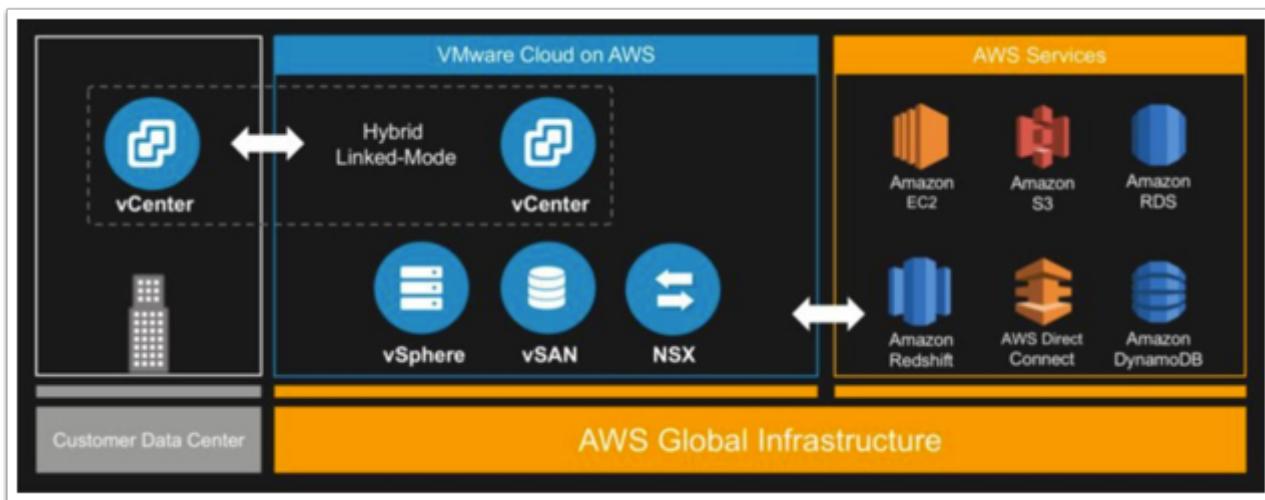


# Lab 03 - SDDC Networking & Native AWS Integration

## 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

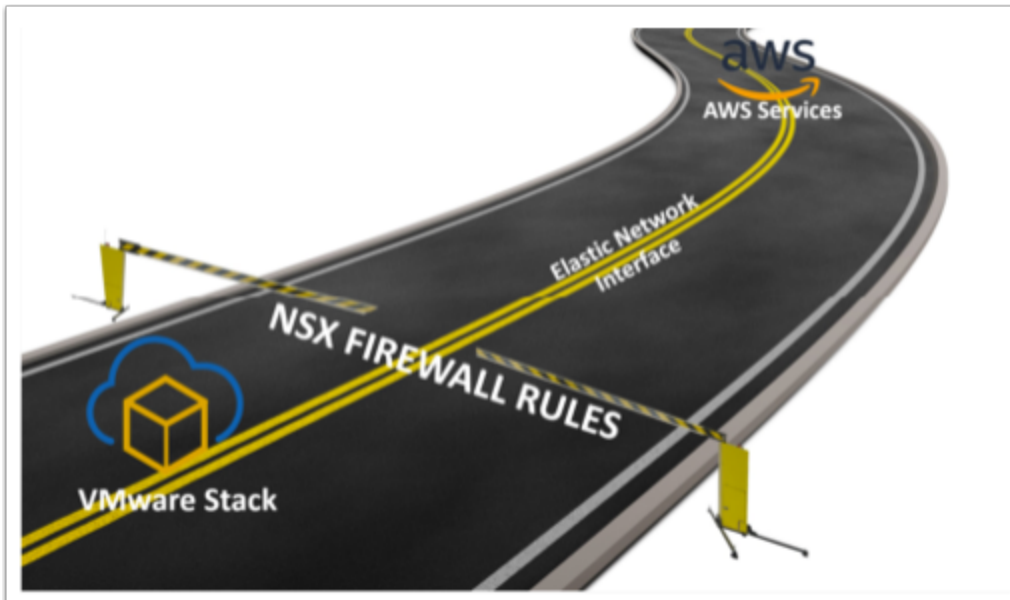
These are only a few of the integrations we've seen. There are many different services that can be integrated into your environment. In this exercise we'll be exploring integrations with both AWS Simple Storage Service (S3) and AWS Relational Database Service (RDS).

