Google

Virtual Desktop Service

NetApp
July 19, 2022

目錄

Google

Google Cloud RDS部署指南（GCP）

總覽

本指南將提供逐步指示、以在Google Cloud中使用NetApp虛擬桌面服務（VDS）建立遠端桌面服務（RDS）部署。

本概念驗證（POC）指南旨在協助您在自己的測試GCP專案中快速部署及設定RDS。

正式作業部署（尤其是現有AD環境）非常常見、但此POC指南並未考慮此程序。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。

本POC文件將帶您瀏覽整個RDS部署、並提供VDS平台部署後組態主要領域的簡短說明。完成後、您將擁有完整部署且功能完善的RDS環境、並隨附工作階段主機、應用程式和使用者。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、雲端備份、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。

部署架構

[寬=75%]

RDS基礎知識

VDS部署功能完整的RDS環境、從零開始提供所有必要的支援服務。此功能包括：

- RDS閘道伺服器
- Web用戶端存取伺服器
- 網域控制器伺服器
- RDS授權服務
- ThinstPrint授權服務
- FileZilla FTPS伺服器服務

指南範圍

本指南將從GCP和VDS管理員的觀點、引導您使用NetApp VDS技術來部署RDS。您將GCP專案帶入零預先設定、本指南可協助您設定RDS端點對端點

建立服務帳戶

1. 在GCP中、瀏覽（或搜尋）*IAM & Admin > Service Accounts*

   []

2. 按一下「_」「*create service account*」

[]

3. 輸入唯一的服務帳戶名稱、然後按一下_cred_。記下服務帳戶的電子郵件地址、稍後將會使用該地址。

   []

4. 選取服務帳戶的_Owner_角色、然後按一下_Continue

   []

5. 下一頁不需要變更（*Grant*使用者存取此服務帳戶（選用））、請按一下_DOY_

   []

6. 從「*Service Accounts*」頁面、按一下動作功能表、然後選取「*_Create key*」

   []

7. 選取「*P12*」、然後按一下「*cre_*」

   []

8. 下載.P12檔案並儲存至您的電腦。保持_Private金鑰密碼_不變。

   []

   []

啟用**Google**運算**API**

1. 在GCP中、瀏覽（或搜尋）*APIs & Services*（*API*與服務）> *Library*

   []

2. 在GCP API程式庫中、瀏覽（或搜尋）*Compute Engine API*、按一下_enable

   []

建立新的**VDS**部署

1. 在VDS中、瀏覽至_Deployments_、然後按一下「__ New Deployment」（新部署）

   []

2. 輸入部署名稱

   []

3. 選取「_Google Cloud Platform」

   []

基礎架構平台

1. 輸入_Project ID_和OAUTH電子郵件地址。請從本指南稍早的版本上傳.P12檔案、然後為此部署選擇適當的區域。按一下「*Test*」以確認項目正確、並已設定適當的權限。

   Oauth電子郵件是本指南先前建立的服務帳戶地址。

   []

2. 確認之後、按一下「*CONTINU_*」

   []

帳戶

本機**VM**帳戶

1. 提供本機系統管理員帳戶的密碼。請記錄此密碼以供日後使用。
2. 提供SQL SA帳戶的密碼。請記錄此密碼以供日後使用。

密碼複雜度至少需要8個字元、其中3個字元類型為：大寫、小寫、數字、特殊字元

SMTP帳戶

VDS可透過自訂的SMTP設定傳送電子郵件通知、或選取「*Automatic*」（自動_）來使用內建的SMTP服務。

1. 輸入VDS傳送電子郵件通知時要用作_寄 件者地址的電子郵件地址。_noReply@<您的網域>.com是一種通用格式。
2. 輸入應指示成功報告的電子郵件地址。
3. 輸入應指示故障報告的電子郵件地址。

[]

第**3**級技術人員

第3級技術人員帳戶（也稱為_.tech帳戶_）是VDS管理員在VDS環境中執行VM管理工作時所使用的網域層級帳戶。您可在此步驟及/或更新版本建立其他帳戶。

1. 輸入層級3管理員帳戶的使用者名稱和密碼。您輸入的使用者名稱會加上「.tech」、以協助區分終端使用者與技術帳戶。請記錄這些認證資料以供日後使用。

   最佳實務做法是為所有應具有環境網域層級認證的VDS管理員定義命名帳戶。沒有這類帳戶的VDS管理員仍可透過VDS內建的_Connect to server_功能、取得VM層級的管理存取權。

