VMware Cloud on AWS Integration with AWS Storage Gateway

VMware General

vmware by Broadcom © VMware LLC.

Table of contents

vmware by Broadcom © VMware LLC.

VMware Cloud on AWS Integration with AWS Storage Gateway

Overview

Introduction

VMware's multi-cloud strategy enables customers to seamlessly migrate on-premises vSphere workloads into a vSphere platform on their cloud provider of choice. Two significant factors in the selection of provider are the native services they offer and the ease of integration.

VMware customers looking to leverage the 200+ products and services offered through Amazon Web Services (AWS) choose VMware Cloud on AWS (VMC on AWS) as their cloud-based migration platform.

The AWS Storage Gateway service provides secure, scalable cloud-based storage that is directly accessible from workloads in VMC on AWS. VMC on AWS flexibility allows the use of different methods of integration with native AWS services, depending on customer preference.

We will examine different ways to connect from VMC on AWS to AWS Storage Gateway, allowing Solution Architects and Administrators within a Cloud Centre of Excellence to determine the most appropriate method for their organization.

Purpose of This Tutorial

This article will provide a setup guide and illustrate the integration between VMware Cloud on AWS and the AWS Storage Gateway service using two separate approaches: via Transit Connect to a customer's existing Virtual Private Cloud (VPC) and via the VPC directly connected to the VMC on AWS software-defined datacentre (SDDC).

Following the configuration walkthrough, we'll discuss the pros and cons of each approach.

Audience

This tutorial is intended for Cloud Solution Architects and Administrators. It assumes the reader has a basic understanding of native Amazon Web Services and VMware Cloud on AWS terminology and infrastructure.

© VMware LLC.

Procedure

Introduction

AWS Storage Gateway is a set of hybrid cloud storage services that provide access to virtually unlimited cloud storage. We will deploy and configure AWS Storage Gateway appliances in a VMware Cloud on AWS SDDC in File Gateway mode. Workloads in the SDDC can map to file shares provided by an AWS Storage Gateway appliance, which also acts as a file cache. Shares are available as either SMB or NFS, and the actual data is kept in an AWS S3 bucket under control of the customer.

To demonstrate connectivity options to the AWS Storage Gateway, we will configure two gateways and corresponding gateway appliances:

1. AWS-Storage-Gateway-1 will share files stored in S3 bucket s3-sgw-1. The S3 bucket will be accessed from the SDDC through the Connected VPC (a.k.a. the "Sidecar VPC") using an S3 Interface Endpoint in a Connected VPC subnet. A Storage Gateway Interface Endpoint will be placed in the same VPC to allow control plane communication between the appliance and Storage Gateway.
2. AWS-Storage-Gateway-2 will share files stored in S3 bucket s3-sgw-2. The S3 bucket will be accessed from the SDDC through a VMware-managed Transit Gateway (vTGW) to an S3 Interface Endpoint in a subnet of a customer's existing VPC ("External VPC"). A Storage Gateway Interface Endpoint will be placed in the same VPC to allow control plane communication between the appliance and Storage Gateway.

Here's what we will build out:

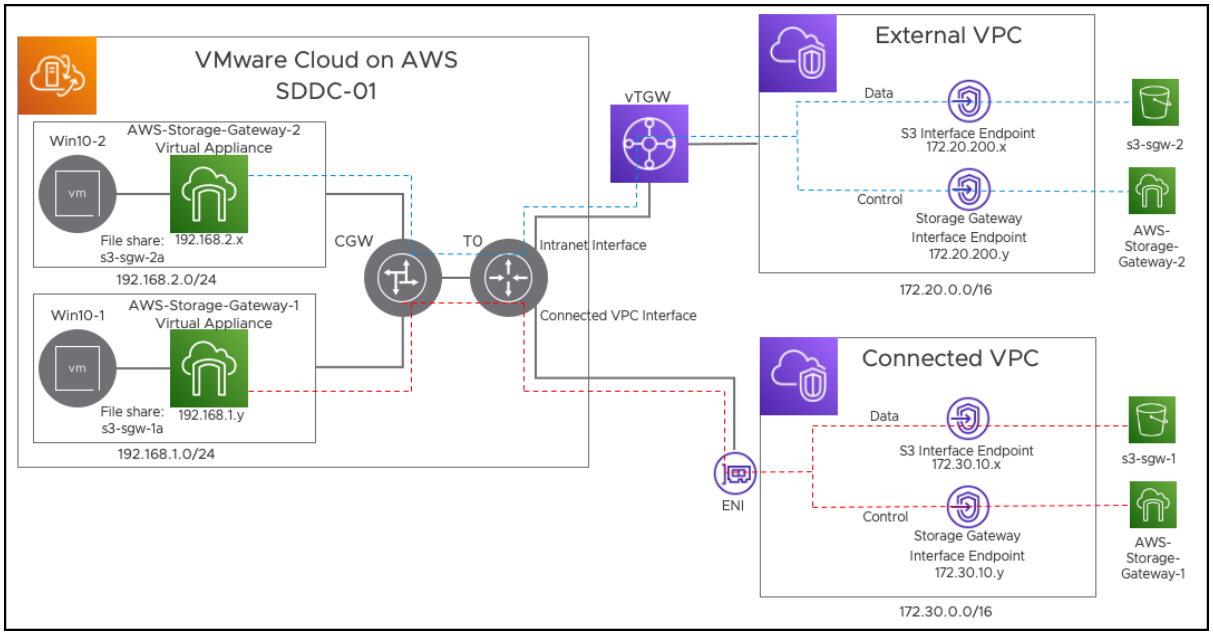

Figure 1: Final Setup

Prerequisites

SDDC, SDDC Group, VPC Connectivity

We will focus on the deployment, configuration, and connectivity of the Storage Gateways, not on the detail of provisioning the underlying SDDC and AWS infrastructure. The following has been deployed and configured:

- Single-host VMC on AWS SDDC (SDDC-01)

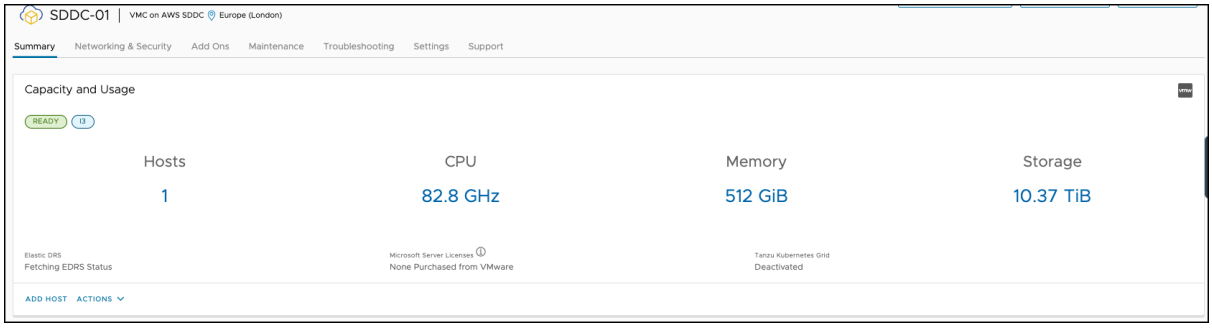

Figure 2: VMware Cloud on AWS SDDC, view from VMC on AWS Console

- SDDC Group containing the one SDDC (SDDC-Group-01), which results in the automatic creation of a VMware-managed transit gateway (vTGW or Transit Connect) with an attachment to the SDDC

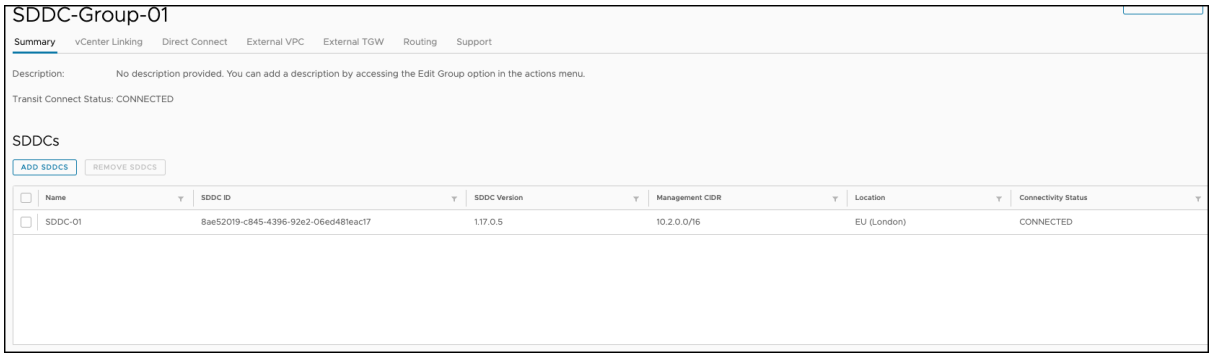

Figure 3: SDDC Group, view from VMC on AWS Console

- An External VPC in AWS has been created and connected to the vTGW using a VPC attachment. The process for this can be found in the documentation for VMware Cloud on AWS, here: Attach a VPC to an SDDC Group

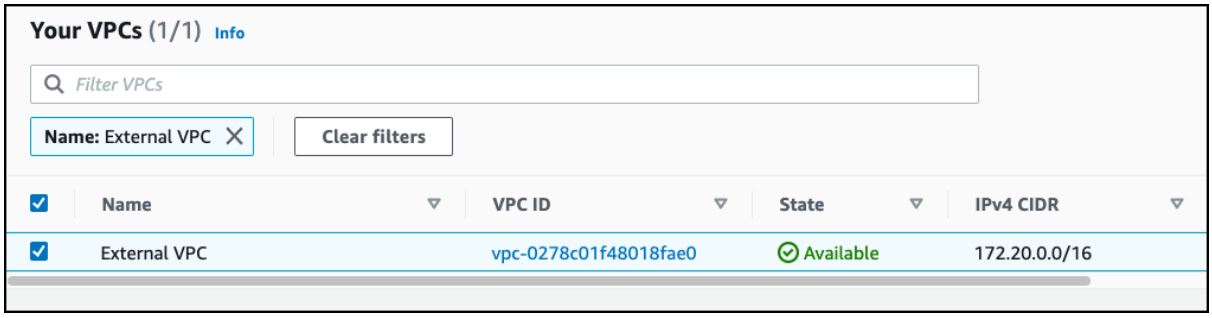

Figure 4: External VPC, view from AWS Console

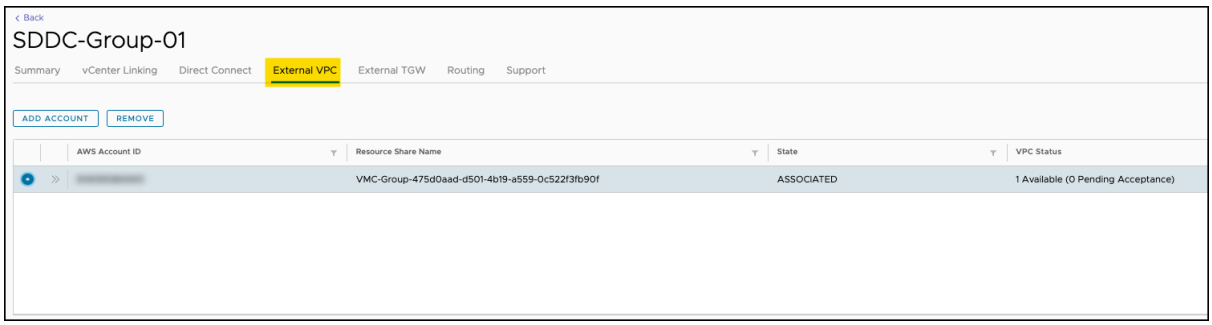

Figure 5: External VPC attachment in SDDC Group, view from VMC on AWS Console

SDDC / VPC Routes

External VPC

The SDDC and External VPC need routes over which to send traffic. To accomplish this, we have added a route for the External VPC CIDR to the VPC Attachment, as well as a return route to the SDDC in the External VPC.