## How are these integrations possible?

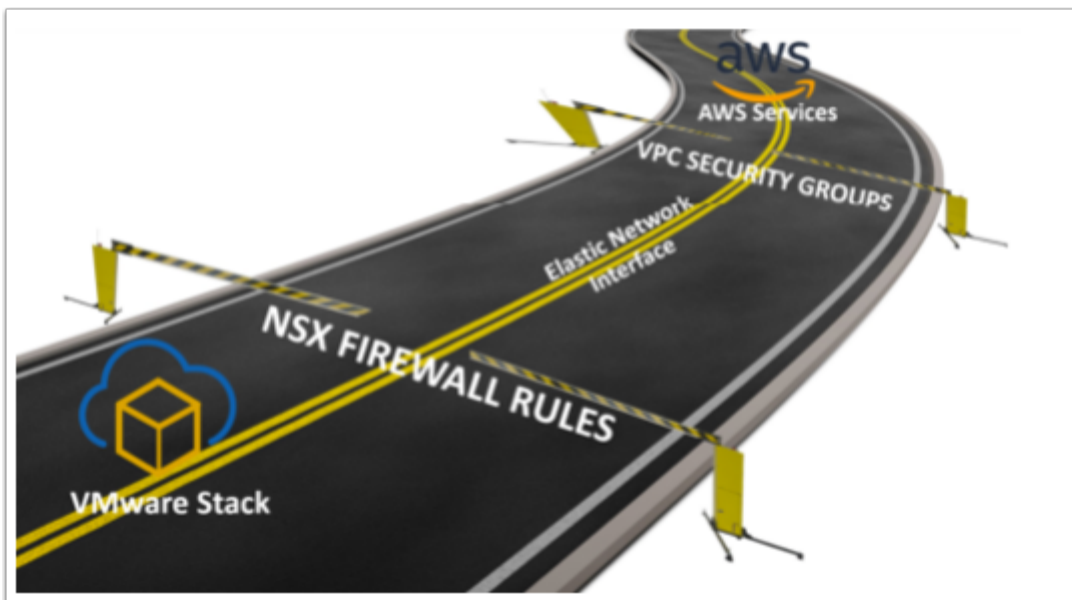
In addition to sitting within the AWS Infrastructure, there is an Elastic Network Interface (ENI) connecting VMware Cloud on AWS and the customer's Virtual Private Cloud (VPC), providing a high-bandwidth, low latency connection between the VPC and the SDDC. This is where the traffic flows between the 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 charge.


## 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 (see image below), 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.



 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.

