



## **Azure**

### **Virtual Desktop Service**

NetApp  
May 03, 2022

This PDF was generated from [https://docs.netapp.com/zh-tw/virtual-desktop-service/Deploying.Azure.AVD.Deploying\\_AVD\\_in\\_Azure.html](https://docs.netapp.com/zh-tw/virtual-desktop-service/Deploying.Azure.AVD.Deploying_AVD_in_Azure.html) on May 03, 2022. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# 目錄

Azure .....	1
Azure虛擬桌面 .....	1

## Azure 虛擬桌面

### AVD 部署指南

#### 總覽

本指南將提供逐步指示、說明如何使用 Azure 中的 NetApp 虛擬桌面服務 (VDS) 來建立 Azure 虛擬桌面 (AVD) 部署。

本指南的開頭為：<https://cwasetup.cloudworkspace.com/>

本概念驗證 (POC) 指南旨在協助您在自己的測試 Azure 訂閱中快速部署及設定 AVD。本指南假設將綠色現場部署至乾淨、非正式作業的 Azure Active Directory 租戶。

正式作業部署、尤其是現有 AD 或 Azure AD 環境、非常常見、但此流程不在本 POC 指南中考量。複雜的 POC 與正式作業部署應由 NetApp VDS 銷售/服務團隊啟動、而非以自助服務方式執行。

此 POC 文件將帶您瀏覽整個 AVD 部署、並提供 VDS 平台部署後組態的主要區域簡介。完成後、您將擁有完整部署且功能完善的 AVD 環境、並隨附主機集區、應用程式群組和使用者。您也可以選擇設定自動化應用程式交付、安全群組、檔案共用權限、Azure Cloud Backup、智慧型成本最佳化。VDS 透過 GPO 部署一組最佳實務做法設定。此外、如果您的 POC 不需要安全控制、也會隨附如何選擇性停用這些控制項的指示、類似於未受管理的本機裝置環境。

#### AVD 基礎知識

Azure Virtual Desktop 是一套全方位的桌面與應用程式虛擬化服務、可在雲端上執行。以下是一些主要特色與功能的快速清單：

- 平台服務、包括閘道、代理、授權及登入、並以 Microsoft 提供的服務形式提供。如此可將需要託管與管理的基礎架構降至最低。
- Azure Active Directory 可做為身分識別供應商使用、因此可分層提供額外的 Azure 安全服務、例如條件式存取。
- 使用者體驗 Microsoft 服務的單一登入體驗。
- 使用者工作階段透過專屬的反向連線技術連線至工作階段主機。這表示不需要開啟傳入連接埠、而是由代理程式建立並傳出連線至 AVD 管理層、進而連線至終端使用者裝置。
- 即使是反轉連線、也能讓虛擬機器在不受公共網際網路影響的情況下執行、即使在維持遠端連線的情況下、也能實現隔離的工作負載。
- AVD 可存取 Windows 10 多工作階段、讓 Windows 10 企業級使用者工作階段的效率更高。
- FSLogix 設定檔容器化技術包括：提升使用者工作階段效能、儲存效率、以及在非持續性環境中提升 Office 體驗。
- AVD 支援完整的桌面和 RemoteApp 存取。持續性或非持續性、以及專屬和多工作階段體驗。
- 因為 AVD 可以運用「每位使用者 Windows 10 Enterprise e3」來取代對 RDS CALS 的需求、並大幅降低 Azure 中工作階段主機 VM 的每小時成本、因此組織可以節省 Windows 授權成本。

## 指南範圍

本指南將從Azure和VDS管理員的觀點、引導您使用NetApp VDS技術來部署AVD。您將Azure租戶與訂閱的預先設定為零、本指南可協助您設定AVD端點對端點

本指南涵蓋下列步驟：

1. 確認Azure租戶、Azure訂閱及Azure管理員帳戶權限的先決條件
2. 收集必要的探索詳細資料
3. 使用專為Azure設定所設計的VDS精靈來建置Azure環境
4. 使用標準Windows 10 EVD映像建立第一個主機集區
5. 指派虛擬桌面給Azure AD使用者
6. 將使用者新增至預設的應用程式群組、以便將桌面環境提供給使用者。（可選） 建立額外的主機集區以提供RemoteApp服務
7. 透過用戶端軟體和/或Web用戶端以終端使用者身分連線
8. 以本機和網域管理員的身分連線至平台和用戶端服務
9. 選擇性地為VDS管理員& AVD終端使用者啟用VDS的多因素驗證
10. 您也可以選擇逐步瀏覽整個應用程式權利工作流程、包括填入應用程式程式庫、應用程式安裝自動化、使用者和安全性群組的應用程式遮罩
11. 您也可以依群組建立及管理Active Directory安全性群組、資料夾權限及應用程式權利。
12. 選擇性地設定成本最佳化技術、包括工作負載排程和即時擴充
13. （可選） 建立、更新及SysPrep虛擬機器映像、以供未來部署之用
14. 可選擇設定Azure Cloud Backup
15. 選擇性停用預設的安全性控制群組原則

## Azure必備條件

VDS使用原生Azure安全性內容來部署AVD執行個體。在啟動VDS安裝精靈之前、需要先建立幾項Azure先決條件。

在部署期間、服務帳戶和權限會透過驗證Azure租戶內現有的管理帳戶、授予VDS。

快速先決條件檢查清單

- Azure租戶搭配Azure AD執行個體（可為Microsoft 365執行個體）
- Azure訂閱
- Azure虛擬機器可用的Azure配額
- 具備全域管理員和訂閱所有權角色的Azure管理帳戶



詳細的先決條件記錄於 ["本PDF"](#)

## Azure AD的Azure管理員

此現有Azure管理員必須是目標租戶中的Azure AD帳戶。Windows Server AD帳戶可透過VDS安裝程式部署、但

需要執行其他步驟才能設定與Azure AD的同步（本指南超出範圍）

您可在Azure Management Portal的「Users」（使用者）>「All Users」（所有使用者）下找到使用者帳戶、以確認此情況。[]

#### 全域系統管理員角色

Azure系統管理員必須被指派Azure租戶的全域系統管理員角色。

若要檢查您在**Azure AD**中的角色、請依照下列步驟操作：

1. 請登入Azure Portal、網址為：<https://portal.azure.com/>
2. 搜尋並選取Azure Active Directory
3. 在右側的下一個窗格中、按一下「管理」區段中的「使用者」選項
4. 按一下您要檢查的管理員使用者名稱
5. 按一下「目錄角色」。在最右窗格中、應列出「全域管理員」角色[]

如果此使用者沒有全域管理員角色、您可以執行下列步驟來新增（請注意、登入帳戶必須是全域管理員才能執行這些步驟）：

1. 在上述步驟5的「使用者目錄角色詳細資料」頁面中、按一下「詳細資料」頁面頂端的「新增指派」按鈕。
2. 按一下角色清單中的全域管理員。按一下「新增」按鈕。[]

#### Azure訂購所有權

Azure管理員也必須是訂閱中包含部署的訂閱擁有者。

若要檢查管理員是否為訂閱擁有者、請依照下列步驟操作：

1. 請登入Azure Portal、網址為：<https://portal.azure.com/>
2. 搜尋、然後選取「訂閱」
3. 在右側的下一個窗格中、按一下訂閱名稱以查看訂閱詳細資料
4. 按一下左側窗格中的存取控制（IAM）功能表項目
5. 按一下「角色指派」索引標籤。Azure管理員應列在「擁有者」區段中。[]

如果未列出**Azure Administrator**、您可以依照下列步驟將帳戶新增為訂閱擁有者：

1. 按一下頁面頂端的「Add（新增）」按鈕、然後選擇「Add role Assignment（新增角色指派）」選項
2. 右側會出現一個對話方塊。在「角色」下拉式清單中選擇「擁有者」、然後在「選取」方塊中輸入管理員的使用者名稱。系統管理員的全名出現時、請選取該名稱
3. 按一下對話方塊底部的「Save（儲存）」按鈕[]

#### Azure運算核心配額

CWA設定精靈和VDS入口網站將會建立新的虛擬機器、Azure訂閱必須有可用的配額才能成功執行。

若要檢查配額、請執行下列步驟：

1. 瀏覽至「訂閱」模組、然後按一下「使用量+配額」
2. 在「供應商」下拉式清單中選取所有供應商、然後在「供應商」下拉式清單中選取「Microsoft.Compute」

3. 在「Locations」（位置）下拉式清單中選取目標區域
4. 應顯示虛擬機器系列可用配額的清單[]如果您需要增加配額、請按一下「Request add（申請增加）」、然後依照提示新增額外容量。針對初始部署、特別要求「Standard DSv3 Family vCPU」的報價增加

收集探索詳細資料

完成「CWA設定精靈」之後、需要回答幾個問題。NetApp VDS已提供連結的PDF、可在部署前用於記錄這些選擇。項目包括：

項目	說明
VDS管理認證	如果您已經擁有現有的VDS管理認證、請收集這些認證資料。否則在部署期間會建立新的管理帳戶。
Azure區域	根據服務的效能與可用度來判斷目標Azure區域。這 " <a href="#">Microsoft工具</a> " 可根據所在地區預估終端使用者體驗。
Active Directory類型	VM需要加入網域、但無法直接加入Azure AD。VDS部署可建置新的虛擬機器或使用現有的網域控制器。
檔案管理	效能高度仰賴磁碟速度、尤其是與使用者設定檔儲存有關的速度。VDS安裝精靈可部署簡單的檔案伺服器或設定Azure NetApp Files 功能（ANF）。對於幾乎任何正式作業環境、建議使用POC、但檔案伺服器選項可提供足夠的效能。您可以在部署後修改儲存選項、包括使用Azure中現有的儲存資源。如需詳細資訊、請參閱ANF定價： <a href="https://azure.microsoft.com/en-us/pricing/details/netapp/">https://azure.microsoft.com/en-us/pricing/details/netapp/</a>
虛擬網路範圍	部署需要可路由的/20網路範圍。VDS安裝精靈可讓您定義此範圍。此範圍必須與Azure中或內部部署的任何現有VNets不重疊（如果兩個網路將透過VPN或ExpressRoute連線）。

## VDS設定區段

登入 <https://cwasetup.cloudworkspace.com/> 您可以在「必要條件」一節中找到Azure管理員認證。

IaaS與平台

[]

## Azure AD網域名稱

Azure AD網域名稱由所選租戶繼承。

位置

請選擇適當的「\*\* Azure區域」。這 "[Microsoft工具](#)" 可根據所在地區預估終端使用者體驗。

## Active Directory類型

VDS可以配置一個用於域控制器功能的\*\*新虛擬機\*或用於設置以利用現有的域控制器。在本指南中、我們將選取「New Windows Server Active Directory（新Windows Server Active Directory）」、這會根據訂閱內容建立一或兩個VM（根據在此程序中所做的選擇）。

您可在本文中找到有關現有AD部署的詳細資訊 "[請按這裡](#)"。

## Active Directory 網域名稱

輸入一個\*網域名稱。建議從上述位置鏡射Azure AD網域名稱。

## 檔案管理

VDS可配置簡單的檔案伺服器虛擬機器、或是設定Azure NetApp Files 及設定功能。在正式作業中、Microsoft建議每位使用者分配30GB、我們發現每位使用者需要分配5-15 IOPS、才能獲得最佳效能。

在POC（非正式作業）環境中、檔案伺服器是一種低成本且簡單的部署選項、不過Azure託管磁碟的可用效能可能會因小型正式作業部署的IOPS消耗而無法負荷。

例如、4TB標準固態硬碟可支援高達500 IOPS、最多只能支援每位使用者5 IOPS的100位使用者。使用ANF Premium、相同大小的儲存設備設定將可支援16、000 IOPS、並可增加32倍的IOPS。

