Lab 03 - SDDC Networking & Native AWS Integration

Introduction

One of the most compelling reasons to adopt VMware Cloud on AWS is to integrate your existing systems which sit in your VMware Cloud environment, with application platforms that reside in your AWS Virtual Private Cloud (VPC) environment. The integration which VMware and AWS have created allows for these services to communicate, for free, across a private network address space for services such as EC2 instances, which connect into subnets within a native AWS VPC, or with platform services that have the ability to connect to a VPC Endpoint, such as S3 Storage.

Understanding Integration with AWS Services



As the above diagram illustrates, the VMware stack not only sits next to the AWS services but is tightly integrated with these services. This introduces a new way of thinking about how to design and leverage AWS services with your VMware SDDC. Some integrations our customers are using include:

- VMware front-end and RDS backend
- VMware back-end and EC2 front-end

- AWS Application Load Balancer (ELBv2) with VMware front-end (pointing to private IPs)
- Lambda, Simple Queueing Service (SQS), Simple Notification Service (SNS), S3, Route53, and Cognito
- AWS Lex, and Alexa with the VMware Cloud APIs

These are only a few of the integrations we've seen. Many different services that can be integrated into your environment. In this exercise, we'll be exploring integrations with both AWS Simple Storage Service (S3) and AWS Relational Database Service (RDS).

How are these integrations possible?

In addition to sitting within the AWS Infrastructure, there is an Elastic Network Interface (ENI) connecting VMware Cloud on AWS and the customer's Virtual Private Cloud (VPC), providing a high-bandwidth, low-latency connection between the VPC and the SDDC. This is where the traffic flows between the two technologies (VMware and AWS). To leverage native AWS services on your SDDCs, deploy your AWS EC2 workloads in the same availability zone to avoid cross-AZ traffic charges.

How is traffic across the ENI secured?

From the VMware side (see image below), the ENI comes into the SDDC at the Compute Gateway (NSX Edge). This means, on this end of the technology we allow and disallow traffic from the ENI with NSX Firewall rules. By default, no ENI traffic can enter the SDDC. Think of this as a security gate blocking traffic to and from AWS Services on the ENI until the rules are modified.

On the AWS Services side, Security Groups are utilized. For those who are not familiar with Security Groups, they act as a virtual firewall for different services (VPCs, Databases, EC2 Instances, etc). This should be configured to deny traffic to and from the VMware SDDC unless otherwise configured.



Note: There is a requirement in this lab to have completed all the steps in Lab 2
 Working with your SDDC.

TASKS

In this lab, you will configure service integration and consumption between the SDDC and AWS Connected VPC. We will use the web server VMs you created in the previous lab to consume services in AWS. We start by consuming an RDS database. We then have optional exercises where you'll consume other services such as ELB, & NFS

In this exercise, everything has been configured on the AWS side for you. You will however walk through how to open AWS traffic to come in and out of your VMware Cloud on AWS SDDC.

Task 1 - Create Security Groups

Before we can communicate between our SDDC and the connected VPC, we need to allow traffic through the ENI. We will start by create a security group we will use in the firewall rules to allow traffic to and from the AWS RDS.

1. In the VMware Cloud on AWS portal click the **OPEN NSX MANAGER** button



2. Click ACCESS VIA THE INTERNET to connect to NSX Manager UI

Click ACCESS VIA THE INTERNET to connect to NSX Manager via the In	iternet. <u>Learn more</u>
	CLOSE 2 ACCESS VIA THE INTERNET

- 3. Wait till page with NSX Manager will be loaded and you will see Overview dashboard.
- 4. Click on **Inventory** tab

vmw NSX			¢	?`∳	vmcexpert2-3	1@ ×
Home Networking	Security Inventory Plan & Troubleshoot	System				
Overview Alar	ms			٥	Documentation	
				GET ST	ARTED	
3	VPN Public IP: 54.149.134.153 Management Gateway VPN Public IP: 54.149.134.153 NSX, vCenter, Gateway NSX, vCenter, ESXi NSX, vCenter, ESXi 10.23112.0/22 Infrastructure Subnet: 10.23112.0/22 Infrastructure Subnet: 10.23112.0/22 Gateway Firewall Rules: 4 Groups: 3	No IPsec VPN Configured No Direct Connect Private VIFs Configured		es / External sites		

- 5. Click **Groups** in the left pane
- 6. Click Compute Groups
- 7. Click ADD GROUP
- 8. Name: PhotoAppVM
- 9. Click the **Set** link

vmw NSX						🗘 (?) - 🔆 instructor0	1@v ~
Home Networking Secu	urity Inventory Plan & Tr	ubleshoot System					
*	Groups						?
Groups 5	7 ADD GROUP						
ତ Profiles	Name		Туре 🕦	Compute Members	Where Used	Status	
	V 8 PhotoApp	им		9 Set			
	Description	Description		Tags	Max 30 allowed.		
	SAVE	CANCEL					

- 10. In the popup, Select Members Tab
- 11. From the Drop Down change the Category from **Groups** to **Virtual Machines**
- 12. Check the box next to **webserver01** and **webserver02**
- 13. Click Apply
- 14. Click Save

Set	Mer	nbe	rs PhotoAppVM	I						×
To ad	ld com	oute m	nembers to a Group, you c	an statically or dynam	nically add members to a	a group.				
Group	o Type (D (🖸 Generic 🛛 🔿 IP Addre	esses Only						
Mem	bership	o Crite	ria (00000 Members (2)	IP Addresses (0)	MAC Addresses (0)	AD Groups (0)				
Catego	° <mark>11)</mark>	Virtua	I Machines (2) ∨		Source	Tags	Filter by Na 	me, Path and m Power State	ore -	=
12			webserver01		esx-10.40.0.68		Ubuntu Linux (64- bit)	Running		
			webserver02		esx-10.40.0.68		Ubuntu Linux (64- bit)	Running		

Task 2 - Create Gateway Firewall rule

We will now create the required firewall rules to allow the PhotoAppVM access to Services running in the Connected VPC and vice versa.

- 1. If your NSX Manager UI tab is active then go to step #3. If you already closed NSX Manager tab then Select your SDDC, if you aren't currently within it, then click **View Details**
- Click the OPEN NSX MANAGER button and click ACCESS VIA THE INTERNET to connect to NSX Manager UI. Wait till page with NSX Manager will be loaded and you will see Home -Overview dashboard.
- 3. Click **Security** tab in your NSX Manager UI
- 4. Click Gateway Firewall in the left pane
- 5. Click and select Compute Gateway
- 6. Click +ADD RULE
- 7. Click on the "New Rule" Text and enter AWS Inbound
- 8. Hover over the Source field and click on the blue Edit Pencil
- 9. In the popup, Select Connected VPC Prefixes
- 10. Click Apply
- 11. Hover over the **Destination** field and click on the blue **Edit icon**
- 12. In the popup, Select **PhotoAppVM**
- 13. Click Apply
- 14. Leave Service as **Any**
- 15. Leave applied to as All Uplinks
- 16. **REPEAT STEPS: 4 13** to create an additional rule with the following changes:
 - Name: AWS Outbound

- Source: **PhotoAppVM**
- Destination: Connected VPC Prefixes
- Service: MySQL
- 17. **REPEAT STEPS: 4 13** to create a third rule with the following changes:
 - Name: Public In
 - Source: Any
 - Destination: PhotoAppVM
 - Services: HTTP
- 18. To the far right of each rule click the **GEAR**
- 19. Slide the **Slider** in the Dialog to **enable** logging
- 20. Click APPLY
- 21. Click **PUBLISH** to save and activate the rules

Note: Make sure to leave **All Uplinks** in the **Applied To** section.



Task 3 - Request a public IP address

The PhotoAppVM (webserver01) currently has a private IP address (10.10.X.X) and thus not internet routable. to allow public internet access to the VM You'll first need to request a Public IP address. After the public IP address is provisioned, you will configure NAT to direct traffic from the public IP address to the private IP address of the PhotoAppVM. You can request public IP addresses to assign to workload VMs to allow access to these VMs from the internet. VMware Cloud on AWS provisions the IP address from AWS.

As a best practice, release the public IP addresses that are not in use.

