Google Compute Platform (GCP) and VDS Prerequisites

Virtual Desktop Service

Toby vanRoojen
December 02, 2020

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-service/Deploying.GCP.vds_v5.4_prerequisites.html on December 18, 2020. Always check docs.netapp.com for the latest.

Table of Contents

Google Compute Platform (GCP) and VDS Prerequisites . . . 1
GCP and VDS requirements and notes . . . 1
Quick checklist . . . 1
VDS deployment detailed requirements . . . 1
NetApp VDS Deployment Requirements for Existing Components . . . 3
APPENDIX A: VDS control plane URLs and IP addresses . . . 4

Google Compute Platform (GCP) and VDS Prerequisites

GCP and VDS requirements and notes

This document describes the required elements for deploying Remote Desktop Services (RDS) using NetApp Virtual Desktop Service (VDS). The “Quick Checklist” provides a brief list of required components and pre-deployment steps to take to ensure an efficient deployment. The rest of the guide provides greater detail for each element, depending on the configuration choices that are made.

Quick checklist

GCP requirements

- GCP tenant
- GCP project
- Service Account with Owner role assigned

Pre-deployment information

- Determine total number of users
- Determine GCP region and zone
- Determine active directory type
- Determine storage type
- Identify session host VM image or requirements
- Assess existing GCP and on-premises networking configuration

VDS deployment detailed requirements

End user connection requirements

The following Remote Desktop clients support RDS in GCP:

- NetApp VDS Client for Windows
    - NetApp VDS Client for Windows outbound url whitelisting requirements
        - api.cloudworkspace.com
        - vdsclient.app
        - api.vdsclient.app
        - bin.vdsclient.app
        - vdsclient.blob.core.windows.net

    - Enhanced features:
        - VDS Wake on Demand
        - ThinPrint client and lice nsing
        - Self-service password reset
        - Automatic server and gateway address negotiation
        - Full desktop & streaming application support
        - Available custom branding
        - Installer switches for automated deployment and configuration
        - Built-in troubleshooting tools
- NetApp VDS web client
- Microsoft RD Client
    - Windows
    - MacOS
    - iSO
    - Android
- 3rd party software and/or thin clients
    - Requirement: Support RD gateway configuration

Storage layer

In RDS deployed by VDS, the storage strategy is designed so that no persistent user/company data resides on the WVD session VMs. Persistent data for user profiles, user files and folders, and corporate/application data are hosted on one or more data volume(s) hosted on an independent data layer.

FSLogix is a profile containerization technology that solves many user profile issues (like data sprawl and slow logins) by mounting a user profile container (VHD or VHDX format) to the session host at session initialization.

Due to this architecture a data storage function is required. This function must be able to handle the data transfer required each morning/afternoon when a significant portion of the users login/logoff at the same time. Even moderately sized environments can have significant data transfer requirements. The disk performance of the data storage layer is one of the primary end user performance variables and special care must be taken to appropriately size the performance of this storage, not just the amount of storage. Generally, the storage layer should be sized to support 5-15 IOPS per user.

Networking

Required: An inventory of all existing network subnets including any subnets visible to the GCP project via a VPN. The deployment needs to avoid overlapping subnets.

The VDS setup wizard allows you to define the network scope in case there is a range that is required, or must be avoided, as part of the planned integration with existing networks.

Determine an IP range to user during your deployment. Per best practices, only IP addresses in a private range are supported.

Supported choices include the following but default to a /20 range:

- 192.168.0.0 through 192.168.255.255

- 172.16.0.0 through 172.31.255.255
- 10.0.0.0 through 10.255.255.255

CWMGR1

Some of the unique capabilities of VDS such as the cost saving Workload Scheduling and Live Scaling functionality require an administrative presence within the organization and project. Therefore, an administrative VM called CWMGR1 is deployed as part of the VDS setup wizard automation. In addition to VDS automation tasks this VM also holds VDS configuration in a SQL express database, local log files and an advanced configuration utility called DCConfig.

