Dell Technologies Cloud PowerScale for Google Cloud: Overview and Solution Design Considerations

November 2022

H18598.2

White Paper

Abstract

This document provides technical details about PowerScale for Google Cloud, including the solution architecture and integration with the Google Cloud console. It also introduces key considerations for planning and deploying the solution.

Dell Technologies

Copyright

Published in the USA November 2022 H18598.2.

Contents

Executive summary

Overview

Many organizations use the public cloud as a part of their IT infrastructure. Unstructured data in the public cloud is usually stored as objects, while on-premises unstructured data is stored as files. As unstructured data grows exponentially, organizations are also looking to store unstructured data as files in the public cloud. In this scenario, organizations can migrate file-based workloads to the cloud to increase business agility, reduce cost, and simplify management.

To provide the native-cloud experience of file services with high performance, we have partnered with Google to create the Dell Technologies Cloud PowerScale for Google Cloud solution. PowerScale for Google Cloud is a scalable file service that provides high-speed file access over multiple protocols, including SMB, NFS, and HDFS. PowerScale for Google Cloud enables customers to run their cloud workload on the PowerScale scale-out NAS storage system.

This document introduces how PowerScale for Google Cloud provides enterprise file services, and it includes key considerations for planning and deploying the solution into a production environment. For step-by-step deployment details, see the Google User Documentation.

Revisions

Date	Description
November 2020	Initial release
October 2021	Updated for feature change
January 2022	Updated template and DNS setup for SmartConnect
November 2022	Minor updates.

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Lieven Lin

Contributors: Mark Church, Anjan Dave

Note: For links to other documentation for this topic, see the PowerScale Info Hub.

Architecture and features

Introduction

This section introduces the PowerScale for Google Cloud architecture and the exposed OneFS features on Google Cloud Console.

PowerScale for Google Cloud enables the most demanding high-performance and bandwidth-intensive workloads to run in Google Cloud. The file system scales up to a massive size with multiple PBs in a single namespace, with performance that scales along with capacity. Besides its unprecedented scale, PowerScale for Google Cloud includes enterprise-grade data-management features, durability, reliability, and availability, backed by enterprise service-level agreements (SLAs) and 24x7 support.

PowerScale for Google Cloud features include the following:

- Multiprotocol access with NFS, SMB, and HDFS
- Snapshots
- Native replication
- Active Directory integration

Leaders from every industry—including life sciences, media and entertainment, oil and gas, and financial services—now have a cloud-native file service to meet the needs of demanding file-based applications.

Customers can provision and manage OneFS clusters directly from the Google Cloud Console. They can also use some OneFS features within the console, such as SMB share and NFS export management, and storage tiering. For OneFS features that are not exposed through the Google Cloud Console, customers can use these features with the assistance of Dell Technologies services experts.

Architecture overview

PowerScale for Google Cloud is a file service that is powered by PowerScale storage and managed by Dell Technologies in Google Cloud. It provides extreme performance and a throughput file service to enterprises who need to run the most demanding file-based workloads in the public cloud instead of an on-premises environment. It also enables enterprises to take advantage of flexible cloud-consumption models and cloud economics. On the other hand, PowerScale OneFS provides Data at Rest Encryption (DARE) through self-encrypting drives and a key management system. The data on SEDs is encrypted, and the data may not be accessed if the SED is stolen or removed from the cluster. See Dell PowerScale OneFS: Security Considerations for more details regarding DARE.

As the name suggests, PowerScale for Google Cloud is tightly integrated with Google Cloud. When users adopt this solution, they can subscribe, order, and configure a OneFS cluster through Google Cloud Console directly. For the step-by-step details, see the Google User Documentation.

The following figure shows the architecture of PowerScale for Google Cloud. It mainly consists of the Dell Technologies partner data center, Dell Technologies Google Cloud organization, and customer Google Cloud organization.

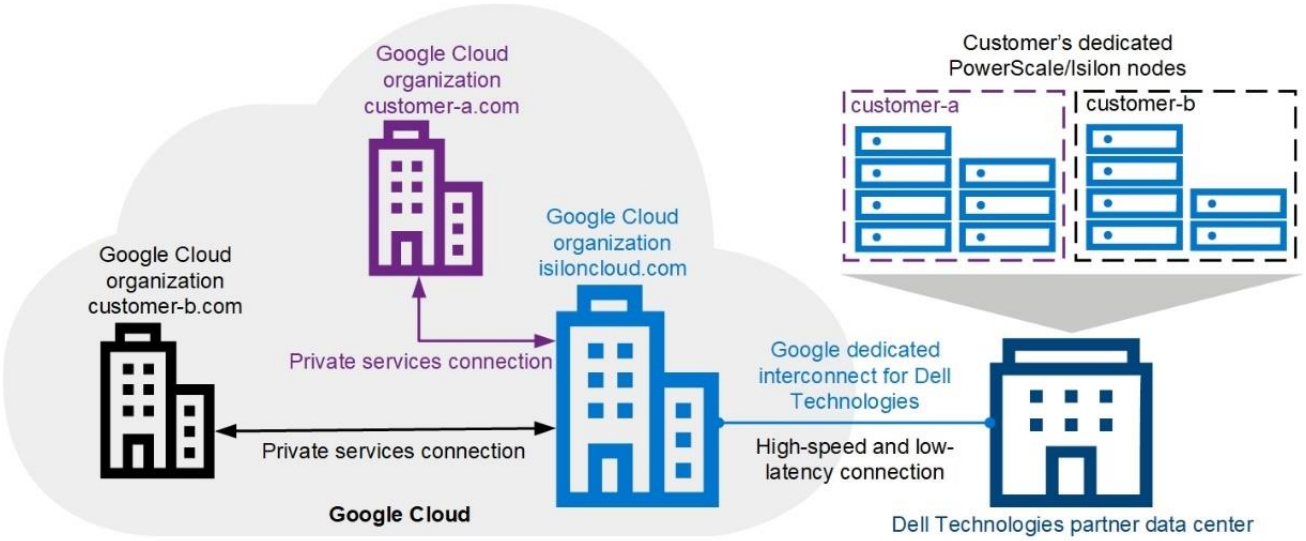

Figure 1. **PowerScale for Google Cloud architecture overview**

- **Dell Technologies partner data center:** This data center enables low-latency and high-throughput connections between PowerScale hardware running OneFS and the Google Cloud compute engine of customers. Dell Technologies deploys data centers around the globe to host the PowerScale hardware over data-center providers that are also partnered with Google. The Dell Technologies partner data center is transparent to end users.
- **Dell Technologies Google Cloud organization:** This organization is also transparent to end users. It bridges customer traffic to the customer's physical OneFS clusters in the back-end data center through the dedicated interconnect. It also connects with the customer organization through the Google Cloud private service connection which is implemented using Google VPC peering.
- **Customer Google Cloud organization:** This organization is the end-user Google Cloud organization which accesses the physical OneFS cluster data. After the customer Google Cloud organization enables and configures the PowerScale for Google Cloud service, they can create private service connections with Dell Technologies to use the OneFS file service.

Self-service features on Google Cloud Console

PowerScale for Google Cloud is a Dell Technologies managed service that uses a cloud consumption model. For an optimal native-cloud experience, it also allows users to manage some OneFS cluster features within the Google Cloud Console. This section introduces the OneFS features that are available through self-service on the Google Cloud Console.

For the nonexposed OneFS features on Google Cloud Console, you must use them with the assistance of Dell Technologies services experts through a support ticket. The ticket-enabled features include the following:

- HDFS protocol access

- Active Directory

Service tiers

To meet the needs of a varied dataset and wide spectrum of workloads, PowerScale for Google Cloud allows users to purchase different types of service tiers. You can also add tiers seamlessly at any time to scale both capacity and compute resources.