針對正式作業AVD部署、\* Azure NetApp Files 《Microsoft推薦》\*。



您想要部署的訂閱需要提供協助、請聯絡您的NetApp客戶代表或使用此連結：Azure NetApp Files <https://aka.ms/azurenetafiles>

您也必須將NetApp註冊為訂閱的供應商。您可以執行下列動作來完成此作業：

- 瀏覽至Azure入口網站中的「訂閱」
  - 按一下資源提供者
  - NetApp篩選工具
  - 選取供應商、然後按一下「Register（註冊）」

## RDS授權編號

NetApp VDS可用於部署RDS和/或AVD環境。部署AVD時、此欄位可以\*保留空白\*。

## ThinstPrint

NetApp VDS可用於部署RDS和/或AVD環境。部署AVD時、此切換可維持為「關機」（左切換）。

## 通知電子郵件

VDS會將部署通知和持續的健全狀況報告傳送至提供的\*\*電子郵件。稍後可以變更。

## VM與網路

為了支援VDS環境、需要執行各種服務、這些服務統稱為「VDS平台」。視組態而定、可能包括CWMGR、一或兩個RDS閘道、一或兩個HTML5閘道、一個FTPS伺服器、以及一或兩個Active Directory VM。

大多數的AVD部署都採用單一虛擬機器選項、因為Microsoft將AVD閘道當作PaaS服務來管理。

對於將納入RDS使用案例的較小和較簡單環境、所有這些服務都可精簡為單一虛擬機器選項、以降低VM成本（擴充性有限）。對於使用超過100位使用者的RDS使用案例、建議使用「多個虛擬機器」選項、以利RDS和（或）HTML5閘道擴充性[]

## 平台VM組態

NetApp VDS可用於部署RDS和/或AVD環境。部署AVD時、建議選擇單一虛擬機器。對於RDS部署、您需要部署和管理其他元件、例如代理商和閘道、在正式作業中、這些服務應在專用和備援的虛擬機器上執行。對於AVD、所有這些服務均由Azure以隨附服務的形式提供、因此建議使用\*單一虛擬機器\*組態。

### 單一虛擬機器

這是專屬使用AVD（而非RDS或兩者組合）的部署建議選項。在單一虛擬機器部署中、Azure中的單一VM上都會裝載下列角色：

- 連續波管理程式
- HTML5閘道
- RDS閘道
- 遠端應用程式
- FTPS伺服器（選用）
- 網域控制器角色

此組態中RDS使用案例的建議使用者人數上限為100位使用者。負載平衡RS/HTML5閘道並非此組態的選項、可限制未來擴充規模的備援和選項。同樣地、此限制也不適用於AVD部署、因為Microsoft將閘道管理為PaaS服務。



如果此環境是針對多租戶設計、則不支援單一虛擬機器組態、也不支援AVD或AD Connect。

### 多個虛擬機器

將VDS平台分割成多個虛擬機器時、下列角色會裝載在Azure中的專屬VM上：

- 遠端桌面閘道

VDS設定可用於部署及設定一或兩個RDS閘道。這些閘道會將RDS使用者工作階段從開放式網際網路轉送到部署中的工作階段主機VM。RDS閘道可處理重要功能、保護RDS免受來自開放式網際網路的直接攻擊、並加密環境中進出的所有RDS流量。選取兩個遠端桌面閘道時、VDS安裝程式會部署2個VM、並將其設定為在傳入的RDS使用者工作階段之間取得負載平衡。

- HTML5閘道

VDS設定可用於部署及設定一或兩個HTML5閘道。這些閘道主控VDS中的\_Connect to Server\_功能和Web型VDS用戶端（H5 Portal）所使用的HTML5服務。選取兩個HTML5入口網站時、VDS安裝程式會部署2個VM、並將其設定為在傳入的HTML5使用者工作階段之間進行負載平衡。



使用多個伺服器選項時（即使使用者只能透過安裝的VDS用戶端連線）、強烈建議至少使用一個HTML5閘道、以從VDS啟用\_Connect to Server\_功能。

- 閘道擴充性附註

在RDS使用案例中、環境的最大大小可隨著額外的閘道VM一起橫向擴充、每個RDS或HTML5閘道可支援約500位使用者。稍後可透過最少的NetApp專業服務協助來新增其他閘道



如果此環境是針對多租戶設計、則需要選擇多個虛擬機器。

## 時區

雖然終端使用者的體驗會反映其當地時區、但仍需選取預設時區。從執行環境的\*\*主要管理\*的時區中選取。

## 虛擬網路範圍

根據虛擬機器的用途、將虛擬機器隔離到不同子網路是最佳做法。首先、定義網路範圍並新增/20範圍。

VDS安裝程式會偵測並建議一個範圍、以證明其成功。根據最佳實務做法、子網路IP位址必須屬於私有IP位址範圍。

這些範圍包括：

- 從192到168、255、168、0到255
- 從172.16.0.0到172.31.255
- 10.0.0.0到10.255.255.255

視需要檢閱及調整、然後按一下「驗證」以識別下列各項的子網路：

- 租戶：這是工作階段主機伺服器和資料庫伺服器所在的範圍
- 服務：這是PaaS服務（如Azure NetApp Files NetApp）的範圍
- 平台：這是平台伺服器所在的範圍
- 目錄：這是AD伺服器所在的範圍

## 檢閱

最後一頁提供檢閱您選擇的機會。完成審查後、請按一下「驗證」按鈕。VDS安裝程式會檢查所有項目、並確認部署作業可以繼續執行所提供的資訊。此驗證可能需要2到10分鐘的時間。若要追蹤進度、您可以按一下記錄標誌（右上角）來查看驗證活動。

驗證完成後、綠色資源配置按鈕會顯示取代「驗證」按鈕。按一下「資源配置」以開始部署的資源配置程序。

## 狀態

根據Azure工作負載和您所做的選擇、資源配置程序需時2-4小時。您可以按一下「Status（狀態）」頁面來追蹤記錄中的進度、或等待電子郵件通知您部署程序已完成。部署會建置虛擬機器和Azure元件、以支援VDS和遠端桌面或AVD實作。這包括可同時做為遠端桌面工作階段主機和檔案伺服器的單一虛擬機器。在AVD實作中、此虛擬機器只會做為檔案伺服器。

## 安裝及設定AD Connect

安裝成功之後、必須立即在網域控制器上安裝和設定AD Connect。在single平台VM設定中、CWMGR1機器是DC。AD中的使用者必須在Azure AD與本機網域之間同步。

若要安裝及設定AD Connect、請遵循下列步驟：

1. 以網域管理員的身分連線至網域控制器。
  - a. 從Azure Key Vault取得認證（請參閱 ["此處提供重要的Vault說明"](#)）

## 2. 安裝AD Connect、以網域管理員（具備企業管理員角色權限）和Azure AD Global Admin登入

### 啟動AVD服務

部署完成後、下一步是啟用AVD功能。AVD啟用程序要求Azure管理員執行數個步驟、註冊Azure AD網域並訂閱使用Azure AVD服務的存取權。同樣地、Microsoft也要求VDS針對Azure中的自動化應用程式要求相同的權限。以下步驟將引導您完成此程序。

### 建立AVD主機集區

終端使用者對AVD虛擬機器的存取權由主機集區管理、其中包含虛擬機器和應用程式群組、而這些群組又包含使用者和使用者存取類型。

#### 建置第一個主機集區

1. 按一下AVD主機資源池區段標題右側的「Add（新增）」按鈕。[]
2. 輸入主機集區的名稱和說明。
3. 選擇主機集區類型
  - a. 「共享的」\*表示多位使用者將會使用安裝相同應用程式的相同虛擬機器集區來存取。
  - b. \*\*個人化\*會建立一個主機集區、將使用者指派給自己的工作階段主機VM。
4. 選取負載平衡器類型
  - a. 在從集區中的第二部虛擬機器開始之前、先將第一部共享虛擬機器填入最大使用者數\*
  - b. 首先是「廣度」\*會以循環配置資源池中的所有虛擬機器來分配使用者
5. 選取Azure虛擬機器範本、以在此資源池中建立虛擬機器。雖然VDS會顯示訂閱中所有可用的範本、但我們建議您選擇最新的Windows 10多使用者建置、以獲得最佳體驗。目前的建置版本是Windows - 10-20h1-EVD。（您也可以使用資源配置收集功能、建立黃金映像、從自訂虛擬機器映像建置主機）
6. 選取Azure機器尺寸。出於評估目的、NetApp建議使用D系列（多位使用者適用的標準機器類型）或E系列（針對較重負載的多位使用者案例、提供增強的記憶體組態）。如果您想要嘗試不同的系列和大小、可以在VDS稍後變更機器大小
7. 從下拉式清單中、為虛擬機器的託管磁碟執行個體選取相容的儲存類型
8. 選取要在建立主機集區程序中建立的虛擬機器數量。您可以稍後將虛擬機器新增至集區、但VDS會建置您要求的虛擬機器數量、並在建立後將其新增至主機集區
9. 按一下「新增主機集區」按鈕、開始建立程序。您可以在AVD頁面上追蹤進度、也可以在「工作」區段的「部署/部署名稱」頁面上查看程序記錄的詳細資料
10. 建立主機集區之後、它就會出現在AVD頁面的主機集區清單中。按一下主機集區的名稱即可查看其詳細資料頁面、其中包含其虛擬機器、應用程式群組和作用中使用者的清單



VDS中的AVD主機是以不允許使用者工作階段連線的設定所建立。這是為了允許在接受使用者連線之前進行自訂。您可以編輯工作階段主機的設定來變更此設定。 []

### 為使用者啟用VDS桌面

如上所述、VDS會在部署期間建立支援終端使用者工作區所需的所有元素。部署完成後、下一步是為您想要導入AVD環境的每個使用者啟用工作區存取。此步驟會建立設定檔組態、並建立虛擬桌面預設的終端使用者資料層存取。VDS會重新使用此組態、將Azure AD終端使用者連結至AVD應用程式集區。

若要為終端使用者啟用工作區、請執行下列步驟：

1. 登入VDS、網址為 <https://manage.cloudworkspace.com> 使用您在資源配置期間建立的VDS主要系統管理員帳戶。如果您不記得您的帳戶資訊、請聯絡NetApp VDS以取得擷取資訊的協助
2. 按一下「工作區」功能表項目、然後按一下資源配置期間自動建立的工作區名稱
3. 按一下「Users and Groups（使用者和群組）」索引標[]
4. 針對您要啟用的每位使用者、捲動使用者名稱、然後按一下Gear圖示
5. 選擇「啟用雲端工作區」選項[]
6. 完成啟用程序大約需要30到90秒的時間。請注意、使用者狀態將從「Pending（擱置）」變更為「Available（可用）」



啟動Azure AD網域服務會在Azure中建立託管網域、並將所建立的每部AVD虛擬機器加入該網域。為了讓傳統登入虛擬機器正常運作、Azure AD使用者的密碼雜湊必須同步、才能支援NTLM和Kerberos驗證。若要完成此工作、最簡單的方法就是變更Office.com或Azure入口網站中的使用者密碼、這會強制進行密碼雜湊同步。網域服務伺服器的同步週期最多可能需要20分鐘。

#### 啟用使用者工作階段

依預設、工作階段主機無法接受使用者連線。此設定通常稱為「排卸模式」、因為它可用於正式作業、以防止新的使用者工作階段、讓主機最終移除所有的使用者工作階段。當主機上允許新的使用者工作階段時、此動作通常稱為「將工作階段主機設為「輪替」」。

