



系統管理 Virtual Desktop Service

NetApp
May 03, 2022

目錄

系統管理	1
建立網域管理員（「層級3」）帳戶	1
提供第三方的暫時存取權限	3
設定備份排程	4
複製虛擬機器	6
自動增加磁碟空間功能	8
存取Azure Key Vault中的VDS認證資料	8
套用監控和防毒軟體	9
新增及移動對應的磁碟機	10

系統管理

建立網域管理員（「層級3」）帳戶

總覽

VDS系統管理員偶爾需要網域層級的認證來管理環境。在VDS中、這些稱為「層級3」或「.tech」帳戶。

這些指示說明如何以適當的權限建立這些帳戶。

Windows伺服器網域控制器

執行內部託管網域控制器（或透過VPN/Express Route連結至Azure的本機DC）時、可直接在Active Directory Manager中管理.tech帳戶。

1. 使用網域管理員（.tech）帳戶連線至網域控制器（CWMGR1、DC01或現有VM）。
2. 建立新使用者（如有需要）。
3. 將使用者新增至「Level 3技術人員」安全性群組

[Management.System Administration。建立網域管理帳戶9ee17] |

- a. 如果缺少「Level 3技術人員」安全性群組、請建立該群組、並將其成為「CW-Infrastructure」安全性群組的成員。

[管理：系統管理。建立網域管理帳戶0fc27] |



在使用者名稱結尾新增「.tech」是建議的最佳實務做法、有助於從終端使用者帳戶劃分管理帳戶。

Azure AD網域服務

如果在Azure AD網域服務中執行或管理Azure AD中的使用者、則可在Azure管理入口網站中以一般Azure AD使用者的身分管理這些帳戶（例如變更密碼）。

您可以建立新帳戶、將新帳戶新增至這些角色、應賦予他們所需的權限：

1. AAD DC管理員
2. ClientDHPAccess
3. 目錄中的全域管理。



在使用者名稱結尾新增「.tech」是建議的最佳實務做法、有助於從終端使用者帳戶劃分管理帳戶。

□

提供第三方的暫時存取權限

總覽

在移轉至任何雲端解決方案時、提供第三方存取權是一種常見做法。

VDS系統管理員通常會選擇不讓這些第三方擁有相同的存取層級、以遵循「最低需求」的安全性存取原則。

若要設定協力廠商的管理存取權、請登入VDS並瀏覽至「組織」模組、按一下「組織」、然後按一下「使用者與群組」。

接下來、為第三方建立新的使用者帳戶、並向下捲動、直到看到「管理存取」區段、然後勾選方塊以啟用管理權限。

□

接著會顯示「管理存取設定」畫面、顯示VDS管理。無需變更使用者名稱、登入或密碼、只要新增電話號碼和/或電子郵件、即可強制執行多因素驗證、並選取要授予的存取層級。

對於VAR或ISV等資料庫管理員而言、_Servers_通常是唯一需要的存取模組。

□

儲存後、終端使用者可使用標準Virtual Desktop使用者認證登入VDS、即可存取自我管理功能。

當新建立的使用者登入時、他們只會看到您指派給他們的模組。他們可以選取組織、向下捲動至「Servers（伺服器）」區段、然後連線至您告訴他們的伺服器名稱（例如、<XYZ>D1、其中XYZ是您的公司代碼、而D1則表示伺服器是資料伺服器。在下例中、我們會告訴他們連線至TSD1伺服器以執行指派作業。

設定備份排程

總覽

VDS能夠在某些基礎架構供應商（包括Azure）中設定及管理原生備份服務。

Azure

在Azure中、VDS可以使用原生環境自動設定備份 ["Azure Cloud Backup"](#) 使用本機備援儲存設備（LRS）。如有需要、可在Azure管理入口網站中設定地理備援儲存設備（GRS）。