- 1. In your vCenter interface for VMware Cloud on AWS, find your **Webserver01** VM you deployed, and ensure it has been assigned an IP address as shown in the graphic.
- 2. Take note of the IP address (Record the IP in the Excel Workbook provided)



- 3. Go back to your NSX Manager UI on the **Networking** tab in order to request a Public IP address
- 4. Click **Public IPs** in the left pane
- 5. Click on **REQUEST NEW IP**
- 6. In the notes area type **PhotoAppIP**
- 7. Click SAVE
- 8. Take note of and record this Public IP address

The Public IP address will be used in the next task to setup Network Address Translation (NAT) for webserver01

vmw NSX		$\hat{\Box}$? · ·	∳- Instruc	:tor01@v ~
Home 3 Networking Sec	urity Inventory Plan & Troubleshoot System				
*	Public IPs				?
Connectivity	REQUEST NEW IP				
① Tier-1 Gateways	Dublic ID Notae				
🔄 Segments					
Network Services	<request a="" ip="" new="" public=""> 6 PhotoAppIP 7 SAVE CANCEL</request>				
⇒• NAT					
Cloud Services	Public IPs				
Direct Connect	REQUEST NEW IP				
Transit Connect	Public IP Notes				
	52.36.176.222 PhotoApplP				
IP Management					
E DNS					
Settings					No Public IPs

Task 4 - Create a NAT Rule

- 1. Click **NAT** in the left pane
- 2. Click ADD NAT RULE
- 3. Name: PhotoApp NAT
- 4. Public IP: From Task 3 (it should auto populate, but if it does not, select it)
- 5. Service: All Traffic (no change)
- 6. Internal IP: <IP address of your **Webserver01** VM you noted in task 2.1> See your Excel workbook for this IP if you've forgotten it
- 7. Logging: **YES** (Move the **Slider** to the right)
- 8. Click **SAVE**

vmw NSX		
Home Networking S	ecurity Inventory Plan & Troubleshoot System	
«	NAT	?
Connectivity	2 Internet Tier-1 Gateway	
① Tier-1 Gateways	ADD NAT RULE COLLAPSE ALL	
💼 Segments	Name Public IP Service Public Port Internal IP	Internal Port Firewall ()
Network Services	✓ ③ PhotoApp NAT ④ 52.36.176.222 ⊗ ✓ ⑤ All Traffic ⊗ ✓ Any ⑥ 10.10.1.11	Match Intern
VPN	Logging (7) (C) Yes (0) Rule Enabled	Yes
	Description	
Cloud Services		
🚳 Direct Connect	8 SAVE CANCEL	
🚯 Transit Connect		

Task 5 - View AWS RDS Instance and Security Settings

Amazon RDS makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching, and backups. It frees you to focus on your applications so you can give them the fast performance, high availability, security, and compatibility they need.

In this exercise, you will be able to integrate a VMware Cloud on AWS virtual machine to work in conjunction with a relational database running in Amazon Web Services (AWS) that has been previously set up on your behalf.



On your browser, open a new tab and go to: https://vmcexpert{#}.signin.aws.amazon.com/ console where {#} indicates your AWS environment (1, 2 or 3)

The Credentials below are from the AWS Console portion of your student lab assignment sheet

- 1. Account ID or alias: vmcexpert# i.e vmcexpert1, vmcexpert2 or vmcexpert3
- 2. IAM user name: VMCEXPERT#-XX(where # is your Environment ID and XX is the number assigned to you)
- 3. Password:

<AWS Console PW provided By your instructor>

4. Click Sign In

aws
Sign in as IAM user
Account ID (12 digits) or account alias
vmcexpert1
IAM user name
kmcexpert1-01
Password
Remember this account
Sign in
Sign in using root user email
Forgot password?

- Make sure the region selected is US West (Oregon) us-west-2 If you are using vmcexpert1 or vmcexpert2 environments or chose Europe (Frankfurt) eu-central-1, if your using vmcexpert3 or your instructor instructs you to do so.
- 6. Expand the Services drop down
- 7. Select Database
- 8. Select RDS



- 9. In the **Amazon RDS** left pane click on **Databases**
- 10. Search for your student number (i.e. 01 through 31)
- 11. Click the blue text under the **DB Identifier** column for the RDS instance that corresponds to your designated student number
- 12. Ensure that you are on the **Connectivity & Security** Tab.
- 13. Look inside the **Security subsection** at the **Public Accessibility** details. You may need to scroll down
- 14. Note the name and click on the link under VPC Security Groups

Note the RDS instance is not publicly accessible, meaning this instance can only be accessed from within AWS.

Amazon RDS $ imes$	RDS > Databases				
Dashboard	Amazon DevOps Guru is turned on, but you	u lack permissions to see the insight:	s. Request permissions from your a	ccount administrator. Learn more [2 ×
Query Editor					
Performance insights Snapshots Exports in Amazon S3 Automated backups	Consider creating a Blue/Green Deploy You may want to consider using Amazon environment for changes to production of	ment to minimize downtime durin n RDS Blue/Green Deployments and databases. RDS User Guide 🔀 Auror	g upgrades minimize your downtime during up a User Guide 🛃	igrades. A Blue/Green Deployment	provides a staging
Reserved instances Provies	Databases	Group re	esources C Modify	Actions v Restore f	rom S3 Create database
	10 Q 01		×		< 1 > ©
Subnet groups Parameter groups	DB identifier	vmc-vmcexpert1-01db			Modify Actions V
Option groups Custom engine versions	• (11) vmc-vmcexpert1-01db	Summary			
		DB Identifier vmc-vmcexpert1-01db	CPU 5.17%	Status Ø Available	Class db.t2.micro
		Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ us-west-2a
		Connectivity & security Monitoring	Logs & events Configuration M	laintenance & backups Tags	
		Endpoint & port Endpoint vmc-vmcexpert1-01db.cdwdkiqp&run.us-	Networking Availability Zone us-west-Za	Security VPC security groups VMCEXPERT1-01-RDS-inbound (sg-	
		west-2.rds.amazonaws.com Port 3306	VPC VMCEXPERT1-01 (vpc- 079feb893ebd82776) 13	Oddee7d7107895467} ⊘ Active Publicly accessible No	
			Subnet group vmcexpert1-01subnetgroup	Certificate authority Info rds-ca-2019	
			Subnets subnet-03dd8383806bd007f subnet-09a5e5a45037004b3	Certificate authority date August 22, 2024, 11:08 (UTC-06:00)	

- 15. Check the box next to your **security group** ie. VMCEXPERT#-XX-RDS-Inbound (may not match your student number).
- 16. Click on the **Inbound rules** tab in the pane below
- 17. Review the Inbound rules, and note that your PhotoAppVM should be allowed access to TCP Port 3306
- 18. Click **Outbound rules** tab
- 19. You can see **All traffic** (internal to AWS) is allowed; this includes your VMware Cloud on AWS SDDC logical networks.

Security Groups (1/1) mis	C Actions 🔻	Export security groups to CSV	Create security group
Q Filter security groups			< 1 >
search: sg-02dee7d710f8954e7 X			
Security group ID ⊽ Security group	name 🔻 VPC ID	ত Description অ	v Owner ⊽ Int
Sg-02dee7d710f8954e7 VMCEXPERT1- 5	01-RDS vpc-079feb893ebd	82776 🖸 VMCEXPERT1-01-RDS	011727134347 2 F
sg-02dee7d710f8954 VMCEX/PERT1- by Charles Outbound rules Tags sg-02der/071069546 2-MCEX/PERT1-01-805 Inbound betwin Weinstein 2-MCEX/PERT1-01-805 Inbound Details Inbound rules Tags			
Inbound rules (2)		C Manage tags Edit Inbound rules	
Q. Fitter security group rules		< 1 > @	
Q. Filter uscurity group rules IP version V Type V Name 17 Security group rule IP version V Type V uscutture 19 V V V V V	Protocol V Port range		
Q. There serving yange notes Name 10 yep-ctsde/TraitedSt91s PH yep-ctsde/TraitedSt91s PH w100, Juners w100, Juners w100, Juners	Protocol V Port range TCP 3306 TCP 3306	 \$ource \$ource 0 Escription 10.10.0/16 - 67.198.12.121/32 	
A There security group note Age of the distance of th	Protocol V Port range TCP 3366 TCP 3306		
C Thir sound yang has Sound y group hile. V Sound y group	Protocol V Port range TCP 3306 TCP 3306		G Managa taga Edit curbeund r
Alter sounds graap Alle Processing graap Alle Processing graap Alle Sounds graap Alle Processing graap Alle	Protocol V Port-range TCP 3306 TCP 3306		G Minage tags fill to the under
Atter sound y page Alle Tor sound y prog Alle Tor sound y prog Alle South y prog Alle Tor sound y pro	Protocol V Port range TOY 3300 TOY 3306		G Manage tagi Edit outbound n < 1 > v Description v

• Note: VMware Cloud on AWS establishes routing in the default VPC Security Group, RDS can leverage this or create its own

Task 6 - View the AWS RDS ENI Settings

AWS Relational Database Service (RDS), also creates its own Elastic Network Interface (ENI) for access which is separate from the ENI created by VMware Cloud on AWS.

- 1. Click on the Services drop down to go back to the Main Console
- 2. Click on **Compute**
- 3. Click on **EC2**



All Student environments belong to the same AWS account, therefore, hundreds of ENI's may exist. We will search for RDS to trim the results.