File share management

PowerScale for Google Cloud allows users to manage SMB and NFS file shares within the Google Cloud Console. The following file shares are created within the Google Cloud Console:

- **File share with SMB enabled:** OneFS creates an SMB share for users. By default, all users access the SMB share as guest users, and the guest has full control permissions on the SMB share. In Microsoft Windows 10, Windows Server 2019, or Windows Server 2016, the SMB client no longer allows guest user access to a remote server. You must therefore change the SMB share permission or enable the guest-user access on the Windows versions. See the article Guest access in SMB2 disabled by default in Windows. If your organization has specific requirements for the SMB share settings, you can modify them through the storage administration or ask assistance from Dell Technologies services experts.
- **File share with NFSv3 enabled:** OneFS creates an NFSv3 export for users with root squash disabled. By default, PowerScale for Google Cloud only enables NFSv3 service for users' clusters. If you require NFSv4 access, request assistance from Dell Technologies services experts.
- **File share capacity:** OneFS creates a hard quota to define the maximum capacity of the share, which is a limit that cannot be exceeded. If an operation such as a file write causes the used-capacity target to exceed the file-share capacity, the operation fails. For more information about the OneFS hard quota, see the document Storage Quota Management and Provisioning with Dell PowerScale SmartQuotas.
- **File share deletion:** You can delete the file shares within Google Cloud Console. The operation deletes all the data permanently under the file shares, and you cannot recover the data.

Punchout WebUI administration portal

To provide a more seamless interaction with OneFS key features, PowerScale for Google Cloud allows users to access the OneFS WebUI to manage cluster settings with limited privileges. These OneFS features are exposed in the OneFS WebUI pages **Storage Administration** and **Data Protection Administration**, which are shown in the following figure.

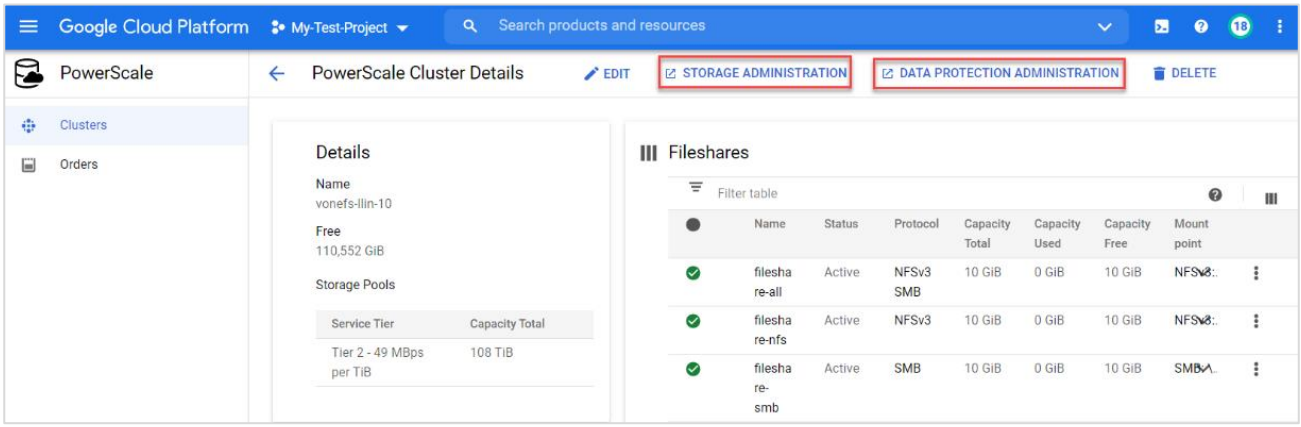

Figure 2. **Administration portal**

To access the administration portal, the computer that logs in to the Google Cloud Console must also be able to access the project VPC network internal IP addresses directly. As mentioned in the section Architecture overview, PowerScale for Google Cloud connects with the end-user network through private services access, and only internal IP addresses are assigned to PowerScale nodes. Therefore, the administration portal is only accessible through internal IP addresses. We recommend implementing a bastion host (for example, a Windows VM in Google Cloud) or setting up a VPN connection to your project VPC network to access the administration portal.

Storage administration

The Storage Administration page enables users to manage authentication-provider settings and protocols settings based on business requirements, which provides more flexibility to end users. This page in the OneFS WebUI lists the following features:

- **File system explorer:** View and manage the data under your OneFS access zone path.
- **Access zones:** View and modify settings of your OneFS access zone. Do not modify the access zone name, which causes file-share creation in the Google Cloud Console to fail.
- **Authentication providers:** Manage the authentication providers for your OneFS access zone.
- **User and group management:** View and manage the users in your OneFS access zone. You can also manage OneFS user mapping for multiprotocol access. You can view the ACL policy and on-disk identity settings.
- **SMB protocol management:** View and modify the SMB share default setting for your OneFS access zone. The SMB global setting is read-only. You can also create, modify, or delete SMB shares within the WebUI directly based on your requirements.

- **NFS protocol management:** View and modify the NFS settings for your access zone. The NFS global setting is read-only. You can also create, modify, or delete NFS exports and alias within the WebUI directly based on your requirements.

For more details, see the OneFS Web Administration Guide.

Data protection administration

The Data Protection Administration page enables users to protect their data with the OneFS enterprise-level features of SnapshotIQ, SyncIQ, and SmartQuotas. This page in the OneFS WebUI lists the two features. For more details, see the OneFS Web Administration Guide.

- **SnapshotIQ:** The SnapshotIQ can take read-only, point-in-time copies (snapshots) of any directory or subdirectory in OneFS. When a snapshot is taken, it preserves the exact state of a file system at that instant, which can be accessed later. This immutable, point-in-time copy has various applications. For example, snapshots can be used to make consistent backups, or to restore files which were inadvertently changed or deleted. You can also use snapshots to quickly identify file-system changes. For more technical details, see the document Data Protection with Dell PowerScale SnapshotIQ.

  Note: In PowerScale for Google Cloud, we recommend taking a snapshot on the subdirectory of your OneFS access zone path only. Do not create a snapshot to the **/ifs** path.

- **SyncIQ:** OneFS SyncIQ delivers unique, highly parallel replication performance that scales with the dataset to provide a solid foundation for disaster recovery. To protect your data, you can use this feature to replicate your critical data to another cluster, and conversely. We recommend replicating the data within your access zone path only, and not using the entire root path of **/ifs**. Only unencrypted SyncIQ connections are supported in Google Cloud. For more details, see the document Dell PowerScale SyncIQ: Architecture, Configuration, and Considerations.
- **SmartQuotas:** PowerScale SmartQuotas enables administrators to understand, predict, control, and limit storage usage across their organization and provision a cluster to best meet their storage needs. SmartQuotas also facilitates **thin provisioning,** or the ability to present more storage capacity to applications and users than is physically present (overprovisioning). This ability allows customers to buy and provision storage as they grow rather than having to make large, speculative purchasing decisions ahead of time. For more details, see the document Storage Quota Management and Provisioning with Dell EMC PowerScale SmartQuotas.

Network considerations

Introduction

This section introduces the network details of PowerScale for Google Cloud. As mentioned in the section Architecture overview, different Google Cloud organizations connect with the Dell Technologies organization over a private-services connection. A dedicated project is created within the Dell Technologies organization for each customer's VPC network which is authorized to access the PowerScale cluster. Meanwhile, a separate routing table is also implemented in the network devices of the Dell

Technologies partner data center for each authorized customer VPC network. Different organizations, or even different projects in a same organization, are separated as a multitenancy experience, from the perspective of the network.

After your organization purchases storage capacity through orders, you can deploy a PowerScale cluster by following the Google User Documentation. You must prepare the following items before deployment:

- **Choose a VPC network that is authorized to deploy your PowerScale cluster.** Each PowerScale cluster is associated with only one VPC network, but a single VPC network can have multiple clusters deployed. By default, only the resources within the authorized VPC network can access the associated PowerScale cluster. You can establish additional VPC peering by opening a ticket.
- **Prepare a cluster IP address range with Classless Inter-Domain Routing (CIDR) format.** The PowerScale cluster allocates these IP addresses to each node, and they are routable within the authorized VPC network.
- **Prepare a cluster service FQDN that is used to access PowerScale data.** Users must use the FQDN to mount cluster file shares and access data.