Create a Route from the SDDC to the External VPC

This is done from "SDDC Groups" in the VMware Cloud Console:

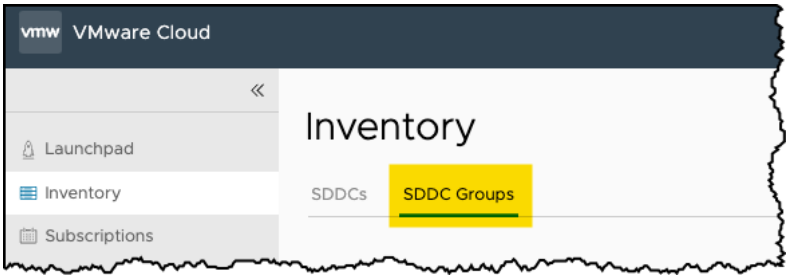

Figure 6: SDDC Groups, view from the VMC on AWS Cloud Console

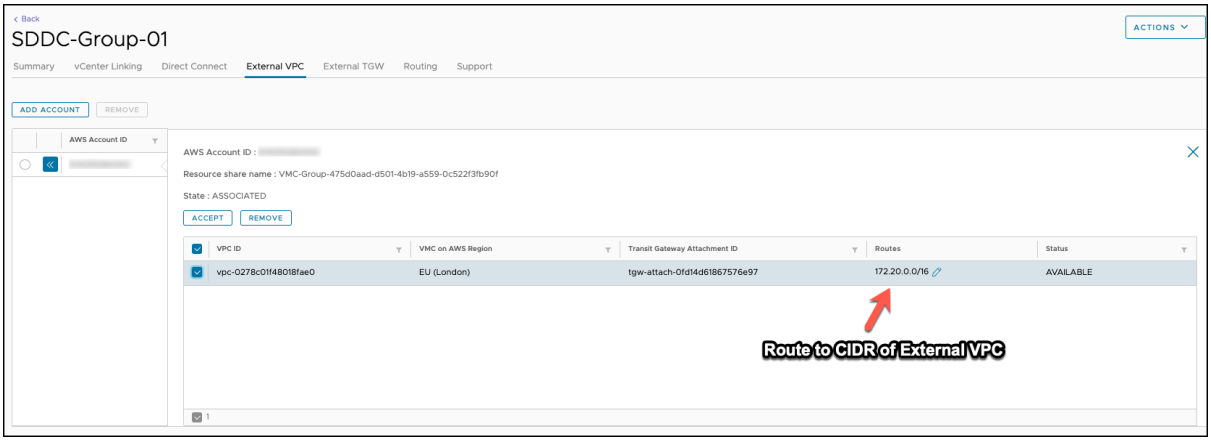

Figure 7: Route added to the VPC Attachment for the External VPC

Create a Route from the External VPC to the SDDC

This is done from "Route Tables" in the AWS Console:

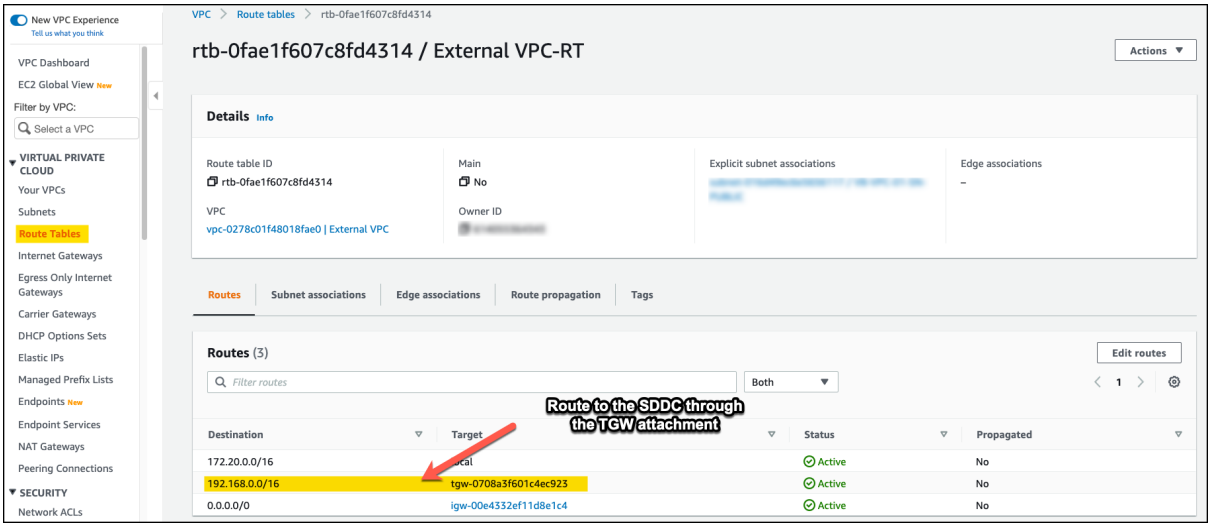

Figure 8: Route from External VPC to SDDC Subnets Containing Storage Gateway Appliances

© VMware LLC.

Connected VPC

The routing table of the T0 router in the SDDC is automatically populated with routes to the Connected VPC. Conversely, the main route table of the Connected VPC knows the routes back to all subnets within the SDDC. Nothing needs to be done here – this automatic route configuration is part of the VMware Cloud on AWS service.

SDDC Network Segments and Firewall Rules

We have created two segments/subnets within the SDDC and will place an AWS Storage Gateway appliance within each.

- The first appliance will be placed in "Segment-192-168-1-0"
- The second appliance will be placed in "Segment-192-168-2-0"

Firewall rules on the Compute Gateway allow all traffic to pass freely both to and from these segments for the purpose of illustration. A production environment should be more restrictive.

Storage Gateway Service Prerequisites

AWS S3 Buckets

AWS Storage Gateway uses S3 buckets in which to store file share data. We will create two S3 buckets, one for each AWS Storage Gateway.

From within the AWS Console, navigate to S3. Create an S3 bucket from the AWS Console. This will be bucket "s3-sgw-1" for the first Storage Gateway:

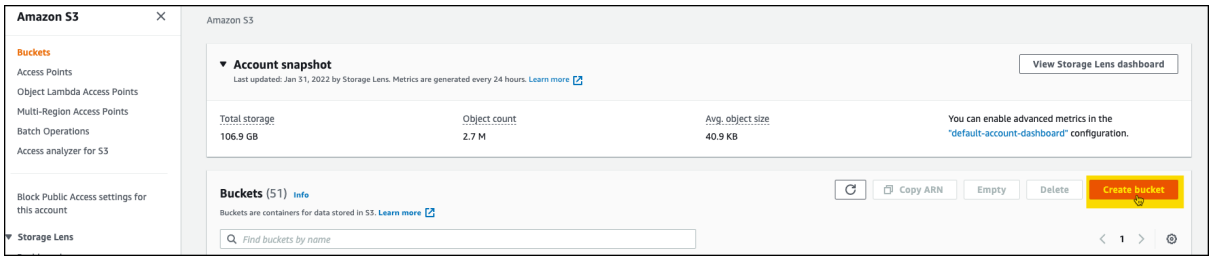

Figure 9: Bucket Creation

Default values can be used for the bucket:

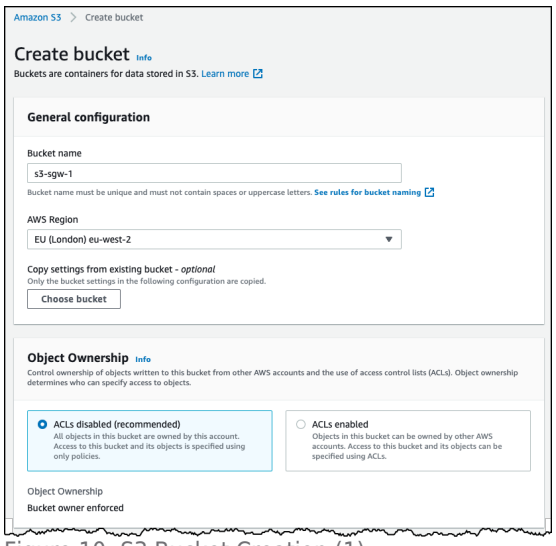

Figure 10: S3 Bucket Creation (1)

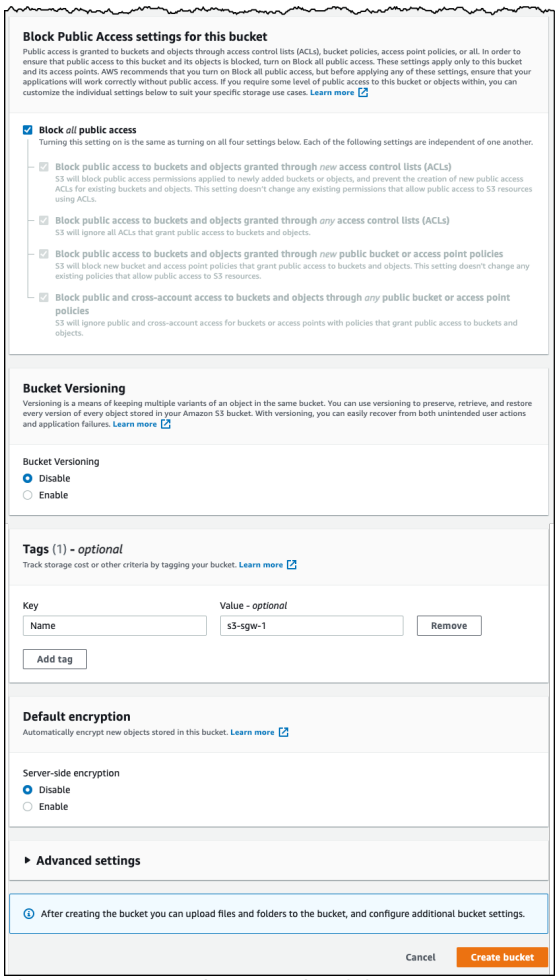

Figure 11 - S3 Bucket Creation (2)

The identical steps should be used to created bucket “s3-sgw-2”. When complete, we have two S3 buckets:

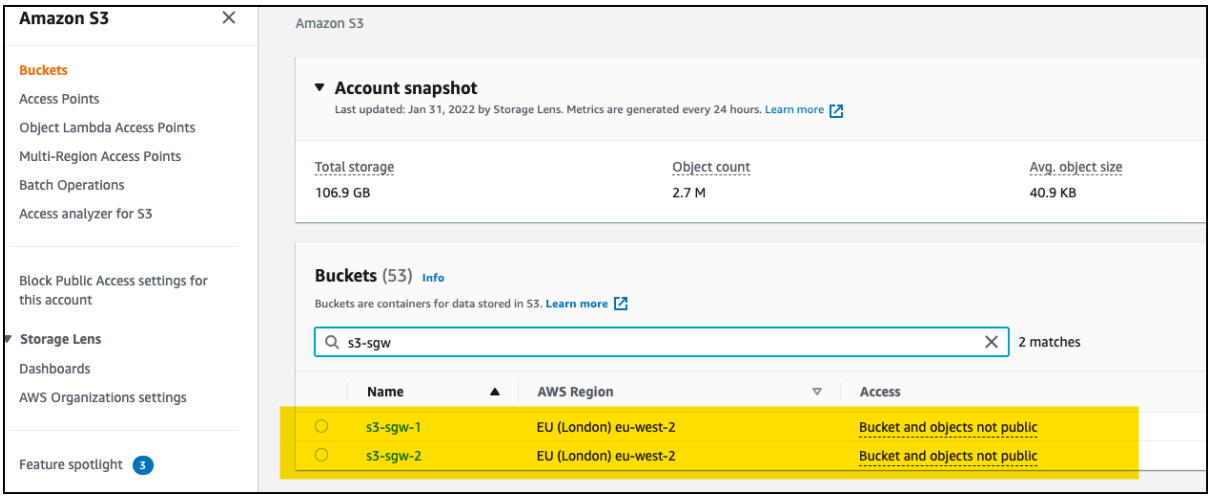

Figure 12: S3 Buckets for Storage Gateways 1 & 2

AWS Security Groups

Access to the S3 Buckets and Storage Gateway service will be provided by AWS Endpoints (see section below). Prior to creating the endpoints, we will create AWS Security Groups that restrict the traffic allowed to flow across the endpoints.

The Security Groups will be associated with a VPC. We will need a Security Group for S3 and for the Storage Gateway in both the External VPC and the Connected VPC.

- Access to S3 requires the endpoint to allow traffic to TCP 443 (HTTPS)
- Access to the Storage Gateway requires that the endpoint allow traffic to TCP ports 443, 1026-1028, 1031 and 2222

From the AWS Console, navigate to VPC Services and select Security Groups.

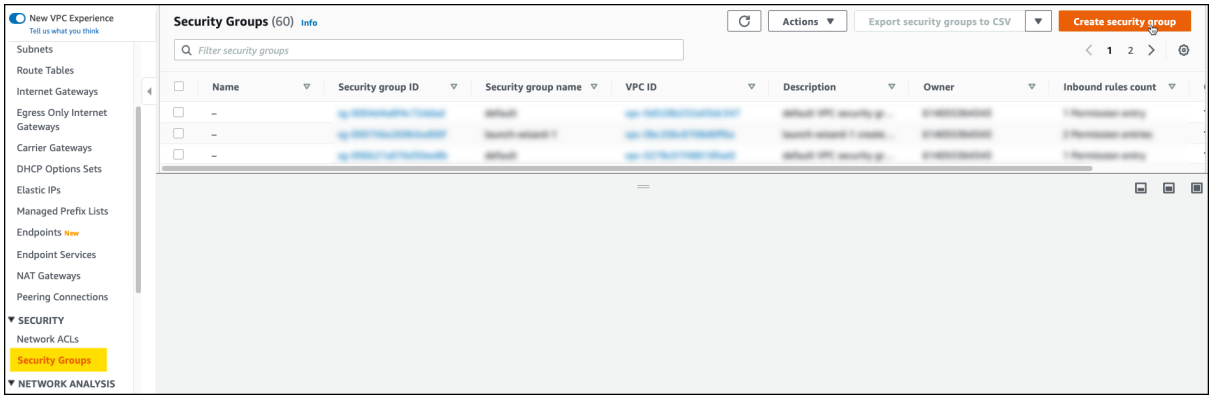

Figure 13: Create a Security Group

Create a Security Group named “S3-Endpoint-SG-External-VPC” for the External VPC allowing HTTPS Inbound:

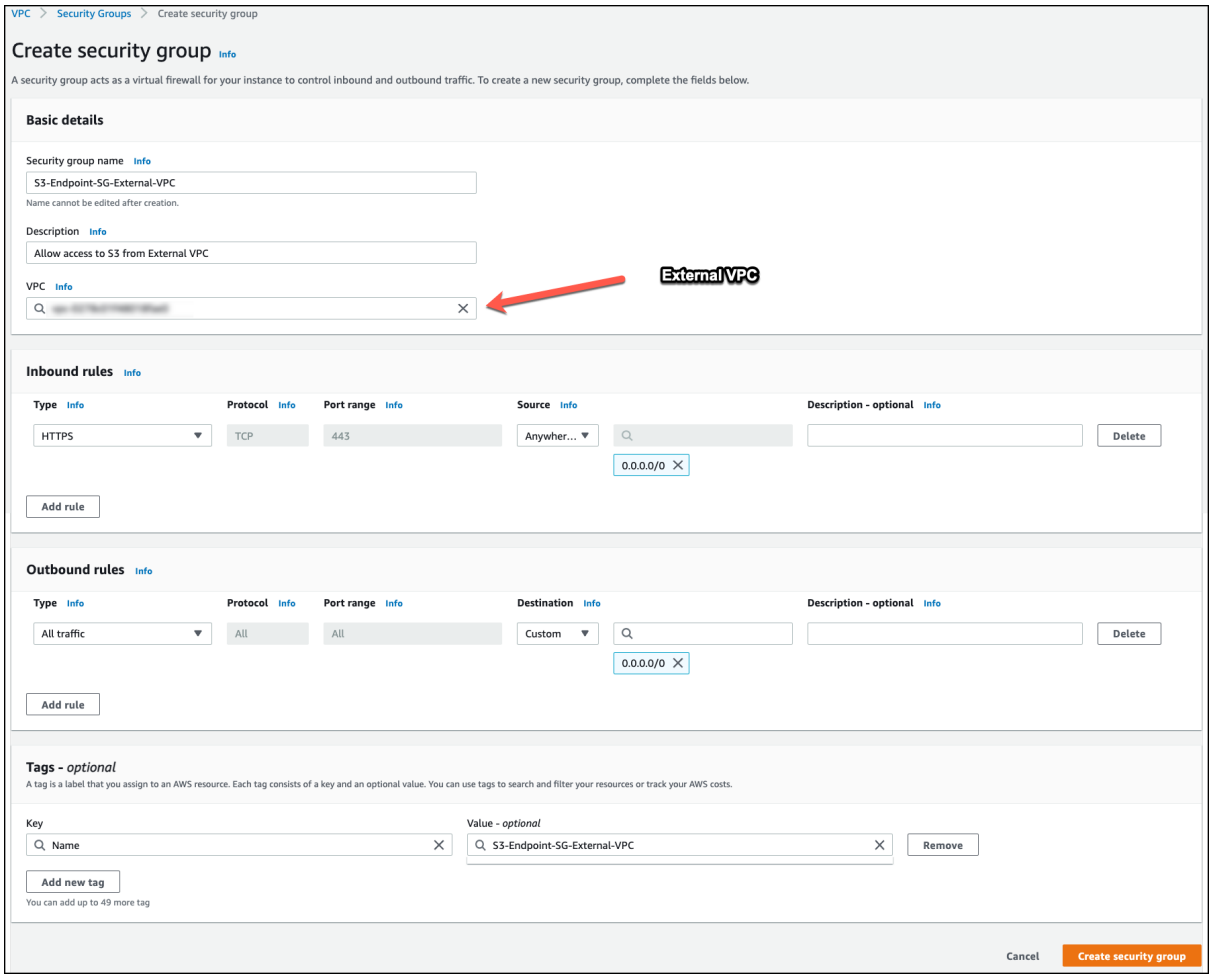

Figure 14: S3 Security Group for External VPC

Create a Security Group named “SGW-Endpoint-SG” for the External VPC allowing HTTPS 443, 1026-1028, 1031, 2222 Inbound:

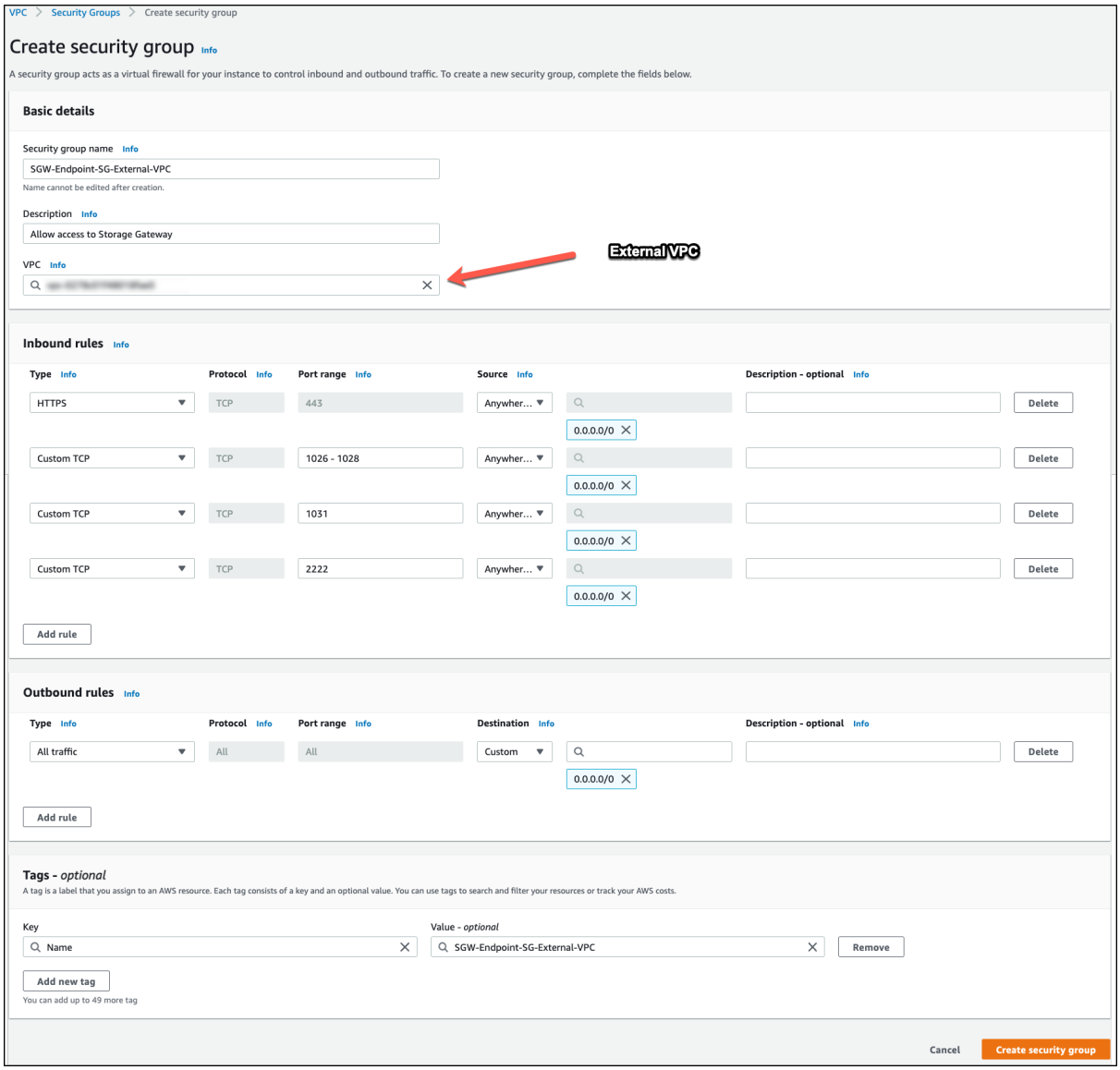

Figure 15: Storage Gateway Security Group for External VPC

Use the same process to create S3 and Storage Gateway Security Groups for the Connected VPC. After this step is complete, we have:

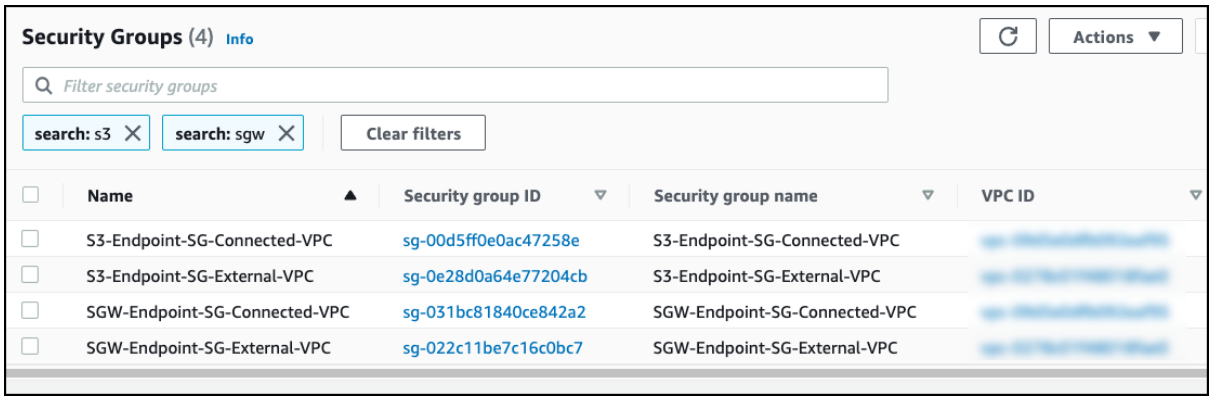

Figure 16: Full List of Required Security Groups

AWS Endpoints

An AWS Endpoint is a 'portal' to an AWS service. By placing an endpoint within an AWS VPC subnet, workloads that have access to the subnet can connect to the endpoint and access the desired service as if it was local to that subnet. For added security, traffic from the endpoint to the service can be routed over AWS PrivateLink, meaning it will stay within the AWS backbone and not travel over the public Internet.

The AWS Storage Gateway, configured in File Gateway mode, requires two endpoints:

- An AWS Storage Gateway endpoint for Storage Gateway control
- An AWS S3 endpoint for access to the S3 buckets containing the file share data

There are three kinds of AWS Endpoints: Interface Endpoints, Gateway Load Balancer Endpoints and Gateway Endpoints. We will use Interface Endpoints for our Storage Gateways. A Storage Gateway endpoint and an S3 interface endpoint will be created in both the External VPC and the Connected VPC.

NOTE: To avoid cross-Availability Zone (AZ) traffic charges, endpoints should be created in the same AZ as the workloads that will access them.

Endpoints are created from the AWS Console, within the VPC service:

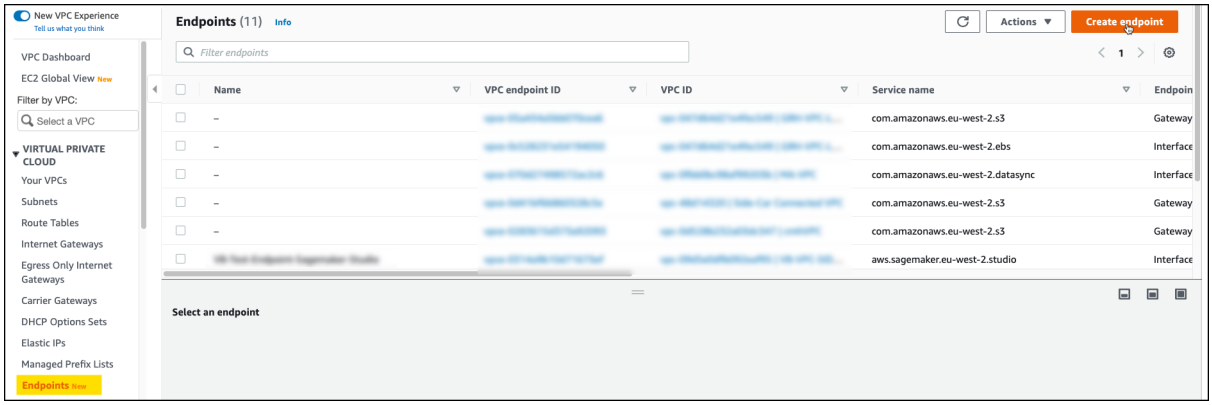

Figure 17: Endpoint Creation

Storage Gateway Interface Endpoints

After selecting "Create endpoint", populate the endpoint fields as shown below for the Storage Gateway endpoint for the External VPC:

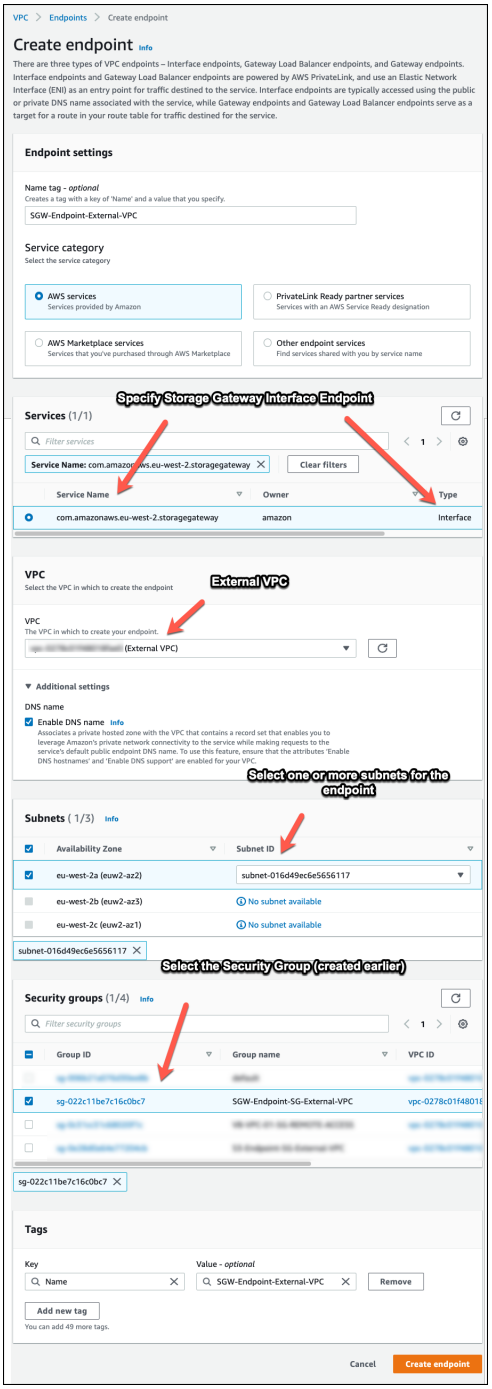

Figure 18: Storage Gateway Endpoint

Use the same process to create a Storage Gateway Interface Endpoint for the Connected VPC.