- 4. Under **Network & Security** in the left panel click on **Network Interfaces.** (you may have to scroll down)
- 5. Type **RDS** in the search area and press Enter to add a filter
- 6. Expand the Security Group name column to see the names
- 7. Find your **VMCEXPERT#-XX-RDS-Inbound** security group corresponding to your student number and check the box on the left (Don't click on the blue link)
- 8. Once selected, look in the details pane below to find the **Private IPv4 address.** (you may have to scroll down)
- 9. Copy this address to your notes for the next step

aws Services Q Search	[Option+5]		∑
Spot Requests Savings Plans Reserved Instances Dedicated Hosts	Network interfaces (1/2) Info Q. RDS S X Clear filters	×	C Actions
Scheduled Instances Capacity Reservations	■ Name ▼ Network interface ID ▼ Subnet ID □ - eni-045a29fc865d96b1c subnet-03dd838380 ☑ - eni-05eb2b13050d74898 subnet-00bf274057	♥ VPC ID ♥ Availability Zone ♥ S i6bd007f [2] vpc-079feb893ebd82776 [2] us-west-2a N 8180e68 [2] vpc-0e7548418f524a9bb [2] us-west-2a N	Security group names VINCEXPERT 1-01-RDS-Inbound VINCEXPERT 1-02-RDS-Inbound
AMis AMi Catalog • Elastic Block Store Volumes Snapshots Lifecycle Manager			
Network & Security Security Groups Elastic IPs Placement Groups Key Pairs	Network interface: eni-05eb2b13050d74898	=	True
 ✓ Load Balancing Load Balancers Target Groups 	Private IPv4 address D 172.202.0.238 Public IPv4 address -	Private IPv4 DNS D Ip-172-202-0-238.us-west-2.compute.Internal Public IPv4 DNS -	Elastic Fabric Adapter False IPv6 addresses -
 Auto Scaling Launch Configurations Auto Scaling Groups 	Secondary private IPv4 addresses - MAC address 1 02:2c:e4:b1:c1:cd 2 Instance details	Association ID - IPv4 Prefix Delegation -	Elastic IP address owner - IPv6 Prefix Delegation -

Task 7 - Configure & Test the PhotoApp against the AWS

You will now access the PhotoApp and update it's Database Connection (DSN - Data Source Name) by pointing it to the RDS instance. Once this is done you'll test the app by uploading some photos into the gallery.

- 1. Click the VMC on AWS browser Tab and Click the Open vCenter button
- 2. Click Show Credentials
- 3. Copy the **password** and click **Open vCenter**
- 4. Log into vCenter as:
 - Username: Cloudadmin@vmc.local
 - Password: {Your_Saved_CloudAdmin_Password_From_Step_3}
- 5. Click on **webserver01** in the Inventory on the left (you may have to expand the inventory)
- 6. Click on Launch Web Console
- 7. In the **webserver01** browser tab, log into the Virtual Machine as:
 - Login: root
 - Password: VMware1!

vSphere Client Q Search in all environment	ents			
< ጠ		D 🗳 🚭 😂	ACTIONS	
vcenter.sddc-52-38-206-216.vmwarevmc.com	Summary Monitor Contig	ire Permissions	Datastores Ne	etworks Snapshots
 ✓ ■ SDDC-Datacenter ✓ ■ Cluster-1 	Guest OS	III Virtual Ma	achine Details	ACTIONS ~
10.201.2.4 Compute-ResourcePool		-	Power Status	Powered On
5 🗟 webserver01	$ \begin{array}{c} \log (2n+2) & = 0 \\ \log (2n+2) & = 0 $		Guest OS	👌 Ubuntu Linux (64-bit)
ট webserver02 聞 Win10-Desktop	Control of a second		VMware Tools	Running, version:11360 (Guest Managed)
> @ Mgmt-ResourcePool	41 Fight of the first first of the started of the start is a start of the start		DNS Name (1)	webserver01
	The second secon		IP Addresses (2)	10.10.1.12 fe80::250:56ff:feb2:22de
	LAUNCH REMOTE CONSOLE		Encryption	Not encrypted
C	6 LAUNCH WEB CONSOLE		실 🦷	
	VM Hardware			II PCI Devices
	200	U(s) 91 MHz used		
	198	1 GB memory active		
Ubuntu 20.04.3 LTS webs	server01 tty1			
Hint: Num Lock on				(i) No PCI devices
▶ R (7) webserver01 login: root Password: Welcome to Ubuntu 20.04	4.3 LTS (GNU/Linux 5.4.	0–131–generic	×86_64)	

We will now modify the Lychee environmental file. This file will be used later to connect to the RDS database and configure the required database tables

7. In the **webserver01** Console, navigate to the Lychee application directory make a copy of the .env file and open it in an editor by typing the following commands

```
cd /var/www/html/Lychee
cp .env .env_orig
nano .env
```

Click to copy

root@webserver01:~# cd /var/www/html/Lychee
root@webserver01:/var/www/html/Lychee# cp .env .env_orig
root@webserver01:/var/www/html/Lychee# nano .env

- 9. With the environment file opened, modify the following values:
 - App_URL: {Replace_the_IP_With_the IP_address_of your_WebServer01}
 - DB_HOST: {Replace_the_IP_with_the_IP_address_of_the_RDS_DB} NOTE: This IP was recorded in Task 6, Step 9
 - DB_PASSWORD: {AWS_Console_Password_Provided_By_your_Instructor}

The DB Password is the same one you used to log in to the AWS Console in Task 5



- 10. Press CTRL+O, then Enter to save the changes
- 11. Press **CTRL+X** to close the file

We will now run the configuration wizard, to confirm the configuration values, link the application to the RDS Database and create the necessary database tables

- 12. In a new browser tab, type/paste in the Public IP Address you requested in <u>Task 3 Step 6</u> and used for your NAT rule in <u>Task 4</u>
- 13. In the Lychee Installer Wizard, Click Next

Lychee-installer	
13 Red P	

- 14. Click **Next** on the requirements page
- 15. Click **Next** on the Permissions page
- 16. Review the values in the Environment page to confirm the values you entered in **step 9** are correct (you may have to scroll to see all the values)
- 17. Click Install (An error message is expected, as we are not migrating an old database.)

A If any of the values are incorrect return to Steps 8 through 11 to correct the erroneous values and repeat steps 12 onward

Lychee-installer	
Lychee does not create the database. Annually create your database and then enter the sql details bellow. I - Manually create your database and then enter the sql details bellow. I - If you are migrating from the v3, copy your pictures from version3/uploads/ to version4/public/uploads/. Set the form below to reflect your desired confinuation.	
For more details of how those values are used, look in the "config" folder. APP_INARE-Lychee APP_INARE-Cycles	
APP_URV-base64/salN+e8tpFEpHypeTuEDuUkVeLUASR4UGRObgOk2A8= APP_URV-brow/r001010.1.12 # enable or disable debug bar. By default it is disabled. DEBUGRAR #MARLED-Max	# DB_CONMECTION can be safet, mysal or pgod. For safet the other entries are # not required, but an existing angleta distatease may be specified if desired, in # this case, please use an absolute path. DB_DATABASE may be omitted but should # molt be left blank. DB_CONMECTIONLessed
иезинаниезаниельныезикествееранельныезикествееранеельныезикествееранеельныезикествееранеельные и MPORTANT: To migrate from Lychee v3 you "MUS": use the same MySQL/MariaD8 е и вонного ла v3. е и вонного ла v3.	DB_INSTAIN 12_2011110 DB_INTERSE
II Table prefix (e.g. lychee_) of a Lychee v3 instance for migration. #DB_OLD_LVCHEE_PREFIX= III DB_OCNVECTION can be solite, mysol or pgrod. For solite the other entries are	
R not required, but an existing softed dislabase may be specified if desired. In	
✓ Field 8	

VMware Cloud - VM 🗙 🗗 vSphere - w	ebserve 🗙 🕲 webserver01	🗙 🔋 🔋 Network interface d	Error	×	÷	×	-	1	×
← → C ▲ Not secure 44.231.1	165.18/install/migrate				Q	Ŀ	☆		:
_									
This is an expect	ed error								
	<u> </u>								
500	HttpExceptio	on							
	file_put_contents(/var/www	w/html/Lychee/.env): Failed to	o open stream: Perm	ission o	lenied				

Now that we have Lychee configured, the first time we connect it will ask us to create an account.