Cluster IP address range

To ensure the IP address range can accommodate future cluster growth to a maximum node, you must allocate at least a CIDR block in the RFC 1918 private address ranges. The RFC 1918 private address ranges include the following: 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.

In an auto-mode VPC network of Google Cloud, a specific private IP range is assigned for the automatically created subnets. The specific private IP range is a portion of the 10.128.0.0/9 CIDR block, and Google Cloud reserves the unused portion of 10.128.0.0/9 for future use. We recommend preventing your PowerScale cluster IP address range from overlapping with the 10.128.0.0/9 CIDR block. You can create your own VPC network with custom mode if you must use the 10.128.0.0/9 CIDR block. See the article VPC network for details about Google Cloud valid VPC IP ranges.

The PowerScale cluster IP address range must be a unique CIDR block that cannot overlap with any existing IP address range in the authorized VPC network. If your organization's on-premises resources must access the PowerScale cluster in the future, you must ensure there is no conflict between the PowerScale cluster IP addresses and your on-premises network IP addresses.

Network port usage

Network security is always an important area to focus on. Malicious attacks could result in a disaster and may result in service interruption to end users. Firewall devices are the most common choice to secure the network by controlling TCP/IP ports. The following table shows the required ports for some key features of PowerScale for Google Cloud services. For more details, see the PowerScale OneFS Security Configuration Guide.

Table 1. Network usage

Feature	Port	Service	Protocol	Usage description
File share access	53	DNS	TCP/UDP	SmartConnect DNS requests and incoming DNS request responses
	111	rpc.bind	TCP/UDP	ONC RPC portmapper that is used to locate services such as NFSv3, mountd, and isi_cbind_d
	300	mountd	TCP/UDP	NFSv3 mount service
	302	statd	TCP/UDP	NFS Network Status Monitor (NSM)
	304	lockd	TCP/UDP	NFS Network Lock Manager (NLM)
	445	microsoft-ds	TCP	SMB service
	2049	nfs	TCP/UDP	Network File Service (NFS) server
Storage administration and data protection administration	8080	apache2	TCP	• OneFS web administration interface • OneFS API
HDFS	585	hdfs (datanode)	TCP	HDFS (Hadoop file system)
	8020	hdfs(namenode)	TCP	HDFS (Hadoop file system)
	8080	WebHDFS	TCP	WebHDFS over HTTPS
	8082	WebHDFS	TCP	WebHDFS over HTTP
SyncIQ	2097	n/a	TCP	SyncIQ: isi_migr_pworker
	2098	n/a	TCP	SyncIQ: isi_migr_pworker
	3148	n/a	TCP	SyncIQ: isi_migr_bandwidth
	3148	n/a	TCP	SyncIQ: isi_migr_bandwidth
	5667	n/a	TCP	SyncIQ: isi_migr_sworker
	5668	n/a	TCP	SyncIQ: isi_migr_sworker
	8470	n/a	TCP	SyncIQ: isi_replicate

VPC network

PowerScale for Google Cloud aims to provide a truly scale-out and high-performance NAS storage for your cloud applications. It is important to design your Google Cloud VPC network correctly for different requirements. This section provides reference VPC network architectures when integrating PowerScale cluster with your cloud environment.

A PowerScale cluster can only have one VPC network authorized, and only compute resources within the VPC network can access the cluster by default. A private services connection is created between the authorized VPC network and Dell Technologies organization by implementing VPC peering. You can verify your settings within the VPC details page after the cluster is deployed. Perform the following steps to view the private service connection details.

1. Under your Google Cloud project page > **VPC network** tab, click **VPC network.**
2. Under the VPC network details, choose your authorized VPC network.
3. Click **Private service connection** to view the connection details, as shown in the following figure.

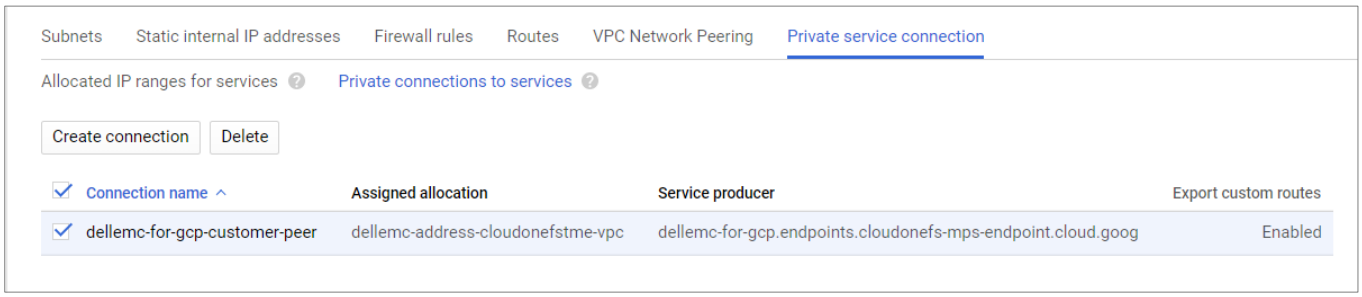

Figure 3. **Private service connection**

Perform the following steps to view the VPC network peering details.

1. Under your Google Cloud project page > **VPC network** tab, click **VPC network.**
2. Under the VPC network details, choose your authorized VPC network.
3. Click **VPC Network Peering** to view the network peering details, as shown in the following figure.

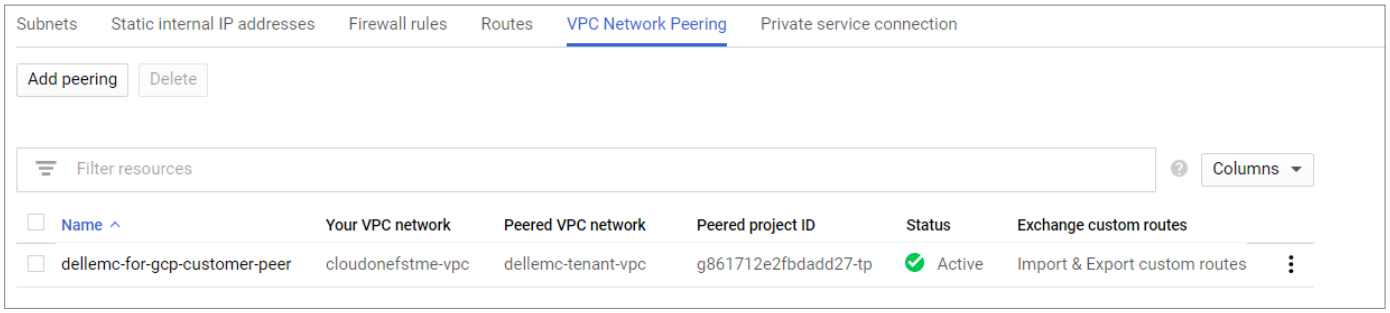

Figure 4. **VPC network peering**

When deploying a cluster, you can either use a shared VPC network or nonshared VPC network, depending on your business requirements. Figure 5 shows a reference architecture for using a shared VPC network. For more details, see the Google Cloud article Shared VPC Overview. Administrators can purchase storage capacity and create a cluster only in the host project, and the PowerScale cluster is associated with the shared VPC network in the host project. In this way, the shared network can be attached to any service project that requires access to the PowerScale data. Also, PowerScale cluster management is centralized within a single host project by default, you can also enable cluster management in service projects by opening a ticket.

