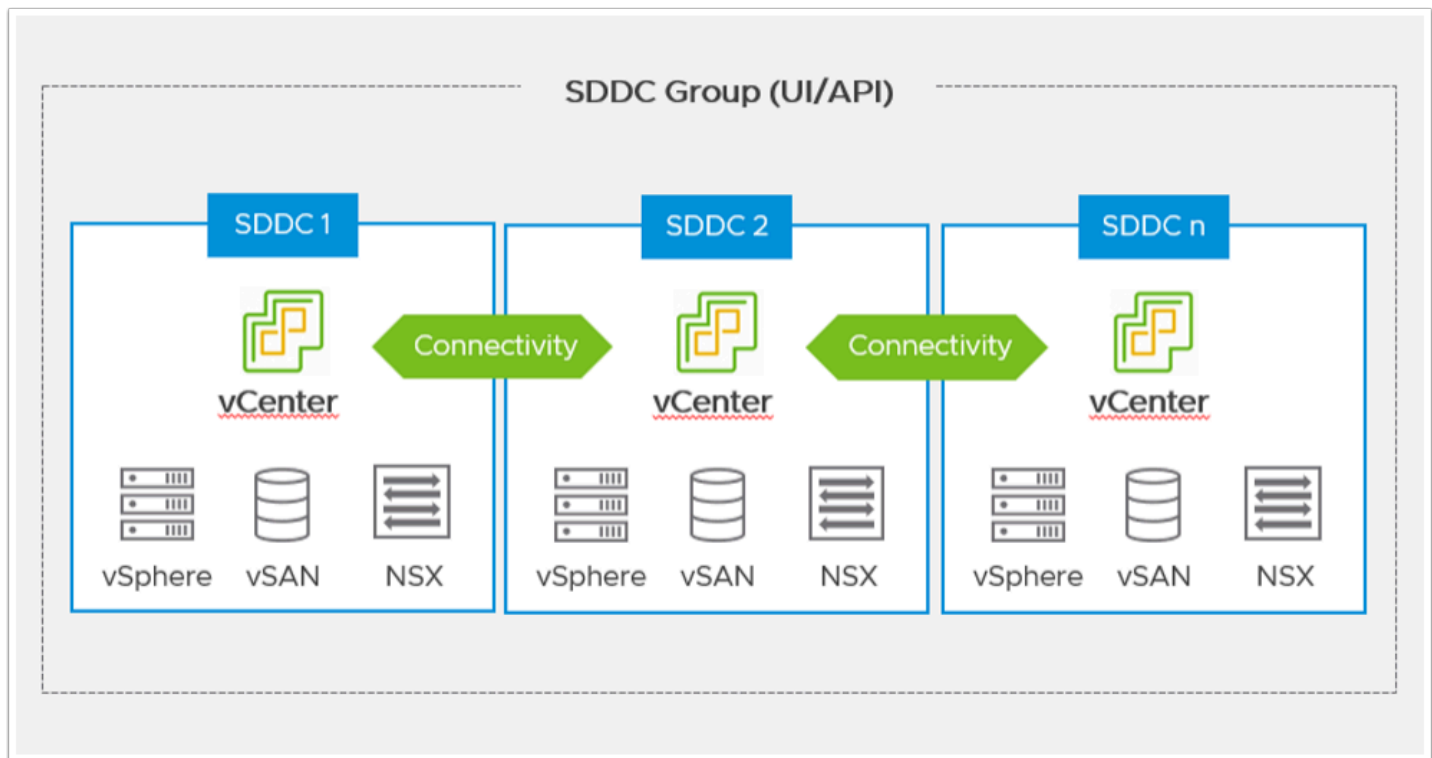


Lab 07 - Inter-SDDC and Native VPC Connectivity

Introduction

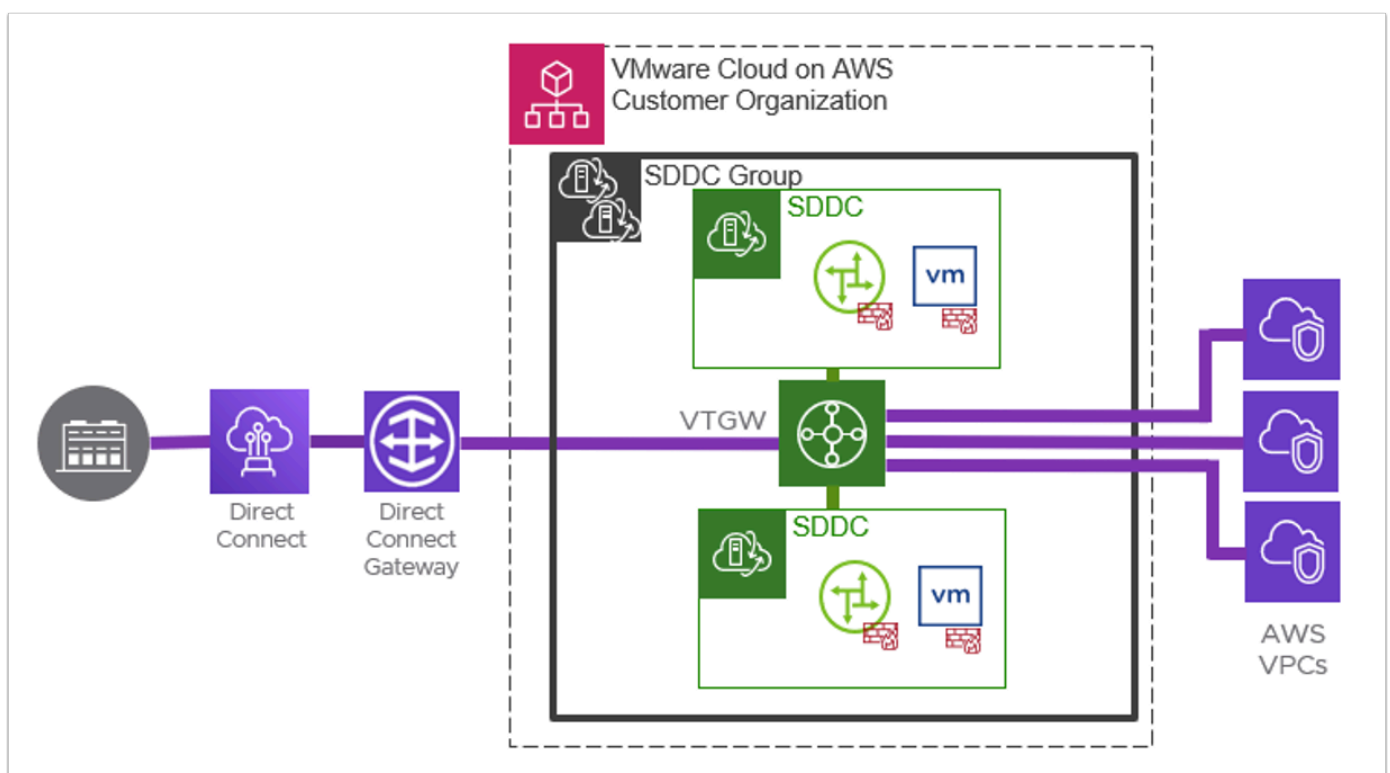
An SDDC deployment group uses VMware Transit Connect to provide high-bandwidth, low-latency connections between SDDCs in the group and to other VPCs in the same region. You can also add a Direct Connect Gateway (DXGW) to provide centralized connectivity to your on-premises SDDCs.