Depending on the selections made in the VDS setup wizard, this VM can be used to host additional functionality including:

- An RDS gateway
- An HTML 5 gateway
- An RDS license server
- A Domain Controller

Decision tree in the Deployment Wizard

As part of the initial deployment a series of questions are answered to customize the settings for the new environment. Below is an outline of the major decisions to be made.

GCP region

Decide which GCP region or regions will host your VDS virtual machines. Note that the region should be selected based on the proximity to end users and available services.

Data Storage

Decide where the data for user profiles, individual files, and corporate shares will be placed. Choices include:

- Cloud Volumes Service for GCP
- Traditional File Server

NetApp VDS Deployment Requirements for Existing Components

NetApp VDS Deployment with Existing Active Directory Domain Controllers

This configuration type extends an existing Active Directory domain to support the RDS instance. In this case VDS deploys a limited set of components into the domain to support automated provisioning and management tasks for the RDS components.

This configuration requires:

- An existing Active Directory domain controller that can be accessed by VMs on the GCP VPC network, typically via VPN or a domain controller that has been created in GCP.
- Addition of VDS components and permissions required for VDS management of RDS hosts and data volumes as they are joined to the domain. The deployment process requires a Domain user with domain privileges to execute the script that will create the needed elements.

- Note that the VDS deployment creates a VPC network by default for VDS created VMs. The VPC network can be either peered with existing VPC networks or the CWMGR1 VM can be moved to an existing VPC network with the required subnets pre-defined.

Credentials and domain preparation tool

Administrators must provide a Domain Administrator credential at some point in the deployment process. A temporary Domain Administrator credential can be created, used and deleted later (once the deployment process completes).
Alternatively, customers who require assistance in building out the pre-requisites can leverage the Domain Preparation Tool.

NetApp VDS deployment with existing file system

VDS creates Windows shares that allow user profile, personal folders, and corporate data to be accessed from RDS session hosts. VDS will deploy either the File Server by default, but if you have an existing file storage component VDS can point the shares to that component once the VDS deployment is complete.

The requirements for using and existing storage component:

- The component must support SMB v3
- The component must be joined to the same Active Directory domain as the RDS session host(s)
- The component must be able to expose a UNC path for use in the VDS configuration – one path can be used for all three shares or separate paths may be specified for each. Note that VDS will set user level permissions on these shares, ensure the appropriate permissions have been granted to the VDS Automation Services.

APPENDIX A: VDS control plane URLs and IP addresses

VDS components in the GCP project communicate with the VDS global control plane components that are hosted in Azure, including the VDS Web Application and the VDS API endpoints. For access, the following base URI addresses need to be whitelisted for bi-directional access on port 443:

api.cloudworkspace.com
autoprodb.database.windows.net
vdctoolsapi.trafficmanager.net
cjbootstrap3.cjautomate.net

If your access control device can only white list by IP address, the following list of IP addresses should be whitelisted. Note that VDS uses a load balancer with redundant public IP addresses, so this list may change over time:

13.67.190.243
13.67.215.62
13.89.50.122
13.67.227.115
13.67.227.230
13.67.227.227
23.99.136.91
40.122.119.157
40.78.132.166
40.78.129.17
40.122.52.167

40.70.147.2
40.86.99.202
13.68.19.178
13.68.114.184
137.116.69.208
13.68.18.80
13.68.114.115
13.68.114.136
40.70.63.81
52.171.218.239
52.171.223.92
52.171.217.31
52.171.216.93
52.171.220.134
92.242.140.21

Optimal performance factors

For optimal performance, make sure your network meets the following requirements:

- Round-trip (RTT) latency from the client's network to the GCP region where session hosts have been deployed should be less than 150ms.
- Network traffic may flow outside country/region borders when VMs that host desktops and apps connect to the management service.
- To optimize for network performance, we recommend that the session host's VMs are collocated in the same region as the management service.

Supported virtual machine OS images

RDS session hsots, deployed by VDS, support the following x64 operating system images:

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

Copyright Information

Copyright © 2020 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.