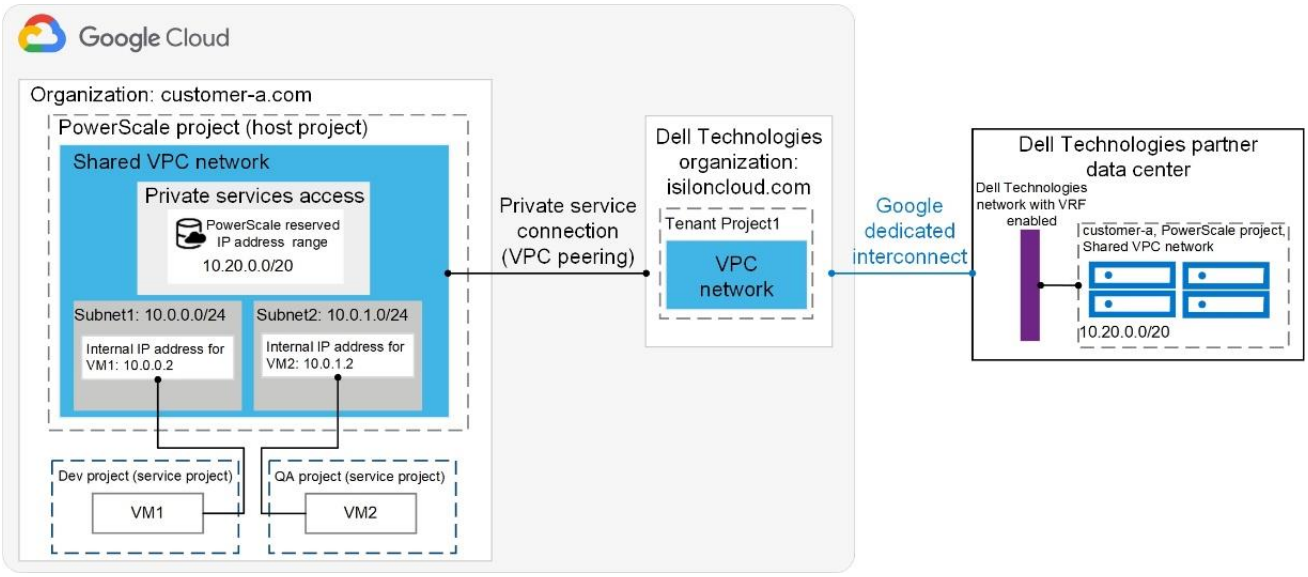

Figure 5. **Shared VPC network reference architecture**

Figure 6 shows a reference architecture for using a nonshared VPC network. Administrators must purchase storage capacity and create a cluster for each project or VPC network. The cluster is associated with a VPC network within the project, and the project administrators can manage the cluster based on business needs.

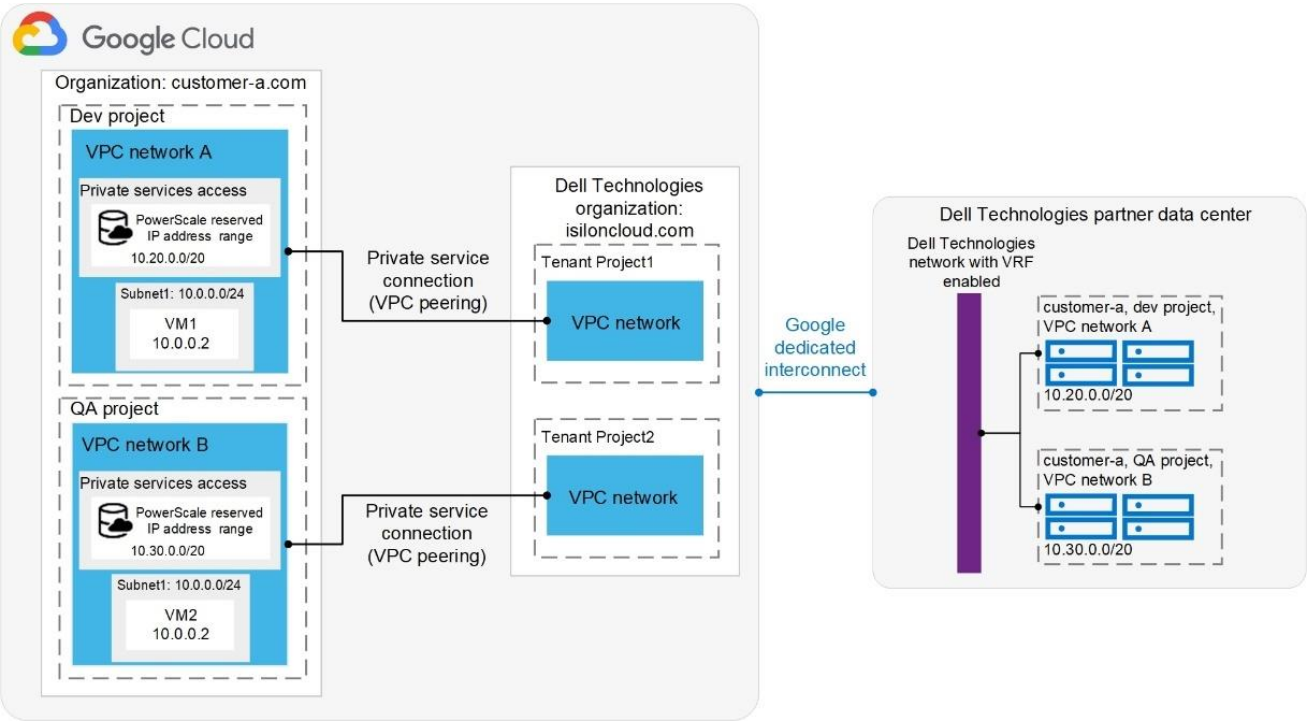

Figure 6. **Nonshared VPC network reference architecture**

Note: We recommend deploying your compute engine resource at the same region with your PowerScale cluster. This deployment enables a fast network by minimizing network latency.

Before you deploy PowerScale clusters, we recommend choosing an appropriate VPC network architecture based on your business needs. The following table is a comparison between a shared VPC network and a nonshared VPC network deployment model.

Table 2. VPC network deployment model

	Shared VPC network	Nonshared VPC network
Management	Centralized within a single host project by default.	Each project owns its cluster without sharing with other projects.
Data sharing	Accessible across different projects.	Accessible within project by default.
Flexibility	Any service project can be attached to the host project as needed.	A new cluster should be created if a new project added.
Storage utilization and cost	Multiple business units can use the same cluster, improving storage utilization and reducing TCO.	May leave more unused capacity as each project owns a dedicated cluster.

Cluster service FQDN

OneFS uses the cluster service FQDN as its SmartConnect Zone name with a round-robin client-connection balancing policy. The round-robin policy is a default setting and is recommended for most cases in OneFS. For more details about the OneFS SmartConnect load-balancing policy, see Dell PowerScale: Network Design Considerations.

After the cluster is deployed, you must find the OneFS SmartConnect service IP in the clusters page within Google Cloud Console. Then, configure your DNS server to delegate the cluster service FQDN zone to the OneFS Service IP. Figure 7 shows the DNS configuration by leveraging Google Cloud DNS along with a DNS server in the project. You must configure a forwarding rule in Google Cloud DNS which forwards the cluster service FQDN query to the DNS server and set up a zone delegation on the DNS server which point to the cluster service IP. The following steps illustrate the final DNS query flow for Cluster service FQDN. See Appendix B: SmartConnect setup example for a configuration example.

1. VM clients send the DNS request for the Cluster service FQDN to the Google Cloud DNS service.
2. The Google Cloud DNS forwards the request to the DNS server.
3. The DNS server forwards the request to the cluster service IP. The service IP is responsible for translating the cluster service IP into an available node IP.
4. SmartConnect returns a node IP to the client. The client can access the cluster data through the cluster service FQDN.

