

VMware General



Table of contents

VMware Cloud on AWS Integration with AWS Storage Gateway
Overview
Introduction
Purpose of This Tutorial
Audience
Procedure 4
Introduction
Prerequisites
SDDC, SDDC Group, VPC Connectivity 4
SDDC / VPC Routes
External VPC 6
Connected VPC
SDDC Network Segments and Firewall Rules
Storage Gateway Service Prerequisites
AWS S3 Buckets
AWS Security Groups
AWS Endpoints
Storage Gateway Deployment
Gateway
File Shares
Test the Storage Gateway 23
Confirm Traffic Flow
Comparing Approaches
Summary and Additional Resources
Summary
Additional Resources
About the Author



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.



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:

- 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.
- 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)



SDDC-01 VMC on AWS SDDC () Europe (London)			· · · · · · · · · · · · · · · · · · ·
Summary Networking & Security Add Ons Maintenance	e Troubleshooting Settings Support		
Capacity and Usage			umo
(READY) (13)			
Hosts	CPU	Memory	Storage
1	82.8 GHz	512 GiB	10.37 TiB
Elastic DRS Fetching EDRS Status	Microsoft Server Licenses U None Purchased from VMware	Tanzu Kubernetes Grid Deactivated	
ADD HOST ACTIONS V			

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

SDDC-Group-01									
Summary vCenter Linking Direct	Connect External VPC External TGW Routing	Support							
Description: No description provided. You can add a description by accessing the Edit Group option in the actions menu.									
Transit Connect Status: CONNECTED									
SDDCS									
Name Y	SDDC ID	T SDDC Version T	Management CIDR T	Location Y	Connectivity Status				
SDDC-01	8ae52019-c845-4396-92e2-06ed481eac17	1.17.0.5	10.2.0.0/16	EU (London)	CONNECTED				

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

Your VPCs (1/1) Info							
Q Filter VPCs							
Name: External VPC X	ear filters						
Name Name	∇	VPC ID	\bigtriangledown	State	∇	IPv4 CIDR	∇
External VPC		vpc-0278c01f48018fae0		🕗 Available		172.20.0.0/16	

Figure 4: External VPC, view from AWS Console

SDDC-Group-01			
Summary vCenter Linking Direct Connect	External TGW Routing Support		
ADD ACCOUNT REMOVE			
AWS Account ID	Resource Share Name	⊤ State	T VPC Status
• »	VMC-Group-475d0aad-d501-4b19-a559-0c522f3fb90f	ASSOCIATED	1 Available (O Pending Acceptance)

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

SDDC / VPC Routes

by Broadcom © VMware LLC.

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:

vmw VMware Cloud			
«			
🖞 Launchpad	Inver	ntory	
Inventory	SDDCs	SDDC Groups	
Subscriptions	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~

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

< Back			
SDDC-Group-01			ACTIONS V
SDDC-Gloup-Ol			
Summary vCenter Linking Direct Connect External VPC External TGW Routing Support			
AWS Account ID T			
AWS Account ID :			×
Resource share name : VMC-Group-475d0aad-d501-4b19-a559-0c522/3/b90	И		
State : ASSOCIATED			
Accert Remove			
VPC ID Y VMC on AWS Region	Transit Gateway Attachment ID	Y Routes Status	Υ
vpc-0278c01148018fae0 EU (London)	tgw-attach-0fd14d61867576e97	172.20.0.0/16 🧷 AVAILABLE	
		4	
	_		
	Re	oute to CIDR of External VPC	
I			

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:

New VPC Experience Tell us what you think	VPC > Route tables > rtb-0fae1f607c8fd4314				
VPC Dashboard EC2 Global View New	rtb-0fae1f607c8fd4314 /	External VPC-RT			Actions 🔻
Filter by VPC:	Details Info				
VIRTUAL PRIVATE CLOUD Your VPCs Subnets Pourte Tables	Route table ID Trb-0fae1f607c8fd4314 VPC vpc-0278c01f48018fae0 External VPC	Main D No Owner ID	Explicit subnet associations	Edge associations -	
Egress Only Internet Gateways Carrier Gateways	Routes Subnet associations Edge ass	ociations Route propagation Tags			
DHCP Options Sets Elastic IPs	Routes (3)				Edit routes
Managed Prefix Lists Endpoints New	Q Filter routes	RoutetotheSDDOt	Both 💌		< 1 > @
Endpoint Services NAT Gateways	Destination \bigtriangledown	Target the TGW attachm	Status	▽ Propagated	∇
Peering Connections	172.20.0.0/16	scal	⊘ Active	No	
▼ SECURITY	192.168.0.0/16	tgw-0708a3f601c4ec923	⊘ Active	No	
Network ACLs	0.0.0/0	igw-00e4332ef11d8e1c4	⊘ Active	No	

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



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:

Amazon S3	×	Amazon S3			
Buckets Access Points Object Lambda Access Points Multi-Region Access Points Batch Operations Access analyzer for S3		Account snapshot Lat updated. Jan 31, 2022 by Storage Lens. Metrics are gene Total storage 106.9 GB	rated every 24 hours. Learn more 🔀 Object count 2.7 M	Avg. object size 40.9 KB	View Storage Lens dashboard You can enable advanced metrics in the "default-account-dashboard" configuration.
Block Public Access settings for this account	_	Buckets (51) Info Buckets are containers for data stored in 53. Learn more C Q. Find buckets by name			C Copy ARN Empty Delete Crasts bucket

Figure 9: Bucket Creation

Default values can be used for the bucket:



	Block public Access to Bundess and Bajects through access control lists (ACLA) bucket policies, access point policies, or all. In order to main the public access is buckets and adjects through access control lists all public access. These settings apply only to this bucket and adjects through access access point policies, or all. In order to applications will work correctly without public access. If you require some level of public access to this bucket on order to applications will work correctly without public access. If you require some level of public access to this bucket or adjects within, you can access the individual settings below to an adject settings below. Each of the following settings are independent of one another. Soft public access to buckets and abjects granted through now access control lists (ACLA) when the public access to buckets and abjects granted through now access control lists (ACLA)
Innazon 53 > Create bucket Create bucket Info Indexs are containers for data stored in 53. Learn more [2] General configuration	ACLs for entiting blockets and objects. This setting deservir change any existing permissions that allow public access to 53 resources using ACLs. Block public access to blockets and objects granted through any access control lists (ACLs) starting public access to blockets and objects granted through new public blocket or access point policies S1 will block new blocket and access to blockets and objects. Block public access to blockets and objects granted through new public blocket or access point policies S1 will block new blocket and access point policies through any exact through any public blocket or access point down't change any exact through policies through access to blockets and objects through any public blocket or access point policies S1 will bloce and cross-account access to blockets and objects through any public blocket or access point policies S1 will bloce and cross-account access to blockets and objects through any public blocket and cose- S1 will bloce and cross-account access to blockets and objects through any public blocket or access point policies S1 will bloce and cross-account access for blockets or access points with policies that grant public access to blockets and objects.
Bucket name S-5-grow-1 Bucket name must be unique and must not centain spaces or uppercase letters. See rules for bucket naming [2] AWS Region EU (London) eu-west-2 Copy settings from existing bucket - optional Only the bucket settings in the following configuration are copied. Choose bucket	Bucket Versioning Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more Bucket Versioning Bucket Versioning Disable Enable
Object Ownership Info Control ownership of objects write to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership direttminus who can supply access to objects. ACLs disabled (recommended) Alcases to this bucket and its bucket and the super access to the bucket and its objects is specified using only policies.	Tags (1) - optional Track storage cost or other offeria by tagging your bucket. Learn more C Key Value - optional Name \$3-sgw-1 Add tag
object Ownership Bucket owner enforced gure 10: S3 Bucket Creation (1)	Default encryption Automatically encrypt new objects stored in this bucket. Learn more Server-side encryption Server-side encryption Disable Enable
	Advanced settings After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.
	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:

Amazon S3 ×	Amazon S3				
<mark>Buckets</mark> Access Points Object Lambda Access Points	▼ Account snapshot Last updated: Jan 31, 2022 by Storage Lens. Metrics are gene	rated every 24 hours. Learn more [
Multi-Region Access Points Batch Operations Access analyzer for S3	Total storage 106.9 GB	Object count 2.7 M			
Block Public Access settings for this account • Storage Lens	Buckets (53) Info Buckets are containers for data stored in S3. Learn more I		X 2 matches		
AWS Organizations settings	Name AWS Region		not public		
Feature spotlight 3	S3-sgw-1 EU (London) eu-we s3-sgw-2 EU (London) eu-we	st-2 Bucket and objects i st-2 Bucket and objects i			

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.