An SDDC deployment group (SDDC Group) is a logical entity designed to simplify the management of your organization's VMware Cloud on AWS resources at scale. Collecting SDDCs into an SDDC Group provides several benefits to an organization with multiple SDDCs whose workloads need a high-bandwidth, low-latency connection to each other. All network traffic between group members travels over a VMware Transit Connect network. Routing between compute networks of all SDDCs in a group is managed automatically by VMware Transit Connect as subnets are added and deleted. You control network traffic among group member workloads with compute gateway firewall rules.



- i** VMware Transit Connect is a VMware Managed Transit Gateway. It Eliminates the overhead of self-deploying and managing complex configurations to establish a connectivity fabric across VMware Cloud on AWS SDDCs, AWS VPCs, and on-premises environments.

VMware Transit Connect easily enables connectivity across environments and adds networks with automatic set up of all the necessary routing policy configuration, transparent to the user. The solution is based on the highly available AWS Transit Gateway. It integrates with AWS Direct Connect Gateway to simplify connectivity to on-premises data centers.



- i** Any organization member who has a VMC service role of Administrator or Administrator (Delete Restricted) can create or modify an SDDC Group.

In this lab, we will first create an SDDC Group with a single SDDC, the purpose of this exercise is to show that an SDDC group can contain a single SDDC, but also to highlight that the VMware Transit connect of the SDDC Group can be used to allow high-bandwidth, low-latency connectivity from SDDC(s) in a group to Native AWS VPC(s). We'll later in the lab, create a new SDDC Group, and populate it with 2 SDDCs.

TASKS

Task 1 - Create a Single SDDC SDDC Group

In the Google Chrome Browser from the VDI desktop

1. Click the **VMware Cloud SDDC** bookmark
 - Login as **vmcexpert#-xx@vmware-hol.com** (Where **#** is the Environment ID and **xx** is your student number) i.e. **vmcexpert1-01@vmware-hol.com**
 - Password = **VMware1!**
2. Navigate to the SDDC item in the menu. You should see both your SDDC and your partner's SDDC
3. In the top right, Click **Actions**
4. Under the Actions Dropdown Click **Create SDDC Group**
5. In the **Name and Description** page Name the Group **vmcexpert#-XX-SDDC-Grp** (Where **#** is the Environment ID and **xx** is your student number)
6. Click **Next**

Software-Defined Data Centers (SDDC)

CREATE SDDC ACTIONS

Purchase Term Subscription

Create SDDC Group

VMCEXP3-02

Ready Expires in 30 days

Region	EU (Frankfurt)	Clusters	1
Type	VMC on AWS	Hosts	1
Availability Zones	eu-central-1b	Cores	36

CPU Memory Storage

82.8 GHz 512 GiB 10.37 TiB

VIEW DETAILS OPEN VCENTER ACTIONS

VMCEXP3-01

Ready Expires in 30 days

Region	EU (Frankfurt)	Clusters	1
Type	VMC on AWS	Hosts	1
Availability Zones	eu-central-1b	Cores	36

CPU Memory Storage

82.8 GHz 512 GiB 10.37 TiB

VIEW DETAILS OPEN VCENTER ACTIONS

BACK TO TOP GO TO GRID VIEW

7. On the **Membership** page Select **<your SDDC>**
NOTE: Only add your Student SDDC to the group

8. Click **Next**
9. on the **Acknowledgment** page Check the **Configuring VMware Transit Connect for your group will incur charges per attachment and Data Transfer** checkbox
10. Click **Create Group**
11. Monitor the Group creation status (this could take up to 10 minutes to complete)
12. While you are waiting, review the blue box below and explore the SDDC Groups tab
13. Click **View Details** once the status changes to **Connected**

1. Name and Description

Create a name and description for your group

Name

vmcexpert3-01-SDDC-gr

1

Description

NEXT

2

2. Membership

Select SDDCs to be part of your group

3. Acknowledgement

Review and acknowledge requirements before creating the group

vmcexpert3-01-SDDC-Grp

Summary

vCenter Linking

Direct Connect

External VPC

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

ADD SDDCS

REMOVE SDDCS

<input type="checkbox"/>	Name	SDDC ID	SDDC Version	Management CIDR	Location	Connectivity Status
<input type="checkbox"/>	VMCEXP3-01	3740b298-9b84-46c3-929e-85c84816dbab	1.15.0.7	10.101.0.0/20	EU (Frankfurt)	CONNECTED

- i

While waiting for the process to complete, let's review the SDDC Group tabs
- vCenter Linking** Tab

Allows Cloud administrator to log in as cloudadmin@vmc.local and use the vSphere Client to manage all the vCenter Server systems in the group. If the cloudadmin@vmc.local account configures these systems to use single sign-on,

then users with accounts in that single sign-on domain can access all the linked systems in the group.

After vCenter linking has been enabled in an SDDC group, the vCenter Server systems in SDDCs added to the group are linked automatically, and vCenter Server systems in SDDCs that are removed from the group are unlinked automatically.


Direct Connect Gateway Tab After you create an SDDC Group, you can attach an AWS Direct Connect Gateway to it to support high-bandwidth, low-latency connections to your on-premises SDDC.

VMware Transit Connect handles all compute and management network traffic among SDDC group members. Many SDDC group members will also need to make network connections to external endpoints such as on-premises SDDCs, VPCs outside the group, and AWS services that run in them. To enable these kinds of connections, associate an AWS Direct Connect Gateway with the group's VMware Managed Transit Gateway.

Attaching a Direct Connect Gateway to the SDDC group is a multi-step process that requires you to use both the VMC Console and the AWS console. You use the VMC Console to make the VTGW (an AWS resource) available for sharing. You then use the AWS console to accept the shared resource and associate it with the Direct Connect Gateway you'd like to attach to the SDDC Group.

VPC Connectivity Tab Once the SDDC Group has been configured, you can add existing Native AWS VPC to the group. Doing so allows the VMware Transit connect to establish and manage a High-bandwidth, low-latency connection between the SDDC and the Native VPC(s).

Routing Tab The Routing tab displays all of the learned routes to the VMware Transit connect as well as all of the Advertised routes from the Transit Connect.

 **Note:** SDDC Groups will typically include 2 or more SDDCs and not a Single SDDC as we have done in this task. The only exception is when you have one or more Native AWS VPC with Services you need to consume in your SDDC or vice-versa and/or connect your On-Premises to your SDDC(s) via a Direct Connect Gateway.