S3 Interface Endpoints

After selecting “Create endpoint” from VPC Endpoints in the AWS Console, populate the endpoint fields as shown below for the S3 endpoint for the External VPC:

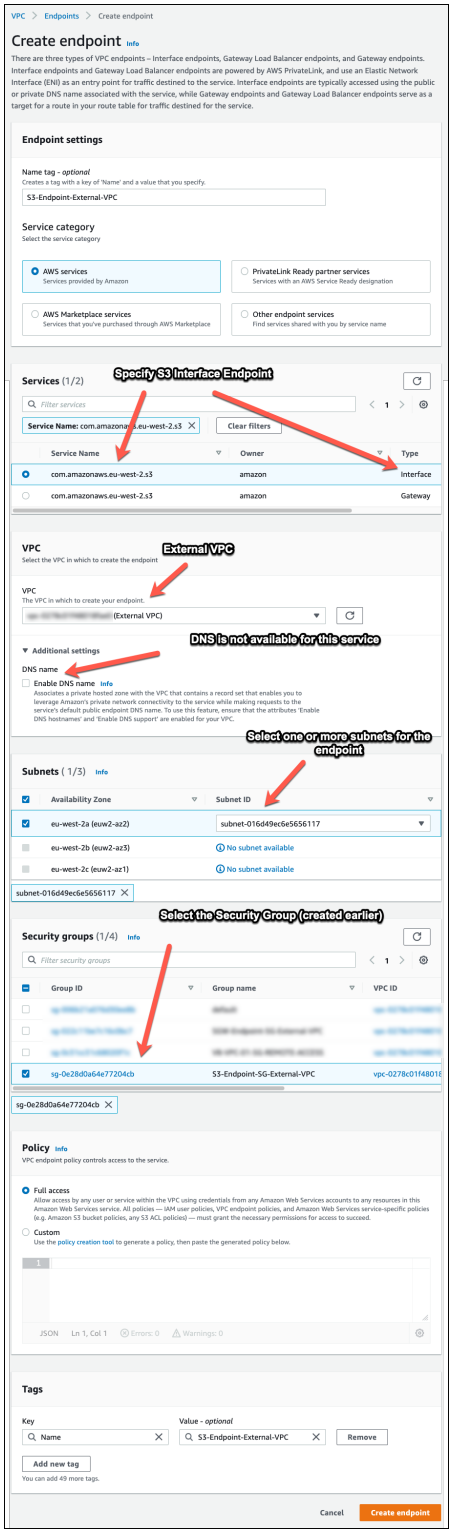

Figure 19: S3 Endpoint

Use the same process to create an S3 Interface Endpoint for the Connected VPC.

Storage Gateway Deployment

Gateway

At this point we have all the prerequisites in place to deploy the AWS Storage Gateways. We will call our first gateway “AWS-Storage-Gateway-1” and it will use the Connected VPC.

From within the AWS Console, navigate to Storage Gateway and select “Create Gateway”:

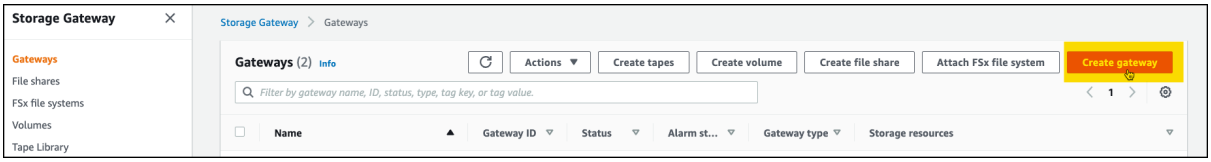

Figure 20: Create Storage Gateway

We will build an Amazon S3 File Gateway and will first download and install the Storage Gateway appliance (OVF Template) on our VMware Cloud on AWS SDDC.

If building more than one Storage Gateway, upload the template to a VMware Content Library in the SDDC and deploy from that location.

The steps for deploying the OVF template are given directly on the web page under “Set up gateway on VMware ESXi”:

© VMware LLC.

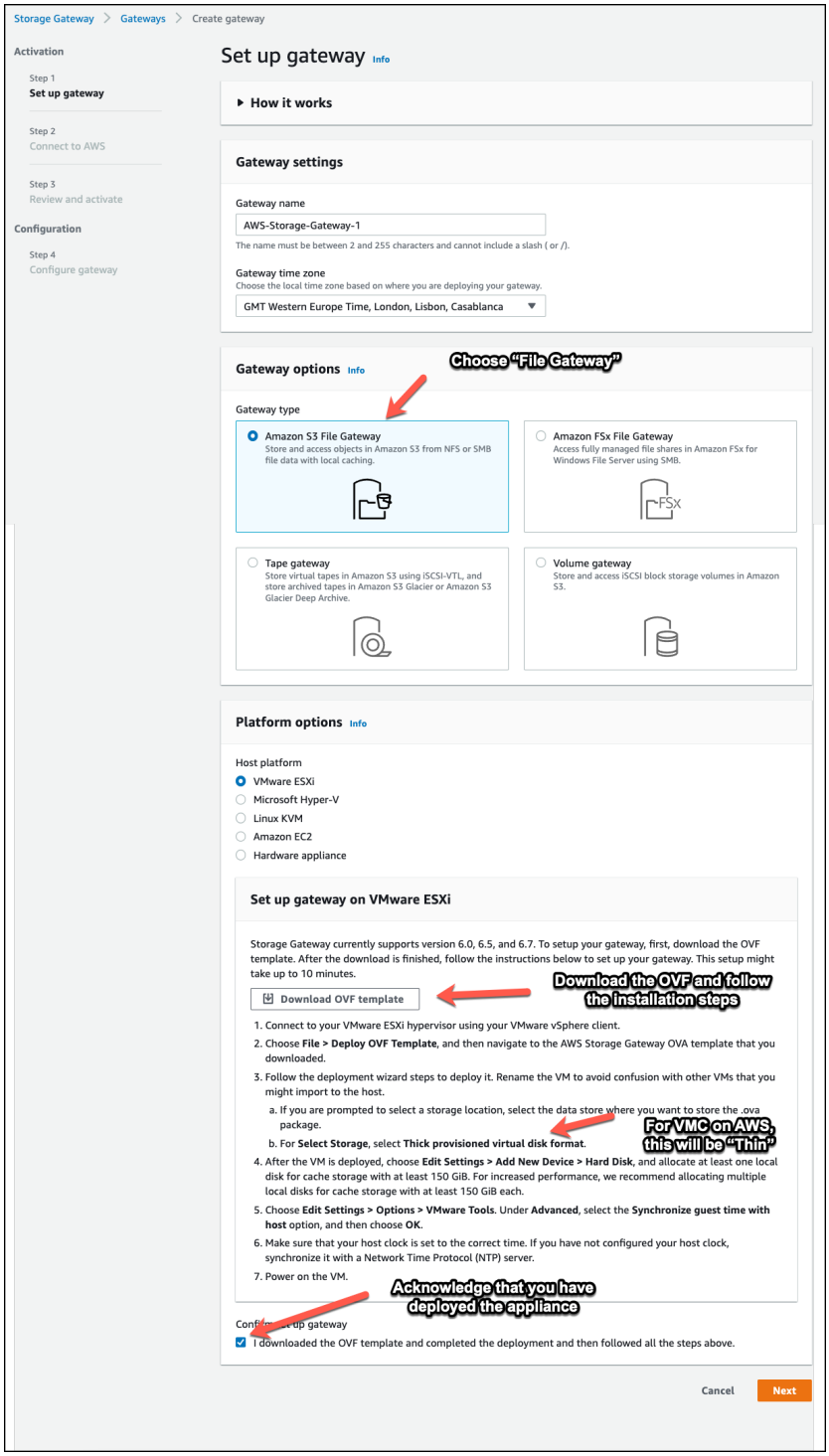

Figure 21: Storage Gateway Activation Step 1: Set up gateway

Once the appliance has been installed in the SDDC, note its IP address in vCenter:

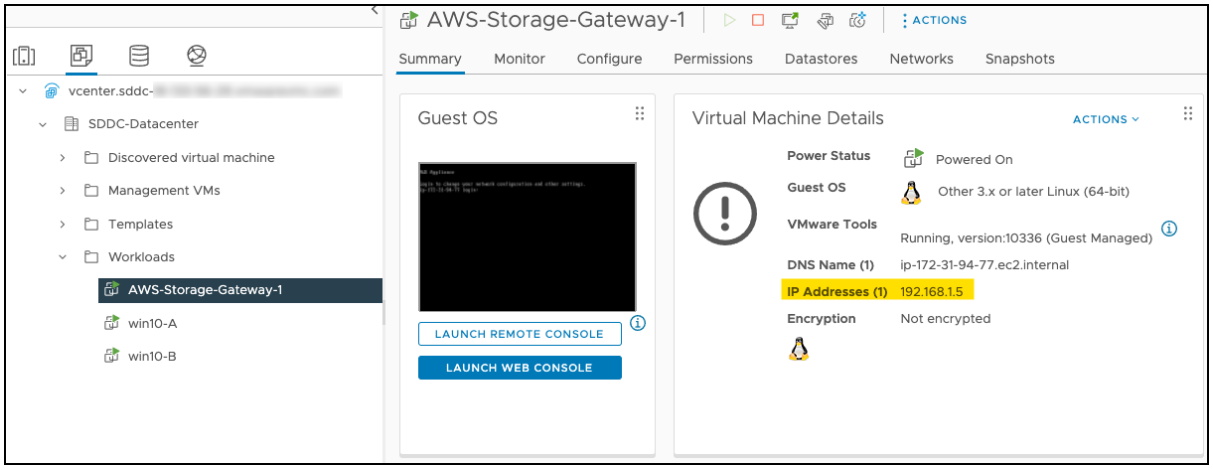

Figure 22: IP Address for Storage Gateway Appliance

IMPORTANT NOTE: The next step requires that the browser from which you are installing has access to the appliance deployed in the SDDC.

