

取消連結：

- AADDC使用者>雲端工作空間公司
- AADDC使用者> Cloud Workspace使用者

檢視：

- AADDC電腦>雲端工作區電腦

取消「使用者」與「公司」 GPO的連結影片

 | <https://img.youtube.com/vi/cb68ri3HKUw/maxresdefault.jpg>

## 關閉CWMGR1

套用GPO變更之後、我們現在可以關閉CWMGR1 VM。一旦確認繼續使用AVD功能、此VM便可永久刪除。

在極少數情況下、如果另一個伺服器角色正在執行（例如 DC、FTP伺服器...）。在此情況下、可停用三項服務來停用CWMGR1上的VDS功能：

- 連續波代理程式（請參閱上述內容）
- 連續波自動化服務
- 連續波VM自動化

關閉CWMGR1視訊

 | [https://img.youtube.com/vi/avk9HyliC\\_s/maxresdefault.jpg](https://img.youtube.com/vi/avk9HyliC_s/maxresdefault.jpg)

## 刪除NetApp VDS服務帳戶

VDS使用的Azure AD服務帳戶可以移除。登入Azure Management Portal並刪除使用者：

- CloudWorkspaceSVC
- CloudWorkspaceCASvC

其他使用者帳戶可保留：

- 終端使用者
- Azure系統管理員
- TECH網域管理員

刪除**NetApp VDS**服務帳戶影片

 | [https://img.youtube.com/vi/\\_VToVNp49cg/maxresdefault.jpg](https://img.youtube.com/vi/_VToVNp49cg/maxresdefault.jpg)

刪除應用程式註冊

部署VDS時會進行兩次應用程式登錄。可以刪除：

- 雲端工作區API
- 雲端工作空間AVD

刪除應用程式註冊影片

 | <https://img.youtube.com/vi/iARz2nw1Oks/maxresdefault.jpg>

刪除企業應用程式

部署VDS時會部署兩個企業應用程式。可以刪除：

- 雲端工作區
- 雲端工作空間管理API

刪除企業應用程式影片

 | <https://img.youtube.com/vi/3eQzTPdIlWk/maxresdefault.jpg>

確認已停止**CWMGR1**

在測試終端使用者仍可連線之前、請確認已停止CWMGR1以進行實際測試。

確認**CWMGR1**已停止影片

 | <https://img.youtube.com/vi/Ux9nkDk5IU4/maxresdefault.jpg>

登入與終端使用者

若要確認成功、請以終端使用者身分登入、並確認功能是否維持正常。

登入與終端使用者影片

 | <https://img.youtube.com/vi/SuS-OTHJz7Y/maxresdefault.jpg>

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.