Task 2 - Connect a Native VPC to your SDDC Group

Task 2.1 - Associate you AWS account with the SDDC Group

1. Click the **SDDCs** tab
2. Click **view details** at the bottom of your SDDC tile
3. Click **Networking & Security** tab
4. In the left pane, click **Connected VPC**
5. Record the **AWS Account ID**, We will use it to Attach a Native VPC to your SDDC Group

VMCEXP3-02 | VMC on AWS EU Central (Frankfurt)

Summary Overview **Networking & Security** Add Ons Maintenance Troubleshooting Settings Support

Connected Amazon VPC

Network
Segments
VPN
NAT
Tier-1 Gateways
Transit Connect

Security
Gateway Firewall
Distributed Firewall
Distributed IDS/IPS

Inventory
Groups
Services
Virtual Machines
Context Profiles

Tools
IPFIX
Port Mirroring

System
Identity Firewall AD
DNS
DHCP
Global Configuration
Public IPs
Direct Connect
Connected VPC

Routing Between Your SDDC and the Connected VPC

VMware Cloud on AWS adds routes to the main route table (default route table) of the Connected VPC upon creation. We dynamically update this route table to reflect route changes over time. We do not update any entries that you manually add to this route table or any other route tables.

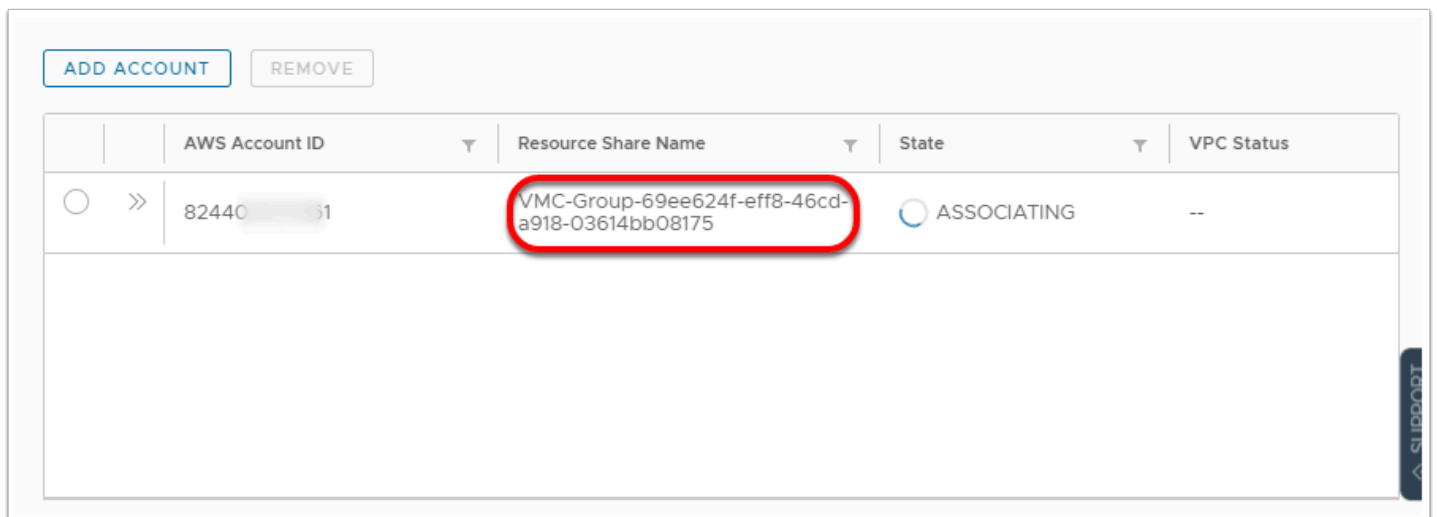
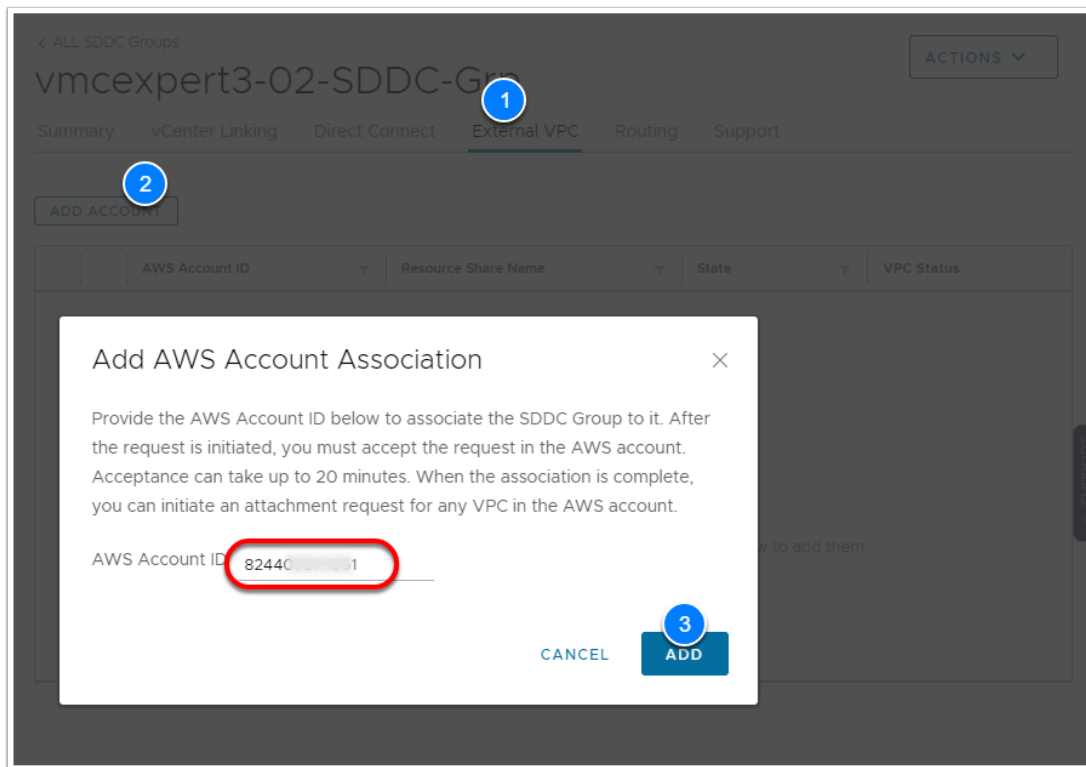
AWS Account ID	VPC ID	VPC Subnet	Active Network Interface
824407...	vpc-0f27782e03caaff62	subnet-0e6c4426aa9190597 172.102.16.0/20 eu-central-1b	eni-052d707d88bf66c48

IAM Role Names
arn:aws:iam::824407877961:role/vmware-sddc-formation-abb900f-b3c2-4d6-RemoteRole-DD5IOHH75XN
arn:aws:iam::824407877961:role/vmware-sddc-formation-abb900f-b-RemoteRoleService-1FY8ENZ24J40D

CloudFormation Stack Names
vmware-vmc

Service Access
EC2 - Enabled
S3 - Enabled | [DISABLE](#)

6. At the top left hand corner of the page, click **All SDDCs**
7. Click **SDDC Groups**
8. Click **View Details** at the bottom of your SDDC Group Tile
9. Click the **External VPC** Tab
10. Click **Add account**
11. In the Dialog, Type in/Paste in the **<AWS Account ID>** you recorder in Step 5
12. Click **ADD**
13. Record your **Resource Share Name**, You'll need it to confirm the association in AWS



Once added the State of the Account should read ASSOCIATING, we'll go to the AWS Console to approve the association