   []

網域

Active Directory

輸入所需的AD網域名稱。

公有網域

外部存取受到SSL憑證的保護。您可以使用自己的網域和自我管理的SSL憑證來自訂。或者、選取「*Automatic*」（自動_）可讓VDS管理SSL憑證、包括自動更新憑證90天。使用自動時、每個部署都會使用_cloudWorkclase.app_的獨特子網域。

[]

虛擬機器

對於RDS部署、必須在平台伺服器上安裝必要的元件、例如網域控制器、RDS代理商和RDS閘道。在正式作業中、這些服務應在專用且備援的虛擬機器上執行。針對概念驗證部署、可使用單一VM來裝載所有這些服務。

平台**VM**組態

單一虛擬機器

這是POC部署的建議選項。在單一虛擬機器部署中、下列角色全部託管在單一VM上：

- 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

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。

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。

多部伺服器

將VDS平台分割成多個虛擬機器時、下列角色會裝載在專用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、則必須選擇「_multiple servers」（多重伺服器）。

服務角色

- Cwmgr1.

  此VM是NetApp VDS管理VM。它會執行SQL Express資料庫、輔助程式公用程式及其他管理服務。在單一伺服器部署中、此VM也可以裝載其他服務、但在_multiple server_組態中、這些服務會移到不同的VM。

- CWPortal1（2）

  第一個HTML5閘道名稱為_CWPortal1_、第二個名稱為_CWPortal2_。部署時可建立一或兩個。可在部署後新增額外的伺服器、以增加容量（每部伺服器約500個連線）。

- CWRDSGateway1(2)

  第一個RDS閘道名為_cWRDSGateway1_、第二個為_cWRDSGateway2_。部署時可建立一或兩個。可在部署後新增額外的伺服器、以增加容量（每部伺服器約500個連線）。

- 遠端應用程式

  應用程式服務是專屬的集合、用於託管RemotApp應用程式、但會使用RDS閘道及其RDWeb角色來路由傳送終端使用者工作階段要求、以及託管RDWeb應用程式訂閱清單。此服務角色未部署VM專屬VM。

- 網域控制器

  在部署時、可自動建置一或兩個網域控制器、並將其設定為搭配VDS使用。

[]

作業系統

選取要部署於平台伺服器的伺服器作業系統。

時區

選取所需的時區。平台伺服器現在將設定為、記錄檔將反映此時區。無論此設定為何、終端使用者工作階段仍會反映自己的時區。

其他服務

FTP

VDS可選用安裝及設定Filezilla來執行FTPS伺服器、以便將資料移入或移出環境。這項技術較舊、建議採用更現代化的資料傳輸方法（例如Google雲端硬碟）。

[]

網路

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。

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Cloud Volumes Service （如NetApp）的常駐範圍
- 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

[]

授權

SPLA編號

輸入您的SPLA號碼、讓VDS可以設定RDS授權服務、以利更輕鬆地報告SPLA RDS CAL。POC部署可輸入臨時號碼（例如12345）、但試用期（約120天）之後、RDS工作階段將停止連線。

SPLA產品

輸入透過SPLA授權之任何Office產品的MAK授權代碼、以便從VDS報告中簡化SPLA報告。

ThinstPrint

選擇安裝隨附的ThinPrint授權伺服器與授權、以簡化終端使用者印表機重新導向。

[]

審查與資源配置

完成所有步驟後、請檢閱選項、然後驗證及配置環境。[]

後續步驟

部署自動化程序現在將部署新的RDS環境、並提供您在部署精靈中選取的選項。

部署完成後、您會收到多封電子郵件。完成之後、您將有一個環境可以做好第一個工作區的準備。工作區將包含支援終端使用者所需的工作階段主機和資料伺服器。請回頭參考本指南、在1-2小時內完成部署自動化之後、再依照後續步驟進行。

建立新的資源配置集合

資源配置集合是VDS中的功能、可建立、自訂及SysPrep VM映像。進入工作場所部署之後、我們需要部署映像、下列步驟將引導您逐步建立VM映像。

請依照下列步驟建立基本的部署映像：

1. 導覽至「部署」>「資源配置集合」、按一下「*Add*」

   []