New VPC Experience Tell us what you think		Secu	rity Groups (60) Info			(C	Actions 🔻	Export s	ecurity groups to CS	V	Create security gro	oup
Subnets		QI	Filter security grou	ips									< 1 2 >	0
Route Tables														
Internet Gateways	4		Name	∇	Security group ID ∇	Security group name \bigtriangledown	VPC ID	∇	Description	∇	Owner	∇	Inbound rules count	▽ (
Egress Only Internet			-		ap Internative Tomat	antust	an introduction in		Mult IV, much		1.400.064040		1 Revealed arms	
Gateways			-		A DECEMBER OF	Incred-educed 1	-		land-start 1 of		1.000		1 Permission and the	
Carrier Gateways			-		a manufacture of	and a			seture of second				1 Receiption and a	
DHCP Options Sets	11	_						_						
Elastic IPs							—						-	
Managed Prefix Lists														
Endpoints New														
Endpoint Services														
NAT Gateways														
Peering Connections														
▼ SECURITY														
Network ACLs														
Security Groups														
VINETWORK ANALYSIS														

Figure 13: Create a Security Group

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

VPC > Security Groups > Create secu	rity group						
Create security group A security group acts as a virtual firewall for	Info	trol inbound and outbound tra	ffic. To create a new security gr	oup, complete the fields below.			
Basic details							
Security group name Info							
S3-Endpoint-SG-External-VPC							
Name cannot be edited after creation.							
Description Info							
Allow access to S3 from External VPC							
VPC Info				External VPC			
Q			×				
Inbound rules Info							
Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info		
HTTPS	TCP	443	Anywher T	0			Delete
	1.61	110	, any means	_			Detete
				0.0.0.0/0 ×			
Add rule							
Outbound rules Info							
Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info		
All traffic 🛛 🔻	All	All	Custom 🔻	Q			Delete
				0.0.0.0/0 ×			
Add rule							
Tags - optional A tag is a label that you assign to an AWS reso	urce. Each tag consists of	a key and an optional value. You car	use tags to search and filter your re	sources or track your AWS costs.			
Key			Value - ontional				
Q, Name		×	Q S3-Endpoint-SG-Extern	al-VPC	X Remove		
						_	
Add new tag							
tou call add up to 49 more tag							
						Cancel	Create security group

Figure 14: S3 Security Group for External VPC



VPC > Security Groups > Create secur	ity group					
A security group acts as a virtual firewall for	Info your instance to cor	trol inbound and outbound traffic.	To create a new security grou	up, complete the fields below.		
Basic details						
Security group name Info						
SGW-Endpoint-SG-External-VPC						
Name cannot be edited after creation.						
Description Info						
Allow access to Storage Gateway				G-1		
VPC Info						
Q		×				
Inbound rules Info						
Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
HTTPS 💌	TCP	443	Anywher 🔻	Q		Delete
				0.0.0.0/0 ×		
Custom TCP 💌	ТСР	1026 - 1028	Anywher 🔻	٩		Delete
				0.0.0.0/0 ×		
Custom TCP 💌	ТСР	1031	Anywher 🔻	Q		Delete
				0.0.0.0/0 ×		
Custom TCP 💌	ТСР	2222	Anywher 🔻	Q		Delete
				0.0.0.0/0 ×		
Add rule						
Outbound rules Info						
Type Info	Protocol Info	Port range Info	Destination Info		Description - optional Info	
All traffic 🛛 🔻	All	All	Custom 🔻	Q		Delete
				0.0.0.0/0 ×		
Add rule						
Tage - optional						
A tag is a label that you assign to an AWS resou	rce. Each tag consists of	a key and an optional value. You can use	tags to search and filter your reso	urces or track your AWS costs.		
Key		Va	lue - ontional			
Q. Name		×	C SGW-Endpoint-SG-Extern	nal-VPC	X Remove	
Add now tag						
You can add up to 49 more tag						
						Cancel Create security group

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:

Secur	ity Groups (4) Info				C Actions v	
Q Fi	lter security groups					
searc	h: s3 × search: sgw × Cle	ear filters				
	Name 🔺	Security group ID 🛛 🗢	Security group name	∇	VPC ID	∇
	S3-Endpoint-SG-Connected-VPC	sg-00d5ff0e0ac47258e	S3-Endpoint-SG-Connected-VPC		-	
	S3-Endpoint-SG-External-VPC	sg-0e28d0a64e77204cb	S3-Endpoint-SG-External-VPC			
	SGW-Endpoint-SG-Connected-VPC	sg-031bc81840ce842a2	SGW-Endpoint-SG-Connected-V	PC	-	
	SGW-Endpoint-SG-External-VPC	sg-022c11be7c16c0bc7	SGW-Endpoint-SG-External-VPC			

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:

New VPC Experience Tell us what you think		Endp	oints (11) Info						C Actions 🔻	Create end	point	
VPC Dashboard		Q P	ilter endpoints							< 1	>	0
EC2 Global View New Filter by VPC:	4		Name	∇	VPC endpoint ID	∇	VPC ID	▽	Service name	∇	En	dpoin
Q Select a VPC			-		per l'artistication		# 1018401-04-04 (00-04)		com.amazonaws.eu-west-2.s3		Ga	teway
VIRTUAL PRIVATE			-		-		+ 101840148.04E, 001971		com.amazonaws.eu-west-2.ebs		Int	erface
Your VPCs			-		and 1786174881754114		- Park-Service (19.17)		com.amazonaws.eu-west-2.datasync		Int	erface
Subnets			-		and the following the local		an Alexandra (Marca Consultation		com.amazonaws.eu-west-2.s3		Ga	teway
Route Tables			-		-		- MCMCCARENT; ++++		com.amazonaws.eu-west-2.s3		Ga	teway
Internet Gateways Egress Only Internet Gateways			When Englant Engenater Italia			_	-		aws.sagemaker.eu-west-2.studio		Int	erface
Carrier Gateways						—				-		
DHCP Options Sets		Select	an endpoint									
Elastic IPs												
Managed Prefix Lists												
Endpoints New												

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:



reate endpoint Info	
ere are three types of VPC endpoints – Interface end	points, Gateway Load Balancer endpoints, and Gateway endpoints.
erface endpoints and Gateway Load Balancer endpoi terface (ENI) as an entry point for traffic destined to t	ints are powered by AWS PrivateLink, and use an Elastic Network the service. Interface endpoints are typically accessed using the public
private DNS name associated with the service, while	Gateway endpoints and Gateway Load Balancer endpoints serve as a
get for a route in your route table for traffic destined	d for the service.
For the state section of	
Endpoint settings	
Name tag - ontional	
Creates a tag with a key of 'Name' and a value that you speci	ify.
SGW-Endpoint-External-VPC	
Service category	
Select the service category	
 AWS services Services provided by Amazon 	 PrivateLink Ready partner services Services with an AWS Service Ready designation
AWS Marketplace services	Other endpoint services
Services that you've purchased through AWS Marketp	Hace Hind services shared with you by service name
Specify Storage	Bateway Interface Endpoint
Services (1/1)	C
Q. Filter services	< 1 > @
Service Name: com.amazor ws.eu-west-2.storage	egateway × Clear filters
Service Name	⊽ Owner 🛛 🏹 Type
o com.amazonaws.eu-west-2.storagegateway	/ amazon Interface
DNS name	
DNS name Enable DNS name Info Associates a private hosted zone with the VPC that conta leverage Amazon's private network connectivity to the su	ains a record set that enables you to ervice while making requests to the
DNS name Enable DNS name info Associaties a private hosted zone with the VPC that conta leverage Amazon's private network connectivity to the se service's default public endpoint DIS name. To use the's DIS's hostmanner's and 'Enable Obs support' are enabled fo	ains a record set that enables you to ervice while making requests to the feature, ensure that the attributes 'Enable or your VPC.
DNS name Enable DNS name Info Associates a private hosted zone with the VPC that conta leverage Amazon's private network connectivity to the ser- service's default public endpoint DNS name. To use this for bits hostname: and 'Enable DNS support' are enabled for	ains a vectori set that enables you to errice addite making requests to the the standard standard tradition to the standard tradition of the standard tradition of the standard tradition control addition
DNS name C Enable DNS name Info Associates approvement for the VPC that conta leverage Ansanch private network connectivity to the se- ners's disfidual private network connectivity to the se- DKS hortname" and "Enable DNS support" are enabled fit	the a vector set that evables you to write with making requests to the testion, convert that testions: that is your VYC. Solice: concorrence cobmets: for the endpoint
DNS name Comparing the state of the second s	airs a recert as that evables you to review with making respects to the terry our VPC Collectionocormonocolinatis (corflin confipoint
DNS name Comparison of the second se	sine a record set they enables you to revice with an initiation requests is the transverse work with the transless by your VPC Scilicationocommonsorbinatis(contine concipatint
DNS name Constraints Constrai	ains a vectord set that enables you to provide with making repeats to the stratuse over the analysis is the stratuse to your over the stratuse is the stratuse stratuse over the stratuse over t
DNS name C Enable DNS name info Acadetias private hosted zone with the VPC that conta beening Ansam's private network connectivity to the as DNS hostename' and Table DNS support are enabled fo Subnets (1/3) info Availability Zone C eu-west-2a (euw2-sz2)	the a vector is a that excelles you to write with making requests to the excellent and the statistical faultion Solocition common exclosed is for the enclosed at Subnet ID v v
DDS name C Rube Cost same inde C Rube Cost same inde C Rube Cost same inde C Rube Rube Rube Rube Rube Rube Rube Rube	Air a receif or that evalues you to review with making respects to the testimation respects to the Solocetonocommons colonetist for this Confipoint Submet to Submet t
DNS name C Fulle OFS name info Anxietistes sprivate hooted from with the VFC full cost functions sprivate hooted from the VFC full cost function of the VFC hoot name info Subtracts (1/3) min Anxietistes (1/3) min C Anxietistes (1/3) min C everystes 2a (now2-2x2) everystes 2b (now2-2x3) everystes 2b (now2-2x3)	All a vector last that enables you to provide all the making repeats to the provide all the making repeats to the provide all the making the making the Submet to Submet to Submet all the making the Submet to Submet to Submet all the O No submet valiable O No submet valiable
DNS name	All a vector is at that enables you to evolve with making regrests to the extract work of the instrument of the instrument Solos: Conception of the instrument of the instrument Submet ID v submet-Of6649ec6e5555117 v () No submet available () No submet available
DDS name C Rule DS name inco C Constraint inco C Constraint inco C C Constraint inco C C C C C C C C C C C C C C C C C C C	Alter a verord set that exables you to review with making requests to the exact a set of the statistical state or your VC Soloci ono cormon colonicita (corfution Cardipcint) Subnet to vero cormon colonicita (corfution) Subnet to vero cormon colonicita (corfution) where the state of the state of the state of the state of the subnet available
DDS name C Full Constance Info Analysis Share Info Analysis Share Info Analysis Share Info Subprets (1/3) mfs Analysis Analysis (1/3) mfs A	sins a need of st that enables you to prove with making reports to the your wry. School Concorners or Data School Conclusion Conclusion Subnet to Subnet to Subnet to O No subnet available O No subnet available Scountly Coroup (crostod Conflict)
DNS name C State C St	Aller a vector dart that enables you to provide with making repeats to the constraints of the analysis to the constraints of the analysis of the analysis submet to analysis is ubmet to analysis is to a submet a validate is to
DNS name	All a vector las that enables you to ervice with making repeats to the conception of the international structure Solution of the international structure Submet ID v w w w w w w w w w w w w w
DNS name	the a vector far that excellence you to review with making requests to the Soloci concormence coloncits (for the Cardpoint Subnet 10 v where - 016649ec6e5655117 v 0 No subnet - 016649ec6e5655110 v 0 No subn
DNS name	All a ancord set that enables you to provide with analysing requests to the your your your your your your your your
DNS name	Alter a vector dar that enables you to force with making repeats to the conception of the making metales in the second second second second second second second conception submet to field deceles 565 5177 (a) No submet available (b) No submet available (c) (c) (c) (c) (c) (c) (c) (c) (c) (c)
DNS name	the a second set that enables you to review this making repeats to the conclusion of the second second second second second second second second second second second second second second to the submet of the defected second se
DNS name	Alle a neurol set that enables you to provide analysis of the set over verve. Subset to California Subset to California Subset to California O No subset available O No subset available Security/Circup/(crostoc/Cariflor) California Group name v VPC ID SetW-Endpoint: 56-External-VPC vpc 0278/2014
DNS name	Aller a vector last that enables you to provide with making repeats to the incurpoint Submet to the statement of the statement Submet to Test Statement of the statement of the submet available Security/Group/(crostod/conflict) Coroup name v VPC ID Sow Endpoint-SG-External-VPC vpc-0278c011480
DNS name Comparison of the source of the s	Alter a vectod at that enables you to force with making repeats to an Solution Company of Control Solution Control Solutio
DNS name	Alter a vector dar that enables you to evolve with making repeats to the conclusion your of the state of the state state of the state of the state of the state of the state state of the state of the s
DNS name	Alter a vector dar that enables you to provide with any projects to any conclipional Submet ID Submet ID S
DNS name	Alter a vector dar that enables you to force with multiple results to the conception submet to field decedes 565 61 17 ubmet to field decedes 565 61 17 ubmet to field decedes 565 61 17 vector and the submet available
DNS name	ike a secol as that enables yos to provide with making repeats to in cardpoint Submet ID Submet ID O No submet available O No submet available DECURITY CERCUP (CERCEICOCORTICE) C I D O Group name V VPC ID SOW-Endepoint-SG-External VPC vpc.0278c0116400
DDS name	where a vector of at that enables you to provide whether you have a state of the state of the state of the state with the state of the
DNS name	Aller and an an and an an and an
DNS name	er optional South-Etempi-VYC X Remove
DNS name	All a second set that enables you to provide the shading requests to any conclupiont submet to submet to submet to the submet available to ho submet available to conclusion souther submet souther subme
DDS same	Alter a vector dar that enables you to provide with any projects to any conclipional Submet to any concerner or outpand's (Carfulto Cardipolati Submet to any concerner or outpand's (Carfulto Submet to any concerner or outpand's (Carfulto No submet available O No submet available Societaria (Carfuello) Caroup name v VPC ID Societaria (Carfuello) Societaria (Carfuell

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:



VPC > Endpoints > Create endpoint			
Create endpoint տ			
There are three types of VPC endpoints - Inte	rface endpoints, Gateway Load Balan	cer endpoints, and Gate	way endpoints.
Interface endpoints and Gateway Load Balan Interface (ENI) as an entry point for traffic de	er endpoints are powered by AWS Pr tined to the service. Interface endpo	vateLink, and use an El nts are typically access	astic Network d using the public
or private DNS name associated with the serv target for a route in your route table for traff	ice, while Gateway endpoints and Gat c destined for the service.	eway Load Balancer en	dpoints serve as a
Endpoint settings			
Name tag - ontional			
Creates a tag with a key of 'Name' and a value the	t you specify.		
S3-Endpoint-External-VPC			
Service category			
 AWS services Services provided by Amazon 	PrivateLink Services with	Ready partner services an AWS Service Ready desir	nation
 AWS Marketplace services Services that you've purchased through All 	Other endp /S Marketplace	bint services hared with you by service r	ame
0000000			
Services (1/2)	ounenacelencpoint		G
Q. Filter services		4	1 > @
Service Name: com.amazonar s.eu-west	2.s3 × Clear filters		
Service Name			
com.amazonaws.eu-west-2.s3	amazon		Interface
 com.amazonaws.eu-west-2.s3 	amazon		Gateway
Select the VPC in which to create the endpoint	External VPC		
The VPC in which to create your endpoint.			
(External VPC)		• C	
· Additional continue	DNSisnotavailabl	oforthisservic	9
Additional settings			
Enable DNS name Info			
leverage Amazon's private network connectiv service's default public endpoint DNS name.	that contains a record set that enables you by to the service while making requests to o use this feature, ensure that the attribute	he s'Enable	
DNS hostnames' and 'Enable DNS support' and	e enabled for your VPC.	~~~~~	
	Selection	loon more sub	leistonuio
		encpoint	
Subnets (1/3) Info		encpoint	
Subnets (1/3) Info	T Subast ID	endpoint	7
Subnets (1/3) Info	♥ Subnet ID	endpoint	~
Subnets (1/3) Info Availability Zone eu-west-2a (euw2-az2)	✓ Subnet ID subnet-016d49ec6es	656117	v •
Subnets (1/3) Info Availability Zone eu-west-Za (euw2-az2) eu-west-Zb (euw2-az3)	Subnet ID subnet-016d49ec6es O No subnet available	656117	⊽ ▼
Subnets (1/3) tere Image: Availability Zone Image: Availability Zone	Subnet ID Subnet ID Subnet-016d49ec6et @ No subnet available @ No subnet available	656117	▼
Subnets (1/3) infe Image: Availability Zone Image: Availabil	Subnet ID subnet-016d49ec6et ON subnet available ON subnet available	656117	v v
Subnets (1/3) Ivis Image: Analiability Zone Image: Analiability Zone	Sobnet 10 subnet -016649ec6et olio subnet -016649ec6et olio subnet -016649ec6et olio subnet -016449ec6et subnet -016449ec6et subnet -016449ec6et subnet -016449ec6et	655117	· ·
Subnets: (1/3) inits Image: Anallability Zone Image: Constraint Constrai	subnet ID subnet-016649ec5et or to subnet available Or to subnet available Or to subnet available clocktino-Coccurity-Coccur		۵) ۲
Subnets (1/3) wire If Availability Zone If ex-west-2a (swc2-az2) If ex-west-2b (swc2-az2) If <th>submet 10 submet 10 submet - 016640ec6et 0 No submet available 0 No submet available</th> <td></td> <td>▼ ▼ 1) © 1) 0</td>	submet 10 submet 10 submet - 016640ec6et 0 No submet available 0 No submet available		▼ ▼ 1) © 1) 0
Subnets (1/3) wie Subnets (1/3) wie Subnets (1/3) wie Subnets (1/3) wie Subnet - 016434ec64555117 X Security groups (1/4) wie Q, filter security groups Groups (0)	Subnet ID Subnet ID Subnet-01640ec6e6 Orio subnet available Orio subnet available Diocleftino-Goourfily-Group v Group name		▼ ▼ 1 > © VPC ID
Subnets (1/3) Infe Subnets (1/3) Infe Reverse 20 (env2-22) ev-vent-20 (env2-22) Ev-v	Subnet D subnet -0.16649eceet on to subnet available on to subnet available olocationes available clocationes available	Cric (2011)	▼ ▼ 1) C 1) @ VPC ID
Subnets (1/3) Infe Availability Zone evenet-2a (envC-az2) evenet-2b (env2-az3) evenet-2b (env2-az1) indere-016649ec665556117 X Security groups (1/4) Infe Group ID Group ID	Subnet ID Subnet ID Subnet ID Subnet available This subnet available ChiteStithDeScountityGoroup Group name	Cric (2011)	
Subnets (1/3) tris Availability Zons Availability	Subnet D subnet-016649ec5et subnet-016649ec5et o) to subnet available control of the subnet available control of	Cncpoint3	v v 1 > ⊗ vvc.ib
Subnets (1/3) wie Image: Subnets (1/3) wie Image: Subnets (1/3) wie Image: Subnet (1/3)	Subnet ID Subnet-01640ec6e6 Subnet-01640ec6e6 Or tos uchnet available Otos uchnet available Dioclettino-Bocaurily-Concur Group name S12-Endpoint-S0-Extern	Cnopolni 3	
Subnets (1/3) wire If Anallability Zone If Anallability Zone If ex-west-2a (ewx2-az2) If ex-west-2b (ewx2-az1) If ex-west-2b (ewx2-az1) If ex-west-2c (ewx2-az1) If	Subnet ID Subnet ID Subnet-016494cetet Or No subnet available Or No subnet available State1000ScearfilyCecourg Group name S1-Endpoint-S6-Extern	Createdoanii eseitt (createdoanii v	
Subnets (1/3) Infe Subnets (1/3) Infe Image: Subnets (1/3) Image: Subnets (1/3) Image: Subnet (1/3) Image: Subnet (1/3) Image: Subnet (1/	Subnet ID Subnet ID Subnet -0.16649eceee Or his subnet available Or his subnet available Statistical Constraints/Constraints/ Or Group name S1-Endpoint-SG-Extern	Cnopoln3 655117 (GrontoConfil: • •	v v v v v v v v v v v v v v
Subnets (1/3) uris Subnets (1/3) uris Carlos and the second of the sec	Subnet ID subnet ID subnet -016649eceet O 169 subnet available O 169 subnet available Statistical Generality/General Oreup name S1-Endpoint-S6-Extern	CEEDEDINS 656117 Deferente Coordit Coordination of the Coorditation Coordination of the Coorditation Coordination of the Coorditation of the Coordination of the Coord	v v v v v v v v v v v v v v
Subnets (1/3) wie Image: Subnets (1/3) wie Image: Subnets (1/3) wie Image: Subnets (1/3) wie Image: Subnet (1/3) wie Image: Submet (1/3) wie <tr< td=""><th>Subnet ID Subnet-016424ec4et whore-016424ec4et @ No subnet available @ No subnet available clock(thc)@Cocurilly@Cocur v Greup name S3-Endpoint-S6-Extern</th><td>Createdoarile</td><td>v ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓</td></tr<>	Subnet ID Subnet-016424ec4et whore-016424ec4et @ No subnet available @ No subnet available clock(thc)@Cocurilly@Cocur v Greup name S3-Endpoint-S6-Extern	Createdoarile	v ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
Subnets (1/3) wie Subnets (1/3) wie Autilubility Zone Convert-20 (env2-az2) ev-west-22 (env2-az1) where-016648ec66555117 X Security groups (1/4) wie Group ID Group ID Group ID Group ID Policy wie Vec.extbook4er77204cb Policy wie Vec.extbook4er77204cb	Subnet ID Subnet ID Subnet-OT6649ecetet Or hor subnet available Or hor subnet available Scient (The Scientify Concur Group name S1-Endpoint-SG-Extern	Crectologiii essiii (creatologiii) v	▼ ▼ () () () () () () () () () ()
Subnets (1/3) wie Subnets (1/4) wie Subnets (1/4	Subnet D Subnet D Subnet -D 16649ccete O 169 subnet -D 16649ccete O 169 subnet -D 16649ccetet O 169 subnet-D 16649ccetet O 169 subnet -D 16649ccetet O 169 subnet-		v v
Subnets (1/3) infe Subnets (1/3) infe Autilability Zone Conservation (2002) Conservation	Subnet ID Subnet ID Subnet -0.16649ecetet O his subnet available O his subnet available DEDESTRIDESCENTIFYERCENT V Group name S1-Endpoint-S5-Extern VVC sategrondentifik from any Annuary MV		v v
Subnets (1/3) wie Subnets (1/3) wie Autilubility Zone Convert-24 (6w/2-422) Convert-24 (6w/2-423) Convert-26 (6w/2-423) Convert-2	Subnet ID Subnet ID Subnet-01640ecdet Gries subnet-201640ecdet Gries subnet-201640ecdet Gries subnet available DIDGENERS COLUMNING COLUMNING TO Greep name S1-Endpoint-SC-Extern VVC subg conductivity from any Annator W WVC subg conductivity from any Annator W WVC subg conductivity from any Annator W		
Subbets (1/3) wie Subbets (1/3	Subnet ID Subnet ID Subnet-016484ected Subnet-016484ected Or to subnet available Disclotet AlloseGoardIlyGoard Group name S1-Endpoint-SG-Extern We dara patiently (We metapation and a second patient) We data patiently (We metapation and a second patient)	Crectorial Sectorial Secto	
Subnets (1/3) wie Subnets (1/3	Subnet D Subnet D Subnet Of Selected Or to subnet available Or to subnet available State of the Second Dy Concur Group name S1-Endpoint-SG-Extern Vot earlighted with first may partners Vot earlighted with first may partners S2-Endpoint-SG-Extern Vot earlighted with first may partners Vot earlighted with the excessory partner Vot earlighted with the generated public balance.		
Subnets (1/3) wie Subnets (1/3) wie Autilubility Zene e.e.west-2a (env2-az2) e.e.west-2a (env2-az2) e.e.west-2a (env2-az3) e.e.west-2a (env2-az3	Subnet D Subnet D Subnet O Solution Original Solution Original Solution	Concepcing Concepcing Sector Sector Concepcing Concepcin	v v
Subnets (1/3) wie Subnets (1/3)	Subnet D Induct-016494cetet O his subnet available O his subnet available O his subnet available ClocifithOcCountly/Count V Group name S1-Endpoint-S5-Extern		v v
Subnets (1/3) ini Subnets (1/3)	Subnet D Subnet Of Subnet Available Subnet-Of Subnet Available Control of Subnet Available Telecold the Generating of The Subnet Available Telecold the Generating of The Subnet Available Subnet Sub	Created out it Set 17	
Subbets (1/3) wie Subbets (1/3	Subnet D Subnet D Subnet-O1648ecetet O160 subnet-available O160 subnet-available Discubnet-available Discubnet-available Discubnet-available O160 subnet-Subne-Subnet-Subne-Subnet-Subne-Subnet-Subnet-Subnet-Subne-Subnet-Subn		v v v v v v v v v v v v v v
Subnets (1/3) wie Subnets (1/3	Subnet D Subnet D Subnet O	Crectorial Sectorial	v v
Subnets (1/3) wie Subnets (1/3)	Subnet D Subnet D Subnet O	Concepcing assessments to any and a second second second second as a second second second as a second secon	v v v
Subnets (1/3) wie Subnets (1/3	Subnet 10 Subnet 20	Crectoolins Sestin Sestin VerentedCoardite Verented	v v
Subnets (1/3) wie Subnets (1/3	Subnet D Subnet D Subnet Of Selected Subnet Of Selected Or to subnet available Discubnet available State of the selected of the		v v v v v v v v v v v v v v v v v v v
Subnets (1/3) wie Subnets (1/3	Subnet D Subnet D Subnet Of Selected O To subnet available O To subnet available Constraints available	Concepcinity Conc	
Subnets (1/3) wie Subnet (1/3) wie	Subnet D Subnet D Subnet O	Concepcing Sector according Sector acc	v v v