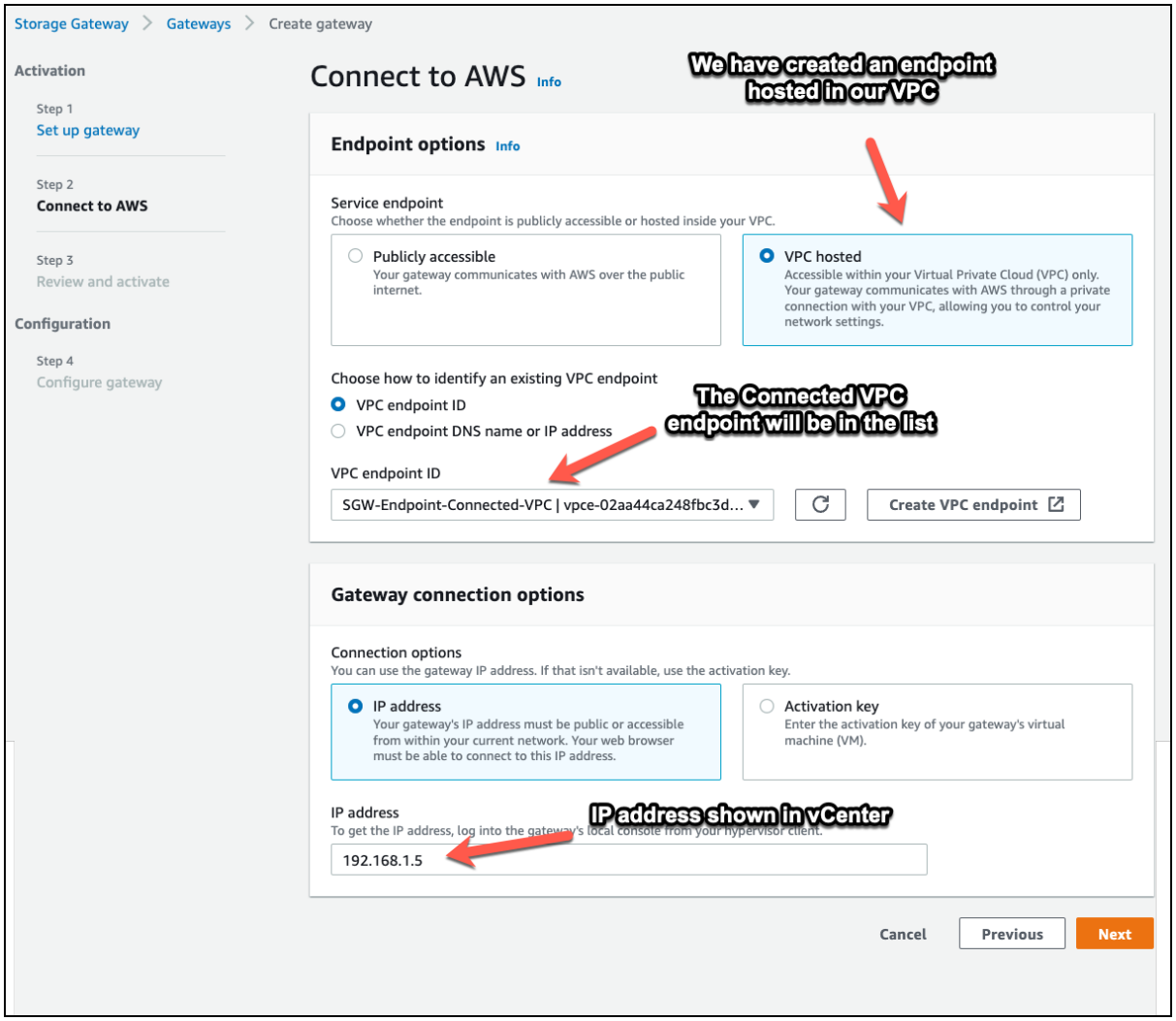

Figure 23: Storage Gateway Activation Step 2: Connect to AWS

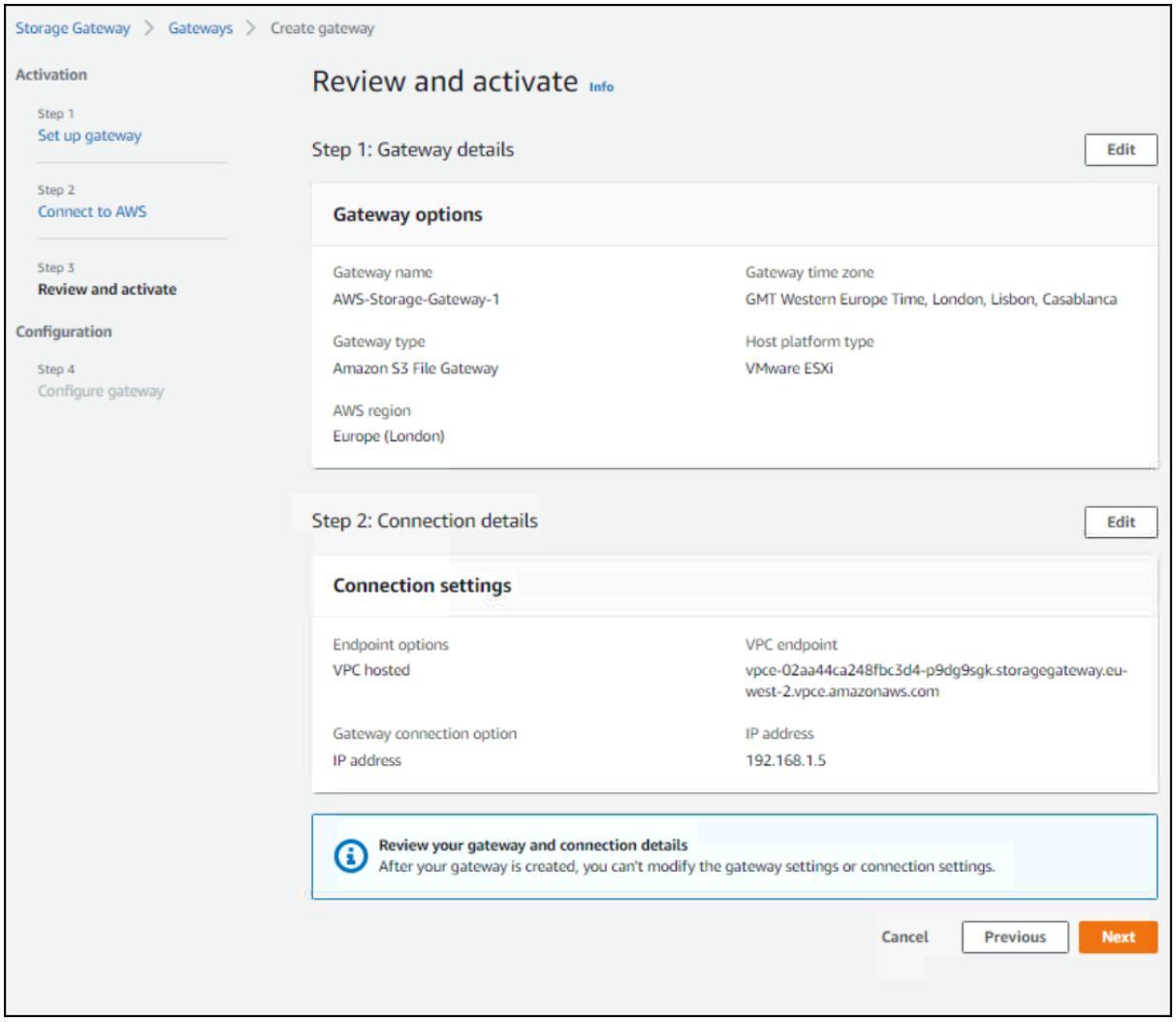

Figure 24: Storage Gateway Activation Step 3: Review and activate

After setting logging and alarm options, you will need to click on “Configure” and set the disk(s) used for caching:

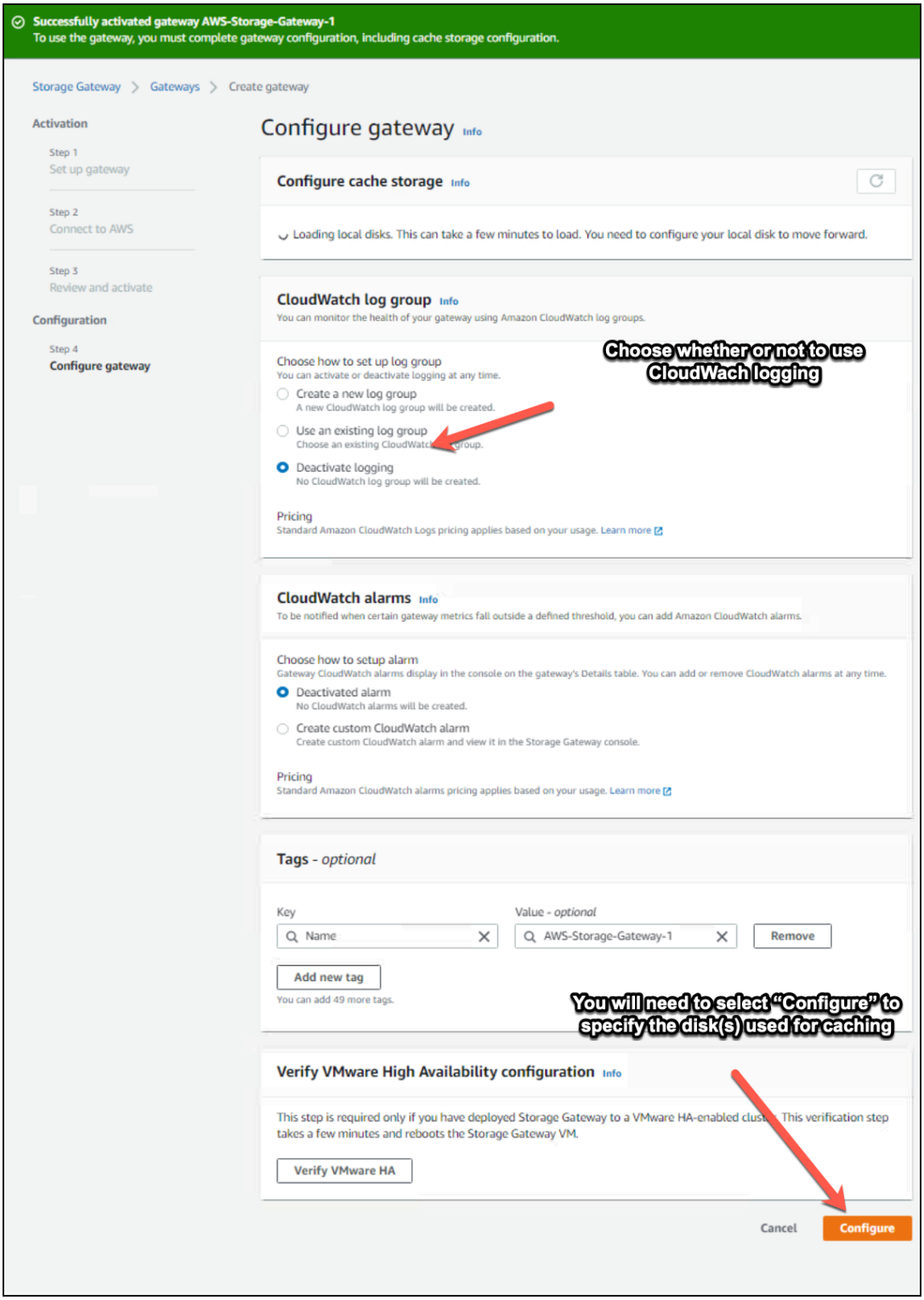

Figure 25: Storage Gateway Activation Step 4: Configure gateway

Note: After clicking on "Configure" there is often a longer-than-expected wait for the disk configuration to come up on screen.

If the disk configuration does not appear under "Configure cache storage", refresh the browser window and then choose "Gateways" from the menu. Select your gateway:

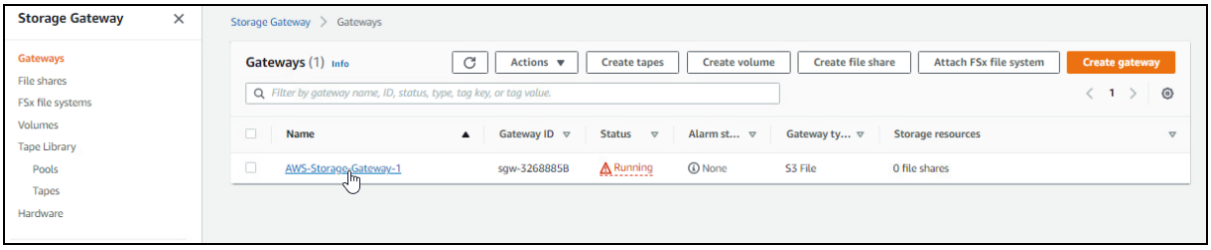

Figure 26: Select Storage Gateway

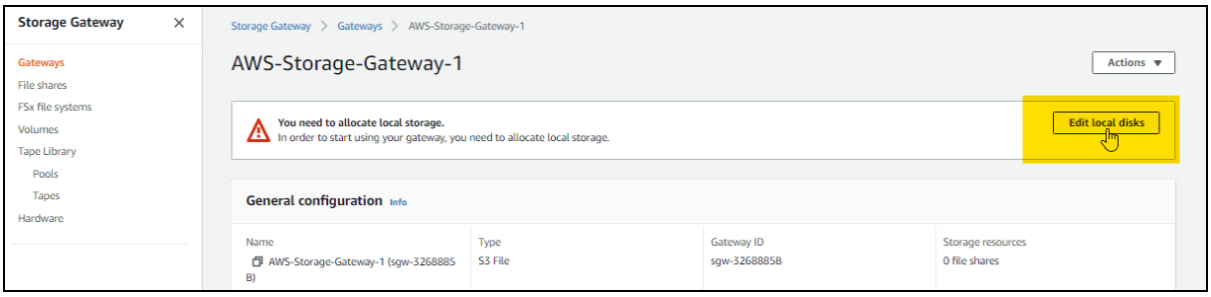

Figure 27: Edit Storage Gateway Disks

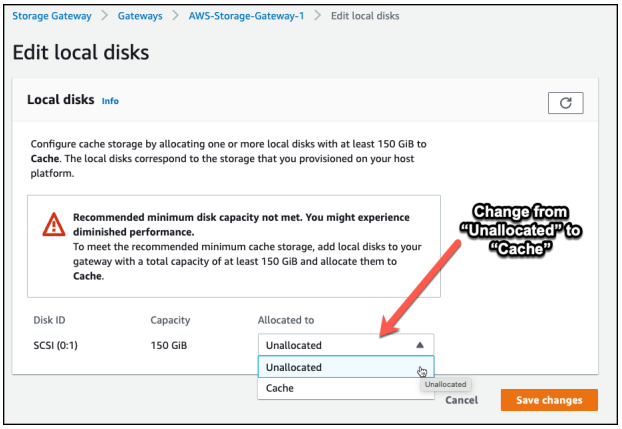

Figure 28: Assign Cache Disks

Your gateway is now up and running:

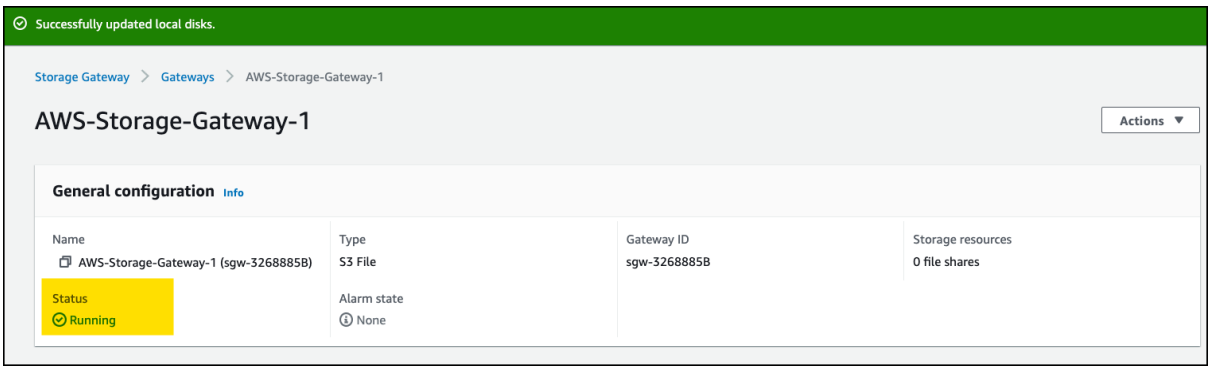

Figure 29: Storage Gateway Running

The next step is to configure File Shares.

File Shares

We have the Storage Gateway, now we need to put it to work. As a File Gateway, the Storage Gateway appliance provides SMB and NFS share points to which client devices will connect. File data is stored in AWS S3 buckets and cached on the appliance.