- 18. From your smartphone, tablet or In a new browser window type/paste in the Public IP Address of your webserver01. This is the IP requested in <u>Task 3 Step 8</u>
- 19. Create an Application admin account by entering the following:
 - New Username: admin
 - New Password: {AWS_Console_Password_Provided_By_your_Instructor}
 - Confirm Password:{AWS_Console_Password_Provided_By_your_Instructor}
- 20. Click **Create Login**

🗧 VMware Cloud - VN: 🗙 🛛 🔁 vSphere - webserve: 🗙 🛛 🗞 webserver01 🛛 🗙 🛛 😰 Network interface : 🗴 💽 Lychee v4 – Albums 🗴	+		~	-	C	3	×
← → C ▲ Not sec 18 44.231.165.18	07	Q	Ê	☆			:
Q Albums							÷
Smart albums							
Unsorted Public Enter a username and password for your installation:							
admin							
19)							
20 Create Login							
ALE MADES ON THIS WEBSITE ARE SUBJECT TO COMPILICITIES JOINT BATTA 6 2010							

21. In the **webserver01** VM Console Browser tab, Type the following command

cd /var/www/html/Lychee/public/uploads/thumb
ls

Click to copy



- Next we will upload some images and you'll notice changes to the file system. As images are stored a directory and thumbnail for each image is created.
- 22. In the Lychee application browser window, click the **Public** folder
- 23. In the upper right-hand corner, Click the "+" icon
- 24. Click **Upload Photo**, and upload a few images

← → C ▲ Not secure 44.231.165.18/#	
¢	Albums
Smart albums	CO CO Recent

25. In the webserver01 VM Console Browser tab, Type the following command to confirm the files were stored on the local filesystem

ls -l

Click to copy

root@webserver01:/var/www/html/Lychee/public/uploads/thumb# ls -1 total 12 drwxr–xr–x 3 www–data www–data 4096 Nov 5 07:25 drwxr–xr–x 3 www–data www–data 4096 Nov 5 07:25 drwxr–xr–x 3 www–data www–data 4096 Nov 5 07:25 0 Oct 25 12:28 index.html -rwxrwxrwx 1 root root root@webserver01:/var/www/html/Lychee/public/uploads/thumb# _

Congratulations, you have successfully logged in to the photo app, configured it to use the AWS RDS Database running in the Connected VPC and uploaded some images.

NOTE: The RDS MySQL DB is not used to store the photos. All photos are stored on the VMs local file system. The RDS stores all metadata about uploaded photos. Such as:

- Folder location
- whether or not the image was tagged as a favorite
- Public vs Private Photo
- etc..

This configuration is great but would prove problematic when the need arises to scale the application. In addition to using a centralize DB for metadata, we may want to store the images in a central repository as opposed to local storage. In the Additional (Optional) tasks you'll see how you can use an Amazon EFS and ALB to scale the application.

Conclusion

In summary, the front end (web server) is running in VMware Cloud on AWS as a VM, the back end which is a MySQL database is running in AWS Relational Database Service (RDS) and communicating through the Elastic Network Interface (ENI) that gets established upon the creation of the SDDC.

You have completed the required AWS Integration Lab.

ADDITIONAL LABS

VMware Cloud on AWS enables you to have a hybrid cloud platform by running your VMware workloads in the cloud while having seamless connectivity to your AWS native services.

The integration which VMware and AWS have created allows for these services to communicate, for free, across a private network address space for services such as EC2 instances, which connect into subnets within a native AWS VPC, or with platform services which have the ability to connect to a VPC Endpoint, such as S3 Storage.

In these optional lab exercises we will build on what we learned from the previous lab tasks by configuring integration with other Native AWS Services such as:

- Amazon Elastic File System (EFS)
- Elastic Load Balancing (ELB)



() When you deploy an SDDC on VMware Cloud on AWS, it is created within an AWS account and VPC dedicated to your organization and managed by VMware. You must also connect the SDDC to an AWS account belonging to you, referred to as the customer AWS account. This connection allows your VMC SDDC to access AWS services belonging to your AWS VPC account.

Additional Lab 1 - Consuming EFS Storage in VMC on AWS

Although the VMware Cloud on AWS SDDC Provides a multi-TB datastore for storing Virtual Machines and supporting files, there may be specific criteria of application data that you want running on your NVMe drives, and other data that is classified as 'lower tier'. If that is the case, one of the options you have with VMware Cloud on AWS is to leverage Amazon

Elastic File System (EFS) for additional data. You can think of EFS as a very simple and easy to use Network File Share. A single EFS can be added to multiple VMs if you choose to do so, or to single VM.

Amazon supports this for Linux operating systems only at this time.

A Prerequisites:

- Lab 2, All Tasks
- Lab 3, All Tasks

Task 1 - Configure VMC on AWS Gateway Firewall Rules

Because all traffic over the ENI is denied by default, you need modify the gateway firewall to allow the required traffic to flow uninterrupted. For this reason we will modify the "**AWS Outbound**" rule on the Compute Gateway to allow access to EFS over the ENI.

- 1. If your NSX Manager UI tab is active then go to step #3. If you already closed NSX Manager tab then Select your SDDC, if you aren't currently within it, then click **View Details**
- Click the OPEN NSX MANAGER button and click ACCESS VIA THE INTERNET to connect to NSX Manager UI. Wait till page with NSX Manager will be loaded and you will see Home -Overview dashboard.
- 3. In the NSX Manager UI interface click the Security tab
- 4. Click Gateway Firewall
- 5. Click Compute Gateway
- 6. Hover over the Services field of the "AWS Outbound" Rule and Click the Edit (Pencil Icon)
- 7. In the Search field of the Set Services Dialog Type **NFS** & Press Enter
- 8. Select NFS(TCP) & NFS(UDP)
- 9. Click Apply
- 10. Click Publish

vmw NSX										۵	⊘ ∽ 🔆 Instructor01@v
Home Networking 3 Sec											
Distributed Firewall Over the second se	Gate Mana	eway Firewall gement Gateway (S) Compute	e Gateway Tier-1 Ga								
🔣 Gateway Firewall 😏										1 Total Unpublished	Change REVER 10 PUBLISH
IDS/IPS				1 Unpublished Change					Gateway F	irewall Status 🔴 Success 😁 🛛 Filter by	
		Public In		2025	Any	22 PhotoAppVM		Онтр	All Uplinks	Allow 🗸	🔍 🖗 🖂
		AWS Outbound		2026	Po PhotoAppVM	DO Connected VPC Prefixes	6	MySQL	All Uplinks	e Allow ~	C 0 2
								O NFS (TCP)			
		Set Services							All Uplinks	Allow ~	
		#Total Selected							VPN Tunnel Interface	Orop 🗸	C @ 2
										Orop	
		🗹 😲 > 🔿 🗅		UDP (Source: Any Destination							
		2 C REFRESH									
		Show Only Selected									
						CANCEL					

()									
Gate	way F	irewall							
Manag		ateway Compute Gateway							
									REVERT PUBLISH
+ AD							Gateway Firewall Status 🔴		
		Name		Sources	Destinations	Services	Applied To	Action	
:		Public In	2025		28 PhotoAppVM	Онттр	All Uplinks	Allow 🗸	🔍 🕸 🔍
:		AWS Outbound	2026	Sa PhotoAppVM	Connected VPC Prefixes	MySQL NFS (TCP) NFS (UDP)	All Uplinks	Allow ~	C @ 2
:		AWS Inbound	2027	Pa Connected VPC Prefixes	器 PhotoAppVM		All Uplinks		🔍 🕲 📿

Task 2 - Review the EFS Settings in AWS

We will now access the AWS Console to confirm the existence of a pre-deployed EFS. We'll also need to identify the IP address of the EFS, as we'll need to to create the mount in your Virtual Machine.

- 1. Log into the AWS console using the AWS console link and credentials in the student lab assignments worksheet.
- 2. Confirm you are administering services in the **Oregon** Region (top right corner drop down)
- 3. If not, Click the drop-down and select **US West (Oregon) us-west-2** (If you are using vmcexpert1 or vmcexpert2 environment)

select Europe (Frankfurt) eu-central-1 (if you are using vmcexpert3)