2. 輸入名稱和說明。選擇_類型：shared _。

   

   您可以選擇「共享」或「VDI」。「共享」可支援工作階段伺服器、以及（選用）適用於資料庫等應用程式的商業伺服器。VDI是VM的單一VM映像、專供個別使用者使用。

3. 按一下「*Add*」以定義要建置的伺服器映像類型。

   []

4. 選取「TSData」做為伺服器角色_、適當的VM映像（本例為Server 2016）和所需的儲存類型。按一下「新增伺服器_」

   []

5. （可選）選擇要安裝在此映像上的應用程序。

   a. 可用的應用程式清單會從應用程式庫填入、您可以按一下右上角的管理名稱功能表、然後在「*Settings* > *App Catalog*」頁面下存取。

      []

6. 按一下「新增收藏」、然後等待虛擬機器建置完成。VDS將建置可存取及自訂的VM。
7. VM建置完成後、請連線至伺服器並進行所需的變更。

   a. 狀態顯示_Collection Validation之後、按一下收藏名稱。

      []

   b. 然後按一下伺服器範本名稱_

[]

c. 最後、按一下「*Connect to Server*」按鈕以連線、並使用本機管理認證自動登入VM。

[]

[]

8. 完成所有自訂之後、按一下「驗證集合」、讓VDS可以進行系統預備並完成映像。一旦完成、虛擬機器就會被刪除、映像將可在VDS部署精靈中用於部署表單。

[]5.

建立新的工作區

工作區是支援一組使用者的工作階段主機和資料伺服器集合。部署可以包含單一工作區（單一租戶）或多個工作區（多租戶）。

工作區會定義特定群組的RDS伺服器集合。在此範例中、我們將部署單一集合來展示虛擬桌面功能。不過、此模型可延伸至多個工作區/ RDS集合、以支援同一個Active Directory網域空間內的不同群組和不同位置。或者、系統管理員可以限制工作區/集合之間的存取、以支援需要有限存取應用程式和資料的使用案例。

用戶端與設定

1. 在NetApp VDS中、瀏覽至_Workspace_、然後按一下「_ *New Workspace*」

   []

2. 按一下「*Add*」以建立新的用戶端。客戶詳細資料通常代表公司資訊或特定地點/部門的資訊。

   []

   a. 輸入公司詳細資料、然後選取要部署此工作區的部署。
   b. *資料磁碟機：*定義要用於公司共用對應磁碟機的磁碟機代號。
   c. *使用者主磁碟機：*定義要用於個別對應磁碟機的磁碟機代號。
   d. 其他設定

      下列設定可在部署和/或所選部署後加以定義。

      i. _啟用遠端應用程式：_遠端應用程式會將應用程式呈現為串流應用程式、而非（或除了）呈現完整的遠端桌面工作階段。
      ii. 啟用應用程式置物櫃： VDS包含應用程式部署與授權功能、依預設、系統會向終端使用者顯示/隱藏應用程式。啟用應用程式置物櫃會透過GPO安全名單強制執行應用程式存取。
      iii. _啟用工作區使用者資料儲存：_判斷終端使用者是否需要在虛擬桌面上存取資料儲存設備。若為RDS部署、應一律勾選此設定、以啟用使用者設定檔的資料存取。
      iv. 停用印表機存取： VDS可封鎖對本機印表機的存取。
      v. 允許存取工作管理員： VDS可在Windows中啟用/停用終端使用者對工作管理員的存取權。
      vi. _需要複雜的使用者密碼：_需要複雜的密碼才能啟用原生的Windows Server複雜密碼規則。它也會停用鎖定使用者帳戶的延遲自動解除鎖定。因此、啟用時、當終端使用者多次嘗試密碼失敗而鎖定

其帳戶時、就需要管理員介入。

vii. 為所有使用者啟用*MFA*： VDS包括免費的電子郵件/ SMS MFA服務、可用於保護終端使用者和/或VDS管理帳戶存取安全。若要啟用此功能、此工作區中的所有終端使用者都必須透過MFA驗證、才能存取桌面和/或應用程式。

選擇應用程式

選取本指南稍早所建立的Windows作業系統版本和資源配置集合。

此時可新增其他應用程式、但在此POC中、我們將針對部署後的應用程式權益進行處理。

[]