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":

Storage Gateway ×	Storage Gateway 🤌 Gateways	
Gateways	Gateways (2) Info C Actions ▼ Create tapes Create volume Create file share Attach FSx file system	m Create gateway
File shares	C Silver bu anterway pame ID, status, buna tao kay as tao yalya	
FSx file systems	There by guteway norme, b2, status, type, tag key, or tag value.	
Volumes	Name ▲ Gateway ID ♡ Status ♡ Alarm st ♡ Gateway type ♡ Storage resources	~
Tape Library		

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":



	► How it works	
	Gateway settings	
vate	Gateway name	
	AWS-Storage-Gateway-1	
	The name must be between 2 and 255 characters and cannot include	a slash (or /).
	Gateway time zone Choose the local time zone based on where you are deploying your ga	iteway.
	GMT Western Europe Time, London, Lisbon, Casablanca	▼
	Gateway options Info	"FileGateway"
	Gateway type	
	Amazon S3 File Gateway Store and access objects in Amazon S3 from NFS or SMB file data with local acchieve	Amazon FSx File Gateway Access fully managed file shares in Amazon FSx for Windows File Same using SMR
	<u>9</u> -1	FSX
	C Tape gateway	O Volume gateway
	Store virtual tapes in Amazon S3 using iSCSI-VTL, and store archived tapes in Amazon S3 Glacier or Amazon S3 Glacier Deep Archive.	Store and access iSCSI block storage volumes in Amazo S3.
	\square	G
	<u>O</u>	
	Microsoft Hyper-V Linux KVM Amazon EC2 Hardware appliance	
	Set up gateway on VMware ESXi	
	Storage Gateway currently supports version 6.0, 6.5, and	6.7. To setup your gateway, first, download the OVF
	template. After the download is finished, follow the instr take up to 10 minutes.	ructions below to set up your gateway. This setup migh
	🕑 Download OVF template	theinstallationsteps
	1. Connect to your VMware ESXi hypervisor using your V	/Mware vSphere client.
	 Choose File > Deploy OVF Template, and then naviga downloaded. 	ate to the AWS Storage Gateway OVA template that yo
	 Follow the deployment wizard steps to deploy it. Ren might import to the host. 	ame the VM to avoid confusion with other VMs that yo
	a. If you are prompted to select a storage location, se package.	elect the data store where you want to store the .ova
	b. For Select Storage, select Thick provisioned virtu	al disk format.
	4. Arter the vm is deployed, choose Edit Settings > Add disk for cache storage with at least 150 GiB. For incre- leand disk for each storage with at least 655 GiB.	avew Device > Hard Disk, and allocate at least one loc ased performance, we recommend allocating multiple
	5. Choose Edit Settings > Options > VMware Tools. Un	der Advanced, select the Synchronize guest time with
	host option, and then choose OK. 6. Make sure that your host clock is set to the correct tir	ne. If you have not configured your host clock,
	synchronize it with a Network Time Protocol (NTP) se	rver.
		abyou have
	Charles and Charle	
	Confilm and gateway	Continees

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:



<	🕆 AWS-Storage	-Gateway-1 🛛 🗅	🗆 🛱 🖗 🔞 🗄 ACTIONS	
[]] <u>B</u> 🖹 🖉	Summary Monitor	Configure Permissio	ons Datastores Networks	Snapshots
 Ø vcenter.sddc- 				
SDDC-Datacenter	Guest OS	II Virtua	al Machine Details	ACTIONS ~
> Discovered virtual machine		_	Power Status Dower	red On
> 🗋 Management VMs	K2 Agginess projis to cheaps your anthemit configuration and other patt p=721-24-94-77 ing pr		Guest OS 🚺 Other	3.x or later Linux (64-bit)
> 🗋 Templates			VMware Tools Running, ver	rsion:10336 (Guest Managed)
~ 🗋 Workloads			DNS Name (1) ip-172-31-94	-77.ec2.internal
🔀 AWS-Storage-Gateway-1			IP Addresses (1) 192.168.1.5	
🔂 win10-A			Encryption Not encrypt	ted
🗊 win10-B				
	LAUNCH WEB CONSC			

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.

vation	Connect to AWS Info We have created an endpoint hosted in our VPC	
et up gateway	Endpoint options Info	
tep 2 onnect to AWS	Service endpoint Choose whether the endpoint is publicly accessible or hosted inside your VPC.	
ep 3 eview and activate iguration	Publicly accessible Your gateway communicates with AWS over the public internet. VPC hosted Accessible within your Virtual Private Cloud (VPC) Your gateway communicates with AWS through a connection with your VPC, allowing you to control network settings.	only. private your
ep 4	Choose how to identify an existing VPC endpoint	
angure gateway	• VPC endpoint ID	
	VPC endpoint DNS name or IP address endpoint will be in the list	
	VPC endpoint ID	
	SGW-Endpoint-Connected-VPC vpce-02aa44ca248fbc3d▼ C Create VPC endpoint C	
	Gateway connection options Connection options You can use the gateway IP address. If that isn't available, use the activation key. IP address Your gateway's IP address must be public or accessible from within your current network. Your web browser must be able to connect to this IP address. IP address IP address To get the IP address, log into the gateway's local consoler from your hypervisor citent. 122 169 15	

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



ctivation	Review and activate Info	
Step 1		
Set up gateway	Step 1: Gateway details	Edit
Step 2		
Connect to AWS	Gateway options	
Step 3	Gateway name	Gateway time zone
Review and activate	AWS-Storage-Gateway-1	GMT Western Europe Time, London, Lisbon, Casablanca
onfiguration	Gateway type	Host platform type
Step 4	Amazon S3 File Gateway	VMware ESXi
Configure gateway	AWS region	
	Europe (London)	
	Step 2. connection details	Edit
	Connection settings	Eor
	Connection settings	VPC endpoint
	Connection settings Endpoint options VPC hosted	VPC endpoint vpce-02aa44ca248fbc3d4-p9dg9sgk.storagegateway.eu- west-2.vpce.amazonaws.com
	Connection settings Endpoint options VPC hosted Gateway connection option	VPC endpoint vpce-02aa44ca248fbc3d4-p9dg9sgk.storagegateway.eu- west-2.vpce.amazonaws.com IP address
	Connection settings Endpoint options VPC hosted Gateway connection option IP address	VPC endpoint vpce-02aa44ca248fbc3d4-p9dg9sgk.storagegateway.eu- west-2.vpce.amazonaws.com IP address 192.168.1.5
	Connection settings Endpoint options VPC hosted Gateway connection option IP address	VPC endpoint vpce-02aa44ca248fbc3d4-p9dg9sgk.storagegateway.eu- west-2.vpce.amazonaws.com IP address 192.168.1.5
	Connection settings Endpoint options VPC hosted Gateway connection option IP address Review your gateway and connection After your gateway is created, you can	VPC endpoint vpce-02aa44ca248fbc3d4-p9dg9sgk.storagegateway.eu- west-2.vpce.amazonaws.com IP address 192.168.1.5
	Connection settings Endpoint options VPC hosted Gateway connection option IP address Review your gateway and connection After your gateway is created, you car	VPC endpoint vpce-02aa44ca248fbc3d4-p9dg9sgk.storagegateway.eu- west-2.vpce.amazonaws.com IP address 192.168.1.5