在正式作業環境中、以排卸模式啟動新的主機是很合理的做法、因為在主機準備好處理正式作業工作負載之前、通常需要先完成一些組態工作。

在測試與評估中、您可以立即將主機移出耗盡模式、以啟用使用者連線並確認功能。若要在工作階段主機上啟用使用者工作階段、請執行下列步驟：

1. 瀏覽至工作區頁面的AVD區段。
2. 按一下「AVD主機集區」下的主機集區名稱。[]
3. 按一下工作階段主機的名稱、然後勾選「允許新工作階段」方塊、再按一下「更新工作階段主機」。針對所有需要輪調的主機重複上述步驟。[]
4. 每個主機行項目的AVD主頁上也會顯示目前的「允許新工作階段」統計資料。

#### 預設應用程式群組

請注意、桌面應用程式群組預設是在主機集區建立程序中建立的。此群組提供所有群組成員的互動式桌面存取。若要新增成員至群組：

1. 按一下應用程式群組的名稱[]
2. 按一下顯示已新增使用者數量的連結[]
3. 勾選要新增至應用程式群組的使用者名稱旁的方塊、即可選取該使用者
4. 按一下「選取使用者」按鈕
5. 按一下「更新應用程式群組」按鈕

## 建立其他AVD應用程式群組

您可以將其他應用程式群組新增至主機集區。這些應用程式群組會使用RemoteApp、將特定應用程式從主機集區虛擬機器發佈給應用程式群組使用者。



AVD只允許終端使用者指派至桌面應用程式群組類型或RemoteApp Group類型、但不允許兩者同時指派至同一個主機集區、因此請務必根據個別情況來分隔使用者。如果使用者需要存取桌面和串流應用程式、則需要第二個主機集區來裝載應用程式。

若要建立新的應用程式群組：

1. 按一下「應用程式群組」區段標題中的「新增」按鈕[]
2. 輸入應用程式群組的名稱和說明
3. 按一下「Add Users（新增使用者）」連結、選取要新增至群組的使用者。按一下每個使用者名稱旁的核取方塊、然後按一下「Select Users（選取使用者）」按鈕、即可選取每個使用者[]
4. 按一下「新增RemoteApps」連結、將應用程式新增至此應用程式群組。AVD會掃描安裝在虛擬機器上的應用程式清單、自動產生可能的應用程式清單。按一下應用程式名稱旁的核取方塊、選取應用程式、然後按一下「選取RemoteApps」按鈕。[]
5. 按一下「新增應用程式群組」按鈕以建立應用程式群組

## 終端使用者AVD存取

終端使用者可以使用Web Client或安裝在各種平台上的用戶端來存取AVD環境

- 網路用戶端：<https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-web>
- 網路用戶端登入URL：<http://aka.ms/AVDweb>
- Windows用戶端：<https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-windows-7-and-10>
- Android用戶端：<https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-android>
- MacOS用戶端：<https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-macos>
- IOS用戶端：<https://docs.microsoft.com/en-us/azure/virtual-desktop/connect-ios>
- IGEL精簡型用戶端：<https://www.igel.com/igel-solution-family/windows-virtual-desktop/>

使用終端使用者使用者名稱和密碼登入。請注意、遠端應用程式和桌面連線（RADC）、遠端桌面連線（mstsc）和CloudWorkspacce Client for Windows應用程式目前不支援登入AVD執行個體的功能。

## 監控使用者登入

主機資源池詳細資料頁面也會在使用者登入AVD工作階段時顯示使用中使用者的清單。

## 管理連線選項

VDS Admins可透過多種方式連線至環境中的虛擬機器。

## 連線至伺服器

在整個入口網站中，VDS系統管理員會找到「連線到伺服器」選項。依預設、此功能會動態產生本機管理認證、並將其注入Web用戶端連線、藉此將管理員連線至虛擬機器。管理員不需要知道（也從未獲得）認證資料即可進行連線。

此預設行為可依個別管理員為單位停用、如下一節所述。

#### **.tech /第3級系統管理帳戶**

在CWA設定程序中、已建立「層級III」管理帳戶。[使用者名稱格式為username.tech@domain.xyz](#)

這些帳戶通常稱為「.tech」帳戶、稱為網域層級的系統管理員帳戶。VDS管理員可以在連線至CWMGR1（平台）伺服器時使用其.tech帳戶、也可以在連線至環境中的所有其他虛擬機器時選用。

若要停用自動本機管理員登入功能、並強制使用等級III帳戶、請變更此設定。瀏覽至VDS > Admins > Admin Name > Check "Tech Account Enabled"。核取此方塊後、VDS管理員將不會自動以本機管理員的身分登入虛擬機器、而是會被提示輸入其.tech認證。

這些認證資料及其他相關認證資料會自動儲存在\_Azure Key Vault\_、並可從Azure管理入口網站存取、網址為：<https://portal.azure.com/>。

#### **可選的部署後行動**

##### **多因素驗證（MFA）**

NetApp VDS包括免費的SMS/電子郵件MFA。此功能可用於保護VDS管理帳戶和（或）終端使用者帳戶的安全。["MFA文章"](#)

##### **應用程式應有權利工作流程**

VDS提供一種機制、可讓終端使用者從預先定義的應用程式清單（稱為「應用程式目錄」）指派應用程式存取權。應用程式目錄涵蓋所有託管部署。



自動部署的TSD1伺服器必須維持原位、才能支援應用程式應有權利。具體而言、請勿針對此虛擬機器執行「轉換成資料」功能。

應用程式管理詳述於本文：[""](#)

#### **Azure AD安全性群組**

VDS包括建立、填入及刪除Azure AD安全性群組所支援的使用者群組的功能。這些群組可在VDS以外使用、如同其他任何安全性群組一樣。在VDS中、這些群組可用來指派資料夾權限和應用程式權利。

#### **建立使用者群組**

建立使用者群組是在工作區的「使用者與群組」索引標籤上執行。

#### **依群組指派資料夾權限**

可將檢視及編輯公司共用資料夾的權限指派給使用者或群組。

[""](#)

#### **依群組指派應用程式**

除了將應用程式個別指派給使用者之外、應用程式也可以配置給群組。



1. 瀏覽至使用者與群組詳細資料。[]
2. 新增群組或編輯現有群組。[]
3. 將使用者和應用程式指派給群組。[]

#### 設定成本最佳化選項

工作區管理也延伸到管理支援AVD實作的Azure資源。VDS可讓您設定工作負載排程和即時擴充、根據終端使用者活動來開啟和關閉Azure虛擬機器。這些功能可讓Azure資源使用率和支出與終端使用者的實際使用模式相符。此外、如果您已設定概念驗證AVD實作、則可從VDS介面來轉用整個部署。

#### 工作負載排程

「工作負載排程」功能可讓管理員建立工作區虛擬機器的設定排程、以支援終端使用者工作階段。當排程時間週期的結束時間達到一週中的特定日期時、VDS會停止/取消分配Azure中的虛擬機器、以便停止每小時的收費。

若要啟用工作負載排程：

1. 登入VDS、網址為 <https://manage.cloudworkspace.com> 使用VDS認證。
2. 按一下「工作區」功能表項目、然後按一下清單中的「工作區」名稱。[]
3. 按一下工作負載排程索引標籤。[]
4. 按一下工作負載排程標頭中的管理連結。[]
5. 從「Status（狀態）」下拉式清單中選擇預設狀態：「Always On（永遠開啟）」（預設）、「Always Off（永遠關閉）」或「scheduled（排程）」
6. 如果您選擇「排程」、「排程」選項包括：
  - a. 每天以指定的時間間隔執行。此選項會將排程設定為一週七天的相同開始時間和結束時間。[]
  - b. 在指定的時間間隔內執行。此選項會將排程設定為同一「開始時間綁定」和「結束時間」、僅適用於一週中所選的日期。未選取的一週天數將導致VDS在這些天內無法開啟虛擬機器。[]
  - c. 以不同的時間間隔和天數執行。此選項會將所選日期的排程設定為不同的開始時間和結束時間。[]
  - d. 完成排程設定後、請按一下「更新排程」按鈕。[]

#### 即時擴充

即時擴充功能會根據並行使用者負載、自動開啟或關閉共用主機集區中的虛擬機器。當每部伺服器都滿時、會開啟另一部伺服器、以便在主機集區負載平衡器傳送使用者工作階段要求時就緒。若要有效使用即時擴充、請選擇「深度優先」作為負載平衡器類型。

若要啟用即時擴充：

1. 登入VDS、網址為 <https://manage.cloudworkspace.com> 使用VDS認證。
2. 按一下「工作區」功能表項目、然後按一下清單中的「工作區」名稱。[]
3. 按一下工作負載排程索引標籤。[]
4. 按一下「Live Scaling（即時縮放）」區段中的「啟用」選項按鈕 []
5. 按一下「每個伺服器的使用者人數上限」、然後輸入最大數目。視虛擬機器大小而定、此數字通常介於4到20之間。[]
6. 選用：按一下「啟用額外的已開啟電源的伺服器」、然後輸入您要用於主機集區的其他伺服器數量。此設定

會啟動指定數量的伺服器、以及作用中填滿伺服器、做為大型使用者群組在同一個時間範圍內登入的緩衝區。



目前「即時擴充」適用於所有共用資源集區。在不久的將來、每個資源池都會有獨立的「即時擴充」選項。

## 關閉整個部署

如果您只打算偶爾在非正式作業的基礎上使用評估部署、則可以在不使用時關閉部署中的所有虛擬機器。

若要開啟或關閉部署（亦即關閉部署中的虛擬機器）、請遵循下列步驟：

1. 登入VDS、網址為 <https://manage.cloudworkspace.com> 使用VDS認證。
2. 按一下「部署」功能表項目。[]將游標捲動到目標部署的行上、以顯示組態檔圖示。[]
3. 按一下齒輪、然後選擇「停止」。[]
4. 若要重新啟動或啟動、請遵循步驟1-3、然後選擇「開始」。[]



部署中的所有虛擬機器可能需要幾分鐘的時間才能停止或啟動。

## 建立及管理VM映像

VDS包含建立及管理虛擬機器映像以供未來部署的功能。若要使用此功能、請瀏覽至：VDS > 「部署」 > 「部署名稱」 > 「資源配置集合」。以下是「VDI Image Collection」功能的說明文件：

## 設定Azure Cloud Backup Service

VDS可原生設定及管理Azure Cloud Backup、這是一項用於備份虛擬機器的Azure PaaS服務。備份原則可依類型或主機集區指派給個別的機器或機器群組。詳情請參閱：

## 選取應用程式管理/原則模式

根據預設、VDS會實作多個群組原則物件（GPO）、以鎖定終端使用者工作區。這些原則會防止存取核心資料層位置（例如：C:\）、也無法以終端使用者的身分執行應用程式安裝。

此評估旨在展示Windows Virtual Desktop的功能、因此您可以選擇移除GPO、以便實作「基本工作區」、提供與實體工作區相同的功能和存取權。若要這麼做、請依照「基本工作區」選項中的步驟進行。

您也可以選擇使用完整的虛擬桌面管理功能集來實作「受控工作區」。這些步驟包括建立及管理終端使用者應用程式權利的應用程式目錄、以及使用管理員層級權限來管理對應用程式和資料夾的存取。請依照「受控工作區」一節中的步驟、在AVD主機集區上實作此類型的工作區。

## 管制AVD工作區（預設原則）

使用受控制的工作區是VDS部署的預設模式。原則會自動套用。此模式需要VDS管理員安裝應用程式、然後使用者透過工作階段桌面上的捷徑獲得應用程式存取權。以類似方式、建立對應的共用資料夾並設定權限、只查看對應的磁碟機代號、而非標準開機和（或）資料磁碟機、即可將資料資料夾的存取權指派給終端使用者。若要管理此環境、請依照下列步驟安裝應用程式並提供終端使用者存取權。