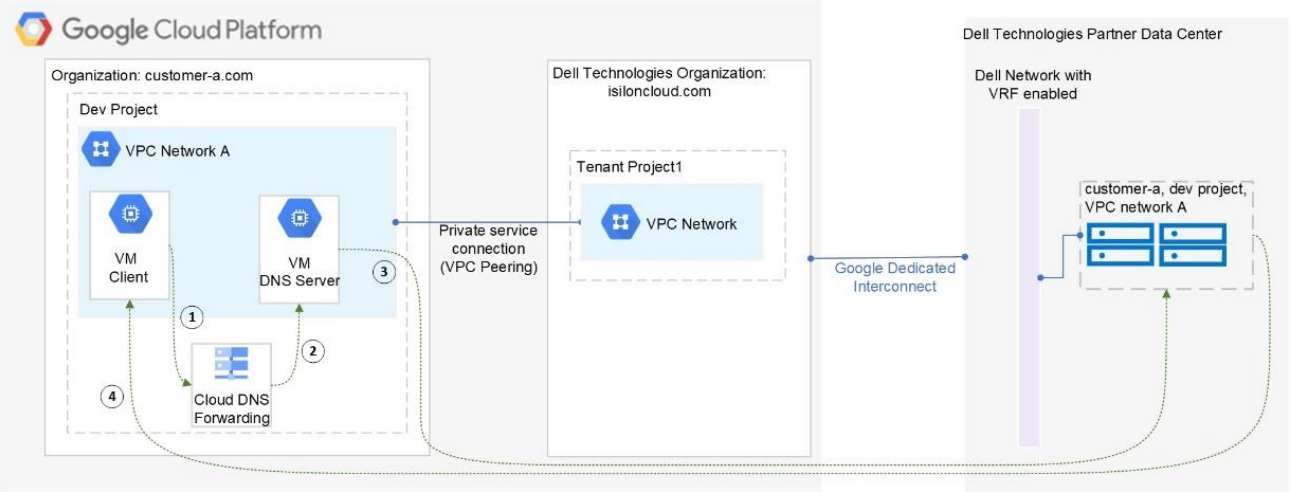

Figure 7. **Cluster service FQDN and DNS setup**

Note: Google Cloud DNS cannot communicate with OneFS cluster directly, therefore, we use a DNS server which is located in the authorized VPC network to forward SmartConnect DNS request to cluster.

IAM roles consideration

Introduction

Google Cloud Identity and Access Management (IAM) enables administrators to control who can perform actions on specific cloud resources. PowerScale for Google Cloud is a managed service for cloud users and is integrated with Google Cloud Console. Appropriate IAM permissions are required to deploy and manage PowerScale clusters. This section introduces the required IAM roles for the solution.

Dell Technologies managed roles

Administrators can purchase storage capacity with different node models and manage clusters within Google Cloud Console. Dell Technologies provides predefined roles that give granular operation control on orders and clusters while preventing unwanted operation on the resources. The following table lists these roles, their description, and the permissions assigned to the roles.

Table 3. Dell Technologies managed roles

Role name	Title	Description	Permissions
roles/dellemccloudonefs.admin	Dell EMC Cloud OneFS Admin	• Create and manage orders in Google Cloud Console • Create and manage cluster in Google Cloud Console, including advanced settings in storage administration portal and data protection administration portal • Must be used along with the predefined roles mentioned in IAM predefined roles requirement	• cloudonefs.isiloncloud.com/clusters.create • cloudonefs.isiloncloud.com/clusters.delete • cloudonefs.isiloncloud.com/clusters.get • cloudonefs.isiloncloud.com/clusters.list • cloudonefs.isiloncloud.com/clusters.update • cloudonefs.isiloncloud.com/clusters.updateAdvancedSettings • cloudonefs.isiloncloud.com/fileshares.create • cloudonefs.isiloncloud.com/fileshares.delete • cloudonefs.isiloncloud.com/fileshares.get • cloudonefs.isiloncloud.com/fileshares.list • cloudonefs.isiloncloud.com/fileshares.update • resourcemanager.projects.get • resourcemanager.projects.list
roles/dellemccloudonefs.user	Dell EMC Cloud OneFS Users	• Create and manage orders in Google Cloud Console • Create and manage cluster in Google Cloud Console, except the advanced settings • Must be used along with the predefined roles mentioned in IAM predefined roles requirement	• cloudonefs.isiloncloud.com/clusters.create • cloudonefs.isiloncloud.com/clusters.delete • cloudonefs.isiloncloud.com/clusters.get • cloudonefs.isiloncloud.com/clusters.list • cloudonefs.isiloncloud.com/clusters.update • cloudonefs.isiloncloud.com/fileshares.create • cloudonefs.isiloncloud.com/fileshares.delete • cloudonefs.isiloncloud.com/fileshares.get • cloudonefs.isiloncloud.com/fileshares.list • cloudonefs.isiloncloud.com/fileshares.update • resourcemanager.projects.get • resourcemanager.projects.list

Role name	Title	Description	Permissions
roles/dellemccloudonefs.viewer	Dell EMC Cloud OneFS Viewer	• Read-only permission to the settings of orders and clusters	• cloudonefs.isiloncloud.com/clusters.get • cloudonefs.isiloncloud.com/clusters.list • cloudonefs.isiloncloud.com/fileshares.get • cloudonefs.isiloncloud.com/fileshares.list • resourcemanager.projects.get • resourcemanager.projects.list

IAM predefined roles requirement

Except for the Dell Technologies managed roles assigned to your administrator account, you must grant the following roles to the account when implementing the PowerScale for Google Cloud solution.

- Organization Viewer (roles/resourcemanager.organizationViewer): Ensure the account is a member of organization.
- Service Networking Admin (roles/servicenetworking.networksAdmin): This is required for creating private service connection by implementing VPC peering.
- DNS Administrator (roles/dns.admin): Allow user to delegate the cluster service FQDN zone to the OneFS Service IP.
- Service Usage Admin (roles/serviceusage.serviceUsageAdmin): This is required for cluster management.
- Compute Network Admin (roles/compute.networkAdmin): This is required when configuring VPC network-related settings.
- Billing Account Administrator (roles/billing.admin): This is required when creating orders to purchase storage capacity.

We recommend only assigning these roles to administrators who are responsible for deploying and managing the PowerScale for Google Cloud solution.

If you require an account that has read-only permissions on the clusters and orders, ensure that only the Dell EMC Cloud OneFS Viewer (roles/dellemccloudonefs.viewer) role is granted to the account. All the control buttons are inaccessible, as shown in the following figure.