 **Note:** There is a requirement in this lab to have completed all the steps in the [Working with your SDDC Lab](#).

## TASKS

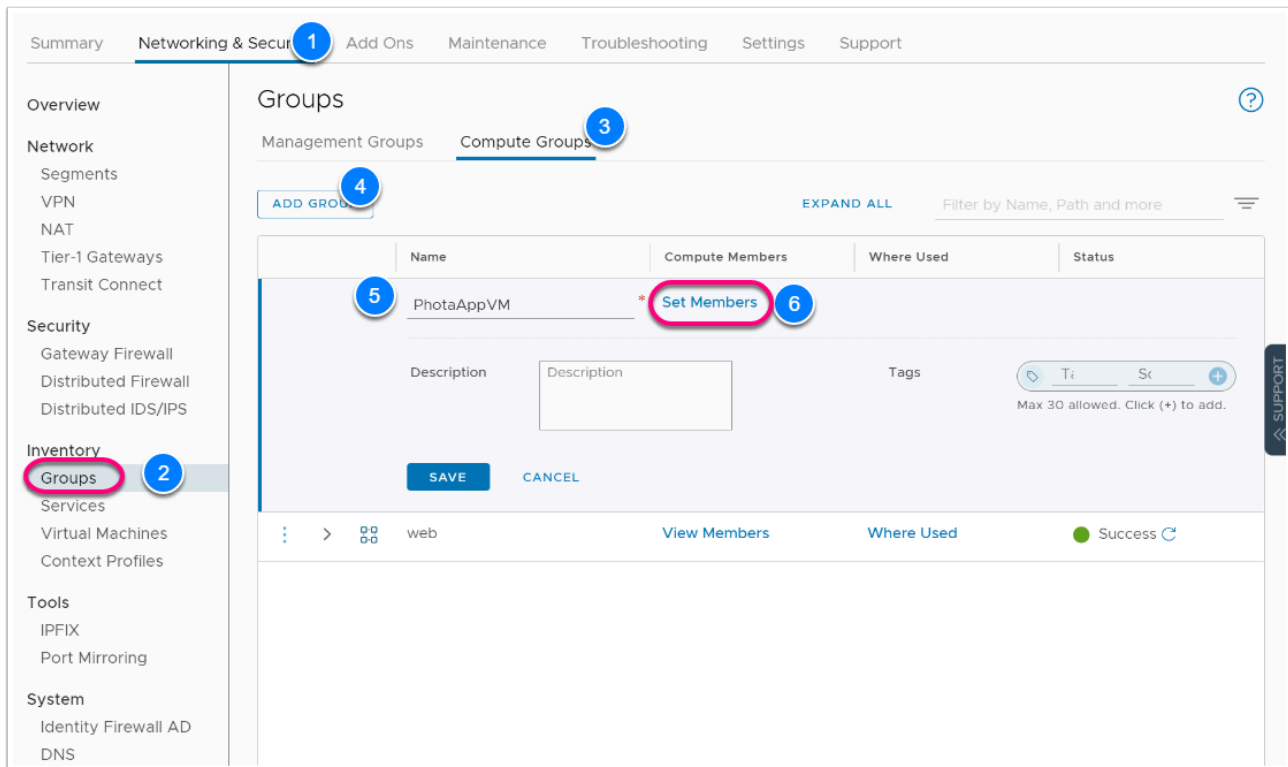
### Task 1 - Allow traffic through the ENI