- 您可以針對每個伺服器類型定義個別的備份原則（附有預設建議）。此外、可從VDS UI中指派獨立排程（從伺服器類型）給個別機器、只要按一下「工作區」頁面上的「伺服器名稱」、即可導覽至「伺服器詳細資料檢視」、以套用此設定（請參閱下方影片：設定個別備份原則）
 - 資料
 - 備份方式包括每日7次、每週5次及每月2次備份。根據業務需求增加保留期間。
 - 這適用於專屬資料伺服器、以及應用程式和資料庫的附加VPS VM。
 - 基礎架構
 - CWMGR1：每日備份、每日備份7次、每週5次、每月2次。
 - RDS閘道：每週備份、每週保留4次。
 - HTML5閘道：每週備份、每週保留4次。
 - PowerUser（又稱為VDI使用者）
 - 請勿備份VM、因為資料應儲存在D1或TSD1伺服器上。
 - 請注意、有些應用程式確實在本機儲存資料、如果發生這種情況、則應特別考量。
 - 如果VM發生故障、可以透過複製另一個VM來建置新VM。如果只有一個VDI VM（或一個獨特的VM組建）、建議您備份它、以便不需要完整重新建置該VM。
 - 如果需要、您可以手動設定單一VM、直接在Azure管理入口網站中進行備份、而非備份所有VDI伺服器、將成本降至最低。
 - TS
 - 請勿備份VM、因為資料應儲存在D1或TSD1伺服器上。
 - 請注意、有些應用程式確實在本機儲存資料、如果發生這種情況、則應特別考量。
 - 如果VM發生故障、可以透過複製另一個VM來建置新VM。如果只有一個TS VM、建議備份、以便不需要完整重建該VM。
 - 如果需要、您可以手動設定單一VM、直接在Azure管理入口網站中進行備份、而非備份所有TS伺服器、將成本降至最低。
 - TSData
 - 備份方式包括每日7次、每週5次及每月2次備份。根據業務需求增加保留期間。
- 原則可設定為每日或每週進行備份、Azure不支援更頻繁的排程。

- 如需每日排程、請輸入偏好的備份時間。針對每週排程、輸入偏好的備份日期和時間。附註：將時間設定為準確的12:00 AM可能會導致Azure備份發生問題、因此建議您在上午12:01時進行備份。
- 定義應保留多少每日、每週、每月和每年備份。

設定部署預設值

[]

若要為整個部署設定**Azure**備份、請依照下列步驟進行：

1. 瀏覽至「部署詳細資料」頁面、選取「備份預設值」
2. 從下拉式功能表中選取伺服器類型。伺服器類型包括：

```
Data: these are for LOB/database server types
Infrastructure: these are platform servers
Power User: these are for Users with a TS server dedicated solely to them
TS: these are terminal servers that Users launch sessions on
TSData: these are servers doubling as terminal and data servers.
```

◦ 這將定義整個部署的整體備份設定。如果需要、可以覆寫這些項目、並在稍後設定伺服器專屬層級。

3. 按一下設定輪、然後出現「編輯」快顯視窗。
4. 選取下列備份設定：

```
On or off
Daily or weekly
What time of day backups take place
How long each backup type (daily, weekly, etc.) should be retained
```

5. 最後、按一下「Create (or Edit) 排程」（建立（或編輯）排程）以將這些設定放在定位。

設定個別備份原則

若要套用伺服器專屬的整合式備份設定、請瀏覽至「工作區詳細資料」頁面。

1. 向下捲動至「Servers（伺服器）」區段、然後按一下伺服器名稱
2. 按一下新增排程
3. 視需要套用備份設定、然後按一下建立排程

從備份還原

若要還原特定**VM**的備份、請先瀏覽至該「工作區詳細資料」頁面。

1. 向下捲動至「Servers（伺服器）」區段、然後按一下伺服器名稱
2. 向下捲動至備份區段、然後按一下定位輪以展開選項、然後選取任一選項

3. 還原至伺服器或還原至磁碟（從備份附加磁碟機、以便將資料從備份複製到現有的VM版本）。
4. 從這個點繼續還原、如同在任何其他還原案例中一樣。



成本取決於您想要維護的排程、而且完全由Azure備份成本所帶動。您可在Azure成本計算機上找到VM的備份價格：<https://azure.microsoft.com/en-us/pricing/calculator/>

複製虛擬機器

總覽

虛擬桌面服務（VDS）可讓您複製現有的虛擬機器（VM）。這項功能可在定義的使用者數增加時自動增加伺服器單元數可用度、或是在可用的資源集區中增加其他伺服器。

管理員在VDS中使用複製的方式有兩種：

1. 隨需從現有用戶端伺服器自動建立新伺服器
2. 主動自動建立新的用戶端伺服器、以根據合作夥伴定義和控制的規則自動擴充資源

複製以新增其他共用伺服器

複本是現有虛擬機器的複本。複製功能可節省時間、並協助管理員擴充規模、因為安裝客體作業系統和應用程式可能相當耗時。有了複本、您就能從單一安裝與組態程序建立多個虛擬機器複本。這種情況通常如下：