- 4. Click the **Services** drop down
- 5. Select Storage
- 6. Select **EFS**

Services Q Search	[Option+S]				D A	Oregon •	VMCEXPERT1-01	@ vmcexpert1 🔻
🖘 AR & VR					C	2 ctions ▼	Create network	k interface
AWS Cost Management		Storage X		<u> </u>		2	1 > @	
Blockchain								
Business Applications	AWS Backup							
Compute	AWS Backup centrally manages and automates backups across AWS services			Availability Zone 🛛 🗢	Security group names	⊽ Secur	ity group IDs 🛛 🔻 🛛	Interface Type
🖮 Containers			48418f524a9bb 🗹	us-west-2a	VMCEXPERT1-02-RDS-Inbound	sg-03	0b569a57ba55	Elastic network
8 Customer Enablement	6 Managed File Storage for EC2		eb893ebd82776 🛂	us-west-2a	VMCEXPERT1-01-RDS-Inbound	sg-02	dee7d710f895	Elastic network
Database	—							
🔀 Developer Tools	AWS Elastic Disaster Recovery Scalable, cost-effective application recovery to AWS							
👜 End User Computing								
🔯 Front-end Web & Mobile	FSx Fully managed third-party file systems optimized for a variety of workloads							
🕫 Game Development								
Internet of Things	S3 Scalable Storage in the Cloud							
Machine Learning								Θ×
Management & Governance	S3 Glacier							
🕞 Media Services	Archive Storage in the Cloud							
Ø Migration & Transfer	Storage Gateway							
💮 Networking & Content	Hybrid Storage Integration				Elactic Eabric Adapter			
Delivery			est-2.compute.internal		False			
Quantum Technologies					IPv6 addresses			
💩 Robotics								
🦪 Satellite					Elastic IP address owner			
🗍 Security, Identity, &								
Compliance					IPv6 Prefix Delegation			
🖀 Storage								
	Review Q. Search A & X N All System A WS Cost Management Business Applications Bosiness Applications Containers Containers Costomer Enablement Database Developer Tools End User Computing Front-end Web & Mobile Game Development Machine Learning Machine Learning Management & Governance Media Services Migration & Transfer Networking & Content Delivery Quantum Technologies Satellite Security, identity, & Compliance Sources Sources Satellite Storage Storage	Earlies Q. Search (Option+S) A ka VR MVS Cost Management Storage MARS Cost Management Business Applications AWS Backup centrally manages and automates backups across AWS services More Contraines Contraines Storage Customer Enablement EFS EFS Developer Tools Easth-effective application recovery to AWS End User Computing FSX Front-end Web & Mobile FSX Game Development S3 Game Development S3 Management & Governance S3 Matagement & Governance S3 Glacier Migration & Transfer Storage Gateway Mybrid Storage in the Cloud Storage Gateway Mybrid Storage in the Cloud Storage Gateway Mybrid Storage in the Cloud Storage Storage in the Cloud	Events Q. Sarch (Option-S) A ka VR AVS Cost Management MSC Cost Management Business Applications Storage Storage Compute AWS Backgue crassly manages and automates backups across AWS services Compute Compute Containers Customer Enablement Database Developer Tools End User Computing Ffors-end Web & Mobile Marageed files Storage for KC2 Game Development Management & Governance Mathine Learning Management & Governance Storage Storage in the Cloud Migration & Transfer Networking & Content Delivers Networking & Content Delivers Storage Cateway Medatics Storage Storage in the Cloud Storage Storage in the Cloud Storage Gateway Medatics Storage Storage in the Cloud Storage Internet Storage in the Cloud Storage Storage Internet Storage in the Cloud Storage Storage Internet Storage	Earlier Q. Souch [Option+S] At & VR AvXS Cost Management X MXS Cost Management Budiness Applications XXS Backup MXS Cost Management AWS Backup centrally manages and automates backups across AWS services * Compute AWS Backup * * Compute AWS Backup centrally manages and automates backups across AWS services * * Containers Customer Enablement *	iteres Q. sarch (Option-S) AWS cost Management Business Subplications AWS Backup Compute Concurse Construers Construers Costomer Enablement Imagement & Computing FSx Fort-end Web & Mobile Fort-end Web & Mobile Management & Governance Statistic Storage in the Cloud Management & Governance Management & Governance Management & Governance Management & Governance Statistic Storage in the Cloud Management & Governance Statistic Storage Statistic Storage in the Cloud Management & Governance Statistic Storage Statistic Storage in the Cloud Management & Governance Statistic Computing Gauta Beeveloping Gauta Developing Gauta Developing Must Storage Statistic Storage in the Cloud Ministic Learning Statistic Computer Management & Governance Statistic Computer Quantum Technologies A Robotics Statistic Computer Statistic Computer Statistic Computer <td< th=""><th>Extra C Containers Max Sock Managament Storage Max Sock Managament Max Sock Managament Containers Max Sock Managament Containers Starage Max Sock Managament Max Sock Managament Containers Starage Max Sock Managament Starage In the Cond Max Sock Managament & Sovemance Starage In the Cond Max Sock Managament & Sovemance Starage In the Cond Max Mark & Storage In the Cond Starage In the Cond Max Sock Sortext Storage Soctext Max Sock Sortext Storage In the Cond Max Sock Sortext Storage Soctext Max Sortext Storage In the Cond Max Sortext Storage Sortext Max Sortext Storage In the Cond Max Sortext Storage Sortext Max Sortext Storage Sortext Max Sortext Storage Sortext Max Sortext Storage Sortext</th><th>intermet intermet <td< th=""><th> </th></td<></th></td<>	Extra C Containers Max Sock Managament Storage Max Sock Managament Max Sock Managament Containers Max Sock Managament Containers Starage Max Sock Managament Max Sock Managament Containers Starage Max Sock Managament Starage In the Cond Max Sock Managament & Sovemance Starage In the Cond Max Sock Managament & Sovemance Starage In the Cond Max Mark & Storage In the Cond Starage In the Cond Max Sock Sortext Storage Soctext Max Sock Sortext Storage In the Cond Max Sock Sortext Storage Soctext Max Sortext Storage In the Cond Max Sortext Storage Sortext Max Sortext Storage In the Cond Max Sortext Storage Sortext Max Sortext Storage Sortext Max Sortext Storage Sortext Max Sortext Storage Sortext	intermet intermet <td< th=""><th> </th></td<>	

- 7. In the list of file systems find your EFS **(VMCExpert#-xx**, where **#** is the Environment ID, and xx is your student number)
- 8. Click <your EFS Instance> vmcexpert#-xx text to view its details

Amazo	n EFS										
Fil	e systems (2)								C View		Create file system
C	1-01				×	1 file system(s) match filter					< 1 > 🐵
	Name	♥ File system ID	Encrypted	Total size ⊽	Size in Standard / One Zone	Size in Standard-IA / ♥ One Zone-IA ♥	Provisioned Throughput (MiB/s) ⊽	File system state 🛛 🕈	Creation time 🔻	Availability Zone	
0		fs- 0485c81e145899 dc0		6.00 KIB	6.00 KIB	0 Bytes			Fri, 24 Feb 2023 07:02:31 GMT	Standard	

9. Click the **Network** tab

10. Record the IP address of your EFS (e.g. 172.120.11.73)

You will need this IP to mount the share in your Webserver01 VM

Amazon EFS	
VMCEXPERT1-01 (fs-0485c81e145899dc0)	Delete Attach
General	Edit
Performance mode General Purpose Throughput mode Bursting Lifecycle management Transition into IA: 30 day(s) since last access Transition out of IA: None Availability zone Standard	Automatic backups ⓒ Disabled Encrypted 664c34fe-fb1e-4ff9-acc4-41807d7914cc (aws/elasticfilesystem) File system state ⓒ Available DNS name ⓓ fs-0485c81e145899dc0.efs.us-west-2.amazonaws.com
Metered size Monitoring Tags File system policy Access points Network Replic	ation
Network	C Manage S
Availability zone 🔺 Mount target ID 🗢 Subnet ID 🗢 Mount target stat	te ⊽ IP address ⊽ Network interface ID ⊽ Security groups ⊽
us-west-2a fsmt-03684c4dc277a6335 03dd83883806bd00	172.201.11.73 eni-01bbde98cb494cedb sg-00ecd85f2af124413 (VMCEXPERT1-01-EF5-SG)
n	

Task 3 - Mount an EFS share in a VM running in VMC on AWS

- 1. If the browser tab to the SDDC vCenter is still open navigate to it. If not Open a new Tab and log onto the VMC SDDC vCenter.
- 2. Select webserver01
- 3. Click LAUNCH WEB CONSOLE
- 4. In the browser tab for **webserver01**
- 5. If needed, Log in as
 - 1. login: root
 - 2. password: VMware1!
 - NOTE: You can access the vCenter Information and login details from the settings tab of the VMC on AWS Console

	ents			
()	webserver01 Summary Monitor	▷ 🗖 🗗 🏶 🚳 : Configure Permissions	ACTIONS Datastores Ne	etworks Snapshots
Veenter.stude-32-33-208-216.vmwarevmc.com SDDC-Datacenter ID Cluster-1 ID 10.201.2.4 O Compute-ResourcePool	Guest OS	ii Virtual Ma	chine Details Power Status	ACTIONS ~ I
2 a webserver01 a webserver02 a Win10-Desktop > @ Mgmt-ResourcePool			UMware Tools DNS Name (1)	Cubuntu Linux (64-bit) Running, version:11360 (Guest Managed) () webserver01 10:10:138
(LAUNCH REMOTE CONS		Encryption	re80::250:56ff:feb2:ted5 Not encrypted
	VM Hardware			II PCI Devices
	CPU Memory	2 CPU(s), 22 MHz used 1 GB, 0 GB memory active		
	Hard disk 1	10 GB Thin Provision (j) WorkloadDatastore		í
	Network adapter 1	Demo-Net (connected) 00:5	i0:56:b2:1e:d5	No PCI devices

6. At the shell prompt enter the following commands

 Note, your current directory **must** be /var/www/html/Lychee/public for the prepwebserver-1.sh script to work correctly - make sure to run the cd command as shown:

```
cd /var/www/html/Lychee/public
./prep-webserver-1.sh {your_efs_ip}
```