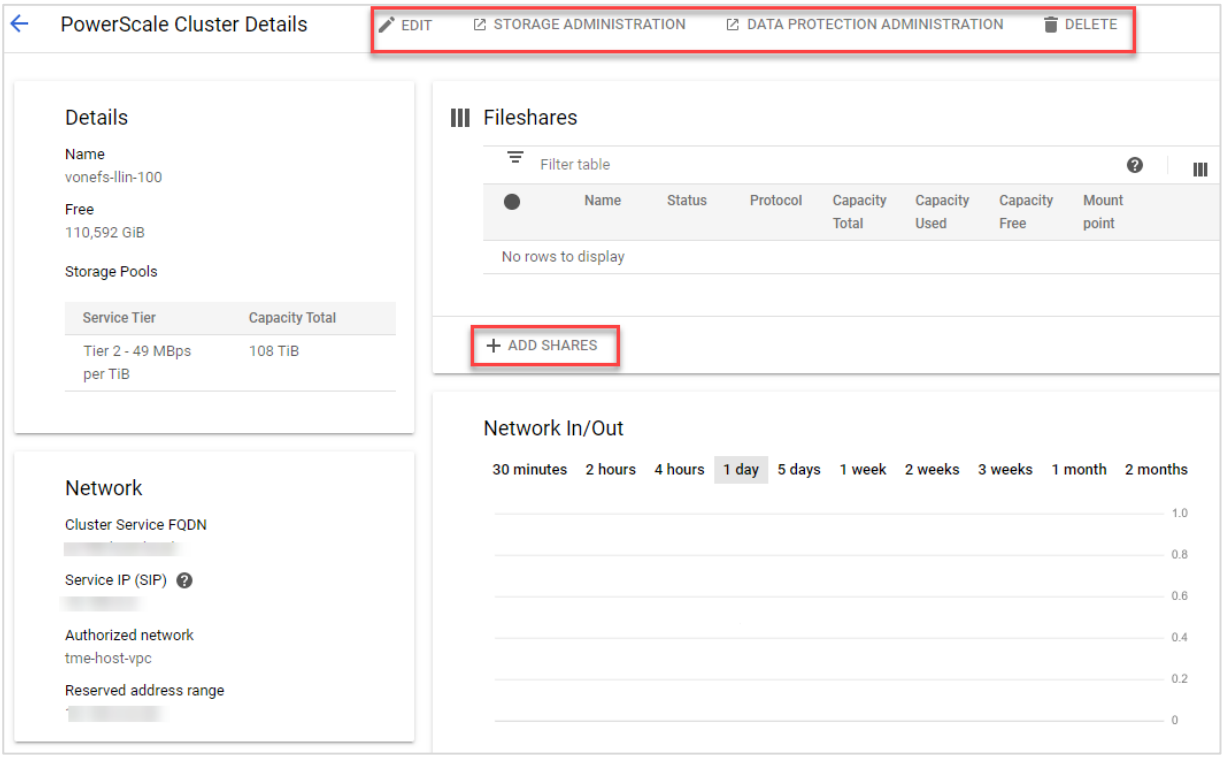

Figure 8. **Dell EMC Cloud OneFS Viewer role**

Appendix A: PowerScale for Google Cloud management responsibility matrix

Google Cloud Console cluster management

The following table shows the cluster management responsibility on Google Cloud Console.

Table 4. Google Cloud Console cluster management

Feature	Availability	Notes
Clusters Overview		
List	Self-service	
Create	Self-service	
Update	Self-service	
Cluster name	Self-service	
Add/remove capacity to existing cluster	Open ticket	
FQDN change	Open ticket	
Delete	Self-service	
Cluster Details		
Cluster Information	Self-service	
Graphs		
Network In/Out	Self-service	
Capacity Used/Total	Self-service	
Read/Write Operations Count	Self-service	
File shares		
List	Self-service	
Create	Self-service	SMB, NFS or both with default settings
Update	Self-service	Update capacity
Delete	Self-service	
GCP Networking		
VPC Peering for single VPC	Self-service	At cluster creation
VPC Peering with additional VPC	Open ticket	

Storage Administration punchout WebUI

The following table shows the Storage Administration management responsibility on punchout WebUI.

Table 5. Storage Administration punchout WebUI

Feature	Availability	Notes
Dashboard		
Access Overview	Self-service	
Cluster Management > **Network configuration** > DNS servers	Open ticket	Open ticket to change from default DNS server
File system		
File system explorer		
Explorer	Self-service	Create and edit directories in customer access zone
Access		
Access zones		
Single Access Zone	Self-service	Extra access zones are not supported
Authentication providers		
Google Cloud Auth Provider	Not supported	
Active Directory	Self-service	
LDAP	Self-service	
NIS	Self-service	
Local provider	Self-service	
File provider	Self-service	
Kerberos provider	Self-service	
Kerberos settings	Self-service	
Membership and roles		
Users	Self-service	
Groups	Self-service	
Roles	Not supported	
User mapping	Self-service	
ACL policy settings		
ACL policy settings	Open ticket	Ability to update settings by support ticket
Settings		
Global provider settings	Open ticket	Ability to update settings by support ticket

Feature	Availability	Notes
Protocols		
SMB		
SMB shares	Self-service	
Default share settings	Self-service	
SMB server settings	Open ticket	SMB V2, V3 Enabled by default, open ticket to change
NFS		
NFS exports	Self-service	
NFS aliases	Self-service	
Export settings	Self-service	
Global settings	Open ticket	NFSv3 Enabled by default, NFSv4 available by support ticket
Zone settings	Self-service	
HDFS		Disabled by default
Settings	Open ticket	
Ranger plugin settings	Open ticket	
Proxy users	Open ticket	
Virtual racks	Open ticket	

Data Protection Administration punchout WebUI

The following table shows the Storage Administration management responsibility on punchout WebUI.

Table 6. Data Protection Administration punchout WebUI

Feature	Availability	Notes
Dashboard		
Access Overview	Self-service	
SnapshotIQ		
Snapshots	Self-service	
Snapshot schedules	Self-service	
Settings	Self-service	
SyncIQ		Only unencrypted SyncIQ connection is supported
Summary	Self-service	
Policies	Self-service	
Reports	Self-service	
Local targets	Self-service	

Feature	Availability	Notes
Performance rules	Self-service	
Settings	Self-service	
File System > SmartQuotas		
Quotas and usage	Self-service	
Generated reports archive	Self-service	
Settings	Self-service	
Job Engine		
Tree Deletes	Open ticket	

Appendix B: SmartConnect setup example

Google Cloud DNS cannot communicate with OneFS cluster directly, therefore, we use a DNS server which is located in the authorized VPC network to forward SmartConnect DNS request to cluster. You can use either a Windows server or a Linux server. This documentation uses a Windows server as example to show the detail steps.

Obtain required cluster information:

The following information is required before setting up SmartConnect:

- **Cluster service FQDN**: This is the OneFS SmartConnect zone name used by clients.
- **Service IP**: This is the OneFS SmartConnect service IP which is responsible for resolving the client DNS request and returning an available node IP to clients.
- **Authorized network**: By default, only the machines on an authorized VPC network can access a PowerScale cluster.

Obtain the required information as follows:

1. In the Google Cloud Console navigation menu, click **PowerScale** and then click **Clusters**.
2. Find your cluster row to see the cluster service FQDN and service IP.

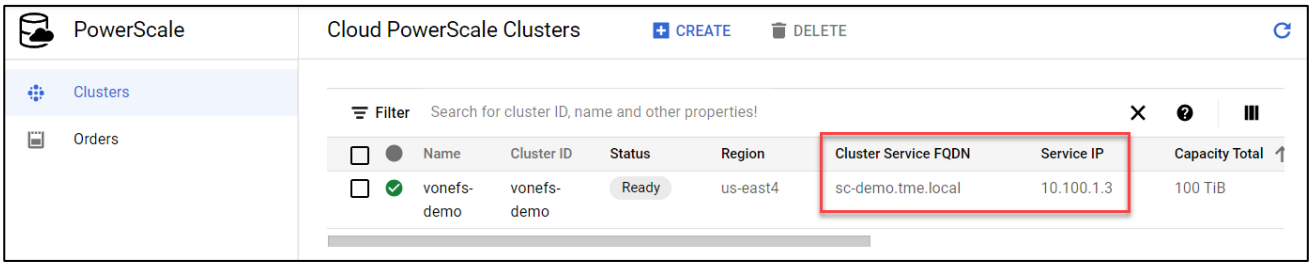

Figure 9. **Cluster service FQDN and service IP**

3. To find the authorized network information, click the name of the cluster. From the **PowerScale Cluster Details** page, find the authorized network from the **Network** information.