## 回復至基本AVD工作區

若要建立基本工作區、必須停用預設建立的預設GPO原則。

若要這麼做、請遵循以下一次性程序：

1. 登入VDS、網址為 <https://manage.cloudworkspace.com> 使用主要管理員認證資料。
2. 按一下左側的「部署」功能表項目。 []
3. 按一下您的部署名稱。 []
4. 在「Platform Servers（平台伺服器）」區段（右側中間頁面）下、捲動至WMGR1行的右側、直到顯示該檔位。 []
5. 按一下齒輪、然後選擇「Connect（連線）」。 []
6. 輸入您在資源配置期間建立的「技術」認證、以使用HTML5存取功能登入CWMGR1伺服器。 []
7. 按一下「Start（Windows）（開始（Windows））」功能表、然後選擇「Windows管理工具」。 []
8. 按一下「群組原則管理」圖示。 []
9. 按一下左窗格清單中的AADDC使用者項目。 []
10. 在右窗格清單中的「Cloud Workspace Users」原則上按一下滑鼠右鍵、然後取消選取「Link Enabled」（啟用連結）選項。按一下「確定」以確認此動作。 [] []
11. 從功能表中選取「行動」、「群組原則更新」、然後確認您要在這些電腦上強制更新原則。 []
12. 重複步驟9和10、但選取「AADDC使用者」和「Cloud Workspace公司」作為原則、以停用連結。在此步驟之後、您不需要強制進行群組原則更新。 [] []
13. 關閉「群組原則管理」編輯器和「系統管理工具」視窗、然後登出。 []這些步驟將為終端使用者提供基本的工作區環境。若要確認、請以終端使用者帳戶的身分登入：工作階段環境不應有任何受控制的工作區限制、例如隱藏的「開始」功能表、鎖定C:\磁碟機存取權、以及隱藏的「控制台」。



在部署期間建立的.tech帳戶可以完整存取、以便在獨立於VDS的資料夾上安裝應用程式並變更安全性。不過、如果您想要Azure AD網域的終端使用者擁有類似的完整存取權、您應該將他們新增至每個虛擬機器的本機「系統管理員」群組。

## AVD部署指南-現有的AD補充程式

### 總覽

VDS安裝程式能夠將新部署連線至現有的AD結構。這些指示將詳細說明該選項。本文並不獨立、而是詳細說明中所述的「新增AD」選項 "[AVD部署指南](#)"

### Active Directory類型

下一節定義VDS部署的Active Directory部署類型。在本指南中、我們將選擇現有的Windows Server Active Directory、以運用現有的AD架構。

### 現有的AD網路

VDS安裝程式會顯示VNets清單、以代表現有AD結構與Azure AD之間的連線。您選擇的vNet應具備您在Azure中設定的Azure代管DC。此外、vNet也會將自訂DNS設定指向Azure代管的DC。



## 現有Active Directory網域名稱

輸入要使用的現有網域名稱。附註：您不想使用Azure Portal Active Directory模組下的網域、因為它可能會造成DNS問題。其中的主要範例是使用者無法從桌面內部存取該網站（例如、<您的網域>.com）。

## 現有的AD使用者名稱和密碼

有三種方法可以提供必要的認證資料、以便使用現有的AD架構進行部署。

### 1. 提供Active Directory網域管理使用者名稱和密碼

這是最簡單的方法、提供用於協助部署的網域管理認證。



此帳戶可以一次性建立、一旦部署程序完成、就會被刪除。

### 2. 建立符合所需權限的帳戶

此方法需要客戶管理員在此手動建立權限結構、然後在此輸入CloudWorkspaceSVC帳戶的認證資料、然後繼續進行。

### 3. 手動部署程序

請聯絡NetApp VDS支援部門、以協助設定具有最低權限帳戶主體的AD存取。

## 後續步驟

本文說明部署至現有AD環境的獨特步驟。完成這些步驟之後、您可以返回標準部署指南 ["請按這裡"](#)。

## VDS元件與權限

### AVD與VDS安全實體與服務

Azure Virtual Desktop (AVD) 需要Azure AD和本機Active Directory中的安全帳戶和元件、才能執行自動化動作。NetApp的虛擬桌面服務 (VDS) 會在部署程序期間建立元件和安全性設定、讓系統管理員能夠控制AVD環境。本文件說明兩種環境中的相關VDS帳戶、元件及安全性設定。

部署自動化程序的元件和權限大多與最終部署環境的元件不同。因此本文分為部署自動化區段和部署環境區段兩個主要區段。

[寬=75%]

### AVD部署自動化元件與權限

VDS部署運用多個Azure和NetApp元件及安全權限來實作部署和工作區。

### VDS部署服務

## 企業應用程式

VDS利用租戶Azure AD網域中的企業應用程式與應用程式登錄。企業應用程式是針對Azure資源管理程式、Azure圖表的通話管道、以及（如果使用AVD Fall版本）Azure AD執行個體安全性內容的AVD API端點、其委派的角色和權限會授予相關的服務主體。根據租戶透過VDS初始化AVD服務的狀態、可能會建立應用程式登錄。

為了能夠建立及管理這些VM、VDS在Azure訂閱中建立多個支援元件：

### 雲端工作區

這是企業應用程式管理員在VDS安裝精靈的部署程序期間所授予及使用的初始Enterprise應用程式管理員。

Cloud Workspace企業應用程式會在VDS安裝程序期間要求一組特定權限。這些權限包括：

- 以登入使用者身分存取目錄（委派）
- 讀寫目錄資料（委派）
- 登入並讀取使用者設定檔（委派）
- 登入（委派）使用者
- 檢視使用者的基本設定檔（委派）
- 以組織使用者身分存取Azure服務管理（委派）

### 雲端工作區API

處理Azure PaaS功能的一般管理需求。Azure PaaS功能的範例包括Azure運算、Azure備份、Azure檔案等。本服務負責人在初始部署期間必須擁有目標Azure訂閱的擁有者權利、以及持續管理的貢獻者權利（附註：使用Azure檔案需要訂閱擁有者權限、才能針對Azure檔案物件設定每個使用者權限）。

Cloud Workspace API Enterprise應用程式會在VDS安裝程序期間要求一組特定權限。這些權限包括：

- 訂閱參與者（若使用Azure檔案則為訂閱擁有者）
- Azure AD圖表
  - 讀寫所有應用程式（應用程式）
  - 管理本應用程式所建立或擁有的應用程式（應用程式）
  - 讀寫裝置（應用程式）
  - 以登入使用者身分存取目錄（委派）
  - 讀取目錄資料（應用程式）
  - 讀取目錄資料（委派）
  - 讀寫目錄資料（應用程式）
  - 讀寫目錄資料（委派）
  - 讀寫網域（應用程式）
  - 讀取所有群組（委派）
  - 讀寫所有群組（委派）

- 讀取所有隱藏的成員資格（應用程式）
- 讀取隱藏成員資格（委派）
- 登入並讀取使用者設定檔（委派）
- 讀取所有使用者的完整設定檔（委派）
- 讀取所有使用者的基本設定檔（委派）
- Azure服務管理
  - 以組織使用者身分存取Azure服務管理（委派）

## NetApp VDS

NetApp VDS元件可透過VDS控制面板來自動化AVD角色、服務和資源的部署與組態。

### 自訂角色

自動化貢獻者角色是透過權限最低的方法來協助部署。此角色可讓CWMGR1 VM存取Azure自動化帳戶。

### 自動化帳戶

自動化帳戶是在部署期間建立的帳戶、是資源配置程序中的必要元件。Automation帳戶包含變數、認證資料、模組和所需的狀態組態、並參考Key Vault。

### 所需的狀態組態

這是用來建置CWMGR1組態的方法、組態檔會下載到VM、並透過VM上的本機組態管理員套用。組態元素範例包括：

- 安裝Windows功能
- 安裝軟體
- 套用軟體組態
- 確保套用適當的權限集
- 套用Let的Encrypt憑證
- 確保DNS記錄正確無誤
- 確保將CWMGR1加入網域

### 模組：

- ActiveDirectory Dsc:所需的狀態組態資源、可用於Active Directory的部署與組態。這些資源可讓您設定新的網域、子網域和高可用度網域控制器、建立跨網域信任關係、以及管理使用者、群組和OU。
- AZ.Accounts：Microsoft提供的模組、用於管理Azure模組的認證和一般組態元素
- AZ.Automation：Microsoft提供的Azure Automation指令模組
- Az.Compute:A Microsoft提供Azure運算命令的模組
- AZ.KeyVault：Microsoft提供的Azure Key Vault指令模組
- AZ.Resources：Microsoft提供的Azure資源管理程式命令模組

- cChocco：使用chocatey下載及安裝套件所需的狀態組態資源
- cjAz：此NetApp建立的模組可為Azure自動化模組提供自動化工具
- cjAzACS：此NetApp建立的模組包含環境自動化功能和PowerShell程序、可從使用者內容中執行。
- cjAzBuild：此NetApp建立的模組包含從系統內容執行的建置與維護自動化與PowerShell程序。
- cNtfsAccessControl：NTFS存取控制管理所需的狀態組態資源
- ComputerManagementDsc:所需的狀態組態資源、可讓您執行電腦管理工作、例如加入網域和排程工作、以及設定虛擬記憶體、事件記錄、時區和電源設定等項目。
- cUserRightsAssignment：所需的狀態組態資源、可讓您管理登入權限和權限等使用者權限
- 網路：網路所需的狀態組態資源
- xCertificate：所需的狀態組態資源、可簡化Windows Server上的憑證管理。
- xDnssServer：所需的狀態組態資源、用於Windows Server DNS伺服器的組態與管理
- xNetworking：與網路相關的所需狀態組態資源。
- "xRemoteDesktopAdmin"：此模組使用儲存庫、其中包含所需的狀態組態資源、可在本機或遠端機器上設定遠端桌面設定和Windows防火牆。
- xRemoteDesktopSessionHost：所需的狀態組態資源（xRDS分離 部署、xRDS分離 集合、xRDS分離 集合組態和xRDRemoteApp）、可用來建立及設定遠端桌面工作階段主機（RDSH）執行個體
- XSmbShare：所需的狀態組態資源、可用於設定及管理SMB共用區
- xSystemSecurity：所需的狀態組態資源、可用於管理UAC和IE Esc



Azure Virtual Desktop也會安裝Azure元件、包括Azure Virtual Desktop和Azure Virtual Desktop Client的企業應用程式和應用程式註冊、AVD租戶、AVD主機集區、AVD應用程式群組和AVD註冊虛擬機器。雖然VDS Automation元件會管理這些元件、但AVD會控制其預設組態和屬性集、因此請參閱AVD文件以取得詳細資料。

## 混合式AD元件

為了協助整合公有雲中的現有AD、現有的AD環境需要額外的元件和權限。

## 網域控制器

現有的網域控制器可透過AD Connect和（或）站台對站台VPN（或Azure ExpressRoute）整合至AVD部署。

## AD Connect

為了透過AVD PaaS服務順利進行使用者驗證、AD連線可用於同步網域控制器與Azure AD。

## 安全性群組

VDS使用名為CW-Infrastructure的Active Directory安全性群組、來包含自動化Active Directory相依工作（例如網域加入和GPO原則附加）所需的權限。

## 服務帳戶

VDS使用名為CloudworkspaceSVC的Active Directory服務帳戶、做為VDS Windows服務和IIS應用程式服務的

識別身分。此帳戶是非互動式（不允許RDP登入）、是CW-Infrastructure帳戶的主要成員

## VPN或ExpressRoute

站台對站台VPN或Azure ExpressRoute可用於直接將Azure VM加入現有網域。這是可選的組態、可在專案需求決定時使用。

## 本機AD權限委派

NetApp提供可簡化混合式AD程序的選用工具。如果使用NetApp的選用工具、則必須：

- 在伺服器作業系統上執行、而非在工作站作業系統上執行
- 在加入網域或網域控制器的伺服器上執行
- 在執行此工具的伺服器（如果未在網域控制器上執行）和網域控制器上、均已安裝PowerShell 5.0或更新版本
- 由具有網域管理權限的使用者執行、或由具有本機系統管理員權限且能夠提供網域管理員認證的使用者執行（適用於RunAs）