Click to copy

This script converts the storage of the photo app from the local file system to an NFS share on AWS EFS

webserver01				Enforce US Keyboard Layout View Fullscreen
root@webserve /var/www/html root@webserve Lychee=front CSS FOST favicon.ico root@webserve Test mount of Converting Ly root@webserve	r01:/var/www/html/Ly /Lychee/public r01:/var/www/html/Ly fix-permissions.sh fonts ing index.php er01:/var/www/html/Ly 172.231.0.136 succe ychee application to er01:/var/www/html/Ly	<pre>gchee/public# pwd gchee/public# ls installer js mix-manifest.json plugins gchee/public# ./prep geded. use EFS storage gchee/public#</pre>	prep-webserver-1.sh robots.txt src -webserver-1.sh 172.2	test-efs-mount.sh mologods web.config 31.0.136

7. to view the operations performed by the script let's take a look at the script. Type the following command

cat /var/www/html/Lychee/public/prep-webserver-1.sh

Click to copy



Now let's take a look at the NFS mount to confirm the images were copied

8. Type the following command:

ls -l /var/www/html/Lychee/public/uploads/original

Click to copy



9. Shutdown the VM using the following command:

shutdown now

Click to copy

root@webserver01:~# cd /var/www/html/Lychee/public/
root@webserver01:/var/www/html/Lychee/public# ls –l /var/www/html/Lychee/public/uploads/original/
total 16
drwxr–xr–x 3 www–data www–data 6144 Nov 5 07:25 <u>0a</u>
drwxr–xr–x 3 www–data www–data 6144 Nov 5 07:25 <mark>2f</mark>
drwxr–xr–x 3 www–data www–data 6144 Nov 5 07:25 79
-rwxrwxrwx 1 root root 0 Oct 25 12:28 index.html
root@webserver01:/var/www/html/Lychee/public#
root@webserver01:/var/www/html/Lychee/public# shutdown now)

10. Close the **webserver01** browser tab

Task 4 - Clone Webserver01

We will now clone webserver01 to create a new Virtual Machine "webserver03". We perform this task to confirm webserver03 continues to have access to the files in the same central repository as webserver01.

- 1. In the vSphere Client browser tab, Select and right-click webserver01
- 2. Select Clone
- 3. Select Clone to Virtual Machine

Q It should take a couple of minutes for the virtual machine to clone.

🔨 🗇 webserver01 ▷ 🗆 🗳 🚳 : астюля								
	Actions - webserver01		Monitor	Configure	Permissions	Datastores N	Networks Snapshots	
 vcenter.sddc-52-38-20 SDDC-Datacenter 	Power Guest OS		os		Virtual Ma	chine Details		ACTIONS ~
✓ (LL) Cluster-1 I 10.201.2.4	Snapshots					Power Status	D Powered Off	
Compute-Res	ص آي Migrate				E E	Guest OS	Ubuntu Linux (64-bit)	Guest
ت webserve ش Win10-De	Clone	>	3 [®] Clone t	to Virtual Mach	ine	VMWare Tools	Managed) (i)	ouest
> 🥢 Mgmt-Resourd	Fault Tolerance		_∯ ₽ Clone t	to Template		DNS Name (1) IP Addresses	webserverui	
	VM Policies		_ඒ ම් Clone a	as Template to	Library	Encryption	Not encrypted	
	Template Compatibility		CH WEB CONS	OLE				
	Export System Logs							

- 4. On the **Select a Name and Folder** page name the **virtual machine name** enter **webserver03**
- 5. Expand the vCenter > SDDC-Datacenter > and highlight Workloads folder
- 6. Click **Next**
- 7. On the Select a Compute Resource page select the Compute-ResourcePool
- 8. Click Next
- 9. On the Select Storage page select the WorkloadDatastore
- 10. Click **Next**
- 11. On the **Select Clone Options** page click the following check-boxes
 - Customize the operating system
 - Do not Select Power on virtual machine after creation
- 12. Click **Next**
- 13. On the **Customize Guest OS** page select the **LinuxSpec** customization specification.
- 14. Click **Next** to continue.
- 15. Review the information for accuracy and click **Finish** to clone the virtual machine.



Task 4.1 - Add webserver03 to PhotoAppVM Group

In a previous task we created the PhotoAppVM Group which we used in the Gateway firewall rule. We need to add **webserver03** to this group. Doing so will add it to the firewall rule along with **webserver01**

- 1. In the NSX Manager UI browser tab, click the **Inventory** tab
- 2. Click Groups
- 3. Click the 3 vertical dots next to the PhotoAppVM Group
- 4. Click Edit
- 5. Click Members
- 6. Click the **Members** tab
- 7. Select **webserver03** to add it to the group
- 8. Click APPLY
- 9. Click SAVE

vmw NSX	¢ ⊚~ ☀	Instructor01@v ~
Home Networking Securit Inventory Plan & Troubleshoot System		
Home Networking Securit () Inventory Plan & Troubleshoot System Croups Groups Compute Groups Management Groups Inventory Compute Groups Profiles Inventory Profiles Inventory Type () Compute Members Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles Image Profiles <th>Set Members I PhotoAppVM Cast consults members to alsone, you can statistication of synamication and members to a group Set many Cast Cast Cast Cast Cast Cast Cast Cast</th> <th></th>	Set Members I PhotoAppVM Cast consults members to alsone, you can statistication of synamication and members to a group Set many Cast Cast Cast Cast Cast Cast Cast Cast	
C KSHESH		

10. The clone of **webserver03** should be complete by now. In the vSphere Client select **webserver03** and power it on (or reboot it if it's already powered on).

< 	B webserver03 D D D Summary Monitor Conf Power Of	🖗 🐼 <u>: ACTIONS</u> Ions Datastores N	letworks Snapshots
 SDDC-Datacenter Cluster-1 	Guest OS	Virtual Machine Details	ACTIONS ~ II
 □ 10.201.2.4 ○ Compute-ResourcePool □ webserver01 □ webserver02 □ webserver03 □ Win10-Desktop > ○ Mgmt-ResourcePool 	Powered Off	Power Status Guest OS VMware Tools DNS Name (1) IP Addresses Encryption	 Powered Off Ubuntu Linux (64-bit) Not running, version:11360 (Guest Managed) () webserver03 Not encrypted

Task 4.2 - Verify Access to RDS from webserver03

- 1. In the vCenter browser tab , Select webserver03
- 2. Review and record webserver03 IP address
- 3. Click LAUNCH WEB CONSOLE
- 4. In the browser tab for webserver03. Log in as
- 5. login: root
- 6. password: VMware1!

You'll need this IP when creating a NAT rule for webserver03

vSphere Client Q Search in all environments					
	🔠 webserver03 🛛 Þ 🗖 📑 🤞	🖗 🔯 📔 👬 ACTIONS			
	Summary Monitor Configure Per	missions Datastores Net	tworks Snapshots		
🗸 🍘 vcenter.sddc-52-38-206-216.vmwarevmc.com					
SDDC-Datacenter	Guest OS 🗄 🕔	Virtual Machine Details	ACTIONS ~		
 Cluster-1 10.201.2.4 Compute-ResourcePool webserver01 webserver02 webserver03 Win10-Desktop O Mgmt-ResourcePool 	In a state of the second secon	Power Status Guest OS VMware Tools DNS Name (1) IP Addresses (2) Encryption $\ref{eq:eq:eq:eq:eq:eq:eq:eq:eq:eq:eq:eq:eq:e$	Powered On Ubuntu Linux (64-bit) Running, version:11360 (Guest Managed) webserver03 Notencrypted		

6. At the shell prompt enter the following commands



Click to copy

- 7. Replace the **APP_URL** IP with your webserver03 IP (Note: You recorded this IP in the steps above)
- 8. Press CTRL+O and Enter to save the change
- 9. Press **CTRL+X** to close the file



10. Reboot **webserver03** by typing the following command

reboot			

Click to copy

- 11. In the NSX Manager UI browser tab, click Networking tab
- 12. Click **Public IPs**
- 13. Click **Request New IP**
- 14. Type PhotoAppIP-Web03 in the Notes field
- 15. Click Save
- **16.** Record the IP generated, you will use it to configure NAT for webserver03 and access the application

vmw NSX					
Home 11 Networking Security Inver	tory Plan & Troubleshoot Syst	em			
Public IF	⊃ _S				
Connectivity 13 REQUEST N	IEW IP				
Tier-1 Gateways	Public IP Notes				
	<request a="" ip="" new="" public="">14 Photo</request>	AppIP-Web03			
Network Services					
	SAVE CANCEL				
⇒ NAT :	52.36.176.222 Photo	AppIP			
Cloud Services		Public IPs			
😳 Direct Connect		REQUEST NEW IP			
Transit Connect					
Connected VPC		Public IP	Notes		
Public IPs 12		16 35.84.204.137	PhotoAppIP-Web03		
IP Management		52.36.176.222	PhotoAppIP		
E DNS					

- 17. Click NAT
- 18. Click Add NAT Rule
- 19. Configure the rule as follows:
 - Name: PhotoApp Web03-NAT
 - Public IP: {The public IP you generated and store in step 16)
 - Internal IP: {The IP address o}f webserver03}
 - Logging: Enabled

20. Click Save

vmw NSX						© ۵	i∼ ÷∳ Instructor01	1@v ~
Home Networking S								
	NAT							
Connectivity	Internet Tier-							
Tier-1 Gateways	18 ADD NAT RULE							
Segments		Name	Public IP					
Network Services	~ 19	PhotoApp Web03-NAT	35.84.204.137 🙁 ^ *	All Traffic 🛛 🛞 🗸		Match Internal Address		
@ VPN		Logging	35.84.204.137 PhotoAppIP-Web03		C Yes			
		Description						
Cloud Services		L						
lirect Connect	20	SAVE CANCEL						
Transit Connect Connected VPC	: → ⇒							

With webserver03 rebooted, we will now confirm it's connectivity to the RDS MySQL DB. We want to confirm webserver03 can reach the DB and you are able to log in.