新增使用者

您可以選取現有的AD安全性群組或個別使用者來新增使用者。在本POC指南中、我們將在部署後新增使用者。

[]

審查與資源配置

在最後一頁、檢閱所選選選項、然後按一下「_Provision」（資源配置）以開始自動建置RDS資源。

[]

在部署程序期間、會建立記錄檔、並可在「部署詳細資料」頁面底部的「工作歷程記錄」下存取。可透過瀏覽至_VDS >「部署」>「部署名稱」來存取

後續步驟

工作環境自動化程序現在將部署新的RDS資源、並提供您在整個部署精靈中所選的選項。

完成後、您將會遵循幾個常用工作流程、自訂典型的RDS部署。

- "新增使用者"
- "終端使用者存取"
- "應用程式權利"
- "成本最佳化"

Google Compute Platform（GCP）和VDS先決條件

GCP與VDS要求與注意事項

本文件說明使用NetApp虛擬桌面服務（VDS）部署遠端桌面服務（RDS）所需的元素。「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。

[寬=75%]

快速檢查清單

GCP要求

- GCP租戶
- GCP專案
- 已指派擁有者角色的服務帳戶

部署前資訊

- 判斷使用者總數
- 確定GCP區域和區域
- 判斷作用中目錄類型
- 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GCP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**GCP**中的**RDS**：

- "適用於Windows的NetApp VDS用戶端"
  - 適用於Windows的NetApp VDS用戶端傳出URL安全性要求
    - api.cloudworkspace.com
    - vdsclient.app
    - API.vdsclient.app
    - BI.vdsclient.app
  - 增強功能：
    - VDS隨需喚醒
    - ThinstPrint用戶端和lice ning
    - 自助服務密碼重設
    - 自動伺服器和閘道位址交涉
    - 完整的桌面與串流應用程式支援
    - 提供自訂品牌
    - 安裝程式交換器可自動部署及設定
    - 內建疑難排解工具
- "NetApp VDS Web用戶端"
- "Microsoft RD用戶端"

- Windows
- MacOS
- ISO
- Android

- 協力廠商軟體和/或精簡型用戶端
  - 需求：支援RD閘道組態

儲存層

在VDS部署的RDS中、儲存策略的設計目的是讓AVD工作階段VM不會有持續的使用者/公司資料駐留。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。

網路

*必要：*所有現有網路子網路的詳細目錄、包括GCP專案透過VPN所看到的任何子網路。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）需要在組織和專案中有管理人員在場。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
- HTML 5閘道
- RDS授權伺服器
- 網域控制器

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。

GCP區域

決定要裝載VDS虛擬機器的GCP區域或區域。請注意、應根據終端使用者和可用服務的鄰近度來選擇該區域。

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：

- 適用於 GCP Cloud Volumes Service
- 傳統檔案伺服器

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RDS執行個體。在這種情況下、VDS會將一組有限的元件部署到網域、以支援RDS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GCP VPC網路上的VM存取、通常是透過VPN或GCP中建立的網域控制器。
- 在RDS主機和資料磁碟區加入網域時、新增VDS元件和VDS管理所需的權限。部署程序需要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VPC網路。VPC網路可與現有的VPC網路進行對等連接、或將CWMGR1 VM移至現有的VPC網路、並預先定義所需的子網路。

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RDS工作階段主機存取使用者設定檔、個人資料夾和公司資料。VDS預設會部署檔案伺服器、但如果您有現有的檔案儲存元件VDS、則可在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RDS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、確保已將適當的權限授予VDS Automation Services。

附錄**A**：**VDS**控制面板**URL**和**IP**位址

GCP專案中的VDS元件會與Azure中裝載的VDS全域控制面板元件通訊、包括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使用具有備援公有IP位址的負載平衡器、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 13.68.118.118.114.118.618.618.618.618.6120811.811.12.811.12.811.811.611.611.611.611.611.611.811.811.811.0.811.0.811.0.811.12.911.0.811.0.611.0.611.0.811.12.911.0.611.0.613.613.613.811.12.911.0.911.0.611.0.613.613.613.611.0.

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工作階段主機之GCP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區域。

支援的虛擬機器**OS**映像

由VDS部署的RDS工作階段HsoTS支援下列x64作業系統映像：

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

版權資訊

商標資訊