To create a File Share, open the AWS Console and navigate to Storage Gateways. Choose “File shares” and select “Create file share”:

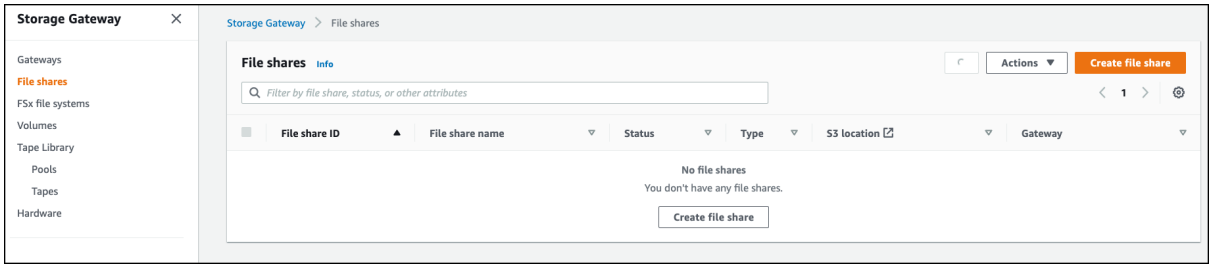

Figure 30: Create file share

We will create an SMB File Share for our AWS-Storage-Gateway-1 which will reach its S3 bucket via the Connected VPC:

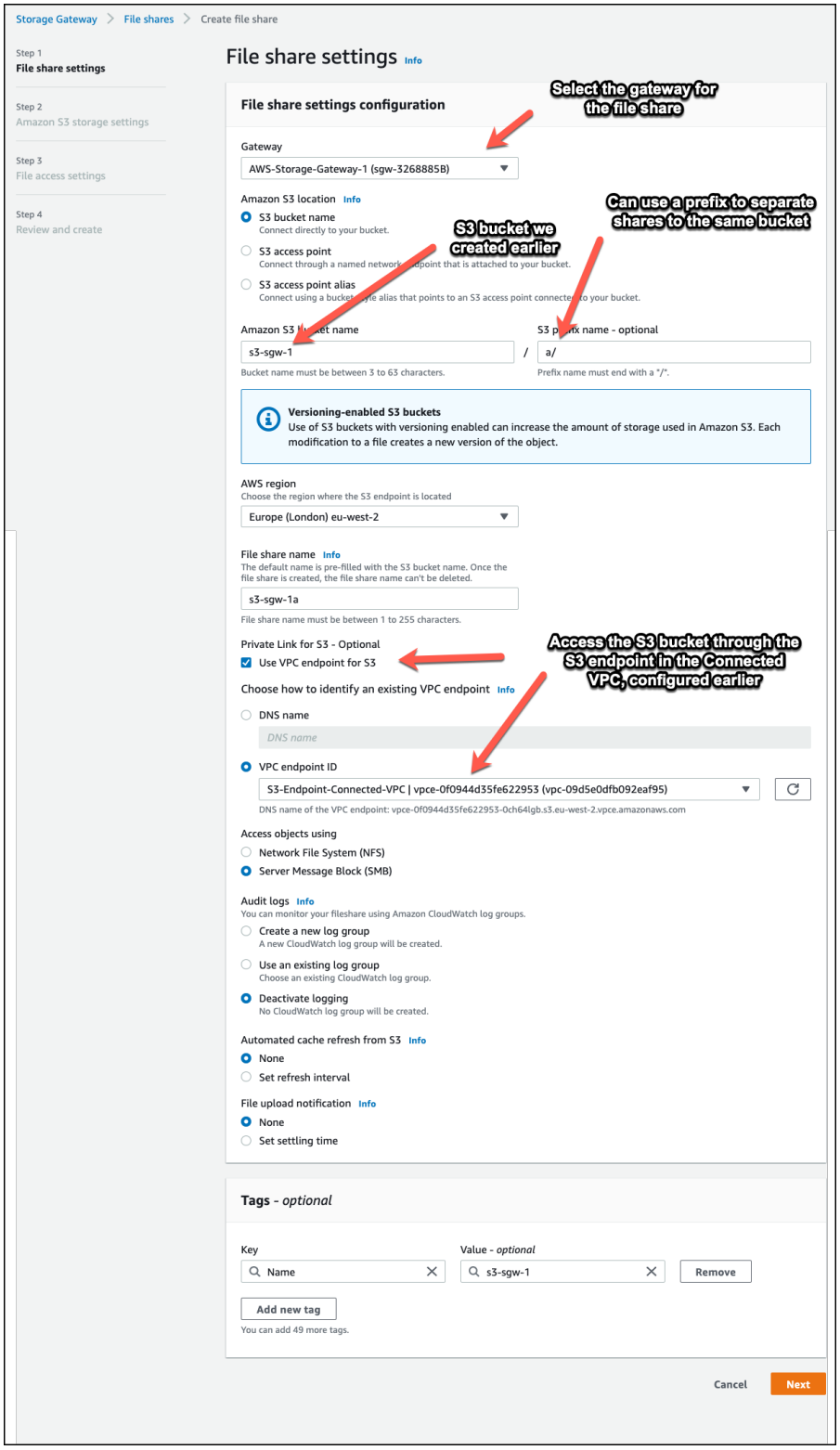

Figure 31: Create File Share Step 1: File share settings

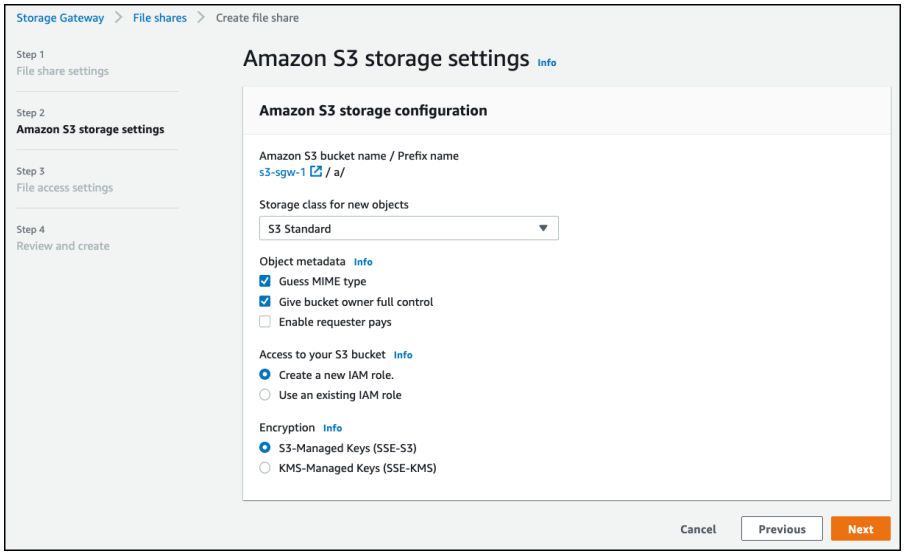

Figure 32: Create File Share Step 2: Amazon S3 storage settings

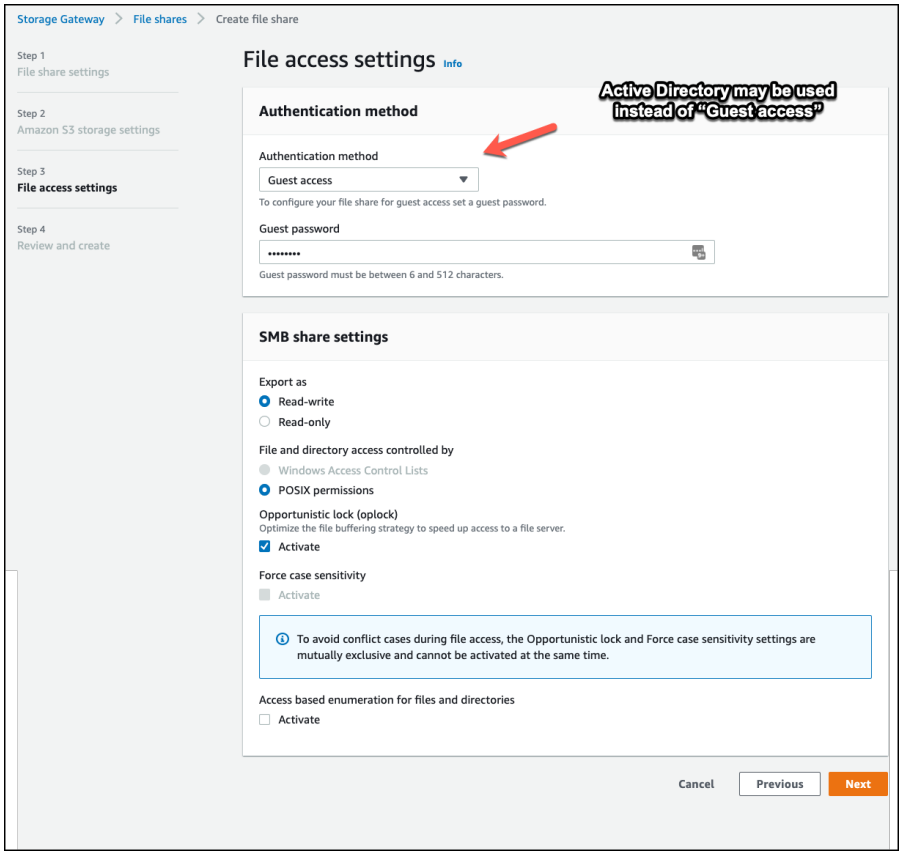

Figure 33: Create File Share Step 3: File access settings

Review the file share parameters and click "Create":

Review the file share parameters and click "Create":

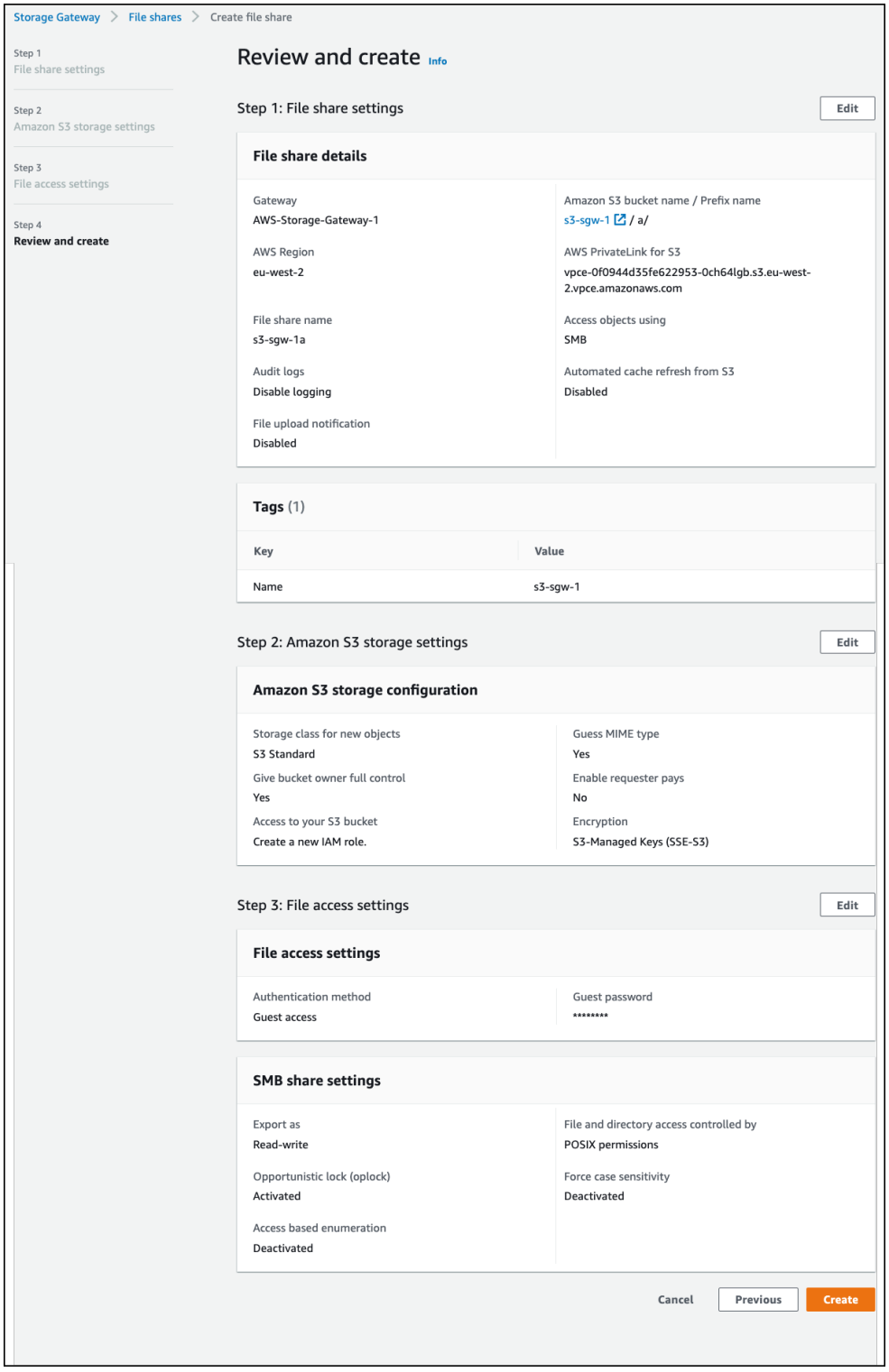

Figure 34: Create File Share Step 4: Review and create

Test the Storage Gateway

Test the Storage Gateway by mapping to the SMB file share and saving some data.