- 21. In a new browser tab, Type in the {**Public IP (NAT IP)**} for **webserver03** (Step 16)
- 22. At the Login screen log in as:
 - Username: admin
 - Password: {AWS Console Password provided by your instructor}

23. Click Sign In

▲ NOTE: This is the same account you created when you configured webserver01 against the RDS DB in Task 3.3, steps 20 & 21. If you created an account other than instructed then use that account instead.

UMware Cloud - VMCEX/PERT2 : 🛪 😰 vSphere - webserver/B - Summ. 🛪	Ø webserver03	🗙 📄 Amazon EPS	× Dychee v4 - Albums	× +	~
← → C ▲ Not secure 44.229.246.4					崆
-					
	P				
	admin				
			Lychee 4.6.1		

24. Click the Public folder, or any folder you previously uploaded an image to

Questions

- 1. Why didn't you have to run the Lychee Configuration wizard on webserver03 as you did on webserver01?
- 2. Are the images you uploaded from webserver01 visible from webserver03?
- 3. If you were to upload new images on Webserver03 will they be visible on webserver01?



Task 4.3 - Confirm EFS Mount on Webserver03

- 1. In the **webserver03** browser tab, If needed, log in to **webserver03** as:
 - user: root
 - **password: VMware1!** (If the browser tab was previously closed, go to vCenter and open console to webserver03 and continue)
- 2. Type the following commands to confirm NFS share is mounted to **webserver03**:

```
cd /var/www/html/Lychee/public/uploads
ls -l
ls -l original
mount | grep nfs
```

Click to copy

```
root@webserver03:~#
root@webserver03:~# cd /var/www/html/Lychee/public/uploads
root@webserver03:/var/www/html/Lychee/public/uploads#
root@webserver03:/var/www/html/Lychee/public/uploads# ls -1
total 36
drwxrwxrwx 2 root root 6144 Oct 25 12:28
drwxrwxrwx 2 root root 6144 Oct 25 12:28
drwxrwxrwx 2 root root 6144 Oct 25 12:28
drwxrwxrwx 5 root root 6144 Nov
                                   5 07:25
drwxrwxrwx 3 root root 6144 Nov
                                   5 07:25
drwxrwxrwx 2 root root 6144 Oct 25 12:28
drwxrwxrwx 5 root root 6144 Nov
                                   5 07:25
drwxrwxrwx 3 root root 6144 Nov
                                     07:25
drwxrwxrwx 2 root root 6144 Oct 25 12:28
root@webserver03:/var/www/html/Lychee/public/uploads#
root@webserver03:/var/www/html/Lychee/public/uploads# 1s -1 original
total 16
drwxr-xr-x 3 www-data www-data 6144 Nov 5 07:25
drwxr–xr–x 3 www–data www–data 6144 Nov
drwxr–xr–x 3 www–data www–data 6144 Nov
                                           5 07:25
                                           5 07:25
                                    0 Oct 25 12:28 index.html
-rwxrwxrwx 1 root
                       root
root@webserver03:/var/www/html/Lychee/public/uploads#
root@webserver03:/var/www/html/Lychee/public/uploads# mount | grep nfs
172.231.0.136:/ on /var/www/html/Lychee/public/uploads type
                                                                   4 (rw,relatime,vers=4.1,rsize=1048576
,wsize=1048576,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.10.31.42,local_lo
ck=none,addr=172.231.0.136)
root@webserver03:/var/www/html/Lychee/public/uploads#
root@webserver03:/var/www/html/Lychee/public/uploads#
```

Additional Lab 2 - Load-balancing Applications in VMC on AWS with Amazon Application Load balancer

In this lab, we will show how to leverage an Amazon Application Load Balancer (ALB) with Virtual Machines running in a VMware Cloud on AWS SDDC.

In this session we will load balance webserver01 and webserver03 (PhotoAppVM). We will then test connectivity to the PhotoVMApp via the Amazon Application Load-Balancer.

We will begin by requesting a public IP for webserver03 and define a NAT rule for it. Doing so ensure webserver03 is addressable from the internet and not just the private application network.

Task 1 - Add Web Servers to the Amazon Application Load Balancer

On your browser, open a new tab and go to: https://vmcexpert{#}.signin.aws.amazon.com/ console where {**#**} indicates your AWS environment (1, 2 or 3)

The Credentials below are from the AWS Console portion of your student lab assignment sheet

- 1. Account ID or alias: vmcexpert# i.e vmcexpert1, vmcexpert2 or vmcexpert3
- 2. IAM user name: VMCEXPERT#-XX(where # is your Environment ID and XX is the number assigned to you)
- 3. Password:
- <AWS Console PW provided By your instructor>
- 4. Click Sign In

aws	
Sign in as IAM user	
Account ID (12 digits) or account alias	
1_imcexpert1	
IAM user name	
2 mcexpert1-01	
Password	
3	
Remember this account	
4 Sign in	
Sign in using root user email	
Forgot password?	

- 5. In the upper left-hand Click **Services**
- 6. Under Recently visited click EC2
- 7. In the Left pane under Load Balancing, Click Target Groups (you may have to scroll down)
- Find and blue click the text for your target group <vmcexpert#-xx-default> (where XX is your student number)

Services Q Search	[Option+5]
Recently visited Favorites All services	Recently visited ×
은 Analytics জ Application integra 등 AR & VR	Annaged File Storage for KC2 stion S S Vertual format Server In the Cloud Vertual format Server In the Cloud
aws iii services Q Search	[Option*5]
Spot Requests Savings Plans Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations	EC2 > Target groups Target groups (1) lins Q. Sourch or Alter target groups Q. Sourch or Alter target groups Q. Sourch or Alter target groups Q. Create target groups Q. Sourch or Alter target groups Q. S
♥ Images AMIS AMI Catalog	Name V ARN V Port V Target type V Load balancer V VPC ID V 1 VMCEXPERTI-01-default C1 arraws:elasticloadbalanci 80 HTTP IP VMCEXPERTI-01 vpcc479feb893ebd82776
 ▼ Elastic Block Store Volumes Snapshots Lifecycle Manager 	
Hetwork & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces	E C target groups selected X Select a target group above.
▼ Load Balancing Load Balancers Target Groups	

9. Click the **Targets** tab

10. Click **Register targets**

	EC2 > Target groups > VMCEXPERT1-01-default						
	VMCEXPERT1-01-default			Actions v			
	Details 🗇 amawselasticloadbalancingsus-west-2:011727134347:targetga	oup/VMCEXPERT1-01-default/4a3810e545a72a5d					
	Target type IP IP address type IPv4	Protocol : Port HTTP: 80 Load balancer VMCEXPERT1-01	Protocol version HTTP1	VPC vpc-079feb893ebd82776 [2]			
	Total targets Healthy 0 \oslash 0	Unhealthy 🙁 0	Unused \bigcirc O	Initial Draining			
•	Targets Monitoring Health checks Attri	butes Tags					
	Registered targets (0) C Deregister Register targets Q. Filter resources by property or value < 1 > ©						
	IP address ∇ P	ort 🗢 Zone 🗢	Health status 🗢 🕨	lealth status details			
	No registered targets 10 Register targets						

- 11. In the Network Drop-Down list, select **Other Private IP address**
- 12. In the IP Field Enter the **<Private IP address of Webserver01**>
- 13. Click Include as pending below

- 14. Repeat steps 12 & 13, this time using the <**Private IP for webserver03**>
- 15. Click **Register pending targets**