無論是手動建立或由NetApp工具套用、所需的權限如下：

- CW-Infrastructure群組
  - Cloud Workspace Infrastructure (\* CW-Infrastructure\*) 安全性群組已獲授予對Cloud Workspace OU層級和所有後代物件的完整控制權
  - 部署程式碼>.cloudWorks.app DNS區域–CW-Infrastructure群組授予的「建立子項目」、「刪除子項目」、「清單子項目」、「ReadProperty」、「刪除樹狀結構」、ExtendedRight、Delete、GenericWrite
  - DNS伺服器–CW-Infrastructure Group授予ReadPropy、Generic執行
  - 所建立VM的本機管理存取權（CWMGR1、AVD工作階段VM）（由受管理AVD系統上的群組原則執行）
- CW-CWMGRAccess群組此群組可在所有範本、單一伺服器、新原生Active Directory範本上、利用內建的群組伺服器操作員遠端桌面使用者和網路組態操作員、為CWMGR1提供本機管理權限。

## AVD環境元件與權限

部署自動化程序完成後、部署與工作區的持續使用與管理作業將需要一組不同的元件與權限、如下所定義。上述的許多元件和權限仍然相關、但本節著重於定義已部署的架構。

VDS部署和工作區的元件可分為多個邏輯類別：

- 終端使用者用戶端
- VDS控制面板元件
- Microsoft Azure AVD-PaaS元件
- VDS平台元件
- Azure租戶中的VDS工作區元件
- 混合式AD元件

## 終端使用者用戶端

使用者可以連線至AVD桌面及/或從各種端點類型連線。Microsoft已針對Windows、MacOS、Android和iOS發佈用戶端應用程式。此外、網路用戶端也可供無用戶端存取。

有些Linux精簡型用戶端廠商已針對AVD發佈端點用戶端。這些資訊列於 <https://docs.microsoft.com/en-us/azure/virtual-desktop/linux-overview>

## VDS控制面板元件

### VDS REST API

VDS以完整記錄的REST API為基礎、因此也可透過API取得Web應用程式中的所有可用動作。API文件如下：  
<https://api.cloudworkspace.com/5.4/swagger/ui/index#>

### VDS Web應用程式

VDS管理員可以透過VDS Web應用程式與ADS應用程式互動。此入口網站位於：  
<https://manage.cloudworkspace.com>

## 控制面資料庫

VDS資料與設定儲存在由NetApp代管及管理的控制面板SQL資料庫中。

## VDS通訊

### Azure租戶元件

VDS部署自動化會建立單一Azure資源群組、以包含其他AVD元件、包括VM、網路子網路、網路安全群組、以及Azure Files Container或Azure NetApp Files F動即可容納的資源集區。注意：預設值為單一資源群組、但VDS有工具可在其他資源群組中建立資源（若有需要）。

## Microsoft Azure AVD-PaaS元件

### AVD REST API

Microsoft AVD可透過API進行管理。VDS廣泛運用這些API來自動化及管理AVD環境。文件位於：  
<https://docs.microsoft.com/en-us/rest/api/desktopvirtualization/>

## 工作階段代理程式

代理程式會決定授權給使用者的資源、並協調使用者與閘道的連線。

## Azure診斷

Azure診斷專為支援AVD部署而打造。

## AVD Web用戶端

Microsoft提供Web用戶端、讓使用者無需在本機安裝用戶端即可連線至AVD資源。

## 工作階段閘道

本機安裝的RD用戶端會連線至閘道、以便安全地與AVD環境通訊。

## VDS平台元件

### CWMGR1

CMWDR1是每個部署的VDS控制VM。依預設、此功能會在目標Azure訂閱中建立為Windows 2019 Server VM。如需安裝在WMGR1上的VDS和協力廠商元件清單、請參閱本機部署一節。

AVD要求AVD VM加入Active Directory網域。為了簡化此程序並提供管理VDS環境的自動化工具、上述的CWMGR1 VM上安裝了數個元件、並將數個元件新增至AD執行個體。這些元件包括：

- \* Windows服務\* - VDS使用Windows服務從部署中執行自動化與管理動作：
  - 連續波自動化服務\*是部署在每個AVD部署中的CWMGR1上的Windows服務、可在環境中執行許多使用者導向的自動化工作。此服務在 CloudWorkspaceSVC\* AD帳戶下執行。
  - 連續波VM自動化服務\*是部署在每個AVD部署中的WMGR1上的Windows服務、可執行虛擬機器管理功能。此服務在 CloudWorkspaceSVC\* AD帳戶下執行。
  - \*連續波代理服務\*是一項Windows服務、部署至VDS管理下的每部虛擬機器、包括CWMGR1。此服務在虛擬機器的\*本機系統\*內容下執行。
  - \* CWManagerX API\*是每個AVD部署中安裝在CWMGR1上的一個以IIS應用程式集區為基礎的接聽程式。這會處理來自全域控制面板的傳入要求、並在\* CloudWorkspaceSVC\* AD帳戶下執行。
- \* SQL Server 2017 Express\* - VDS在WMGR1 VM上建立SQL Server Express執行個體、以管理自動化元件所產生的中繼資料。
- 網際網路資訊服務 (IIS) \*：在CWMGR1上啟用IIS、以裝載CWManagerX和CWApps IIS應用程式（僅在啟用RDS RemoteApp功能時）。VDS需要使用IIS 7.5版或更新版本。
- \* HTML5 Portal（選用）\*：VDS會安裝Spark Gateway服務、以便透過HTML5存取部署中的VM及VDS Web應用程式。這是以Java為基礎的應用程式、如果不需要此存取方法、可以停用和移除。
- \* RD閘道（選用）\* - VDS可讓CWMGR1上的RD閘道角色、提供RDP存取RDS集合型資源集區的權限。如果只需要AVD反向連線存取、則可停用/解除安裝此角色。
- \* RD Web（選用）\* - VDS可啟用RD Web角色並建立CWApps IIS Web應用程式。只要需要AVD存取權限、就可以停用此角色。
- \* DC組態\*：用於執行部署與VDS站台特定組態與進階組態工作的Windows應用程式。
- 測試VDC-Tool：一種Windows應用程式、可支援直接執行虛擬機器和用戶端層級的組態變更、適用於需要修改API或Web應用程式工作以進行疑難排解的罕見情況。
- \* Let's Encrypt通配符證書（可選）\*（由VDS建立和管理）：所有需要HTTPS流量的VM都會在夜間更新憑證。續約作業也由自動化工作處理（憑證為90天、所以續約作業不久前就開始）。客戶可視需要提供自己的萬用字元憑證。VDS也需要數個Active Directory元件來支援自動化工作。設計目的是利用最少數量的AD元件和新增權限、同時仍支援自動化管理環境。這些元件包括：
  - 雲端工作區組織單位（OU） - 此組織單位將做為必要子元件的主要AD容器。將在此層級及其子元件上設定CW-Infrastructure和用戶端DHP存取群組的權限。請參閱附錄A以瞭解此OU中建立的子OU。
  - 雲端工作空間基礎架構群組（CW-Infrastructure）\*是在本機AD中建立的安全群組、可將必要的委派權限指派給VDS服務帳戶（CloudWorkspaceSVC\*）
  - \*用戶端DHP存取群組（ClientDHPAccess）\*是在本機AD中建立的安全性群組、可讓VDS管理公司共用、使

用者主目錄及設定檔資料所在的位置。

- \* CloudWorkspaceSVC\*服務帳戶（Cloud Workspace Infrastructure Group成員）
- \*部署程式碼>.cloudWorkspace應用程式網域\*的DNS區域（此網域可管理工作階段主機VM的自動建立DNS名稱）–由部署組態所建立。
- \* NetApp專屬的GPO \*連結至雲端工作區組織單位的各種子OU。這些GPO包括：
  - \* Cloud Workspace GPO（連結至Cloud Workspace OU）\*–定義CW-Infrastructure Group成員的存取傳輸協定與方法。也會將群組新增至AVD工作階段主機上的本機系統管理員群組。
  - \* Cloud Workspace防火牆GPO（連結至專屬客戶伺服器、遠端桌面及暫存OU）-建立原則、確保工作階段主機與平台伺服器之間的連線並加以隔離。
  - \* Cloud Workspace RDS\*（專屬客戶伺服器、遠端桌面和暫存OU）：設定工作階段品質、可靠性、中斷連線逾時限制的原則限制。對於RDS工作階段、會定義TS授權伺服器值。
  - \* Cloud Workspace Companies \*（預設為未連結）–選用的GPO、可防止存取管理工具和區域、以「鎖定」使用者工作階段/工作區。可連結/啟用以提供受限的活動工作區。



您可應要求提供預設的群組原則設定組態。

## VDS工作區元件

### 資料層

#### Azure NetApp Files

如果您在VDS設定中選擇「支援資料層」選項、就會建立一個「支援能力資源池」和相關的Volume。Azure NetApp Files Azure NetApp FilesVolume可裝載使用者設定檔（透過FSLogix容器）、使用者個人資料夾和公司資料共用資料夾的共享歸檔儲存設備。

#### Azure檔案

如果您在CWS設定中選擇Azure Files做為Data Layer（資料層）選項、則會建立Azure檔案共用及其相關的Azure儲存帳戶。Azure檔案共用主控使用者設定檔（透過FSLogix容器）、使用者個人資料夾和公司資料共用的共用歸檔儲存設備。

#### 具有受管理磁碟的檔案伺服器

如果您在VDS安裝程式中選擇「檔案伺服器」作為「資料層」選項、Windows Server VM就會以託管磁碟建立。檔案伺服器裝載共用歸檔的儲存設備、以供使用者設定檔（透過FSLogix容器）、使用者個人資料夾和公司資料共用資料夾使用。

#### Azure網路

#### Azure虛擬網路

VDS會建立Azure虛擬網路及支援的子網路。VDS需要一個獨立的子網路、用於CWMGR1、AVD主機機器和Azure網域控制器、以及子網路之間的對等關係。請注意、AD控制器子網路通常已經存在、因此部署的VDS子網路需要與現有子網路連接。



## 網路安全群組

建立網路安全群組、以控制對CWMGR1 VM的存取。

- 租戶：包含供工作階段主機和資料VM使用的IP位址
- 服務：包含PaaS服務所需的IP位址（Azure NetApp Files 例如、功能不完整）
- 平台：包含IP位址、可做為NetApp平台VM（WMGR1和任何閘道伺服器）
- 目錄：包含用於Active Directory VM的IP位址

## Azure AD

VDS自動化與協調功能可將虛擬機器部署至目標Active Directory執行個體、然後將機器加入指定的主機集區。AVD虛擬機器在電腦層級受到AD結構（組織單位、群組原則、本機電腦管理員權限等）和AVD結構（主機集區、工作區應用程式群組成員資格）的成員資格（由Azure AD實體和權限管理）的管理。VDS使用VDS Enterprise應用程式/ Azure服務主體進行AVD動作、並使用本機AD服務帳戶（CloudWorkspaceSVC）進行本機AD和本機電腦動作、來處理此「雙重控制」環境。