13. From your VDI desktop open a new browser tab and go to the AWS Console - <https://vmcexpert{#}.signin.aws.amazon.com/console> where {#} indicates your AWS environment (1, 2 or 3)
14. Login using the following details. Your actual credentials can be obtained from the Student lab assignment sheet or Excel workbook
 - Account ID or alias: **vmcexpert# i.e vmcexpert1, vmcexpert2 or vmcexpert3**
 - IAM user name: **VMCEXPERT#-XX**(where # is your Environment ID and XX is the number assigned to you)
 - Password: **<AWS Console PW provided By your instructor>**

15. Click Sign In

aws

Sign in as IAM user

Account ID (12 digits) or account alias

1 vmcexpert1

IAM user name

2 VMCEXP3-02

Password

3

4 Sign in

[Sign in using root user email](#)

[Forgot password?](#)

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

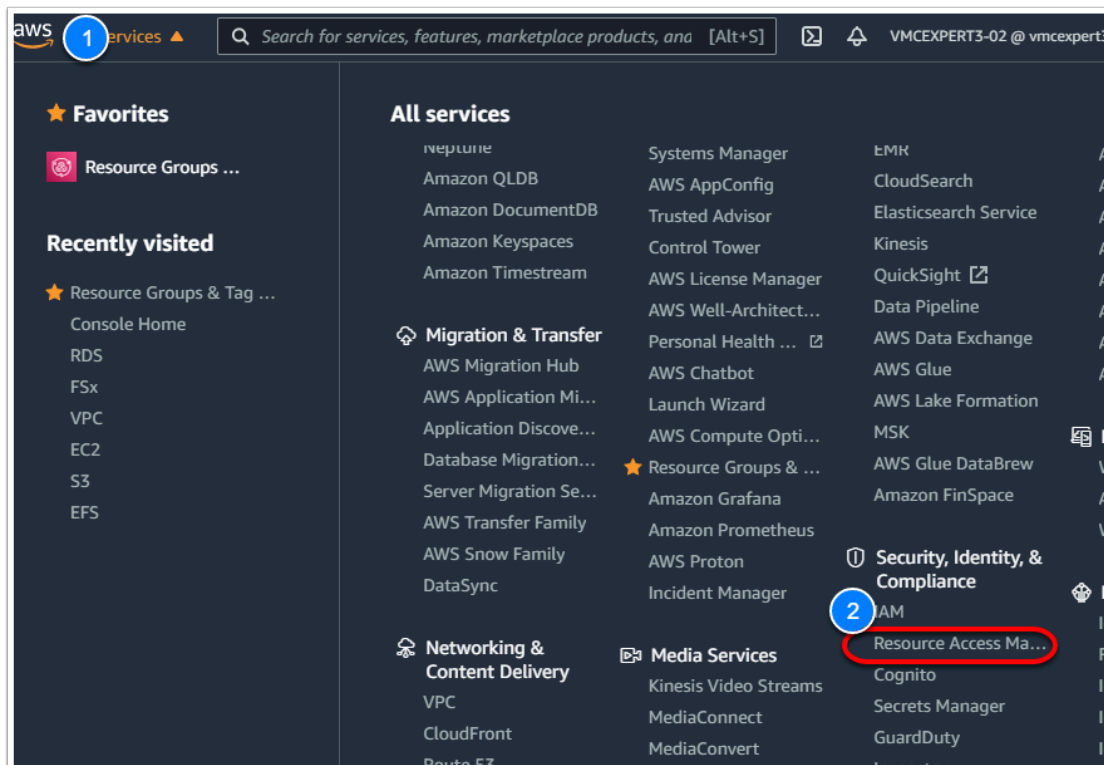
[Learn more »](#)

English

[Terms of Use](#) [Privacy Policy](#) © 1996-2021, Amazon Web Services, Inc. or its affiliates.

16. In the upper left section of the page click **Services**

17. Click **Resource Access Manager** under Security, Identity and Compliance



18. In the left pane click **Resource Shares** under Resources Shared with me

19. You should see your resource share in a **Pending** state

20. Click it
21. Click **Accept Resource Share**
22. Click **OK**

Resource Access Manager

Shared with me : Resource shares

Resource shares (1 selected)

Resource shares my account has access to

Filter by attributes or search by keyword

Name	ID	Owner	Status
VMC-Group-bfac8a0b-2eaa-477e-9581-a410a53181d6	530a6b84-3b73-4a9a-a856-2154265809f1	911691994927	Active
VMC-Group-69ee624f-eff8-46cd-a918-03614bb08175	14db3bcb-04f1-4e39-a62b-c7ebe3c227a8	911691994927	Pending

VMC-Group-69ee624f-eff8-46cd-a918-03614bb08175 (14db3bcb-04f1-4e39-a62b-c7ebe3c227a8)

Details and information relating to this resource share.

Reject resource share Accept resource share

Summary

Name	Owner	Invitation date	Status
VMC-Group-69ee624f-eff8-46cd-a918-03614bb08175	911691994927	2021/07/28	Pending
ARN	Receiver		
arn:aws:ram:eu-central-1:911691994927:resource-share/14db3bcb-04f1-4e39-a62b-c7ebe3c227a8	824407877961		

23. Go back to the browser tab for your SDDC Console. The state of the Association should now read **ASSOCIATED**
NOTE: This can take up to 5 mins to Update. You may need to refresh the page
24. Click the Support tab
25. Record the **TGW ID**, you'll need it for the next task


ADD ACCOUNT

REMOVE

	AWS Account ID	Resource Share Name	State	VPC Status
<div></div> <div>>></div>	824407877961	VMC-Group-69ee624f-eff8-46cd-a918-03614bb08175	ASSOCIATED	--

SUPPORT

[< ALL SDDC Groups](#)

ACTIONS 

vmcexpert3-02-SDDC-Grp

[Summary](#)
[vCenter Linking](#)
[Direct Connect](#)
[External VPC](#)
[Routing](#)
[Support](#)

Support Information

Group ID:

d2e4ff4b-393b-4eed-a258-6837c5905fc5

Created Date:

Wednesday, July 28, 2021 at 12:02:07 PM GMT+00:00

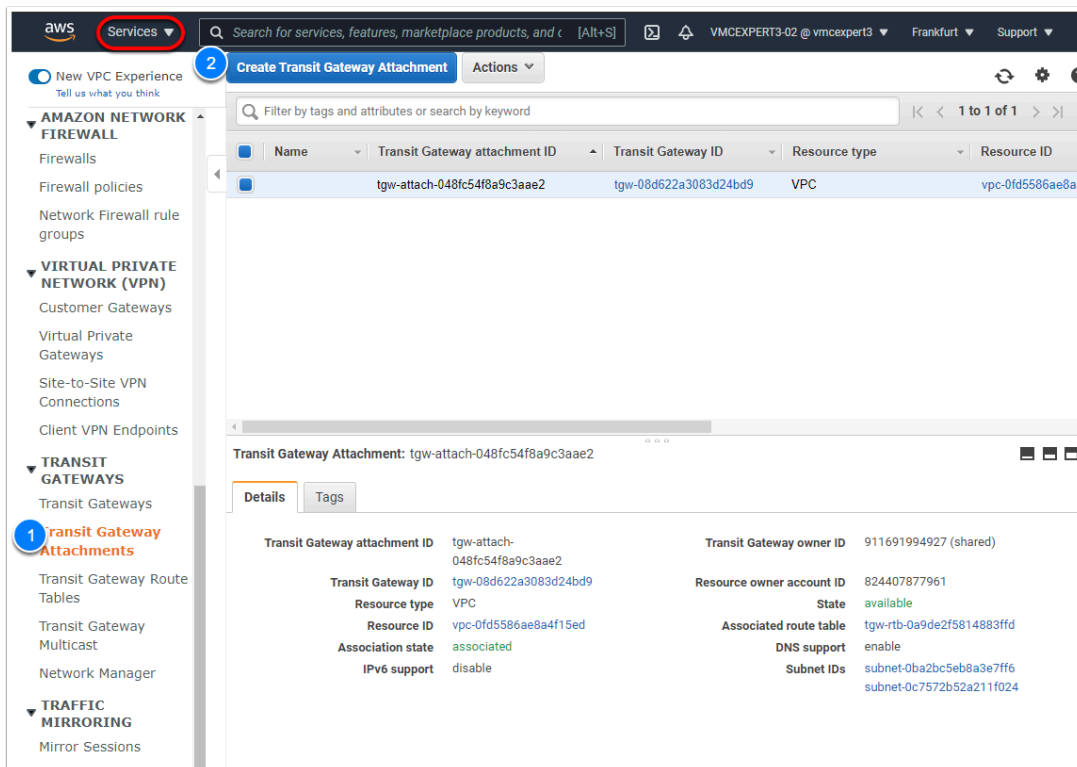
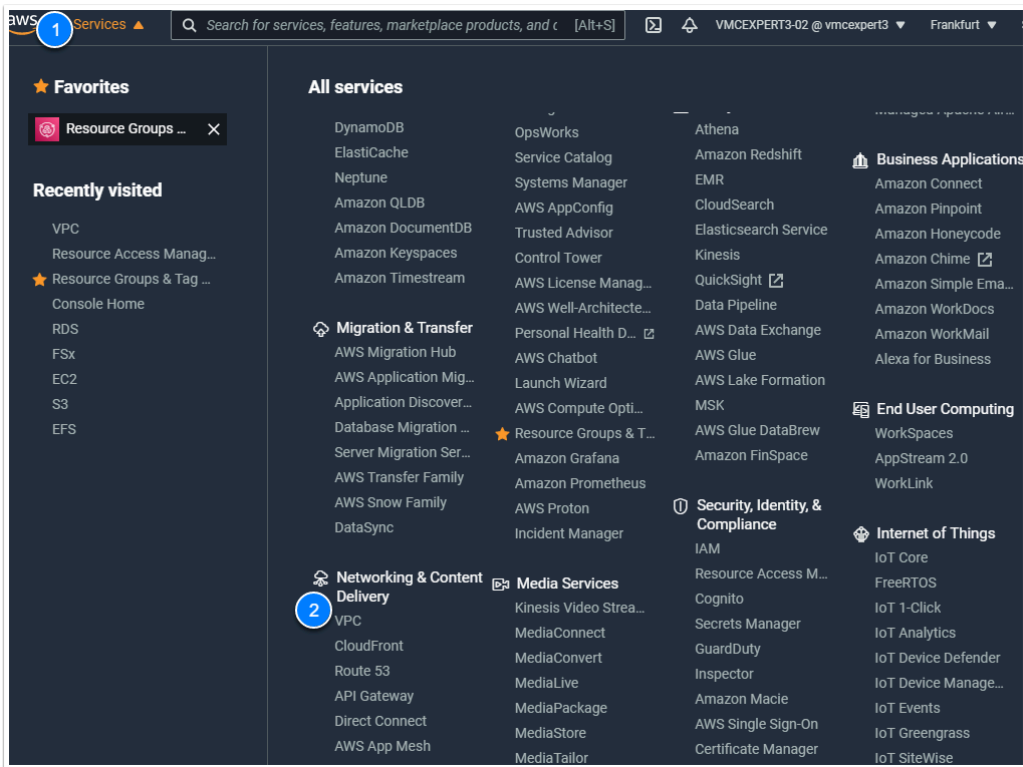
VMware VTGWs

TGW ID	Location
tgw-01c980bc228ac8b40	EU (Frankfurt)

Task 2.2 - Connect the Native VPC to the Transit Connect

With the AWS Account now associated with the SDDC group our next task is to create a transit Gateway attachment for the Native VPC. this task will be performed from the AWS Console.

1. In the AWS Console Browser tab, click **Services**, then **VPC** under Networking and Content Delivery
2. In the Left pane Click **Transit Gateway Attachments**, Under transit Gateways
3. Click the **Create Transit Gateway Attachment** Button



4. In the Create Transit Gateway Attachment page, Select **<your Transit Connect>** from the Transit Gateway ID dropdown list
- NOTE: You can Identify your transit connect by its ID. You recorded the ID in Task 2.1 step 25**

- Select **<your VPC>**. Look the the VPC Name column to identify your VPC
NOTE: your VPC will be VMCEPERT#-XX-FSx (Where # is your Environment ID and XX is your student number)
- Click **Create Attachment**
- Click **Close**

Create Transit Gateway Attachment

Select a Transit Gateway and the type of attachment you would like to create.

Transit Gateway ID*

Attachment type

Transit Gateway ID	Name tag	Description	Owner ID
tgw-01c980bc228ac8b40		TGW for region eu-central-1	911691994927
tgw-08d622a3083d24bd9		TGW for region eu-central-1	911691994927

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag

DNS support ☒ enable

IPv6 support ☐ enable

VPC ID*

* Required

Cancel **Create attachment**

VPC Attachment

Select and configure your VPC attachment.

Attachment name tag

DNS support ☒ enable

IPv6 support ☐ enable

VPC ID*

VPC ID	VPC name	CIDR block
vpc-0d2b172b7400738fb	VMCEPERT3-03-FSx	10.103.16.0/20
vpc-0fd5586ae8a4f15ed	VMCEPERT3-01-FSx	10.101.16.0/20
vpc-01c10adfc405e0c90	VMCEPERT3-08-FSx	10.108.16.0/20
vpc-017dd8c31dbf97b64	VMCEPERT3-07-FSx	10.107.16.0/20
vpc-08bda2db256077d7d	VMCEPERT3-01	172.101.0.0/16
vpc-0eed151f4d8ed9a1a	VMCEPERT3-06-FSx	10.106.16.0/20
vpc-0b5c3f20d0caf1339	VMCEPERT3-08	172.108.0.0/16

* Required

Cancel **Create attachment**

- Back on your SDDC Browser tab, Click External VPC
- Expand the AWS Account attachment by clicking the double arrow (greater-than signs)

10. Select the checkbox for the Attachment association
NOTE: The association can take up to 10 mins to Update (Show up). You may need to refresh the page, and wait for it to appear before proceeding
11. Click **Accept**
12. Wait until the Status changes from **PENDING** to **AVAILABLE** before proceeding
NOTE: This process can take as much as 5 mins

Summary vCenter Linking Direct Connect **1** Final VPC Routing Support

ADD ACCOUNT REMOVE

2 AWS Account ID
824407877961

AWS Account ID : 824407877961
Resource share name : VMC-Group-69ee624f-eff8-46cd-a918-03614bb08175