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:

by Broadcom

Storage Gateway ×	Storage Gateway > Gateways	
Gateways	Gateways (1) Info C Actions 🔻 Create tapes Create volume Create file share Attach FSx file system C	reate gateway
File shares FSx file systems	Q. Filter by gateway name, ID, status, type, tag key, or tag value.	(1) ()
Volumes	Name ▲ Gateway ID ♥ Status ♥ Alarm st ♥ Gateway ty ♥ Storage resources	~
Tape Library Pools	AWS-Storace_Gatewav-1 sow-3268858 Arunning O None 53 File 0 file shares	
Tapes		
Hardware		

Figure 26: Select Storage Gateway

Storage Gateway ×	Storage Gateway > Gateways > AWS-Storage-Gateway-1				
Gateways AWS-Storage-Gateway-1					
FSx file systems Volumes Tape Library	You need to allocate local storage. In order to start using your gateway, you	You need to allocate local storage. In order to start using your gateway, you need to allocate local storage.			
Tapes Hardware	General configuration Info				
	Name D AWS-Storage-Gateway-1 (sgw-3268885 B)	Type S3 File	Gateway ID sgw-32688858	Storage resources O file shares	

Figure 27: Edit Storage Gateway Disks

it local d	isks			
ocal disks Inf	D			C
Configure cache st Cache. The local d blatform.	corage by allocating one isks correspond to the s	e or more local disks with at least to a structure or structure on structure of the structure of t	t 150 GiB to your host	
Recomm diminish To meet gateway Cache.	ended minimum disk c ed performance. the recommended minir with a total capacity of	apacity not met. You might exp mum cache storage, add local di: at least 150 GiB and allocate the	sks to your em to	ange from allocated" (o "Cache"
Recomm diminish To meet gateway Cache.	ended minimum disk c ed performance. the recommended mini with a total capacity of Capacity	apacity not met. You might exp mum cache storage, add local dis at least 150 GiB and allocate the Allocated to	sks to your em to	iange(from) allocated"(to "Cache"
Recomm diminish To meet gateway Cache.	ended minimum disk c ed performance. the recommended mini with a total capacity of Capacity 150 GiB	apacity not met. You might exp mum cache storage, add local di at least 150 GiB and allocate the Allocated to Unallocated	sks to your em to	iange from allocated to "Cache"
Recomm diminish To meet gateway Cache.	ended minimum disk c ed performance. the recommended minia with a total capacity of Capacity 150 GiB	apacity not met. You might exp mum cache storage, add local di at least 150 GiB and allocate the Allocated to Unallocated Unallocated	sks to your m to	iange from allocated to "Cache"

Figure 28: Assign Cache Disks

Your gateway is now up and running:

⊙ Successfully updated local disks.					
Storage Gateway > Gateways > AWS-Storage-Gateway-1 AWS-Storage-Gateway-1					
General configuration Info					
Name D AWS-Storage-Gateway-1 (sgw-3268885B) Status O Running	Type S3 File Alarm state ③ None	Gateway ID sgw-3268885B	Storage resources O file shares		

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":

Storage Gateway \times	Storage Gateway $>$ File shares	
Gateways <mark>File shares</mark> FSx file systems	File shares info C Actions ▼ Cree Q. Filter by file share, status, or other attributes	eate file share
Volumes Tape Library	File share ID Image: File share name Image: V Status Image: V Type Image: S3 location Image: S3 location	∇
Pools Tapes	No file shares You don't have any file shares.	
Hardware	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:



itep 1 File share settings	File share settings տ
Step 2	File share settings configuration
Amazon S3 storage settings	
Step 3 File access settings	Gateway AWS-Storage-Gateway-1 (sgw-3268885B)
Step 4	Amazon 53 location info Can use a prefix to separate S 35 bucket name Shares to the same bucket
Review and create	Connect directly to your bucket. SSIDUCKET WE S3 access point Created earlier
	Connect through a harmed needs to appoint that is attached to your ducket. S3 access point alias Connect using a bucket are alias that points to an S3 access point connected to your bucket.
	Amazon 53 Maret name S3 park name - optional
	s3-sgw-1 / a/
	Bucket name must be between 3 to 63 characters. Prefix name must end with a "/".
	Versioning-enabled 53 buckets Use of 53 buckets with versioning enabled can increase the amount of storage used in Amazon 53. Each modification to a file creates a new version of the object.
	AWS region Choose the region where the S3 endpoint is located
	Europe (London) eu-west-2
	File share name infe The default name is pre-filled with the S3 bucket name. Once the file share is created, the file share name can't be deleted.
	s3-sgw-1a
	File share name must be between 1 to 255 characters.
	Private Link for S3 - Optional Access the S3 bucket through the S3 endpoint in the Connected
	Choose how to identify an existing VPC endpoint Info
	O DNS name
	DNS name
	VPC endpoint ID
	DNS name of the VPC endpoint: vpce-0f0944d35fe622953-0ch64lgb.s3.eu-west-2.vpce.amazonaws.com
	Access objects using Network File System (NFS)
	Server Message Block (SMB)
	Audit logs Info You can monitor your fileshare using Amazon CloudWatch log groups.
	A new CloudWatch log group will be created.
	Use an existing log group Choose an existing CloudWatch log group.
	Deactivate logging No CloudWatch log group will be created.
	Automated cache refresh from \$3 Info
	Set refresh interval
	File upload notification Info
	None Set settling time
	Tags - optional
	Key Value - optional
	Q Name X Q s3-sgw-1 X Remove
	Add new tag You can add 49 more tags.
	Concel New

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



Storage Gateway > File shares >	Create file share	
Step 1 File share settings	Amazon S3 storage settings Info	
Step 2 Amazon S3 storage settings	Amazon S3 storage configuration	
Step 3 File access settings	Amazon S3 bucket name / Prefix name s3-sgw-1 [2] / a/	
Step 4 Review and create	S3 Standard V	
	Guess MIME type	
	Enable requester pays	
	Access to your S3 bucket Info	
	Create a new IAM role.	
	S3-Managed Keys (SSE-S3)	
	KMS-Managed Keys (SSE-KMS)	
	Cancel Previous Next	

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

p 1 e share settings	File access settings Info
p 2 nazon S3 storage settings	Authentication method
	Authentication method
e access settings	Guest access
	To configure your nie share for guest access set a guest password.
p 4 view and create	Guest password
	Guest password must be between 6 and 512 characters.
	SMB share settings
	Export as
	Read-write
	O Read-only
	File and directory access controlled by
	Windows Access Control Lists
	• POSIX permissions
	Opportunistic lock (oplock) Optimize the file buffering strategy to speed up access to a file server.
	Activate
	Force case sensitivity
	Activate
	To avoid conflict cases during file access, the Opportunistic lock and Force case sensitivity settings are mutually exclusive and cannot be activated at the same time.
	Access based enumeration for files and directories
	Activate
	Cancel Previous Nex

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":



rage settings	Step 1: File share settings		Ed
	File share details		
ngs	Gateway	Amazon S3 bucket name / Prefix name	
	AWS-Storage-Gateway-1	s3-sgw-1 🗹 / a/	
ate	AWS Region	AWS PrivateLink for S3	
	eu-west-2	vpce-0f0944d35fe622953-0ch64lgb.s3.eu-v 2.vpce.amazonaws.com	vest-
	File share name	Access objects using	
	s3-sgw-1a	SMB	
	Audit logs	Automated cache refresh from S3	
	Disable logging	Disabled	
	File upload notification		
	Disabled		
	Tags (1)		
	Кеу	Value	
	Name	s3-sgw-1	
	Step 2: Amazon S3 storage setting	5	E
	Amazon S3 storage configuration	Dn	
	Amazon S3 storage configuration	Guess MIME type	
	Amazon S3 storage configuration Storage class for new objects S3 Standard	Guess MIME type Yes	
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control	Guess MIME type Yes Enable requester pays	
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes	Guess MIME type Yes Enable requester pays No	
	Amazon S3 storage configurations Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role.	Guess MIME type Yes Enable requester pays No Encryption 53-Managed Keys (SSE-53)	
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role.	Guess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3)	
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings	Guess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3)	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings	Guess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3)	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method	Guest password	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access	Guess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3)	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings	Cuess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3)	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings Export as	Cuess MIME type Yes Enable requester pays No Encryption 53-Managed Keys (SSE-53)	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings Export as Read-write	DI Guess MIME type Yes Enable requester pays No Encryption 53-Managed Keys (SSE-53) Guest password 	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings Export as Read-write Opportunistic lark (onlock)	DI Guess MIME type Yes Enable requester pays No Encryption 53-Managed Keys (SSE-S3) Guest password 	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings Export as Read-write Opportunistic lock (oplock) Activated	DI Guess MIME type Yes Enable requester pays No Encryption 53-Managed Keys (SSE-S3) Guest password File and directory access controlled by POSIX permissions Force case sensitivity Deactivated	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings Export as Read-write Opportunistic lock (oplock) Activated Access based enumeration	DN Guess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3) Guest password Guest password File and directory access controlled by POSIX permissions Force case sensitivity Deactivated	E
	Amazon S3 storage configuration Storage class for new objects S3 Standard Give bucket owner full control Yes Access to your S3 bucket Create a new IAM role. Step 3: File access settings File access settings Authentication method Guest access SMB share settings Export as Read-write Opportunistic lock (oplock) Activated Access based enumeration Deactivated	DN Guess MIME type Yes Enable requester pays No Encryption S3-Managed Keys (SSE-S3) Guest password Guest password File and directory access controlled by POSIX permissions Force case sensitivity Deactivated	E