The Details pane for the File Share in the AWS Console gives the command to map a drive from a Windows computer to the file share:

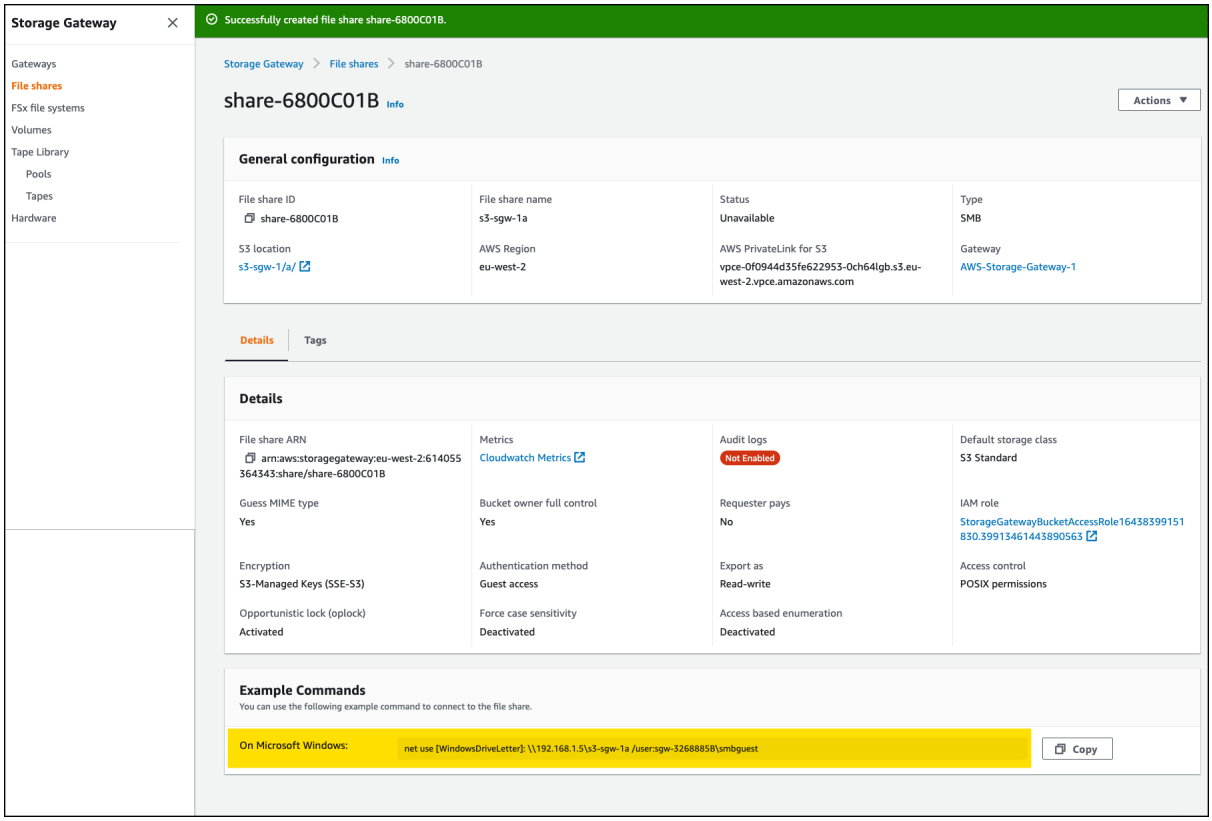

Figure 35: Command for Drive Mapping

Issue the highlighted command from a Windows server or workstation that has network access to the Storage Gateway appliance.

```
C:\Users\bob>net use z: \\192.168.1.5\s3-sgw-1a /user:sgw-3268885B\smbguest
The command completed successfully.
```

Figure 36: Successful Drive Mapping

At this point you can create a simple document and place it in the file share:

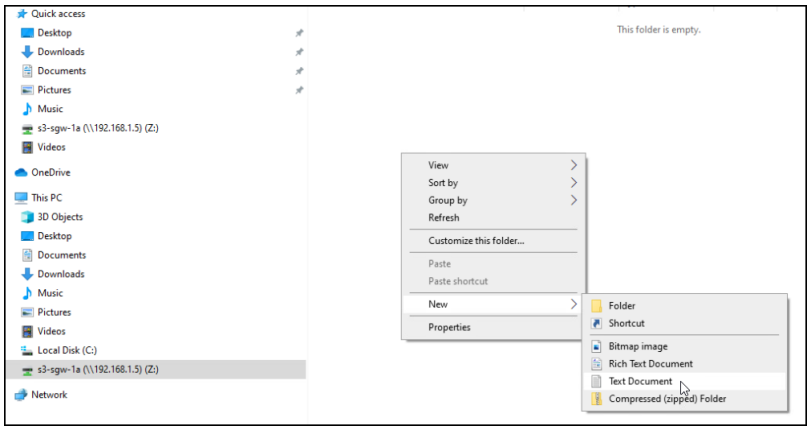

Figure 37: Create and Save a Document (1)

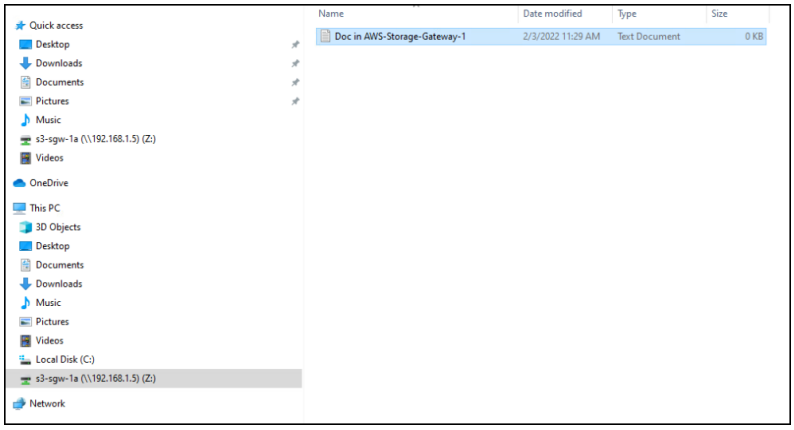

Figure 38: Create and Save a Document (2)

Success!

Now you can check the S3 bucket to show that your file has been stored there. From the AWS Console, navigate to S3, select the bucket we created for the file share ("s3-sgw-1") and check the folder created for the share ("a/"):

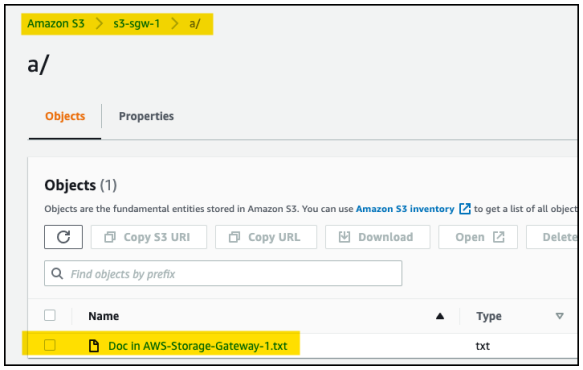

Figure 39: Check the file share

We have successfully created and tested the Storage Gateway AWS-Storage-Gateway-1, which accessed AWS from the SDDC via the Connected VPC.

Use the steps above to create AWS-Storage-Gateway-2. Substitute the Connected VPC endpoints with endpoints for the External VPC and use the S3 bucket s3-sgw-2 for the file share.

Confirm Traffic Flow

We have configured a separate network path for each of our two Storage Gateways. We should confirm that traffic from the appliance AWS-Storage-Gateway-1 is routed through the Interface Endpoints in the Connected VPC, while traffic from AWS-Storage-Gateway-2 goes through Interface Endpoints in the External VPC.

To monitor network traffic through a VPC, we can set up a Flow Log on the VPC subnet we would like to monitor. We can then inspect the flow log in AWS CloudWatch to confirm traffic from the Storage Gateway appliance to the appropriate Interface Endpoints.

First, let's confirm the private IP addresses and Network Interface IDs of the endpoints. From the AWS Console, navigate to VPC and select Endpoints:

© VMware LLC.

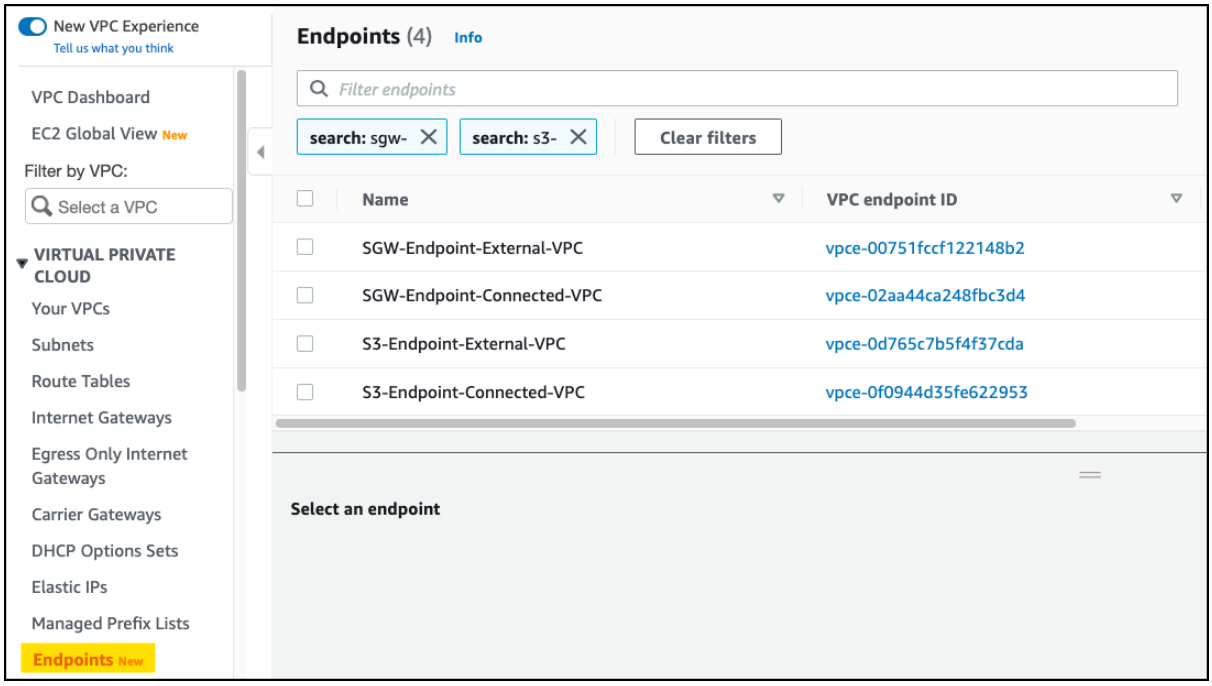

Figure 40: Listing Storage Gateway and S3 Endpoints

Select an endpoint and choose “Subnets”. The private address and network interface ID will be revealed as part of the subnet:

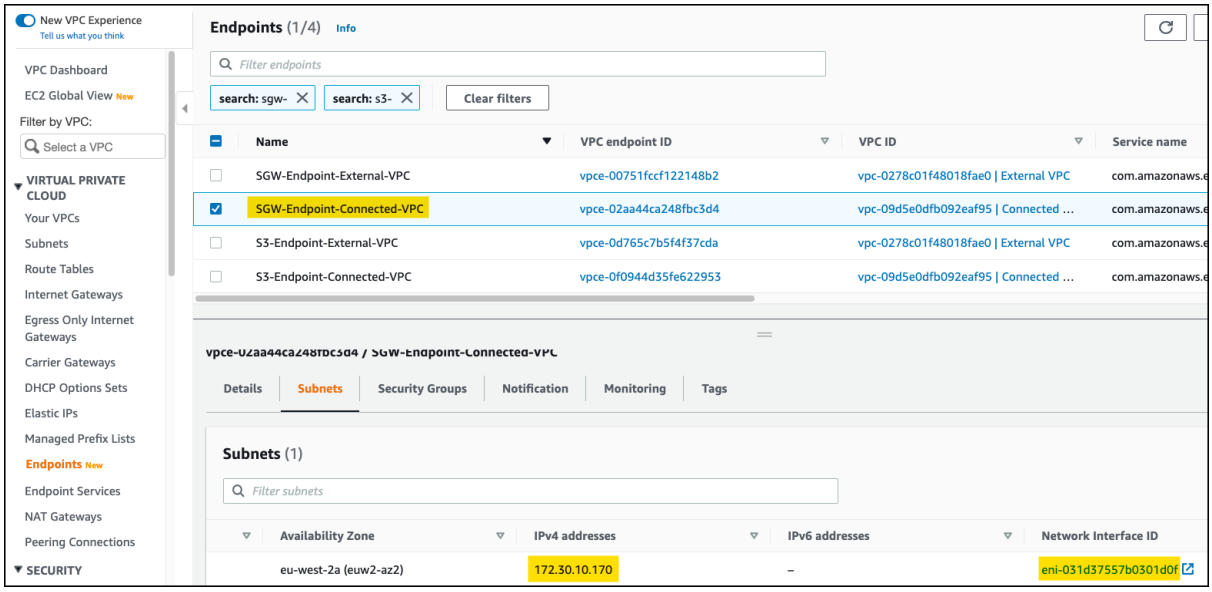

Figure 41: Endpoint IP and Network Interface ID

Record the private IP and Network Interface ID for each of the endpoints. From vCenter, we have the IP addresses of the appliances. In this scenario, we have:

Appliance	Endpoint	IP Address	Network Interface
AWS-Storage-Gateway-1 192.168.1.5	SGW-Endpoint-Connected-VPC	172.30.10.170	eni-031d37557b0301d0f
	S3-Endpoint-Connected-VPC	172.30.10.180	eni-0e712a512712b87af
AWS-Storage-Gateway-2 192.168.2.103	SGW-Endpoint-External-VPC	172.20.200.101	eni-0c7293c72936b5dc0
	S3-Endpoint-External-VPC	172.20.200.59	eni-08368e7d8f73df5f0

Table 1: All IPs and Network Interface IDs

We will not cover the details of Flow Log creation in this article – these can be found here. The figures below show the two Flow Logs that have been configured:

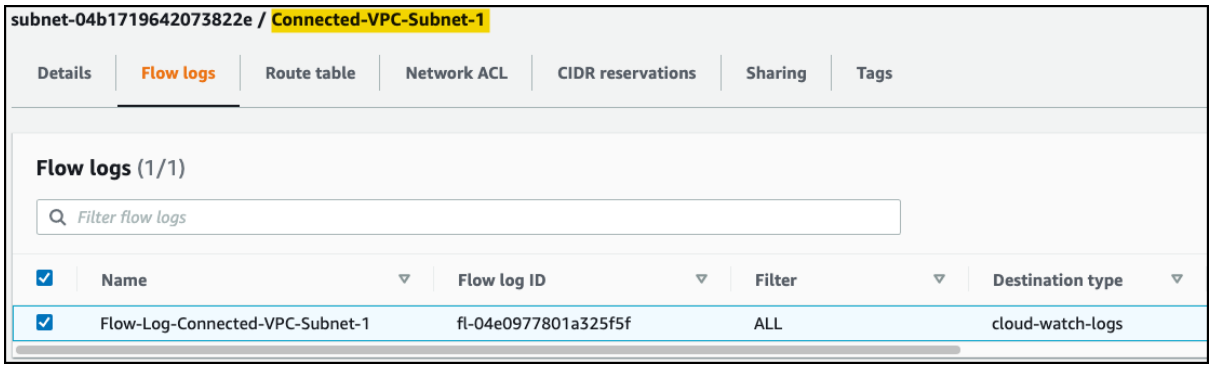

Figure 42: Connected VPC Flow Log

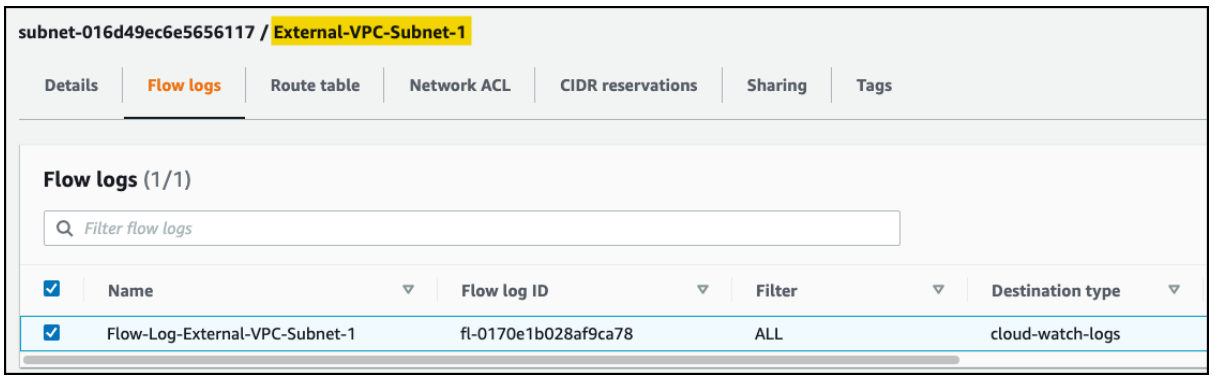

Figure 43: External VPC Flow Log

In the AWS Console, navigate to CloudWatch, expand “Logs” and select “Log groups”. We will open the flow log for the Connected VPC:

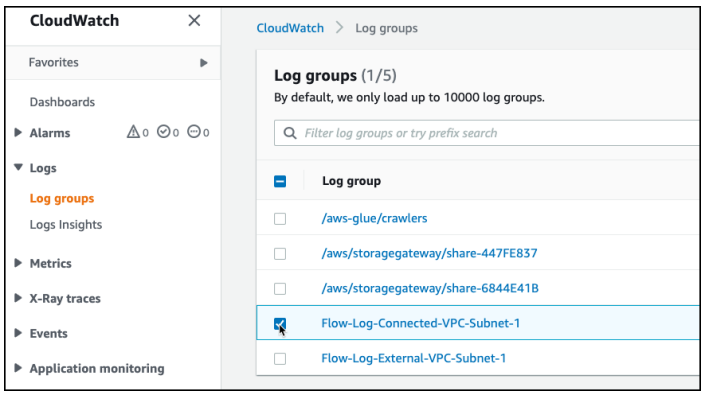

Figure 44: Connected VPC Log Group

To inspect traffic through the Interface Endpoint for the Storage Gateway in the Connected VPC, select eni-031d37557b0301d0f (per Table 1):

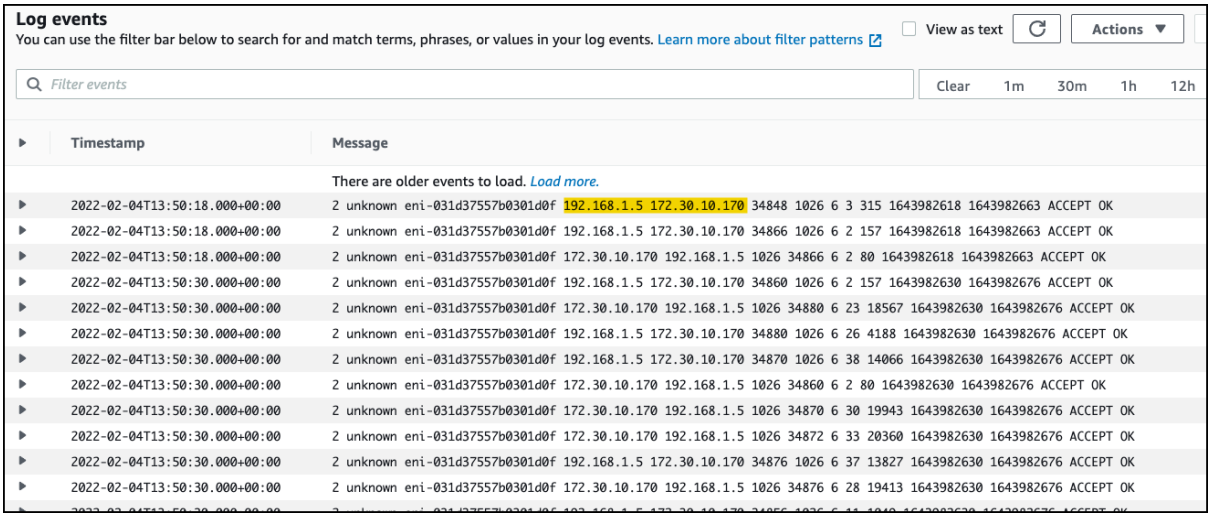

Figure 45: Log Events for Flow Through Storage Gateway Endpoint in the Connected VPC

The logs show traffic is flowing between the AWS-Storage-Gateway-1 appliance (192.168.1.5) and the Storage Gateway endpoint (172.30.10.170). We can similarly confirm flow of traffic for the S3 bucket (172.30.10.180) in the Connected VPC:

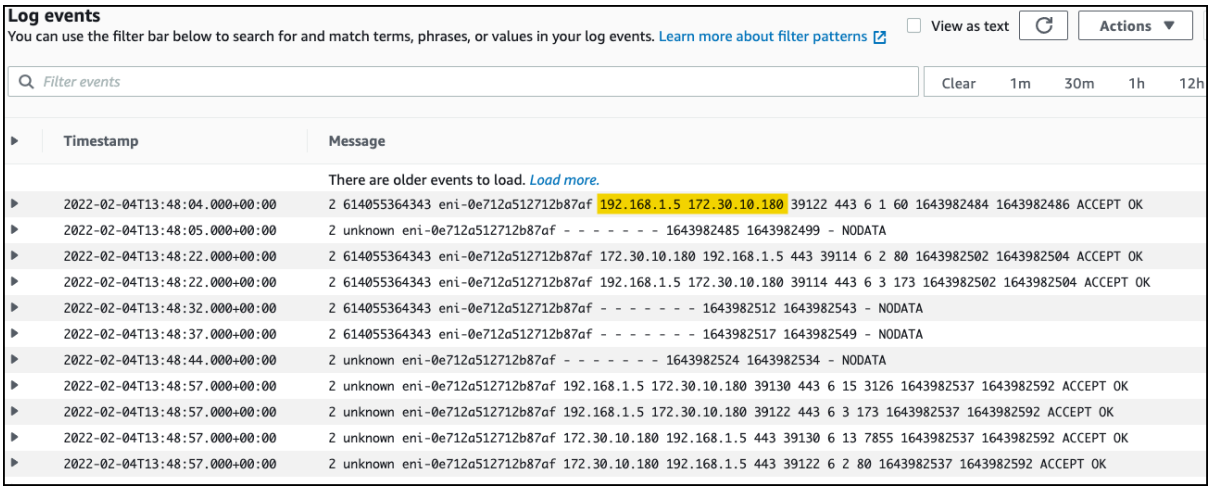

Figure 46: Log Events for Flow Through S3 Endpoint in the Connected VPC

For completeness, we will inspect traffic for AWS-Storage-Gateway-2 (192.168.2.103) to endpoints in the External VPC.

For Storage Gateway (172.20.200.101):

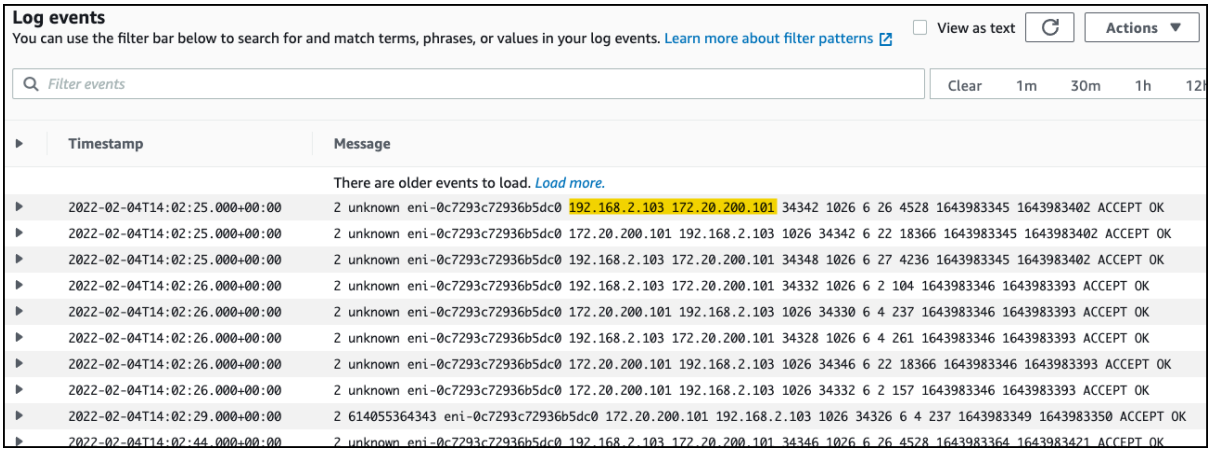

Figure 47: Log Events for Flow Through Storage Gateway Endpoint in the External VPC

And for S3 (172.20.200.59):

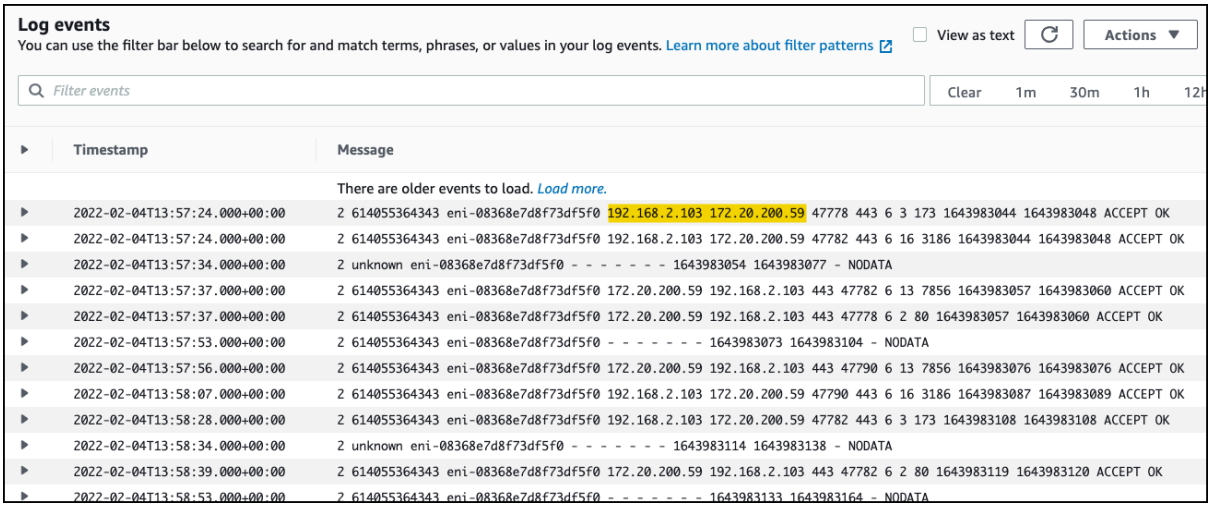

Figure 48: Log Events for Flow Through S3 Endpoint in the External VPC

From inspection of the flow logs, we see that traffic is routed as expected:

- AWS-Storage-Gateway-1 connects to Storage Gateway and S3 services across the ENI and via Interface Endpoints in the Connected VPC
- AWS-Storage-Gateway-2 connects to Storage Gateway and S3 services across the vTGW to the Interface Endpoints in the External VPC

Comparing Approaches

Both connectivity approaches for integration between VMware Cloud on AWS and AWS Storage Gateway illustrated in this article are valid and fully supported. Ultimately, the choice of one method over the other rests with the customer. Here is a list of points in favour of each approach:

Approach	Pros	Cons
Connect from VMware Cloud on AWS SDDC to Storage Gateway/S3 via the Connected/"Sidecar" VPC		
Connect from VMware Cloud on AWS SDDC to Storage Gateway/S3 via a VMware-managed Transit Gateway to an External VPC		

Table 2: Comparing Approaches

Summary and Additional Resources

Summary

In this article we demonstrated two separate approaches for connecting a VMware Cloud on AWS Software Defined Datacentre to an AWS Storage Gateway.

The first approach directed traffic from the SDDC through Storage Gateway and S3 endpoints in the Connected VPC.

The second approach used a VMware-managed Transit Gateway to route traffic to a customer's External VPC.

Both approaches are valid and fully supported and highlight the flexibility of leveraging native AWS services for VMware Cloud workloads.

Additional Resources

For more information about VMware Cloud on AWS and AWS Storage Gateway, you can explore the following resources:

VMware Cloud on AWS

VMware Transit Connect

AWS Storage Gateway

AWS S3

About the Author

Vern Bolinius is a business-focused solution architect with 25+ years in the IT industry. His experience includes roles as an instructor, consultant, engineer, architect and business owner. An avid evangelist of VMware Cloud solutions, Vern enjoys presenting and discussing solutions with partners and customers alike. When not behind a laptop or in front of an audience, Vern enjoys travel and time outdoors running, canoeing, hiking and camping.

- Vern Bolinius, Lead Cloud Solution Architect, VMware

© VMware LLC.

© VMware LLC.

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.