4 State : ASSOCIATED
ACCEPT REMOVE

<input checked="" type="checkbox"/>	VPC ID	VMC on AWS Region	Transit Gateway Attachment ID	Routes	Status
3 <input checked="" type="checkbox"/>	vpc-044ff9afcb1e9cce8	EU (Frankfurt)	tgw-attach-0d7cd5b9883ec8a15	ADD ROUTES	PENDING ACCEPTANCE

☒ 1

Summary vCenter Linking Direct Connect **1** Final VPC Routing Support

ADD ACCOUNT REMOVE

2 AWS Account ID
824407877961

AWS Account ID : 824407877961
Resource share name : VMC-Group-69ee624f-eff8-46cd-a918-03614bb08175

State : ASSOCIATED
ACCEPT REMOVE

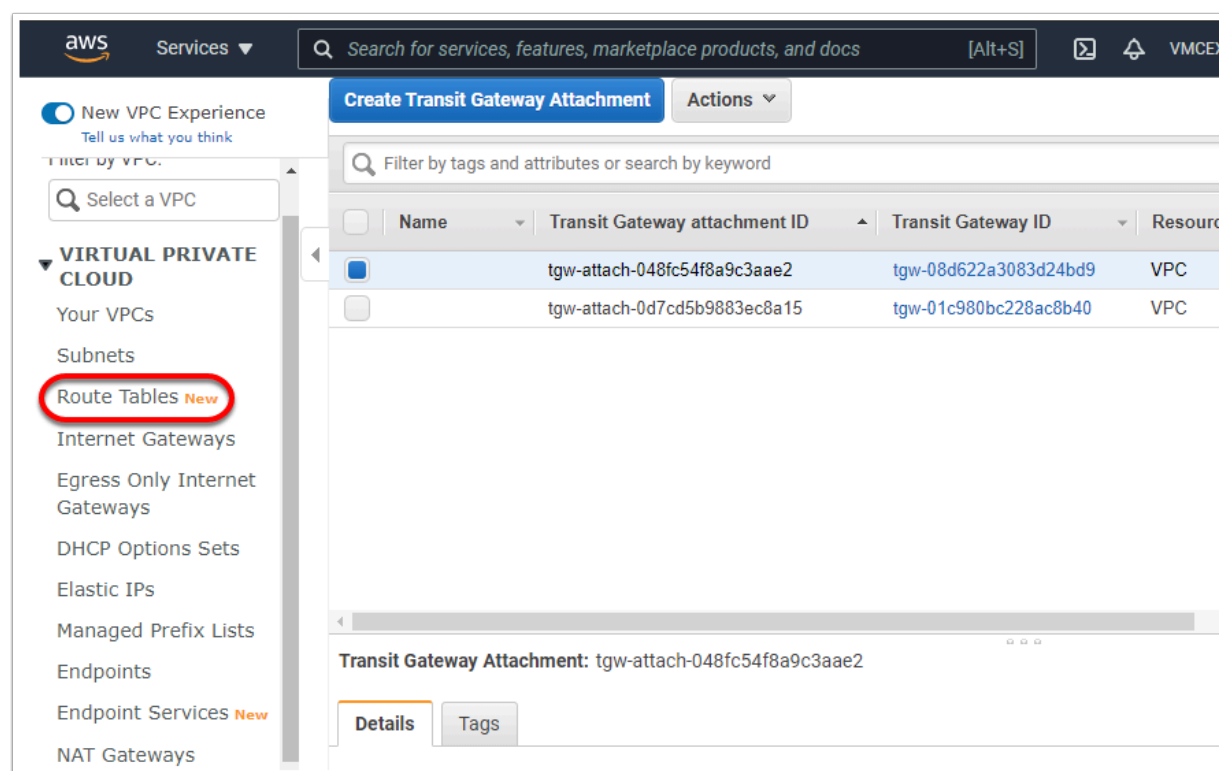
<input checked="" type="checkbox"/>	VPC ID	VMC on AWS Region	Transit Gateway Attachment ID	Routes	Status
<input checked="" type="checkbox"/>	vpc-044ff9afcb1e9cce8	EU (Frankfurt)	tgw-attach-0d7cd5b9883ec8a15	ADD ROUTES	AVAILABLE

☒ 1

Task 2.3 - Add a route to the Native VPC

With the Attachment now complete we need to update the VPC routing table to populate the VMC connected networks as reachable via the VTGW. We will accomplish this in the AWS Console for the FSx VPC (VMCEXPERT#-XX-FSx)

1. Go back to the browser tab for your AWS console
2. Click **Route Tables** in the left pane



3. In the search field type in <**your AWS account string**> to find the routing table for your FSx PC. i.e. **vmcexpert3-02**.
NOTE: Your FSx VPC route table will be named **VMCExpert#-XX-FSx-Public Route Table**
4. Select the **route table**
5. Click the **Routes** tab
6. Click **Edit Routes**

Route tables (1/3) Info

vmcexpert3-02

search: vmcexpert3-02 Clear filters

	Name	Route table ID	Explicit subnet associat...	Edge associations
<input type="checkbox"/>	-	rtb-0c7cac7dcd67b0f12	-	-
<input type="checkbox"/>	-	rtb-0a8316cabe4039f70	-	-
<input checked="" type="checkbox"/>	VMCExpert3-02-FSx Public Route Table	rtb-0abcd7d3835e34b68	2 subnets	-

rtb-0abcd7d3835e34b68 / VMCExpert3-02-FSx Public Route Table

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Edit routes

Filter routes Both

Destination	Target	Status	Propagated
10.102.16.0/20	local	Active	No
0.0.0.0/0	igw-0739d88cb74fbd59	Active	No

7. Click **Add Route**, and configure the route as follows:
 - Destination: <**The Network Segment for Desktop-Net**> i.e 10.10.1xx.0/24
 - Target: <**Your Transit Connect**>
8. Click **Save Changes**

Edit routes

Destination Target Status

10.10.102.0/24 tgw-01c980bc228ac8b40 -

Propagated

No

Remove

Add route

Cancel Preview Save changes

Updated routes for rtb-0abcd7d3835e34b68 / VMCEXP3-02-FSx Public Route Table successfully
 ▶ Details

Actions ▼

Details Info

Route table ID rtb-0abcd7d3835e34b68 VPC vpc-044ff9afcb1e9cce8 VMCEXP3-02-FSx	Main No Owner ID 824407877961	Explicit subnet associations 2 subnets	Edge associations -
--	--	---	------------------------