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

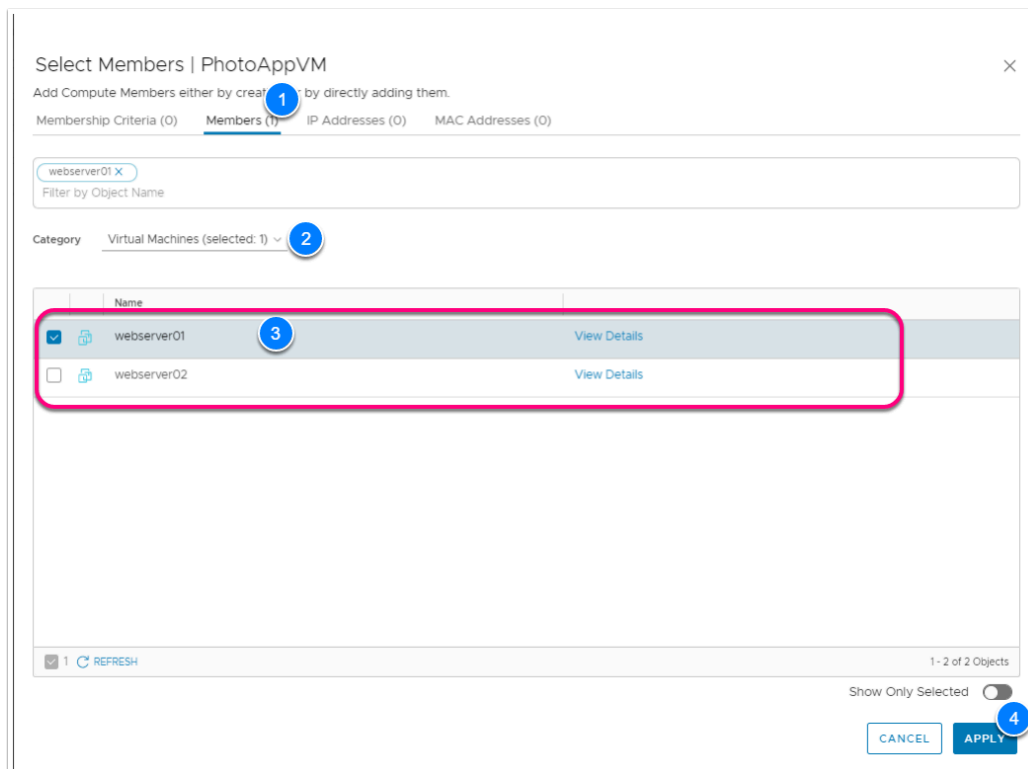
#### Task 1.1 - Create Security Groups

We will now 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 **Networking & Security** tab
2. Click **Groups** in the left pane
3. Click **Compute Groups**
4. Click **ADD GROUP**



5. Type **PhotoAppVM** for the Name
6. Click the **Set Member** link
7. In the popup, Select **Members** Tab
8. From the Drop Down change the Category to **Virtual Machines**
9. Select and check **Webserver01** and **Webserver02**
10. Click **Apply** to close the popup then **Save**



## Task 1.2 - 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. Click **Networking & Security** tab in your VMware Cloud on AWS Portal
2. Click **Gateway Firewall** in the left pane
3. Click and select **Compute Gateway**
4. Click+ **ADD RULE**
5. Click on the "New Rule" Text to change the name of your new rule to **AWS Inbound**
6. Hover over the Source field and click on the blue **Edit button**
7. In the popup, Select **Connected VPC Prefixes**
8. Click **Apply** to close the popup
9. Hover over the Destination field and click on the blue **Edit button**
10. In the popup, Select **PhotoAppVM**
11. Click **Apply**
12. Leave Service as **Any**
13. Leave applied to as **All Uplinks**
14. Repeat **Steps 4 - 13** to create a 2nd rule - This time set
  - Name the Rule **AWS Outbound**
  - **PhotoAppVM** as the Source
  - **Connected VPC** Prefixes as the destination
  - **MySQL** for Services. You can use the filter in top right of the popup or scroll to find it
15. Add a 3rd Firewall rule Named **Public In** & set as follows:
  - **Any** as Source

- **PhotoAppVM** as Destination
- **HTTP** as Services

16. To the far right of each rule click the **GEAR**
17. Slide the **Slider** in the Dialog to **enable** logging
18. Click **APPLY**
19. Click **PUBLISH** to save and activate the rules

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Overview

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

Gateway Firewall

Management Gateway Compute Gateway Tier-1 Gateways

3 Total Unpublished Changes REVERT PUBLISH

+ ADD RULE CLONE UNDO DELETE 3 Unpublished Changes Uninitialized Filter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Applied To	Action	
	AWS Inbound		Conne...	PhotaA...	Any	All Uplinks	Allow	
	AWS Outbound		PhotaA...	Conne...	MySQL	All Uplinks	Allow	
	Public In		Any	PhotaA...	HTTP	All Uplinks	Allow	
	Default VTI Rule	1012	Any	Any	Any	VPN Tunne...	Drop	
	Default Uplink ...		Any	Any	Any	All Uplinks	Drop	

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Overview

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

Gateway Firewall

Management Gateway Compute Gateway Tier-1 Gateways

1 Total Unpublished Change REVERT PUBLISH

+ ADD RULE CLONE UNDO DELETE 1 Unpublished Change Uninitialized Filter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Applied To	Action	
	AWS Inbound	2028	Conne...	PhotaA...	Any	All Uplinks	Allow	
	AWS Outbound	2029	PhotaA...	Conne...	MySQL	All Uplinks	Allow	
	Public In	2030	Any	PhotaA...	HTTP	All Uplinks	Allow	
	Default VTI Rule	1012	Any	Any	Any	VPN Tunne...	Drop	
	Default Uplink ...		Any					