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:



Storage Gateway $\qquad imes$	⊘ Successfully created file share share-6800C01B.					
Gateways File shares FSx file systems Volumes	Storage Gateway > File shares > share-6800C01B share-6800C01B Info Actions					
Tape Library Pools	General configuration Info					
Tapes Hardware	File share ID Stare-6800C01B S3 location s3-sgw-1/a/	File share name s3-sgw-1a AWS Region eu-west-2	Status Unavailable AWS PrivateLink for 53 ypce-0f0944d35fe622953-0ch64lgb.s3.eu-	Type SMB Gateway AWS-Storage-Gateway-1		
	Details Tags					
	File share ARN	Metrics Cloudwatch Metrics 🖸 Bucket owner full control Yes	Audit logs (Net Enabled) Requester pays No	Default storage class 53 Standard IAM role StorageGatewayBucketAccessRole 16458399151 830.39913461443890563 🖸		
	Encryption S3-Managed Keys (SSE-S3) Opportunistic lock (oplock) Activated	Authentication method Guest access Force case sensitivity Deactivated	Export as Read-write Access based enumeration Deactivated	Access control POSIX permissions		
	Example Commands You can use the following example command to connect to the file share.					
	On Microsoft Windows: net use [WindowsDriveLetter]: \\192.168.1.5\\\\\3-sgw-1a /user.sgw-3268858\\smbguest					

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.



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)



5 m m	Name	Date modified	Туре	Size
T Quick access	Doc in AWS-Storage-Gateway-1	2/3/2022 11-29 AM	Text Document	0 KB
Desktop 🖈	E boe in And blondge batering i	LO DI LOLL I ILLO PHILI	ion pocorrent	0100
🕹 Downloads 🛛 🖈				
🗄 Documents 🛷				
E Pictures #				
h Music				
🛫 s3-sgw-1a (\\192.168.1.5) (Z:)				
📕 Videos				
OneDrive				
This PC				
3D Objects				
Cesktop				
🛗 Documents				
🖶 Downloads				
Music				
E Pictures				
📕 Videos				
🏪 Local Disk (C:)				
🛫 s3-sgw-1a (\\192.168.1.5) (Z:)				
i Network				

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/"):

Amazon S3 > s3-sgw-1 > a/	
a/	
Objects Properties	
Objects (1) Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3	inventory to get a list of all object
C 🗇 Copy S3 URI 🗇 Copy URL 🕑 Downloa	d Open 🖸 Delete
Q Find objects by prefix	
Name	▲ Type ▽
Doc in AWS-Storage-Gateway-1.txt	txt

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:



New VPC Experience Tell us what you think		Endpoints (4) Info			
VPC Dashboard EC2 Global View New Filter by VPC:		Q Filter endpoints search: sgw- X search: s3- X	Clear filters		
Q Select a VPC		Name	∇	VPC endpoint ID	∇
VIRTUAL PRIVATE		SGW-Endpoint-External-VPC		vpce-00751fccf122148b2	
CLOUD Your VPCs		SGW-Endpoint-Connected-V	PC	vpce-02aa44ca248fbc3d4	
Subnets		S3-Endpoint-External-VPC		vpce-0d765c7b5f4f37cda	
Route Tables		S3-Endpoint-Connected-VPC		vpce-0f0944d35fe622953	
Internet Gateways					_
Egress Only Internet Gateways	-				=
Carrier Gateways		Select an endpoint			
DHCP Options Sets					
Elastic IPs					
Managed Prefix Lists					
Endpoints New					

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:

New VPC Experience Tell us what you think	Endpoints (1/4) Info					C
VPC Dashboard	Q Filter endpoints					
EC2 Global View New Filter by VPC:	search: sgw- \times search: s3- \times	Clear filters				
Q Select a VPC	Name Name	▼ VPC endpoint ID	∇	VPC ID	\bigtriangledown	Service name
	SGW-Endpoint-External-VPC	vpce-00751fccf122148b2		vpc-0278c01f48018fae0 Exter	nal VPC	com.amazonaws.e
Your VPCs	SGW-Endpoint-Connected-VPC	vpce-02aa44ca248fbc3d4		vpc-09d5e0dfb092eaf95 Conn	ected	com.amazonaws.e
Subnets	S3-Endpoint-External-VPC	vpce-0d765c7b5f4f37cda		vpc-0278c01f48018fae0 Exter	nal VPC	com.amazonaws.e
Route Tables	S3-Endpoint-Connected-VPC	vpce-0f0944d35fe622953		vpc-09d5e0dfb092eaf95 Conn	ected	com.amazonaws.e
Internet Gateways			-			
Egress Only Internet Gateways			_			
Carrier Gateways	vpce-02aa44ca248tbc3d4 / SGW-Endpoint-	Connected-VPC				
DHCP Options Sets	Details Subnets Security Groups	Notification Monitoring Tags				
Elastic IPs						
Managed Prefix Lists	Contractor (1)					
Endpoints New	Subnets (1)					
Endpoint Services	Q Filter subnets					
NAT Gateways						
Peering Connections		▽ IPv4 addresses		dresses \triangledown	Network Int	terface ID
▼ SECURITY	eu-west-2a (euw2-az2)	172.30.10.170	-		eni-031d37	557b0301d0f 🗹

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
		Enapoint	IF Address	Network Interface
AWS-Sto 192.168	AWS-Storage-Gateway-1	SGW-Endpoint-Connected-VPC	172.30.10.170	eni-031d37557b0301d0f
	192.168.1.5	S3-Endpoint-Connected-VPC	172.30.10.180	eni-0e712a512712b87af
AWS-Storage-Gateway-2 192.168.2.103	AWS-Storage-Gateway-2	SGW-Endpoint-External-VPC	172.20.200.101	eni-0c7293c72936b5dc0
	192.168.2.103	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:

subnet-04b1	subnet-04b1719642073822e / <mark>Connected-VPC-Subnet-1</mark>								
Details	Flow logs	Route table	Network ACL	CIDR reservations	Sharing	Tags			
Flow log	gs (1/1)								
Q Filter	r flow logs								
N	ame		▽ Flow log	ID 🗸	Filter		♥ Destination type	∇	
FI FI	ow-Log-Connected	I-VPC-Subnet-1	fl-04e097	7801a325f5f	ALL		cloud-watch-logs		

Figure 42: Connected VPC Flow Log

subnet-016d49ec6e5656117 / External-VPC-Subnet-1									
Details	Flow logs	Route table	Network ACL	CIDR reservations	Sharing	Tags			
Flow log	gs (1/1) r flow logs								
N	lame		▽ Flow log I	D	7 Filter		\bigtriangledown	Destination type	∇
Fl Fl	low-Log-External-V	/PC-Subnet-1	fl-0170e1	b028af9ca78	ALL			cloud-watch-logs	

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):