Routes Subnet associations Edge associations Route propagation Tags

Routes (3) Edit routes

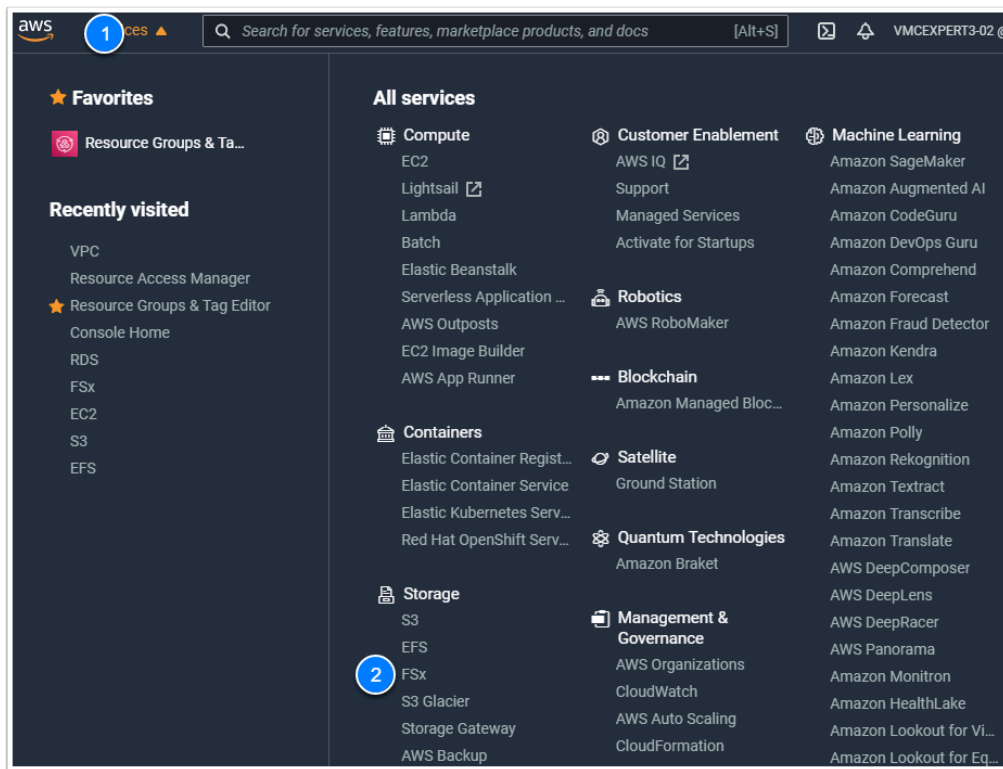
Filter routes Both < 1 > ⚙

Destination	Target	Status	Propagated
10.10.102.0/24	tgw-01c980bc228ac8b40	Active	No
10.102.16.0/20	local	Active	No
0.0.0.0/0	igw-0739d88cb74fbd59	Active	No

Task 3 - Consume a Native AWS service across the Transit Connect

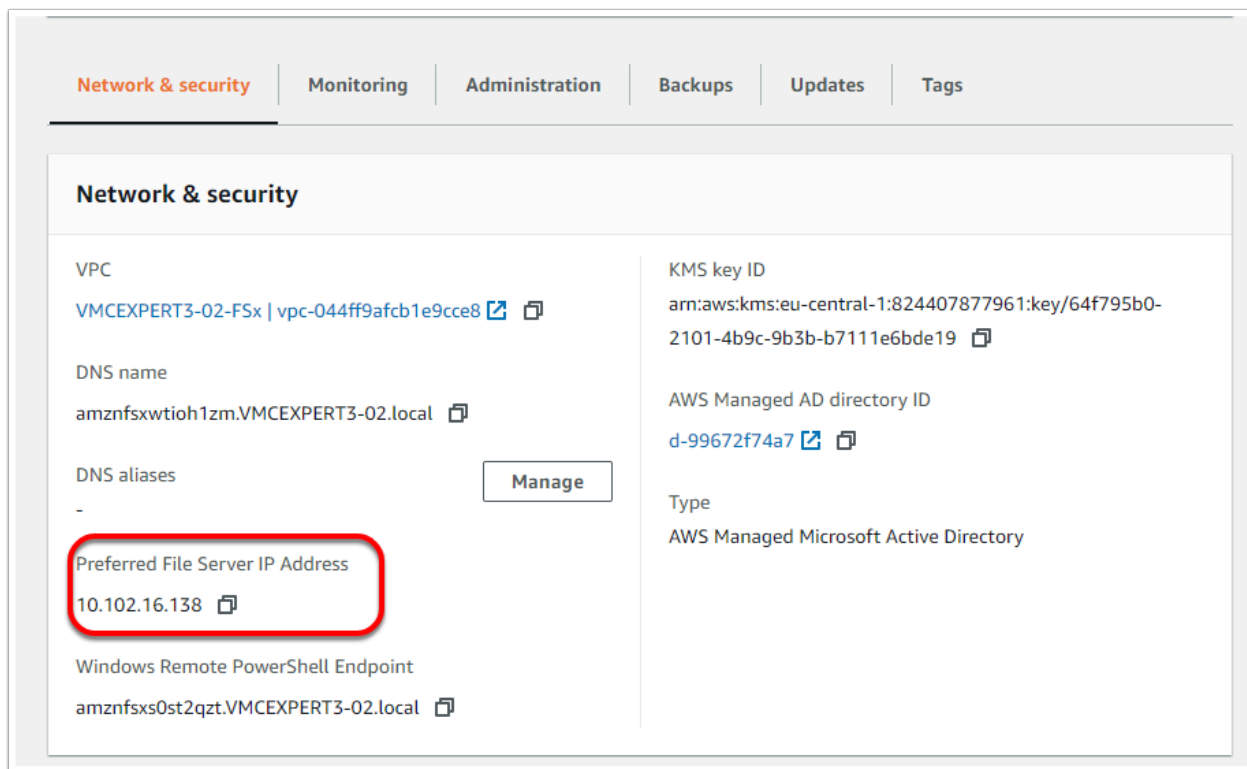
Task 3.1 - Identity the FSx Service for Consumption

1. Go to the browser tab for your AWS Console
2. In the upper left-hand section of the page click Services
3. Click FSx, under Storage



4. Locate your FSx File System Service. It should be named VMCEXP3-XX (Where # is your environment ID and XX is your student number)
5. Click on your FSx File System once located
6. Locate and record the **Preferred File Server IP Address** of the service

File system name	File system ID	File system type	Status	Deployment type	Storage type
VMCEXP3-05	fs-0067d1c52d832480b	Windows	Available	Multi-AZ	SSD
VMCEXP3-01	fs-01e392c95b7307b47	Windows	Available	Multi-AZ	SSD
VMCEXP3-04	fs-068036151c8728ea5	Windows	Available	Multi-AZ	SSD
VMCEXP3-03	fs-06b91ea55ce883a00	Windows	Available	Multi-AZ	SSD
VMCEXP3-07	fs-083f516a55bc6243d	Windows	Available	Multi-AZ	SSD
VMCEXP3-06	fs-0aca2786a355fa73e	Windows	Available	Multi-AZ	SSD
VMCEXP3-02	fs-0c04b98917a9e27ba	Windows	Available	Multi-AZ	SSD
VMCEXP3-08	fs-0d5ec627c6e4ccda5	Windows	Available	Multi-AZ	SSD