建立AVD虛擬機器並將其新增至AVD主機集區的特定步驟包括：

- 從Azure範本建立虛擬機器、與AVD相關的Azure訂閱可見（使用Azure服務主要權限）
- 使用在VDS部署期間指定的Azure vnet檢查/設定新虛擬機器的DNS位址（需要本機AD權限（所有委派給CW-Infrastructure的權限皆在上方）、使用標準VDS命名配置\* {companyCode} TS {seriencenumber} \*來設定虛擬機器名稱。範例：XYZTS3。（需要本機AD權限（置於我們建立的內部部署（遠端桌面/公司代碼/共享）OU結構中）（與上述相同的權限/群組說明）
- 將虛擬機器放置在指定的Active Directory組織單位（AD）中（需要委派OU結構的權限（在上述手動程序期間指定））。
- 使用新的機器名稱/ IP位址更新內部AD DNS目錄（需要本機AD權限）
- 將新的虛擬機器加入本機AD網域（需要本機AD權限）
- 使用新的伺服器資訊更新VDS本機資料庫（不需要額外權限）
- 將VM加入指定的AVD主機集區（需要AVD服務主要權限）
- 將chlchatey元件安裝到新的虛擬機器（\* CloudWorkspaceSVC\*帳戶需要本機電腦管理權限）
- 安裝AVD執行個體的FSLogix元件（需要本機AD中AVD OU的本機電腦管理權限）
- 更新AD Windows防火牆GPO以允許流量傳輸到新的VM（需要針對與AVD OU及其相關聯虛擬機器相關的原則建立/修改AD GPO。需要在本機AD的AVD OU上建立/修改AD GPO原則。如果未透過VDS管理VM、則可在安裝後關閉。）
- 在新虛擬機器上設定「允許新連線」旗標（需要Azure服務主要權限）

## 將VM加入Azure AD

Azure租戶中的虛擬機器需要加入網域、但VM無法直接加入Azure AD。因此、VDS會在VDS平台中部署網域控制器角色、然後使用AD Connect將該DC與Azure AD同步。替代的組態選項包括使用Azure AD網域服務（AADDs）、使用AD Connect同步至混合式DC（內部部署或其他地方的VM）、或透過站台對站台VPN或Azure ExpressRoute將VM直接加入混合式DC。

## AVD主機集區

主機集區是Azure Virtual Desktop環境中一或多個相同虛擬機器（VM）的集合。每個主機集區都可以包含應用程式群組、使用者可以像在實體桌面上一樣與這些應用程式群組互動。

### 工作階段主機

在任何主機集區中、都有一或多個相同的虛擬機器。連線到此主機集區的這些使用者工作階段會由AVD負載平衡器服務進行負載平衡。

### 應用程式群組

根據預設、桌面使用者應用程式群組會在部署時建立。此應用程式群組中的所有使用者都能享有完整的Windows桌面體驗。此外、您也可以建立應用程式群組來提供串流應用程式服務。

### 記錄分析工作區

建立記錄分析工作區、以儲存來自部署和DSC程序及其他服務的記錄。部署後可以刪除此項目、但不建議這麼做、因為它會啟用其他功能。根據預設、記錄保留30天、不需支付保留費用。

### 可用度集

可用度集是部署程序的一部分、可在故障網域之間分隔共享VM（共享AVD主機集區、RDS資源集區）。若有需要、可在部署後刪除此選項、但會停用為共用VM提供額外容錯能力的選項。

## Azure恢復保存庫

恢復服務資料庫是由VDS Automation在部署期間所建立。這項功能目前預設為啟動、因為Azure備份會在部署程序期間套用到CWMGR1。若有需要、可停用及移除此功能、但若在環境中啟用Azure備份、則會重新建立此功能。

## Azure金鑰保存庫

Azure Key Vault是在部署過程中建立的、用於儲存Azure Automation帳戶在部署期間使用的憑證、API金鑰和認證。

## 附錄A—預設的Cloud Workspace組織單位結構

- 雲端工作區
  - 雲端工作空間公司
  - 雲端工作空間伺服器
    - 專屬客戶伺服器
    - 基礎架構
- CWMGR伺服器
- 閘道伺服器
- FTP伺服器
- 範本VM

- 遠端桌面
- 接移
  - 雲端工作區服務帳戶
- 用戶端服務帳戶
- 基礎架構服務帳戶
  - 雲端工作空間技術使用者
- 群組
- 技術3技術人員

## AVD和VDS v5.4先決條件

### AVD和VDS要求與注意事項

本文件說明使用NetApp虛擬桌面服務（VDS）部署Azure Virtual Desktop（AVD）所需的要素。「快速檢查清單」提供所需元件的簡短清單、以及為了確保有效部署所需採取的部署前步驟。本指南的其餘部分將根據所做的組態選擇、提供更詳細的每個元素細節。

#### 快速檢查清單

##### Azure要求

- Azure AD租戶
- Microsoft 365授權支援AVD
- Azure訂閱
- Azure虛擬機器可用的Azure配額
- 具備全域管理員和訂閱所有權角色的Azure管理帳戶
- 具有「企業管理員」角色的網域管理員帳戶、可用於AD Connect設定

##### 部署前資訊

- 判斷使用者總數
- 判斷Azure區域
- 判斷Active Directory類型
- 判斷儲存類型
- 識別工作階段主機VM映像或需求
- 評估現有的Azure和內部部署網路組態

### VDS部署詳細要求

#### 終端使用者連線需求

下列遠端桌面用戶端支援**Azure Virtual Desktop**：

- Windows桌面
- 網路
- MacOS
- iOS
- IGEL思考用戶端 (Linux)
- Android (預覽)



Azure Virtual Desktop不支援RemoteApp和桌面連線 (RADC) 用戶端或遠端桌面連線 (MSTSC) 用戶端。



Azure Virtual Desktop目前不支援Windows Store的遠端桌面用戶端。此用戶端的支援將會新增至未來版本。

遠端桌面用戶端必須能夠存取下列URL：

地址	傳出TCP連接埠	目的	用戶端
*.AVD.microsoft.com	443..	服務流量	全部
*.servicebus.windows.net 443疑難排解資料	全部	go.microsoft.com	443..
Microsoft FWLink	全部	aka.ms	443..
Microsoft URL簡寫器	全部	docs.microsoft.com	443..
文件	全部	privacy.microsoft.com	443..
隱私聲明	全部	query.prod.cms.rt.microsoft.com	443..



開啟這些URL是可靠用戶端體驗的必要條件。不支援封鎖這些URL的存取、並會影響服務功能。這些URL僅對應用戶端站台和資源、不包含Azure Active Directory等其他服務的URL。

## VDS安裝精靈的起點

VDS安裝精靈可處理成功部署AVD所需的大部分必要設定。安裝精靈 ("" ) 建立或使用下列元件。

### Azure租戶

必填： Azure租戶與Azure Active Directory

Azure中的AVD啟動為租戶整體設定。VDS支援每個租戶執行一個AVD執行個體。

### Azure訂閱

必填： Azure訂閱 (請注意您要使用的訂閱ID)

所有已部署的Azure資源都應以單一專屬訂閱方式進行設定。如此一來、AVD的成本追蹤就變得更簡單、而且簡化了部署程序。附註： Azure免費試用版不受支援、因為其點數不足、無法部署功能性AVD部署。

## Azure核心配額

為您要使用的VM系列提供足夠的配額、特別是在初始平台部署時、至少要有10個DS v3系列核心（最多只能使用2個核心、但每個初始部署可能性都有10個核心）。

## Azure管理帳戶

必填：Azure全域系統管理員帳戶。

VDS安裝精靈會要求Azure管理員將委派的權限授予VDS服務主體、並安裝VDS Azure Enterprise應用程式。管理員必須指派下列Azure角色：

- 租戶上的全域管理員
- 訂閱的擁有者角色

## VM映像

\*必要：\*支援多工作階段Windows 10的Azure映像。

Azure Marketplace提供最新版本的基礎Windows 10映像、而且所有Azure訂閱都能自動存取這些映像。如果您想要使用不同的映像或自訂映像、請希望VDS團隊針對建立或修改其他映像提供建議、或是讓我們知道Azure映像的一般問題、我們可以安排對話時間。

## Active Directory

AVD要求使用者身分識別必須是Azure AD的一部分、且VM必須加入與該Azure AD執行個體同步的Active Directory網域。VM無法直接附加至Azure AD執行個體、因此必須設定網域控制器、並與Azure AD同步。

這些支援選項包括：

- 在訂閱中自動建置Active Directory執行個體。AD執行個體通常是由VDS在VDS控制VM（WMGR1）上建立、適用於使用此選項的Azure虛擬桌面部署。AD Connect必須設定並設定為與Azure AD同步、作為設定程序的一部分。

[]

- 整合至現有的Active Directory網域、可透過Azure訂閱存取（通常透過Azure VPN或Express Route）、並使用AD Connect或協力廠商產品將其使用者清單與Azure AD同步。

[]

## 儲存層

在AVD中、儲存策略的設計目的是讓AVD工作階段VM上不會有持續的使用者/公司資料。使用者設定檔、使用者檔案和資料夾的持續資料、以及公司/應用程式資料、均裝載在獨立資料層上的一或多個資料Volume上。

FSLogix是一種設定檔容器化技術、可在工作階段初始化時、將使用者設定檔容器（VHD或VHDX格式）安裝至工作階段主機、以解決許多使用者設定檔問題（例如資料過度擴張和登入緩慢）。

由於此架構、因此需要資料儲存功能。此功能必須能夠處理每天早上/下午大量使用者同時登入/登出時所需的資料傳輸。即使是中等規模的環境、也可能需要大量的資料傳輸需求。資料儲存層的磁碟效能是主要的終端使用者效能變數之一、因此必須特別注意適當調整此儲存設備的效能大小、而不只是儲存容量。一般而言、儲存層的規模應能支援每位使用者5-15 IOPS。

**VDS安裝精靈支援下列組態：**

- 設定及組態Azure NetApp Files 設定（ANF）（建議）。*anf*標準服務層級最多可支援150位使用者、建議使用150至500位使用者的環境、以提供優質服務。對於超過500位使用者、建議使用ANF Ultra。

[]

- 設定及設定檔案伺服器VM

[]

## 網路

\*必填：\*所有現有網路子網路的詳細目錄、包括Azure透過Azure Express Route或VPN訂閱所能看到的任何子網路。部署必須避免重複的子網路。

VDS設定精靈可讓您定義網路範圍、以便在需要或必須避免範圍的情況下、將其納入與現有網路的計畫整合。

在部署期間決定使用者的IP範圍。根據Azure最佳實務做法、僅支援私有範圍內的IP位址。

支援的選項包括下列項目、但預設為/20範圍：

- 從192到168、255、168、0到255
- 從172.16.0.0到172.31.255
- 10.0.0.0到10.255.255.255

## CWMGR1

VDS的某些獨特功能（例如節省成本的工作負載排程和即時擴充功能）需要在租戶內部安裝管理功能、才能訂購。因此、將名為CWMGR1的管理VM部署為VDS安裝精靈自動化的一部分。除了VDS自動化工作之外、此虛擬機器也會將VDS組態保存在SQL Express資料庫、本機記錄檔和稱為DCConfig的進階組態公用程式中。

視**VDS**設定精靈中的選擇而定、此**VM**可用於裝載其他功能、包括：

- RDS閘道（僅用於RDS部署）
- HTML 5閘道（僅用於RDS部署）
- RDS授權伺服器（僅用於RDS部署）
- 網域控制器（若已選擇）

部署精靈中的決策樹狀結構

在初始部署中、我們會回答一系列問題、以自訂新環境的設定。以下是要做出的重大決策概要。

## Azure地區

決定要裝載AVD虛擬機器的Azure地區或地區。請注意Azure NetApp Files、支援GPU的某些VM系列（例如、支援GPU的VM）具有已定義的Azure區域支援清單、而AVD則適用於大部分地區。

- 此連結可用於識別 ["Azure產品供應情況依地區而定"](#)