Log events You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns 🛛 🗘 View as text 🖉 Actions 🔻						
Q	Filter events	Clear 1m 30m 1h 12h				
•	Timestamp	Message				
		There are older events to load. Load more.				
•	2022-02-04T13:50:18.000+00:00	2 unknown eni-031d37557b0301d0f 192.168.1.5 172.30.10.170 34848 1026 6 3 315 1643982618 1643982663 ACCEPT OK				
•	2022-02-04T13:50:18.000+00:00	2 unknown eni-031d37557b0301d0f 192.168.1.5 172.30.10.170 34866 1026 6 2 157 1643982618 1643982663 ACCEPT OK				
•	2022-02-04T13:50:18.000+00:00	2 unknown eni-031d37557b0301d0f 172.30.10.170 192.168.1.5 1026 34866 6 2 80 1643982618 1643982663 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 192.168.1.5 172.30.10.170 34860 1026 6 2 157 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 172.30.10.170 192.168.1.5 1026 34880 6 23 18567 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 192.168.1.5 172.30.10.170 34880 1026 6 26 4188 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 192.168.1.5 172.30.10.170 34870 1026 6 38 14066 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 172.30.10.170 192.168.1.5 1026 34860 6 2 80 1643982630 1643982676 ACCEPT OK				
	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 172.30.10.170 192.168.1.5 1026 34870 6 30 19943 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 172.30.10.170 192.168.1.5 1026 34872 6 33 20360 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 192.168.1.5 172.30.10.170 34876 1026 6 37 13827 1643982630 1643982676 ACCEPT OK				
•	2022-02-04T13:50:30.000+00:00	2 unknown eni-031d37557b0301d0f 172.30.10.170 192.168.1.5 1026 34876 6 28 19413 1643982630 1643982676 ACCEPT OK				
	2022 02 04712 50 20 000 00 00	2 WINTER WY 014 12757 0204 105 402 402 402 40 40 10 10 10 10 10 10 10 10 10 10 10 10 10				

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:

Log e You ca	events In use the filter bar below to search for a	nd match terms, phrases, or values in your log events. Learn more about filter patterns 🖸 🛛 View as text 🔀 🛛 Actions 💌
Q /	ilter events	Clear 1m 30m 1h 12h
Þ	Timestamp	Message
		There are older events to load. Load more.
•	2022-02-04T13:48:04.000+00:00	2 614055364343 eni-0e712a512712b87af <mark>192.168.1.5 172.30.10.180</mark> 39122 443 6 1 60 1643982484 1643982486 ACCEPT OK
•	2022-02-04T13:48:05.000+00:00	2 unknown eni-0e712a512712b87af 1643982485 1643982499 - NODATA
•	2022-02-04T13:48:22.000+00:00	2 614055364343 eni-0e712a512712b87af 172.30.10.180 192.168.1.5 443 39114 6 2 80 1643982502 1643982504 ACCEPT OK
•	2022-02-04T13:48:22.000+00:00	2 614055364343 eni-0e712a512712b87af 192.168.1.5 172.30.10.180 39114 443 6 3 173 1643982502 1643982504 ACCEPT OK
•	2022-02-04T13:48:32.000+00:00	2 614055364343 eni-0e712a512712b87af 1643982512 1643982543 - NODATA
•	2022-02-04T13:48:37.000+00:00	2 614055364343 eni-0e712a512712b87af 1643982517 1643982549 - NODATA
•	2022-02-04T13:48:44.000+00:00	2 unknown eni-0e712a512712b87af 1643982524 1643982534 - NODATA
•	2022-02-04T13:48:57.000+00:00	2 unknown eni-0e712a512712b87af 192.168.1.5 172.30.10.180 39130 443 6 15 3126 1643982537 1643982592 ACCEPT OK
•	2022-02-04T13:48:57.000+00:00	2 unknown eni-0e712a512712b87af 192.168.1.5 172.30.10.180 39122 443 6 3 173 1643982537 1643982592 ACCEPT OK
•	2022-02-04T13:48:57.000+00:00	2 unknown eni-0e712a512712b87af 172.30.10.180 192.168.1.5 443 39130 6 13 7855 1643982537 1643982592 ACCEPT OK
•	2022-02-04T13:48:57.000+00:00	2 unknown eni-0e712a512712b87af 172.30.10.180 192.168.1.5 443 39122 6 2 80 1643982537 1643982592 ACCEPT OK

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):

Log e You car	events n use the filter bar below to search for an	nd match terms, phrases, or values in your log events. Learn more about filter patterns [View as text 🛛 Actions 🔻
Q F	ilter events	Clear 1m 30m 1h 12
•	Timestamp	Message
		There are older events to load. Load more.
•	2022-02-04T14:02:25.000+00:00	2 unknown eni-0c7293c72936b5dc0 192.168.2.103 172.20.200.101 34342 1026 6 26 4528 1643983345 1643983402 ACCEPT OK
•	2022-02-04T14:02:25.000+00:00	2 unknown eni-0c7293c72936b5dc0 172.20.200.101 192.168.2.103 1026 34342 6 22 18366 1643983345 1643983402 ACCEPT OK
•	2022-02-04T14:02:25.000+00:00	2 unknown eni-0c7293c72936b5dc0 192.168.2.103 172.20.200.101 34348 1026 6 27 4236 1643983345 1643983402 ACCEPT OK
•	2022-02-04T14:02:26.000+00:00	2 unknown eni-0c7293c72936b5dc0 192.168.2.103 172.20.200.101 34332 1026 6 2 104 1643983346 1643983393 ACCEPT OK
•	2022-02-04T14:02:26.000+00:00	2 unknown eni-0c7293c72936b5dc0 172.20.200.101 192.168.2.103 1026 34330 6 4 237 1643983346 1643983393 ACCEPT OK
•	2022-02-04T14:02:26.000+00:00	2 unknown eni-0c7293c72936b5dc0 192.168.2.103 172.20.200.101 34328 1026 6 4 261 1643983346 1643983393 ACCEPT OK
•	2022-02-04T14:02:26.000+00:00	2 unknown eni-0c7293c72936b5dc0 172.20.200.101 192.168.2.103 1026 34346 6 22 18366 1643983346 1643983393 ACCEPT OK
•	2022-02-04T14:02:26.000+00:00	2 unknown eni-0c7293c72936b5dc0 172.20.200.101 192.168.2.103 1026 34332 6 2 157 1643983346 1643983393 ACCEPT OK
•	2022-02-04T14:02:29.000+00:00	2 614055364343 eni-0c7293c72936b5dc0 172.20.200.101 192.168.2.103 1026 34326 6 4 237 1643983349 1643983350 ACCEPT OK
•	2022-02-04T14:02:44.000+00:00	2 unknown eni-0c7293c72936b5dc0 192.168.2.103 172.20.200.101 34346 1026 6 26 4528 1643983364 1643983421 ACCEPT OK

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

And for S3 (172.20.200.59):



Log You c	events an use the filter bar below to search for	and match terms, phrases, or values in your log events. Learn more about filter patterns 🖸 🛛 View as text 🔀 🛛 Actions 💌
Q	Filter events	Clear 1m 30m 1h 12h
•	Timestamp	Message
		There are older events to load. Load more.
•	2022-02-04T13:57:24.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 <mark>192.168.2.103 172.20.200.59</mark> 47778 443 6 3 173 1643983044 1643983048 ACCEPT OK
•	2022-02-04T13:57:24.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 192.168.2.103 172.20.200.59 47782 443 6 16 3186 1643983044 1643983048 ACCEPT OK
•	2022-02-04T13:57:34.000+00:00	2 unknown eni-08368e7d8f73df5f0 1643983054 1643983077 - NODATA
•	2022-02-04T13:57:37.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 172.20.200.59 192.168.2.103 443 47782 6 13 7856 1643983057 1643983060 ACCEPT OK
•	2022-02-04T13:57:37.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 172.20.200.59 192.168.2.103 443 47778 6 2 80 1643983057 1643983060 ACCEPT OK
•	2022-02-04T13:57:53.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 1643983073 1643983104 - NODATA
•	2022-02-04T13:57:56.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 172.20.200.59 192.168.2.103 443 47790 6 13 7856 1643983076 1643983076 ACCEPT OK
•	2022-02-04T13:58:07.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 192.168.2.103 172.20.200.59 47790 443 6 16 3186 1643983087 1643983089 ACCEPT OK
•	2022-02-04T13:58:28.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 192.168.2.103 172.20.200.59 47782 443 6 3 173 1643983108 1643983108 ACCEPT OK
•	2022-02-04T13:58:34.000+00:00	2 unknown eni-08368e7d8f73df5f0 1643983114 1643983138 - NODATA
•	2022-02-04T13:58:39.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 172.20.200.59 192.168.2.103 443 47782 6 2 80 1643983119 1643983120 ACCEPT OK
•	2022-02-04T13:58:53.000+00:00	2 614055364343 eni-08368e7d8f73df5f0 1643983133 1643983164 - NODATA

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