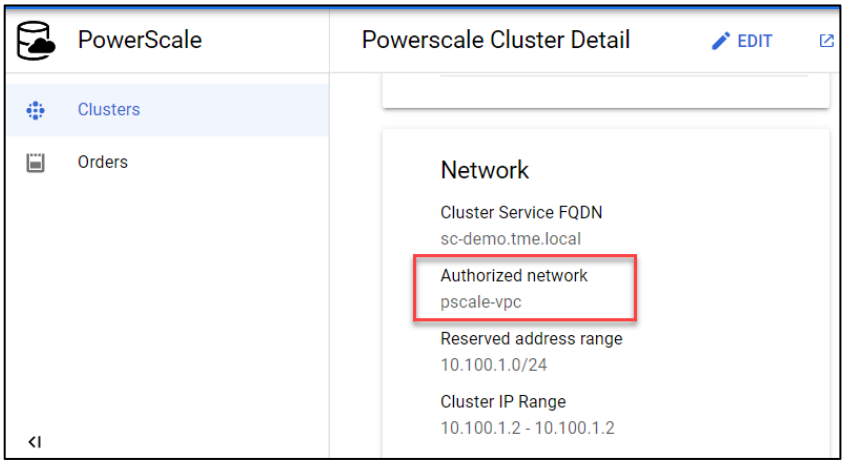

Figure 10. **Cluster authorized network**

Set up DNS server

If you already have an available DNS server that is connected to the cluster authorized network, you can leverage the existing DNS server and skip Step 1 and Step 2.

1. In the Google Cloud Console navigation menu, click **Compute Engine** and then click **VM instances**. This documentation will create a Windows VM instance as a DNS server. Making sure your DNS server is connected to the cluster authorized network.
2. Log in to the DNS server and install DNS Server Role in the Windows machine. If you are using a Linux machine, you can use Bind software instead.
3. Create a new DNS zone in DNS server, as shown in the following figure.

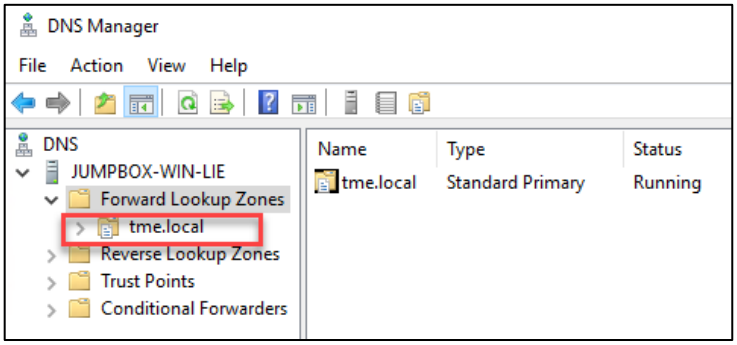

Figure 11. **Create DNS zone**

4. Create an (A) record for the cluster service IP. For more details, see *Dell PowerScale: Network Design Considerations*.

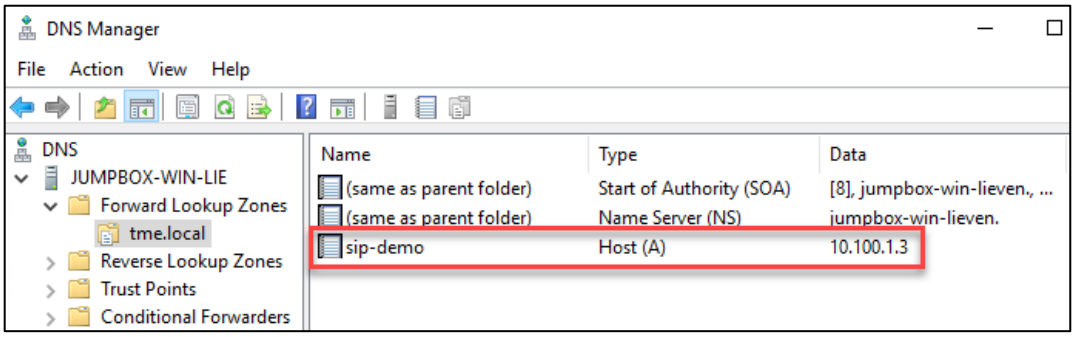

Figure 12. **Create service IP record**

5. Create a new delegation for your cluster service FQDN (it is sc-demo.tme.local in this example) and point the delegation server to the cluster service IP (A) record that you created (it is sip-demo.tme.local in this example).

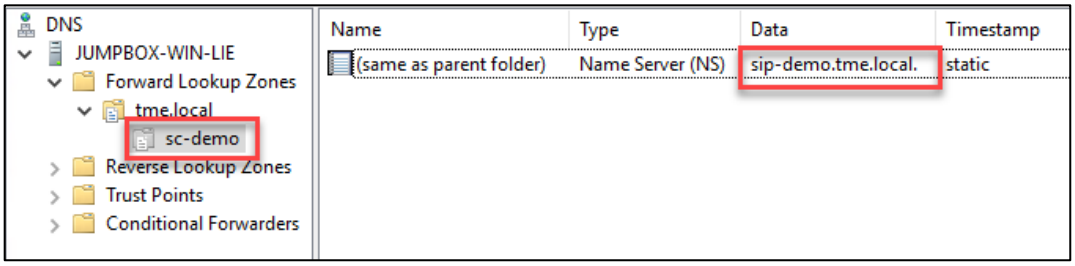

Figure 13. **Cluster service FQDN delegation**

Configure Cloud DNS and firewall rules:

1. In the Google Cloud Console navigation menu, click **Network services,** and click **Cloud DNS**.
2. Click the **CREATE ZONE** button.
3. Choose the **Private** zone type and input your Cluster Service FQDN in the DNS name field. Then, choose the **Forward queries to another server** and your cluster authorized network.

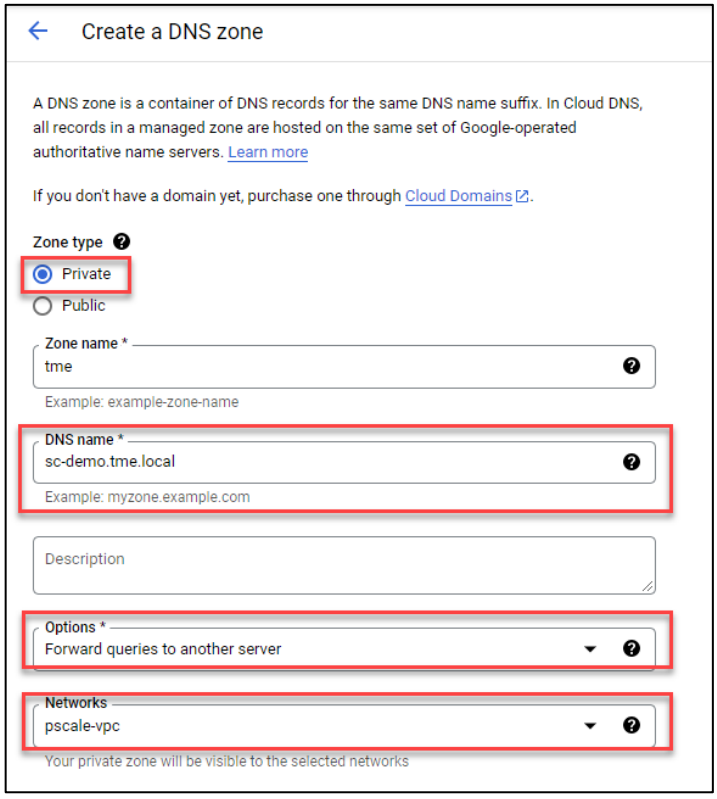

Figure 14. **Create Cloud DNS zone**

4. Obtain the DNS server IP address configured in the **Set up DNS server** step.
5. Point the destination DNS server to your own DNS server IP address. And click **CREATE** button.