EC2 > Target groups > VMCEXPERT1-01-default > Register targets					
Register targets					
Specify IP addresses, specify ports, and add the IP addresses to the list of pending targets. Repeat to add additional combinations of IP addresses	es and ports to the list of pending targets. Once you are satisfied with yo	ur selections, click Register pending targets.			
IP addresses					
Step 1: Choose a network					
You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network	sources by returning to this step and choosing another network.				
Network	Availability Zone				
Other private IP address	All				
vpc/0791eb931eb82776 Bvd: 172.201.0.0/16 V47C2931821844					
11 per private IP address					
- Lowed ranges					
0.10.1.11		Remove			
Add IPv4 address You can add up to 4 more IP addresses.					
Ports Parts for routing to the					
80					
	topie ports with commany				
Include as p	ending below				
Include as pen	ding below				
2 selections are now pending below. Indus	e more or register targets when ready.				
Review targets					
Step 3: Review IP targets to include in your group					
Cenfirm the IP targets to include in your target group. Add more IP targets by repeating steps 1 and 2 on this page. You can also register additional targets after your t	arget group is created.				
Targets (2)		Remove all gending			
All The require hy amount a union					
Remove IPv4 address Health status	IP address V Port	▼ Zone ▼			
× 14 Pending		All			
X (Peeding		All			
2 pending					
		Register penuing targets			

- 10. Wait 10-20 seconds, click the refresh circle, the status should turn from '**initial**' to '**healthy**'
 - Webserver03 should display a Healthy state, but webserver01 should be Unhealthy.
 This is expected because webserver01 is powered-off. Keep it powered-off for now.

Targe	ts Monitoring Health d	checks Attributes	Tags			
Regi	stered targets (1/3) Filter resources by property or value					C Deregister Register targets
=	IP address	♥ Port	♥ Zone	♥ Health status	♥ Health status details	
	10.10.1.13	80	All	🕲 unhealthy	Request timed out	
	10.10.1.26	80	All		Request timed out	
	10.10.1.11	80	All	⊖ draining	Target deregistration is in	progress

Task 2 - Validate the Application Load Balancing

- 1. In the menu on the left, under Load Balancing, click Load Balancers
- Type <VMCEXPERT#-XX> in the Search field to Find your load balance, Where XX = your student number. i.e. VMCEXPERT3-01
- 3. Check the box next to your Load Balancer (don't click on the blue text)

4. From the Description tab copy the DNS name ie. VMCEXPERT#-XX-UID.(region).elb.amazonaws.com

aws Bervices Q Search	[Option+5]	ב 👃 Ø Oregon ▼ VMCEXPERT1-01 @ vmcexpert1 ▼								
Spot Requests	EC2 > Load balancers									
Reserved Instances Dedicated Hosts	Load balancers (1/1) Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.	C Actions Create load balancer								
Scheduled Instances Capacity Reservations	< 1 > 🛛									
♥ Images AMIs	🗹 Name 🔻 DNS name 🗢 State 🗢 VPC ID 🗢 Avai	lability Zones 🗢 Type 🗢 Date created 🗢 Instance ID								
AMI Catalog	VMCEXPERT1-01 @ VMCEXPERT1-01-116188 @ Active Vpc- 079feb893ebd82776 2.Ax	allability Zones application February 24, 2023, 00:02 - (UTC-07:00) -								
 Elastic Block Store Volumes Snapshots Lifecycle Manager 										
 Network & Security Security Groups 	= Load balancer: VMCEXPERT1-01 =									
Elastic IPs Placement Groups	Details Listeners Network mapping Security Monitoring Integrations Attributes Tags									
Key Pairs Network Interfaces Load Balancing	Details Ø am avszelastidoadbalancingsus-west-2:0117271343472ioadbalancer/app/VMCEXPERT1-01/27b5eb75affe2f1f									
Load Balancers 1 t Groups Auto Scaling	Load balancer type Application 4 DNS name DNS name DNS name C VMCEXPERT1-01-1161884029.us-west-Z.elb.amazon G VMCEXPERT1-01-1161884029.us-west-Z.elb.amazon G Active	VPC vpc-079feb893ebd82776 [2]								
Launch Configurations Auto Scaling Groups	IP address type Scheme Availability: IPv4 Internet-facing subnet-05dk subnet-05dk	Cones Hosted zone 88383806bd007f [2] us-west-2a (usw2-sz1) Z1H1FL5HAB5F5 ecsa45037004b5 [2] us-west-2b (usw2-sz2) X								

- 4. Paste the **DNS Name** in your browser to access the PhotoApp via ALB i.e. **vmcexpert3-01-888644610.eu-central-1.elb.amazonaws.com/Lychee**
- 5. If you aren't prompted for a login, Click the exit icon in the upper-right hand of the application page
- 6. When prompted to login in use the following:
 - Username: admin
 - Password: <Password Provided by your instructor>
 - Click Sign In
- 7. Upload some additional images to **webserver03**

A Not secure vmcexpert2-31-21319406.us-west-2.elb.amazonaws.com					
Albuma					
P					
admin					
annone (
Cancel Sign In					

Task 3 - Test Load Balancer functionality

- 1. In your vCenter browser tab, select webserver01
- 2. Right-click webserver01,
- 3. Click Power --> Power-on
- 4. Right-click webserver03
- 5. Click Power--> power-off
- 6. Confirm that **webserver01**'s IP address has not changed 10.10.x.11

NOTE: This was the IP we used when we configured the Load Balancer Target Group

	s wel	bser	rver01 Þ	• • •	♣ tti :				
<u> </u>	Actions - webserver01		Ionitor Cont	figure I	Permissions	Datastores	Network	ks Snapshots	
 vcenter.sddc-52-38-206-2 SDDC-Datacenter Cluster-1 10.2012.4 	Power Guest OS Snapshots	4	Power Or Power Of Suspend	n If	ctrl + alt + B ctrl + alt + E ctrl + alt + Z	wer Status	ē¤ <u> (</u>	Powered Off Ubuntu Linux (64-bit)	
✓ Ø Compute-Resour	📑 Open Remote Console					ware Tools	Not	running, version:11360 (Guest	
3	强 Migrate Clone		🗱 Hard stop	stop Down Guest OS ctrl + alt + i		Ma NS Name (1) We Addresses		naged) (j) Ibserver01	
🖨 Win10-Deskto	Fault Tolerance					cryption	Not	encrypted	
> 🧿 Mgmt-ResourceF	VM Policies		WEB CONSOLE			₫.			
	Template Compatibility								
	Export System Logs		vare					PCI Devices	
	Edit Settings		2	CPU(s), 0 N	Hz used				
	Move to folder Rename Edit Notes Tags & Custom Attributes		10 viter1 D	10 GB Thin Provision () WorkloadDatastore Demo-Net (disconnected) 00:50:56:b2:1e:d5 Disconnected			i No PCI devices		
V Decest Tesla Alarma	Add Permission								

- 7. In the AWS Console, under Load Balancing select Target Groups
- 8. Select your **<VMCEXPERT#-XX>-default** (Your Load Balancer Target Group) where XX is your student number
- 9. Click the **Targets** tab
- 10. After 60 secs the powered off VM state should report unhealthy

Spot Requests Savings Plans	EC2 > Target groups	
Reserved Instances Dedicated Hosts Scheduled Instances Capacity Reservations	Target groups (1/1) Info Q. Search or filter target groups Search: 1-01 X Clear filters	C Actions ▼ Create target group < 1 > ⊗
[,] Images AMIs AMI Catalog	Image: Name Image: ARN Image: ARN Image: Port Image: Protocol Image: VMCEXPERTI-01-default Image: ARN Image: ARN	v Target type v Load balancer v VPC ID v IP VMCEXPERTI-01 vpc-079feb893ebd82776 vpc-079feb894ebd82776 vpc-079feb894ebd82776 <td< th=""></td<>
[•] Elastic Block Store Volumes Snapshots Lifecycle Manager		
Network & Security Security Groups Elastic IPs Placement Groups	Target group: VMCEXPERT1-01-default Details Targets Monitoring Health checks Attributes Tags	
Key Pairs Network Interfaces ¹ Load Balancing	Registered targets (1/3) Q. Filter resources by property or volue	O Deregister Register targets < 1 > O
Load Balancers Target Groups	IP address V Port V Zone V H 10.10.1.13 80 All I	volume volume Property Request timed out
Launch Configurations Auto Scaling Groups	□ 10.10.1.26 80 All 6	② unhealthy Request timed out ○ draining Target deregistration is in progress

- 10. In a new Google Chrome incognito window type <**your ALB DNSName**> i.e. vmcexpert3-01-1218955224.eu-central-1.elb.amazonaws.com
- 11. If prompted to login in use the following:
 - Username: admin
 - Password: <Password Provided by your instructor>
 - Click Sign In
- 12. Power-on your previously powered-off vm in step 2



Conclusion

A separate software load balancer is not required to be deployed in the VMware stack to provide load-balancing functionality for your Applications running in VMware Cloud on AWS. There is no additional updating or maintenance to be performed with your load balancer as you can instead use the one provided by AWS.