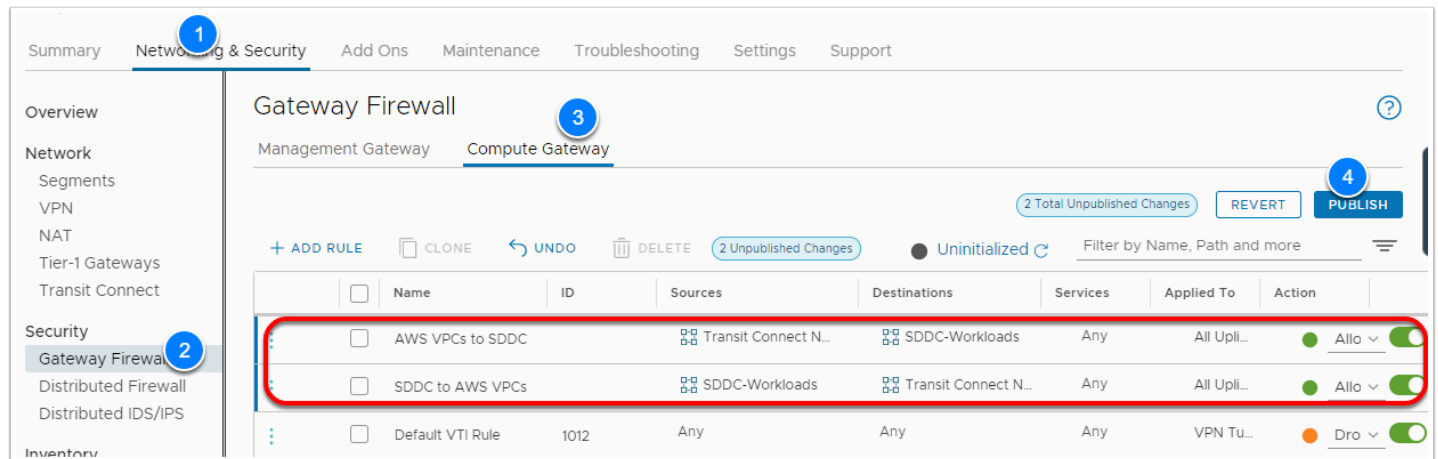
We will use this IP to mount the File System Share on our client Virtual Machine later

Task 3.2 - Configure Firewall Access from the SDDC to the Native VPC

1. In the browser tab for your VMC on AWS SDDC console, login if your previous session timed out
 - **vmcexpert#-xx@vmware-hol.com**
 - **VMware1!**
2. Click **View Details** on your SDDC tile
3. Click **Networking & Security** tab
4. Click **Gateway Firewall**
5. Click the **Compute Gateway** tab
6. Click **ADD RULE**
7. Add 2 rules and Configure them as follows:
 1. **Rule 1**
 - Name: **AWS VPCs to SDDC**
 - Source: **Transit Connect Native VPCs Prefixes**
 - Destination: **SDDC-Workloads**
 - Service: **Any**
 - Applied to: **All Uplinks**
 - Action: **Allow**
 2. Rule 2
 - Name: **SDDC to AWS VPCs**
 - Source: **SDDC-Workloads**

- Destination: **Transit Connect Native VPCs Prefixes**
- Service: **Any**
- Applied to: **All Uplinks**
- Action: **Allow**

8. Click **PUBLISH**



Task 3.3 - Mount the FSx Share on a Windows VM in the SDDC

1. Go to the Browser tab for your **SDDC vCenter**, if you no longer have the tab open, or if your session has expired, Go to the Settings tab of the SDDC to launch a tab to vCenter and/or retrieve the login credentials
2. Once logged into the SDDC vCenter, locate **Win10-Desktop** VM
3. Select it and Click **LAUNCH WEB CONSOLE**
4. In the browser tab for Win10-Desktop Console, click **Send Ctrl+Alt+Delete**
5. login as:
 - **student**
 - **VMware1!**
6. Bring up the windows command prompt or PowerShell window
7. In command prompt or PowerShell
8. Type the following

```
<p>net use z: \\<your efs preferred ip>\share</your></p>
```

Click to copy

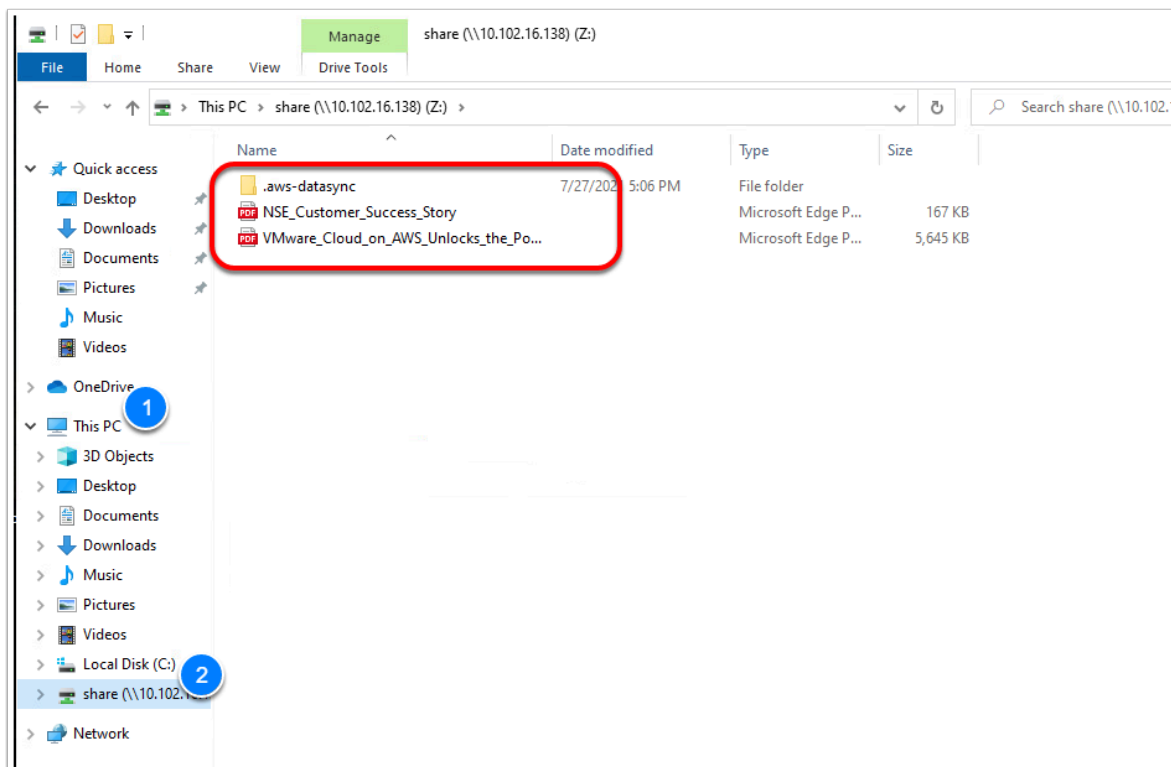
9. when prompted for user credential type the following:
 - username: **<vmcexpert#-xx>\admin** i.e. vmcexpert3-02\admin
 - Password **<Your AWS Console PWD>**

```
Command Prompt

C:\Users\student>net use z: \\10.102.16.138\share
Enter the user name for '10.102.16.138': vmcexpert3-02\admin
Enter the password for 10.102.16.138:
The command completed successfully.

C:\Users\student>
```

10. Open Windows explorer (File Explorer)
11. Click **This PC**
12. You'll see the **Z:** drive
13. Open it



Conclusion