## Active Directory類型

決定您要使用的Active Directory類型：

- 現有內部Active Directory
- 請參閱 ["AVD VDS元件與權限"](#) 請參閱文件、以瞭解Azure和本機Active Directory環境中所需的權限和元件
- 全新Azure訂閱型Active Directory執行個體
- Azure Active Directory網域服務

## 資料儲存

決定使用者設定檔、個別檔案和公司共用的資料放置位置。選項包括：

- Azure NetApp Files
- Azure檔案
- 傳統檔案伺服器（使用託管磁碟的Azure VM）

## 現有元件的NetApp VDS部署需求

使用現有Active Directory網域控制器進行NetApp VDS部署

此組態類型可延伸現有的Active Directory網域、以支援AVD執行個體。在這種情況下、VDS會在網域中部署一組有限的元件、以支援AVD元件的自動化資源配置與管理工作。

此組態需要：

- 現有的Active Directory網域控制器、可由Azure Vnet上的VM存取、通常是透過Azure VPN或Express Route、或是Azure中建立的網域控制器。
- 加入VDS元件和權限、以便在VDS加入網域時管理AVD主機集區和資料磁碟區。AVD VDS元件與權限指南定義所需的元件與權限、而部署程序則要求具有網域權限的網域使用者執行指令碼、以建立所需的元素。
- 請注意、VDS部署預設會為VDS建立的VM建立Vnet。vnet可與現有Azure網路VNets進行對等連接、或將CWMGR1 VM移至已預先定義子網路的現有Vnet。

## 認證與網域準備工具

系統管理員必須在部署程序的某個階段提供網域管理員認證。您可以在稍後建立、使用及刪除暫用網域管理員認證（部署程序完成後）。此外、需要協助建置先決條件的客戶也可以利用網域準備工具。

## NetApp VDS部署搭配現有檔案系統

VDS會建立Windows共用區、以便從AVD工作階段VM存取使用者設定檔、個人資料夾和公司資料。根據預設、VDS會部署檔案伺服器或Azure NetApp檔案選項、但如果您有現有的檔案儲存元件、VDS可在VDS部署完成後、將共用指向該元件。

使用和現有儲存元件的需求：

- 元件必須支援SMB v3
- 元件必須與AVD工作階段主機加入相同的Active Directory網域
- 元件必須能夠公開一個用於VDS組態的UNC路徑、所有三個共用區都可以使用一個路徑、或是分別為每個共

用區指定不同的路徑。請注意、VDS會設定這些共用的使用者層級權限、因此請參閱VDS AVD元件與權限文件、以確保已將適當的權限授予VDS自動化服務。

**NetApp VDS部署搭配現有Azure AD網域服務**

此組態需要程序來識別現有Azure Active Directory網域服務執行個體的屬性。請聯絡您的客戶經理、申請部署此類型的系統。採用現有AVD部署的NetApp VDS部署此組態類型假設已存在必要的Azure vnet、Active Directory和AVD元件。VDS部署的執行方式與「採用現有AD的NetApp VDS部署」組態相同、但新增下列需求：

- AVD租戶的RD擁有者角色必須授予Azure中的VDS企業應用程式
- 需要使用VDS Web App中的VDS匯入功能、將AVD主機集區和AVD主機集區VM匯入VDS此程序會收集AVD主機集區和工作階段VM中繼資料、並將其儲存在VDS中、以便由VDS管理這些元素
- 需要使用CRA工具將AVD使用者資料匯入VDS使用者區段。此程序會將每位使用者的中繼資料插入VDS控制面板、以便VDS管理其AVD應用程式群組成員資格和工作階段資訊

**附錄A：VDS控制面板URL和IP位址**

Azure訂閱中的VDS元件會與VDS全域控制面板元件通訊、例如VDS Web應用程式和VDS API端點。若要進行存取、必須安全地將下列基礎URI位址設定為連接埠443的雙向存取：

....

如果您的存取控制裝置只能依IP位址安全列出清單、則應安全列出下列IP位址清單。請注意、VDS使用Azure Traffic Manager服務、因此此清單可能會隨著時間而變更：

13.67.190.243 13.67.215.62 13.89.50.12213.67.227.115 13.67.227.230 13.67.227.227223.99.136.91  
40.122.119.157 40.78.132.16640.78.129.17 40.122.52.167.70.147.2 40.899.2013.68.178  
13.68.118.118.114.118.618.618.618.618.6120811.811.12.811.12.811.811.611.611.611.611.611.811.811.  
811.0.811.0.811.0.811.12.911.0.811.0.611.0.611.0.811.12.911.0.611.0.613.613.811.12.911.0.911.0.611.0.  
.613.613.613.611.0.

**附錄B：Microsoft AVD要求**

本Microsoft AVD需求一節摘要說明Microsoft的AVD需求。完整且最新的AVD需求請參閱此處：

<https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements>

**Azure Virtual Desktop工作階段主機授權**

Azure Virtual Desktop支援下列作業系統、因此請根據您計畫部署的桌面和應用程式、確定您擁有適當的使用者授權：

作業系統	必要授權
Windows 10 Enterprise多工作階段或Windows 10 Enterprise	Microsoft 365 e3、E5、A3、a5、f3、Business Premium Windows e3、E5、A3、a5
Windows 7企業版	Microsoft 365 e3、E5、A3、a5、f3、Business Premium Windows e3、E5、A3、a5
Windows Server 2012 R2、2016、2019年	具有軟體保證的RDS用戶端存取授權（CAL）



## AVD機器的URL存取

您為Azure Virtual Desktop建立的Azure虛擬機器必須能夠存取下列URL：

地址	傳出TCP連接埠	目的	服務標籤
*.AVD.microsoft.com	443..	服務流量	Windows虛擬桌面
mrsglobalsteus2prod.blob.core.windows.net	443..	代理程式和Sxs堆疊更新	AzureCloud
*.core.windows.net	443..	代理程式流量	AzureCloud
*.servicebus.windows.net	443..	代理程式流量	AzureCloud
prod.warmpath.msftcloudes.com	443..	代理程式流量	AzureCloud
catalogartifact.azureedge.net	443..	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows啟動	網際網路
AVDportalstorageblob.blob.core.windows.net	443..	Azure入口網站支援	AzureCloud

下表列出Azure虛擬機器可存取的選用URL：

地址	傳出TCP連接埠	目的	服務標籤
*.microsoftonline.com	443..	驗證MS Online Services	無
*.events.data.microsoft.com	443..	遙測服務	無
www.msftconnecttest.com	443..	偵測作業系統是否已連線至網際網路	無
*.prod.do.dsp.mp.microsoft.com	443..	Windows Update	無
login.windows.net	443..	登入MS Online Services、Office 365	無
*.SFX.ms	443..	OneDrive用戶端軟體更新	無
*.digicert.com	443..	憑證撤銷檢查	無

## 最佳效能因素

若要獲得最佳效能、請確定您的網路符合下列需求：

- 從用戶端網路到已部署主機集區之Azure區域的往返（RTT）延遲應低於150毫秒。
- 當裝載桌面和應用程式的VM連線至管理服務時、網路流量可能會流向國外/地區邊界。
- 若要最佳化網路效能、建議工作階段主機的VM與管理服務配置在同一個Azure區域。

Azure Virtual Desktop支援下列x64作業系統映像：

- Windows 10 Enterprise多工作階段、版本1809或更新版本
- Windows 10 Enterprise、1809版或更新版本
- Windows 7企業版
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop不支援x86（32位元）、Windows 10 Enterprise N或Windows 10 Enterprise KN作業系統映像。由於磁區大小限制、Windows 7也不支援託管Azure儲存設備上託管的任何VHD或VHDX型設定檔解決方案。

可用的自動化和部署選項取決於您選擇的作業系統和版本、如下表所示：

作業系統	Azure影像庫	手動部署VM	整合範本ARM	在Azure Marketplace上配置主機集區
Windows 10多工作階段、1903版	是的	是的	是的	是的
Windows 10多工作階段、版本1809	是的	是的	否	否
Windows 10 Enterprise、1903版	是的	是的	是的	是的
Windows 10 Enterprise、版本1809	是的	是的	否	否
Windows 7企業版	是的	是的	否	否
Windows Server 2019	是的	是的	否	否
Windows Server 2016	是的	是的	是的	是的
Windows Server 2012 R2	是的	是的	否	否

## AVD和VDS v6.0先決條件

### AVD和VDS要求與注意事項

本文件說明使用NetApp虛擬桌面服務（VDS）部署Azure Virtual Desktop（AVD）所需的要素。「快速檢查清單」提供所需元件的簡短清單、以及為了確保有效部署所需採取的部署前步驟。本指南的其餘部分將根據所做的組態選擇、提供更詳細的每個元素細節。

### 快速檢查清單

#### Azure要求

- Azure AD租戶
- Microsoft 365授權支援AVD
- Azure訂閱

- Azure虛擬機器可用的Azure配額
- 具備全域管理員和訂閱所有權角色的Azure管理帳戶
- 具有「企業管理員」角色的網域管理員帳戶、可用於AD Connect設定

#### 部署前資訊

- 判斷使用者總數
- 判斷Azure區域
- 判斷Active Directory類型
- 判斷儲存類型
- 識別工作階段主機VM映像或需求
- 評估現有的Azure和內部部署網路組態

#### VDS部署詳細要求

##### 終端使用者連線需求

下列遠端桌面用戶端支援**Azure Virtual Desktop**：

- Windows桌面
- 網路
- MacOS
- iOS
- IGEL思考用戶端 (Linux)
- Android (預覽)



Azure Virtual Desktop不支援RemoteApp和桌面連線 (RADC) 用戶端或遠端桌面連線 (MSTSC) 用戶端。



Azure Virtual Desktop目前不支援Windows Store的遠端桌面用戶端。此用戶端的支援將會新增至未來版本。

遠端桌面用戶端必須能夠存取下列**URL**：

地址	傳出TCP連接埠	目的	用戶端
*.wvd.microsoft.com	443..	服務流量	全部
*.servicebus.windows.net	443..	疑難排解資料	全部
go.microsoft.com	443..	Microsoft FWLink	全部
aka.ms	443..	Microsoft URL簡寫器	全部
docs.microsoft.com	443..	文件	全部
privacy.microsoft.com	443..	隱私聲明	全部

地址	傳出TCP連接埠	目的	用戶端
query.prod.cms.rt.microsoft.com	443..	用戶端更新	Windows桌面



開啟這些URL是可靠用戶端體驗的必要條件。不支援封鎖這些URL的存取、並會影響服務功能。這些URL僅對應用戶端站台和資源、不包含Azure Active Directory等其他服務的URL。

## VDS安裝精靈的起點

VDS安裝精靈可處理成功部署AVD所需的大部分必要設定。安裝精靈（""）建立或使用下列元件。

### Azure租戶

必填：Azure租戶與Azure Active Directory

Azure中的AVD啟動為租戶整體設定。VDS支援每個租戶執行一個AVD執行個體。

### Azure訂閱

必填：Azure訂閱（請注意您要使用的訂閱ID）

所有已部署的Azure資源都應以單一專屬訂閱方式進行設定。如此一來、AVD的成本追蹤就變得更簡單、而且簡化了部署程序。附註：Azure免費試用版不受支援、因為其點數不足、無法部署功能性AVD部署。

### Azure核心配額

為您要使用的VM系列提供足夠的配額、特別是在初始平台部署時、至少要有10個DS v3系列核心（最多只能使用2個核心、但每個初始部署可能性都有10個核心）。

### Azure管理帳戶

必填：Azure全域系統管理員帳戶。

VDS安裝精靈會要求Azure管理員將委派的權限授予VDS服務主體、並安裝VDS Azure Enterprise應用程式。管理員必須指派下列Azure角色：

- 租戶上的全域管理員
- 訂閱的擁有者角色

### VM映像

\*必要：\*支援多工作階段Windows 10的Azure映像。

Azure Marketplace提供最新版本的基礎Windows 10映像、而且所有Azure訂閱都能自動存取這些映像。如果您想要使用不同的映像或自訂映像、請希望VDS團隊針對建立或修改其他映像提供建議、或是讓我們知道Azure映像的一般問題、我們可以安排對話時間。