1. 在TS或TSD伺服器上安裝所有所需的應用程式和設定
2. 瀏覽至：「Workspace（工作區）」>「Servers Section（伺服器區段）」>「Gear（來源伺服器的齒輪）」圖示>
3. 允許執行複製程序（一般為45-90分鐘）
4. 最後一個步驟會啟動複製的伺服器、並將其放入RDS集區以接受新的連線。複製的伺服器在複製之後可能需要個別的組態、因此VDS會等待系統管理員手動將伺服器旋轉。

視需要重複多次。[]

若要增加共用工作階段主機環境中的使用者容量、複製工作階段主機是一項簡單的程序、只需幾個步驟即可完成。

1. 選取要複製的工作階段主機、確認目前沒有使用者登入機器。
2. 在VDS中、瀏覽至目標用戶端的工作區。捲動至伺服器區段、按一下齒輪圖示、然後選取複製。此程序需要大量時間、並將來源機器離線。預計完成時間超過30分鐘。

[] []

3. 此程序會關閉伺服器、將伺服器複製到另一個映像、並將映像複製到客戶的下一個Ts#。伺服器會在「伺服器」清單中顯示「Type =分段」和「Status =需要啟動」。

[]

4. 登入伺服器、確認伺服器已準備就緒可供正式作業。

[]

5. 準備好之後、按一下「啟動」、將伺服器新增至工作階段主機集區、以開始接受使用者連線。

[]

VDS複製程序定義

任何Clone Server作業下的VDS > Deployment > Task History (VDS >部署>任務歷史記錄) 中都會詳細說明逐步程序。此程序有20多個步驟、從存取Hypervisor開始、開始複製程序、最後啟動複製的伺服器。複製程序包括下列重要步驟：

- 設定DNS並設定伺服器名稱
- 指派靜態IP
- 新增至網域
- 更新Active Directory
- 更新VDS DB (CWMGR1上的SQL執行個體)
- 建立複本的防火牆規則

除了「工作歷程記錄」之外、任何複製程序的詳細步驟都可在每個合作夥伴的「虛擬桌面部署」中、於CwVmAutomationService登入CWMGR1檢視。檢閱這些記錄檔已記錄下來 ["請按這裡"](#)。

自動建立新伺服器

這項VDS功能的設計旨在隨著定義的使用者數量增加、自動提高伺服器單元數可用度。

合作夥伴透過VDS ("") >用戶端>總覽-VM資源>自動擴充。有幾項控制措施可供合作夥伴啟用/停用自動擴充功能、並為每個用戶端建立自訂規則、例如：數量/使用者/伺服器、每個使用者額外的RAM、以及每個CPU的使用者數量。



以上假設已針對整個虛擬桌面部署啟用自動複製。例如、若要停止所有自動複製、請使用「進階」視窗中的「DCConfig」、取消核取「伺服器建立」→「啟用自動複製」。

自動化複製程序何時執行？

自動複製程序會在每日維護設定為執行時執行。預設值為午夜、但可以編輯。日常維護的一部分是針對每個資源池執行變更資源執行緒。「變更資源」執行緒會根據集區組態的使用者人數（可自訂、每部伺服器可為10、21、30等使用者）來決定所需的共用伺服器數量。

自動建立新伺服器的「隨需」功能

此VDS功能可自動「隨需」複製其他伺服器至可用資源集區。

VDS管理會登入VDS、並在「組織或工作區模組」下找到特定的「用戶端」、然後開啟「總覽」索引標籤。「Servers Tile (伺服器區塊)」會列出所有伺服器 (TSD1、TS1、D1等)。若要複製任何個別伺服器、只要按一下伺服器名稱最右側的cog、然後選取Clone (複製) 選項即可。

一般而言、此程序需要約一小時的時間。不過、持續時間取決於VM的大小和基礎Hypervisor的可用資源。請注意、所複製的伺服器必須重新開機、因此合作夥伴通常會在下班後或排程維護期間執行。