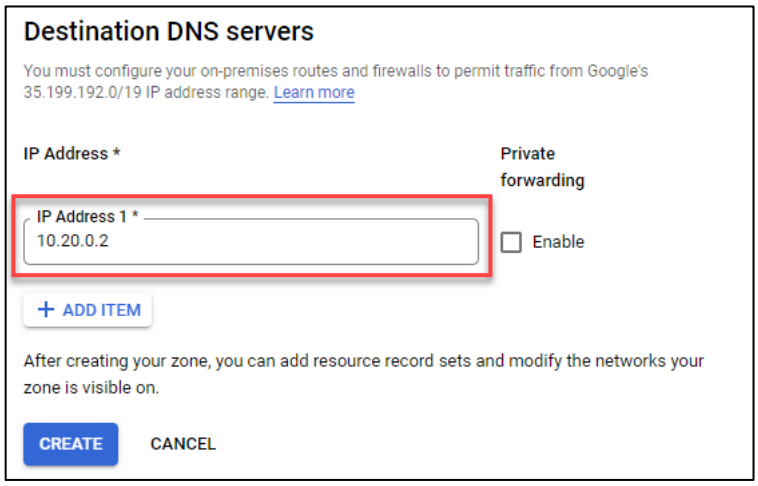

Figure 15. **Destination DNS servers**

6. Adding firewall rules to allow ingress DNS traffic to your DNS server from Cloud DNS. In the Google Cloud Console navigation menu, click **VPC network** and then click **Firewall**.
7. Click the **CREATE FIREWALL RULE** button.
8. Create a new Firewall rule and include the following options, as shown in Figure 16:
   - In the Network field, making sure the cluster authorized network is selected.
   - Source filter: IPv4 ranges
   - Source IPv4 ranges: 35.199.192.0/19. This is the IP range Cloud DNS requests will originate from. See Cloud DNS zones overview for more details.
   - Protocols and ports: TCP 53 and UDP 53.

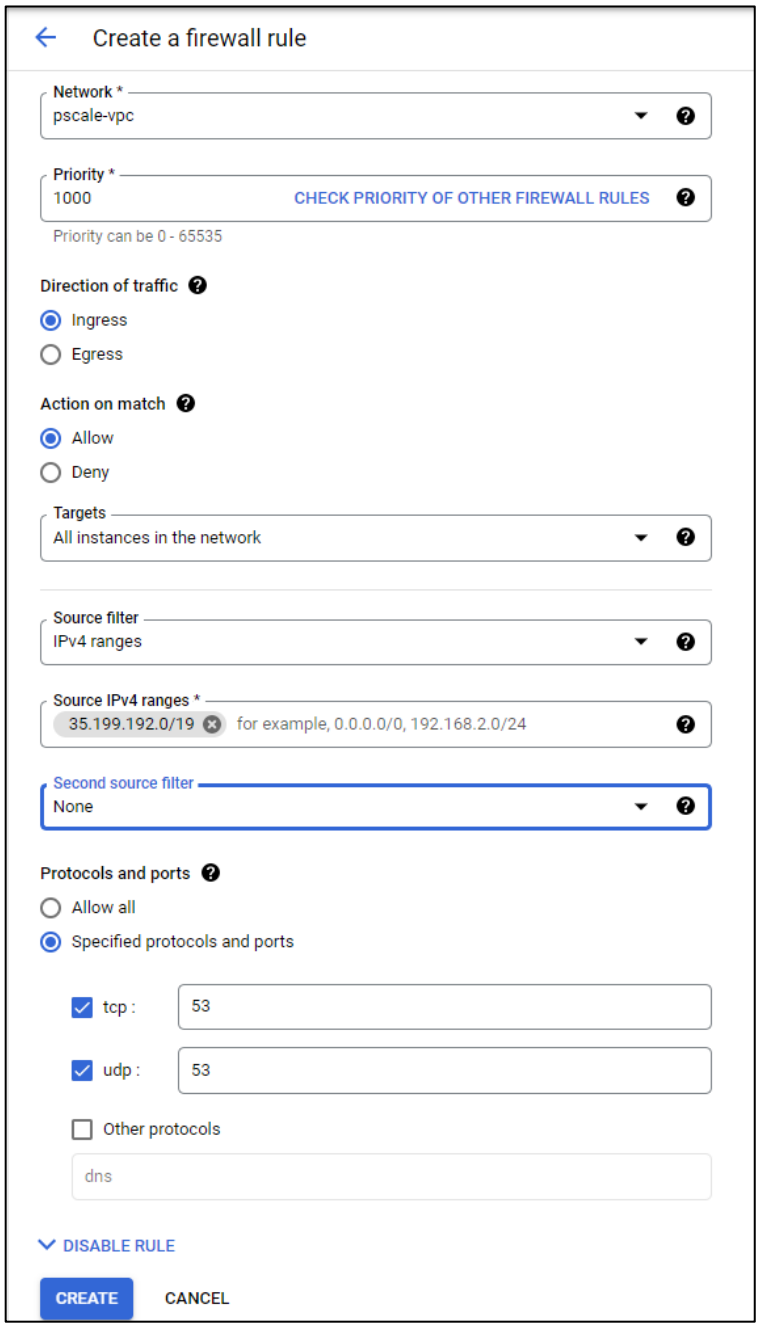

Figure 16. **Create firewall rule**

9. The created firewall rule in Google Cloud is displayed.

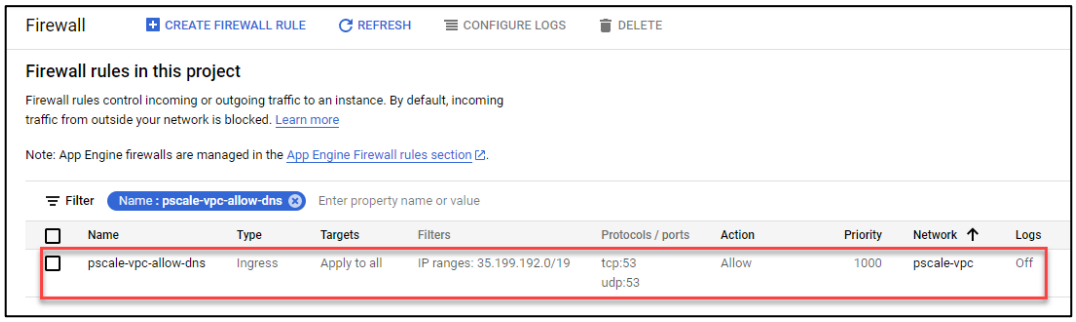

Figure 17. **Google Cloud firewall rule**

Verify your SmartConnect:

1. Log in to a VM instance that is connected to an authorized network. (This example uses a Linux machine.)
2. Resolve the cluster service FQDN using nslookup, and mount a file share using NFS.

```
$ nslookup sc-demo.tme.local
Server:         169.254.169.254
Address:        169.254.169.254#53

Non-authoritative answer:
Name:   sc-demo.tme.local
Address: 10.100.1.2

$ sudo mount -t nfs -vo nfsvers=3 sc-demo.tme.local:/test-fileshare
/mnt
mount.nfs: timeout set for Wed Dec  8 23:46:50 2021
mount.nfs: trying text-based options 'nfsvers=3,addr=10.100.1.2'
mount.nfs: prog 100003, trying vers=3, prot=6
mount.nfs: trying 10.100.1.2 prog 100003 vers 3 prot TCP port 2049
mount.nfs: prog 100005, trying vers=3, prot=17
mount.nfs: portmap query retrying: RPC: Timed out
mount.nfs: prog 100005, trying vers=3, prot=6
mount.nfs: trying 10.100.1.2 prog 100005 vers 3 prot TCP port 300
[lieven_lin@nfs-instance ~]$ df -h /mnt
Filesystem                      Size  Used Avail Use% Mounted on
sc-demo.tme.local:/test-fileshare  100G     0  100G   0% /mnt
```

Appendix C: References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- PowerScale Info Hub
- OneFS quota management
- OneFS Web Administration Guide
- Dell PowerScale: Network Design Considerations
- PowerScale OneFS Technical Specifications Guide
- Dell PowerScale OneFS: Security Considerations
- Service Description Dell Technologies PowerScale for Google Cloud

Google documentation

See the following Google documentation for more information:

- Dell Cloud PowerScale for Google Cloud
- Google Cloud VPC

The procedure to engage Dell support is mostly a Google process. The link for managing cases with the Google Support service is: https://cloud.google.com/support/docs/manage-cases.