Settings

Rule > AWS Inbound

Logging

Log Label

Comments

Enable

CANCEL APPLY



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

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Overview

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

### Gateway Firewall

Management Gateway **Compute Gateway** Tier-1 Gateways

REVERT PUBLISH

+ ADD RULE CLONE UNDO DELETE Uninitialized Filter by Name, Path and more

	Name	ID	Sources	Destinations	Services	Applied To	Action
<input type="checkbox"/>	AWS Inbound	2028	Connected VPC Pr...	PhotoAppVM	Any	All Uplinks	Allow <input checked="" type="checkbox"/>
<input type="checkbox"/>	AWS Outbo...	2029	PhotoAppVM	Connected VPC Pr...	MySQL	All Uplinks	Allow <input checked="" type="checkbox"/>
<input type="checkbox"/>	Public In	2030	Any	PhotoAppVM	HTTP	All Uplinks	Allow <input type="checkbox"/>
<input type="checkbox"/>	Default VTI ...	1012	Any	Any	Any	VPN Tun...	Drop <input checked="" type="checkbox"/>
<input type="checkbox"/>	Default Upli...		Any	Any	Any	All Uplinks	Drop <input type="checkbox"/>

## Task 2 - Enable Public Internet access to the PhotoAppVM

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.

### Task 2.1 - Request a public IP address

**i** 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.

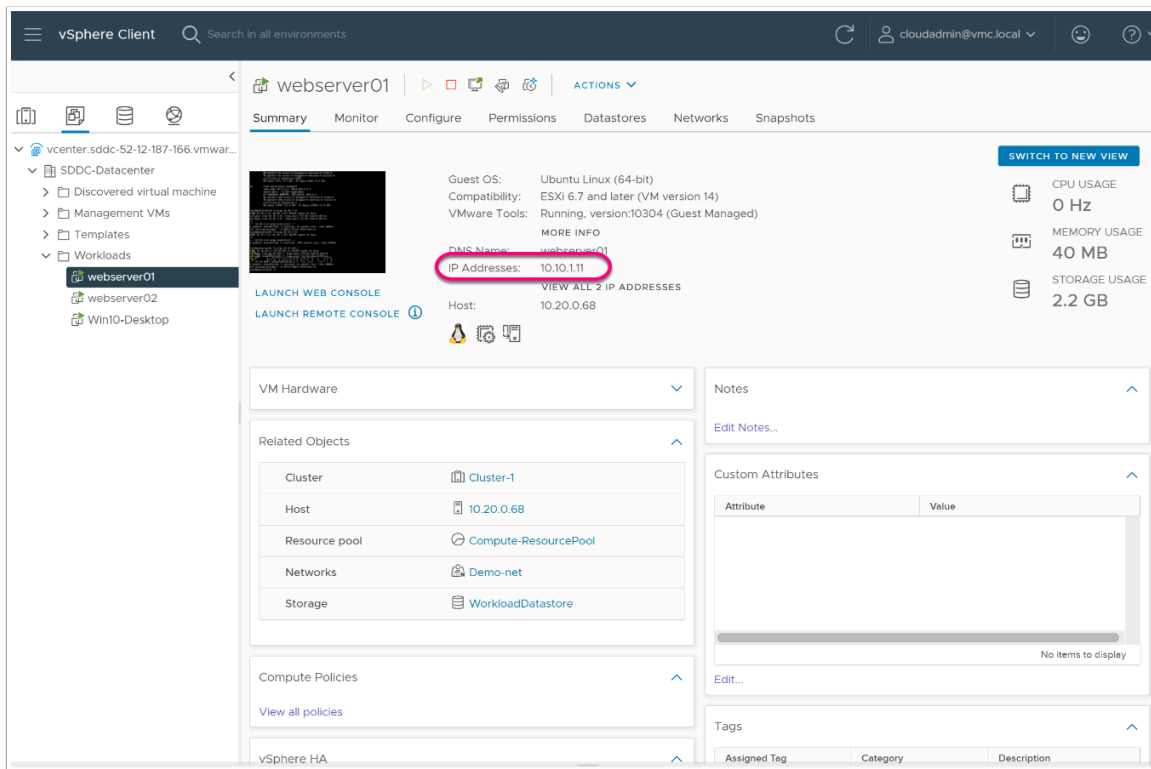
As a best practice, release the public IP addresses that are not in use.



### Prerequisites

Verify that your VM has been assigned an IP address assigned from its logical network.