當複製TSDDData伺服器時，其中一個步驟是刪除c:\Home、c:\Data和c:\Pro資料夾，使它們不會有任何重複的檔案。在此情況下、複製程序失敗、刪除這些檔案時發生問題。這個錯誤很模糊。通常、這表示複製事件因為有開啟的檔案或程序而失敗。下次嘗試時、請停用任何AV（因為這可能會說明此錯誤）。

自動增加磁碟空間功能

總覽

NetApp瞭解需要為系統管理員提供簡單的方法、確保使用者永遠有空間存取及儲存文件。這也可確保VM有足夠的可用空間、能夠順利完成備份、並賦予系統管理員及其災難恢復與營運不中斷計畫以更強大的能力。有鑑於此、我們建置了一項功能、可在磁碟機空間不足時、自動將使用中的託管磁碟擴充至下一層。

這項設定預設會套用至Azure中的所有新VDS部署、確保所有部署均預設保護使用者和租戶的備份。

系統管理員可瀏覽至「部署」索引標籤、然後選取部署、再從該處連線至其CVMGR1伺服器、藉此驗證是否已就緒。接著、開啟桌面上的DCConfig捷徑、然後按一下「進階」、向下捲動至底部。

□

系統管理員可以變更所需的可用磁碟空間量（GB可用空間或磁碟可用磁碟機的百分比）、然後再移至DCConfig相同進階區段中的下一層受管理磁碟。

□

幾個實際應用範例：

- 如果您想要確保磁碟機上至少有50 GB可用空間、請將MinFreeDebasGB設為50
- 如果您想確保至少有15%的磁碟機可用、請將MinFreeDePercent%從10設為15。

此動作會在伺服器時區的午夜執行。

存取Azure Key Vault中的VDS認證資料

總覽

CWASetup 5.4與先前的Azure部署方法不同。簡化組態與驗證程序、以減少開始部署所需的資訊量。許多移除的提示都是提供認證或帳戶、例如本機VM管理、SMTP帳戶、Tech帳戶、SQL SA等。這些帳戶現在會自動產生並儲存在Azure Key Vault中。依預設、存取這些自動產生的帳戶需要額外的步驟、如下所述。

- 找到「金鑰庫」資源、然後按一下：

[寬=75%]

- 在「設定」下、按一下「設定」。您會看到一則訊息、指出您未獲授權檢視：

[寬=75%]

- 新增「存取原則」以授予Azure AD帳戶（例如Global Admin或系統管理員）存取這些敏感金鑰的權限：

[寬=75%]

- 本範例使用全域管理員。選取主體後、按一下「Select」（選擇）、然後按「Add」（新增）：

[寬=75%]

- 按一下「Save」（儲存）：

[寬=75%]

- 已成功新增存取原則：

[寬=75%]

- 請重新造訪「重新設定」以確認帳戶現在可以存取部署帳戶：

[寬=75%]

- 例如、如果您需要網域管理員認證來登入CWMGR1並更新群組原則、請按一下每個項目、檢查cjDomain管理員名稱和cjDomain管理員密碼下的字串：

[寬=75%]

[寬=75%]

- 顯示或複製值：

[寬=75%]

套用監控和防毒軟體

總覽

虛擬桌面服務（VDS）管理員負責監控其平台基礎架構（至少由WMGR1組成）、以及所有其他基礎架構和虛擬機器（VM）。在大多數情況下、系統管理員會直接與資料中心/ IaaS供應商安排基礎架構（Hypervisor / SAN）監控。系統管理員負責監控終端機伺服器 and 資料伺服器、通常是部署他們偏好的遠端管理與監控（RMM）解決方案。

防毒是系統管理員的責任（適用於平台基礎架構和終端機/資料伺服器VM）。為了簡化此程序、Azure伺服器的VDS預設會套用Windows Defender。



安裝協力廠商解決方案時、請勿納入可能會干擾VDS自動化的防火牆或任何其他元件。

更具體地說、如果預設已有非常特定的防毒原則、當這些防毒代理程式安裝在由Virtual Desktop Service管理的伺服器上時、可能會產生不良影響。

我們的整體指引是、雖然VDS平台自動化通常不會受到防毒或防惡意軟體產品的影響、但最佳實務做法是在所有平台伺服器（WMGR1、RDGDS、HTML5閘道、FTP等）上新增下列程序的例外/排除項目：

```
*\paexec.exe
*\paexec_1_25.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CW Automation
Service\cw.automation.service.exe
C:\Program
Files\CloudWorkspace\CwVmAutomationService\CwVmAutomationService.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Printer.exe
C:\Program Files (x86)\Myrtille\bin\Myrtille.Services.exe
```