### Active Directory

AVD要求使用者身分識別必須是Azure AD的一部分、且VM必須加入與該Azure AD執行個體同步的Active

Directory網域。VM無法直接附加至Azure AD執行個體、因此必須設定網域控制器、並與Azure AD同步。

這些支援選項包括：

- 在訂閱中自動建置Active Directory執行個體。AD執行個體通常是由VDS在VDS控制VM (WMGR1) 上建立、適用於使用此選項的Azure虛擬桌面部署。AD Connect必須設定並設定為與Azure AD同步、作為設定程序的一部分。

□

- 整合至現有的Active Directory網域、可透過Azure訂閱存取 (通常透過Azure VPN或Express Route) 、並使用AD Connect或協力廠商產品將其使用者清單與Azure AD同步。

□

## 儲存層

在AVD中、儲存策略的設計目的是讓AVD工作階段VM上不會有持續的使用者/公司資料。使用者設定檔、使用者檔案和資料夾的持續資料、以及公司/應用程式資料、均裝載在獨立資料層上的一或多個資料Volume上。

FSLogix是一種設定檔容器化技術、可在工作階段初始化時、將使用者設定檔容器 (VHD或VHDX格式) 安裝至工作階段主機、以解決許多使用者設定檔問題 (例如資料過度擴張和登入緩慢) 。

由於此架構、因此需要資料儲存功能。此功能必須能夠處理每天早上/下午大量使用者同時登入/登出時所需的資料傳輸。即使是中等規模的環境、也可能需要大量的資料傳輸需求。資料儲存層的磁碟效能是主要的終端使用者效能變數之一、因此必須特別注意適當調整此儲存設備的效能大小、而不只是儲存容量。一般而言、儲存層的規模應能支援每位使用者5-15 IOPS。

**VDS安裝精靈**支援下列組態：

- 設定及組態Azure NetApp Files 設定 (ANF) (建議) 。*anf*標準服務層級最多可支援150位使用者、建議使用150至500位使用者的環境、以提供優質服務。對於超過500位使用者、建議使用*ANF Ultra* 。

□

- 設定及設定檔案伺服器VM

□

## 網路

\*必填：\*所有現有網路子網路的詳細目錄、包括Azure透過Azure Express Route或VPN訂閱所能看到的任何子網路。部署必須避免重複的子網路。

VDS設定精靈可讓您定義網路範圍、以便在需要或必須避免範圍的情況下、將其納入與現有網路的計畫整合。

在部署期間決定使用者的IP範圍。根據Azure最佳實務做法、僅支援私有範圍內的IP位址。

支援的選項包括下列項目、但預設為/20範圍：

- 從192到168、255、168、0到255
- 從172.16.0.0到172.31.255
- 10.0.0.0到10.255.255.255

## CWMGR1

VDS的某些獨特功能（例如節省成本的工作負載排程和即時擴充功能）需要在租戶內部安裝管理功能、才能訂購。因此、將名為CWMGR1的管理VM部署為VDS安裝精靈自動化的一部分。除了VDS自動化工作之外、此虛擬機器也會將VDS組態保存在SQL Express資料庫、本機記錄檔和稱為DCConfig的進階組態公用程式中。

視**VDS**設定精靈中的選擇而定、此**VM**可用於裝載其他功能、包括：

- RDS閘道（僅用於RDS部署）
- HTML 5閘道（僅用於RDS部署）
- RDS授權伺服器（僅用於RDS部署）
- 網域控制器（若已選擇）

部署精靈中的決策樹狀結構

在初始部署中、我們會回答一系列問題、以自訂新環境的設定。以下是要做出的重大決策概要。

### Azure地區

決定要裝載AVD虛擬機器的Azure地區或地區。請注意Azure NetApp Files、支援GPU的某些VM系列（例如、支援GPU的VM）具有已定義的Azure區域支援清單、而AVD則適用於大部分地區。

- 此連結可用於識別 "[Azure產品供應情況依地區而定](#)"

### Active Directory類型

決定您要使用的Active Directory類型：

- 現有內部Active Directory
- 請參閱 "[AVD VDS元件與權限](#)" 請參閱文件、以瞭解Azure和本機Active Directory環境中所需的權限和元件
- 全新Azure訂閱型Active Directory執行個體
- Azure Active Directory網域服務

### 資料儲存

決定使用者設定檔、個別檔案和公司共用的資料放置位置。選項包括：

- Azure NetApp Files
- Azure檔案
- 傳統檔案伺服器（使用託管磁碟的Azure VM）

### 現有元件的NetApp VDS部署需求

使用現有**Active Directory**網域控制器進行**NetApp VDS**部署

此組態類型可延伸現有的Active Directory網域、以支援AVD執行個體。在這種情況下、VDS會在網域中部署一組有限的元件、以支援AVD元件的自動化資源配置與管理工作。

此組態需要：

- 現有的Active Directory網域控制器、可由Azure Vnet上的VM存取、通常是透過Azure VPN或Express Route、或是Azure中建立的網域控制器。
- 加入VDS元件和權限、以便在VDS加入網域時管理AVD主機集區和資料磁碟區。AVD VDS元件與權限指南定義所需的元件與權限、而部署程序則要求具有網域權限的網域使用者執行指令碼、以建立所需的元素。
- 請注意、VDS部署預設會為VDS建立的VM建立Vnet。vnet可與現有Azure網路VNets進行對等連接、或將CWMGR1 VM移至已預先定義子網路的現有Vnet。

系統管理員必須在部署程序的某個階段提供網域管理員認證。您可以在稍後建立、使用及刪除暫用網域管理員認證（部署程序完成後）。此外，需要協助建置先決條件的客戶也可以利用網域準備工具。

VDS會建立Windows共用區、以便從AVD工作階段VM存取使用者設定檔、個人資料夾和公司資料。根據預設、VDS會部署檔案伺服器或Azure NetApp檔案選項、但如果您有現有的檔案儲存元件、VDS可在VDS部署完成後、將共用指向該元件。

- 元件必須支援SMB v3
- 元件必須與AVD工作階段主機加入相同的Active Directory網域
- 元件必須能夠公開一個用於VDS組態的UNC路徑、所有三個共用區都可以使用一個路徑、或是分別為每個共用區指定不同的路徑。請注意、VDS會設定這些共用的使用者層級權限、因此請參閱VDS AVD元件與權限文件、以確保已將適當的權限授予VDS自動化服務。

此組態需要程序來識別現有Azure Active Directory網域服務執行個體的屬性。請聯絡您的客戶經理、申請部署此類型的系統。採用現有AVD部署的NetApp VDS部署此組態類型假設已存在必要的Azure vnet、Active Directory和AVD元件。VDS部署的執行方式與「採用現有AD的NetApp VDS部署」組態相同、但新增下列需求：

## 附錄A：VDS控制面板URL和IP位址

||||   ||||   ||||   ||||   ||||

13.67.190.243 13.67.215.62 13.89.50.122 13.67.227.115 13.67.227.230 13.67.227.227 223.99.136.91  
40.122.119.157 40.78.132.166 40.78.129.17 40.122.52.167 70.147.2 40.899.20 13.68.178  
13.68.118.118.114.118.618.618.618.618.6120811.811.12.811.12.811.811.611.611.611.611.611.811.811.

811.0.811.0.811.0.811.12.911.0.811.0.611.0.611.0.811.12.911.0.611.0.613.613.613.811.12.911.0.911.0.611.0.613.613.613.611.0.

## 附錄B：Microsoft AVD要求

本Microsoft AVD需求一節摘要說明Microsoft的AVD需求。完整且最新的AVD需求請參閱此處：

<https://docs.microsoft.com/en-us/azure/virtual-desktop/overview#requirements>

### Azure Virtual Desktop工作階段主機授權

Azure Virtual Desktop支援下列作業系統、因此請根據您計畫部署的桌面和應用程式、確定您擁有適當的使用者授權：

作業系統	必要授權
Windows 10 Enterprise多工作階段或Windows 10 Enterprise	Microsoft 365 e3、E5、A3、a5、f3、Business Premium Windows e3、E5、A3、a5
Windows 7企業版	Microsoft 365 e3、E5、A3、a5、f3、Business Premium Windows e3、E5、A3、a5
Windows Server 2012 R2、2016、2019年	具有軟體保證的RDS用戶端存取授權（CAL）

### AVD機器的URL存取

您為Azure Virtual Desktop建立的Azure虛擬機器必須能夠存取下列URL：

地址	傳出TCP連接埠	目的	服務標籤
*.AVD.microsoft.com	443..	服務流量	Windows虛擬桌面
mrsglobalsteus2prod.blob.core.windows.net	443..	代理程式和Sxs堆疊更新	AzureCloud
*.core.windows.net	443..	代理程式流量	AzureCloud
*.servicebus.windows.net	443..	代理程式流量	AzureCloud
prod.warmpath.msftcloudes.com	443..	代理程式流量	AzureCloud
catalogartifact.azureedge.net	443..	Azure Marketplace	AzureCloud
kms.core.windows.net	1688	Windows啟動	網際網路
AVDportalstorageblob.blob.core.windows.net	443..	Azure入口網站支援	AzureCloud

下表列出Azure虛擬機器可存取的選用URL：

地址	傳出TCP連接埠	目的	服務標籤
*.microsoftonline.com	443..	驗證MS Online Services	無
*.events.data.microsoft.com	443..	遙測服務	無



地址	傳出TCP連接埠	目的	服務標籤
www.msftconnecttest.com	443..	偵測作業系統是否已連線至網際網路	無
*.prod.do.dsp.mp.microsoft.com	443..	Windows Update	無
login.windows.net	443..	登入MS Online Services、Office 365	無
*.SFX.ms	443..	OneDrive用戶端軟體更新	無
*.digicert.com	443..	憑證撤銷檢查	無

#### 最佳效能因素

若要獲得最佳效能、請確定您的網路符合下列需求：

- 從用戶端網路到已部署主機集區之Azure區域的往返（RTT）延遲應低於150毫秒。
- 當裝載桌面和應用程式的VM連線至管理服務時、網路流量可能會流向國外/地區邊界。
- 若要最佳化網路效能、建議工作階段主機的VM與管理服務配置在同一個Azure區域。

#### 支援的虛擬機器OS映像

Azure Virtual Desktop支援下列x64作業系統映像：

- Windows 10 Enterprise多工作階段、版本1809或更新版本
- Windows 10 Enterprise、1809版或更新版本
- Windows 7企業版
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Azure Virtual Desktop不支援x86（32位元）、Windows 10 Enterprise N或Windows 10 Enterprise KN作業系統映像。由於磁區大小限制、Windows 7也不支援託管Azure儲存設備上託管的任何VHD或VHDX型設定檔解決方案。

可用的自動化和部署選項取決於您選擇的作業系統和版本、如下表所示：

作業系統	Azure影像庫	手動部署VM	整合範本ARM	在Azure Marketplace上配置主機集區
Windows 10多工作階段、1903版	是的	是的	是的	是的
Windows 10多工作階段、版本1809	是的	是的	否	否
Windows 10 Enterprise、1903版	是的	是的	是的	是的
Windows 10 Enterprise、版本1809	是的	是的	否	否
Windows 7企業版	是的	是的	否	否

作業系統	Azure影像庫	手動部署VM	整合範本ARM	在Azure Marketplace上配置主機集區
Windows Server 2019	是的	是的	否	否
Windows Server 2016	是的	是的	是的	是的
Windows Server 2012 R2	是的	是的	否	否

## 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.