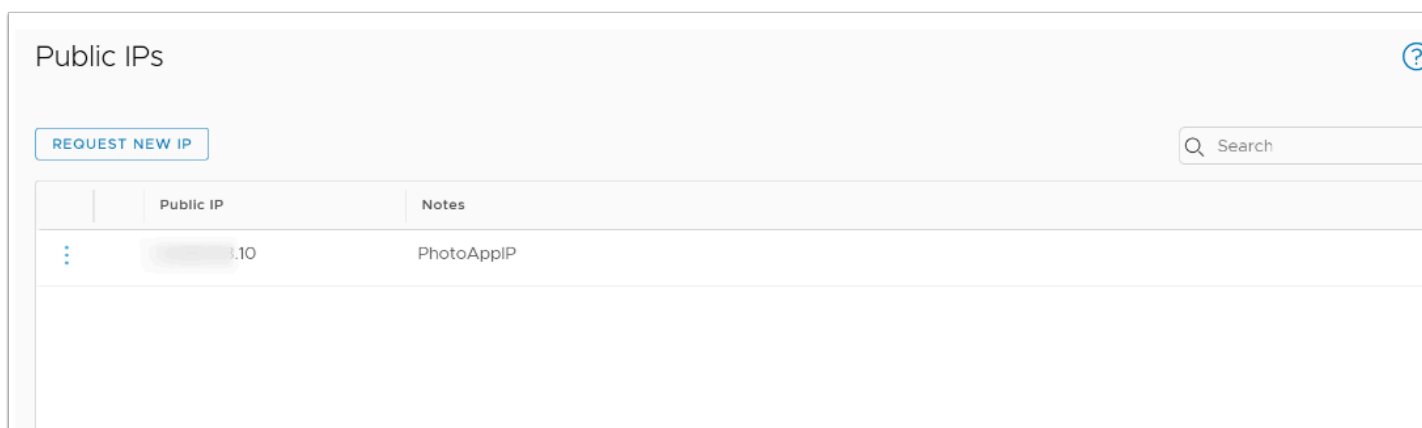
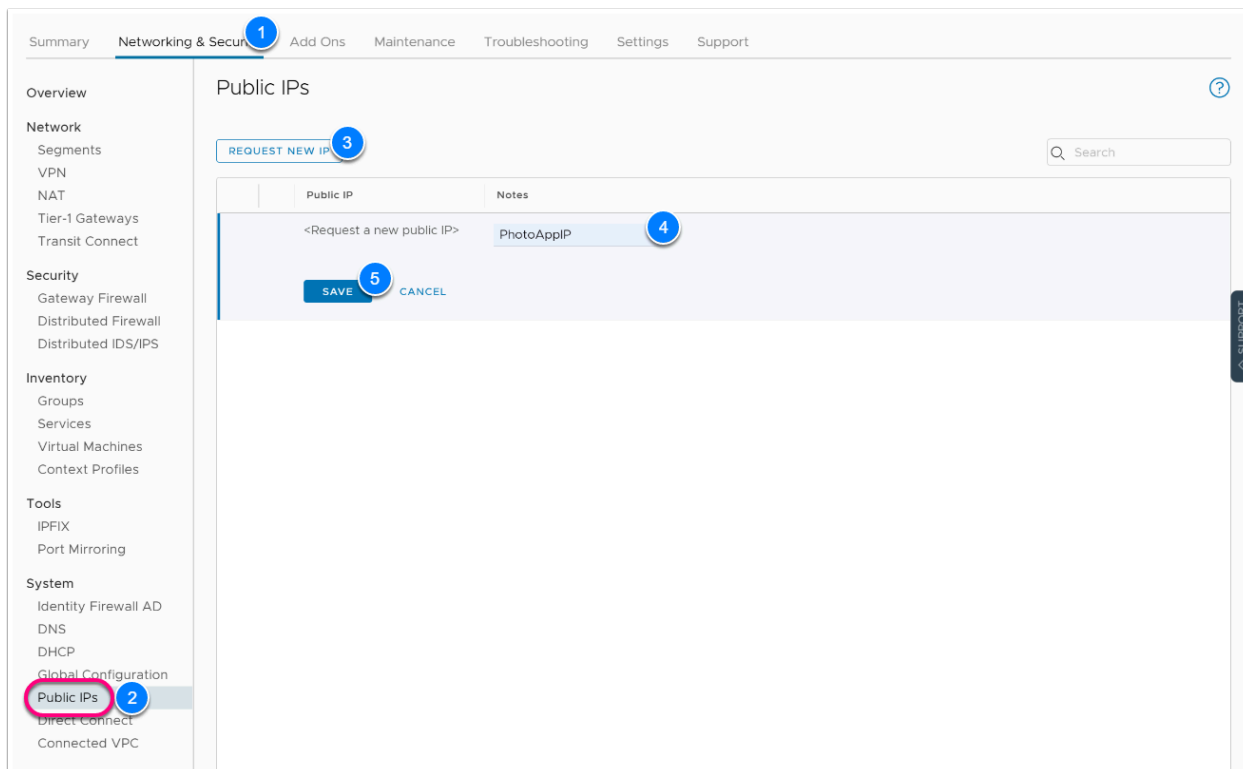