此外、我們建議在用戶端伺服器上安全列出下列程序：

```
C:\Program Files\CloudWorkspace\CwAgent\paexec.exe
C:\Program Files\CloudWorkspace\CwAgent\CwAgent.exe
C:\Program Files\CloudWorkspace\CwRemoteApps\cwra.exe
C:\Program Files\CloudWorkspace\Pen\Pen.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgent.exe
C:\Program Files\CloudWorkspace\MfaAgent\MFAAgentMonitor.exe
```

新增及移動對應的磁碟機

總覽

根據預設、終端使用者工作階段會有三個共用資料夾。這些資料夾位於定義的儲存層。這可能位於檔案伺服器（TSD1或D1）或儲存服務、例如Azure Files、Azure NetApp Files 支援區、NetApp CVO和NetApp CVS。

為了清楚說明、本文將以公司代碼「NECA」為範例客戶。本範例假設已部署名為NECATSD1的單一台TDS1伺服器。我們將逐步將資料夾移至另一個VM（稱為「NECAD1」）。此策略可用於在同一台機器或另一台機器的分割區之間移動、如下列範例所示...

資料夾起始位置：

- 資料：NECATSD1\C:\data\NECA\（TSD1is表示它是第一部終端機伺服器、也可做為資料伺服器）
- FTP：NECATSD1\C:\FTP\NECA\
- 主頁：NECATSD1\C:\home\NECA\

資料夾結束位置：

- 資料：NECAD1\G:\data\NECA\（D1is it is it is the 1st Data Server）
- FTP：相同的程序適用、不需要描述3倍
- 主頁：相同的程序適用、不需要描述3倍

在NECAD1上新增G:磁碟

1. 為了將共享資料夾放在E：磁碟機上、我們需要透過Hypervisor（例如 Azure管理入口網站）、然後初始化並格式化

[]

2. 將現有資料夾（NECATSD1、C:\）路徑複製到新位置（NECAD1、G:\）
3. 將資料夾從原始位置複製到新位置。

[]

從原始資料夾共用（NECATSD1、C：\data\NECA\）收集資訊

1. 使用與原始位置資料夾完全相同的路徑來共用新資料夾。
2. 開啟新的NECAD1、G:\data\資料夾、您會在範例中看到一個名為「NECA」的資料夾。

[]

3. 請注意原始資料夾共用的安全性權限：

[]

4. 這是典型的設定、但如果有需要保留的現有自訂項目、請務必複製原始設定。所有其他使用者/群組權限應從新的資料夾共用區中移除
 - 系統：允許所有權限
 - 本地計算機上的LocalClientDHPAccess：允許的所有權限
 - ClientDHPAccess（網域上）：允許的所有權限
 - NECA-All使用者（網域上）：允許「完全控制」以外的所有權限

將共用路徑和安全性權限複寫到新的共用資料夾

1. 返回新位置（NECAD1、G:\data\NECA\）、並以相同的網路路徑（機器除外）共用NECA資料夾、範例為「NECA-data\$」

[]

2. 為確保使用者安全、請新增所有使用者、並將其權限設定為相符。

[]

3. 移除可能存在的任何其他使用者/群組權限。

[]

編輯群組原則（僅當資料夾移至新機器時）

1. 接下來您將在群組原則管理編輯器中編輯磁碟機對應。對於Azure AD網域服務、對應位於：

"Cloud Workspace Users > User Configuration > Preferences > Windows Settings> Drive Maps"

[]

2. 一旦群組原則更新之後，每位使用者下次連線時，都會看到對應的磁碟機，這些磁碟機會指向新的位置。
3. 此時您可以刪除NECATSD1、C:\上的原始資料夾。

疑難排解

如果終端使用者看到對應的磁碟機有紅色X、請在磁碟機上按一下滑鼠右鍵、然後選取中斷連線。登出磁碟機後再重新登入磁碟機將會正確顯示。[]

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.