You will be using the VM created in the previous module in order to complete this exercise.

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)

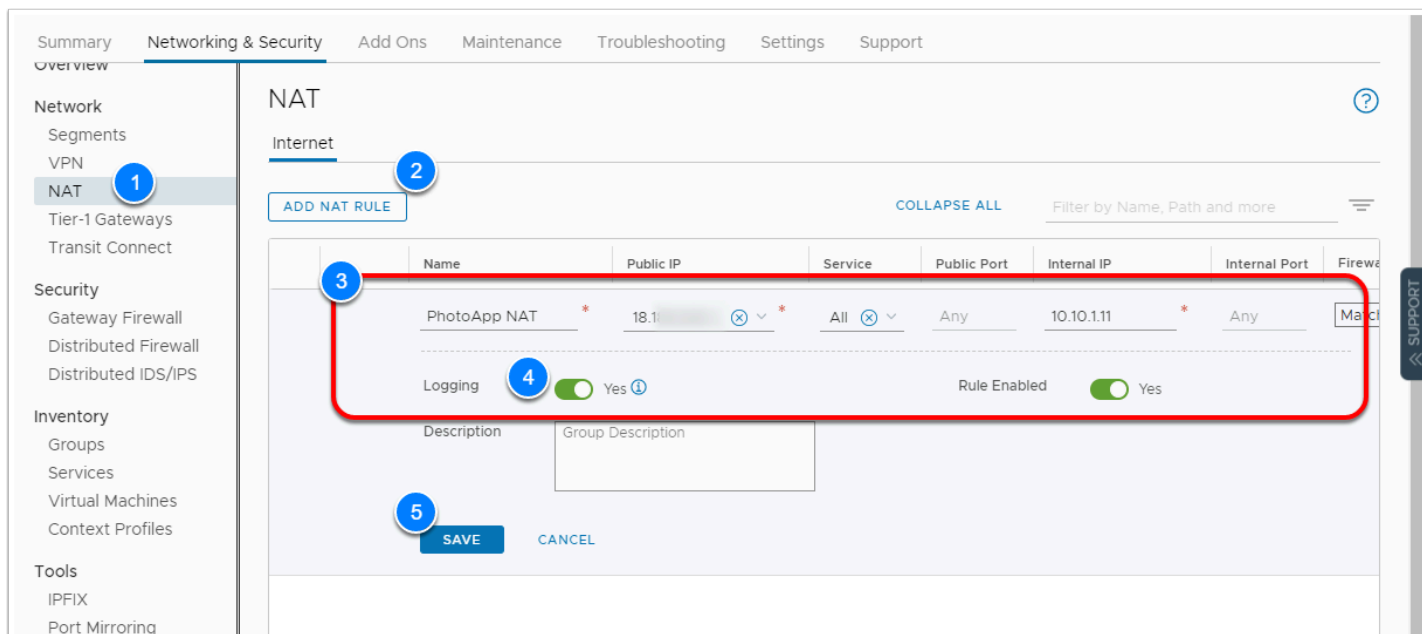
## Task 2.1.1 - Request Public IP

1. Go back to your VMware Cloud on AWS portal and click on the **Networking & Security** tab in order to request a Public IP address
2. Click **Public IPs** in the left pane
3. Click on **REQUEST NEW IP**
4. In the notes area type **PhotoAppIP**
5. Click **SAVE**
6. Take Note of and record this **Public IP address (It will be used in the next task to setup Network Address Translation (NAT) for webserver01)**



## Task 2.2 - Create a NAT Rule

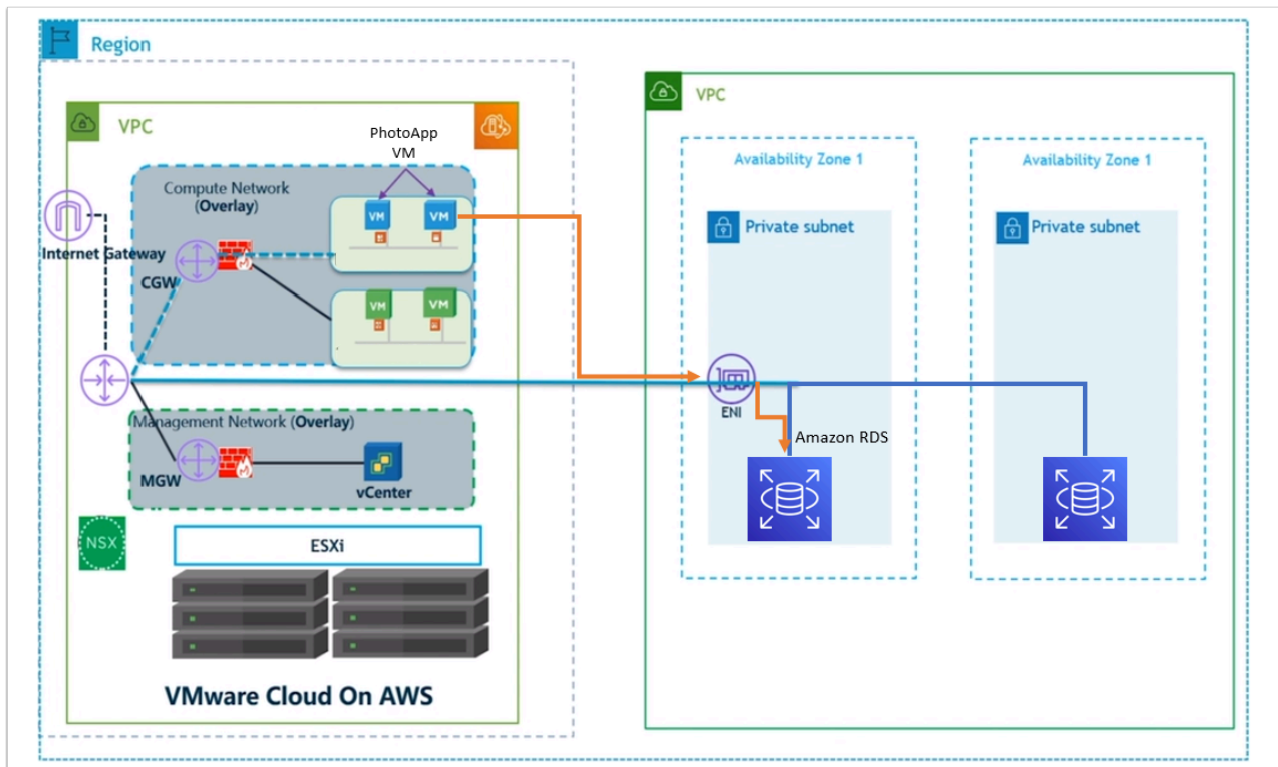
1. Click **NAT** in the left pane
2. Click **ADD NAT RULE**
3. Type **PhotoApp NAT** for Name
4. Ensure the Public IP you requested in the previous step appears under Public IP (it should auto populate, but if it does not click back on the Public IPs menu item and take note of the IP)
5. Leave **All Traffic**(no change)
6. For the Internal IP, type the 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. Move the **Slider** to the right (**YES**) to enable Logging
8. Click **SAVE** (a green successful notification should appear momentarily)



## Task 3 - AWS Relational Database Service (RDS) Integration

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.



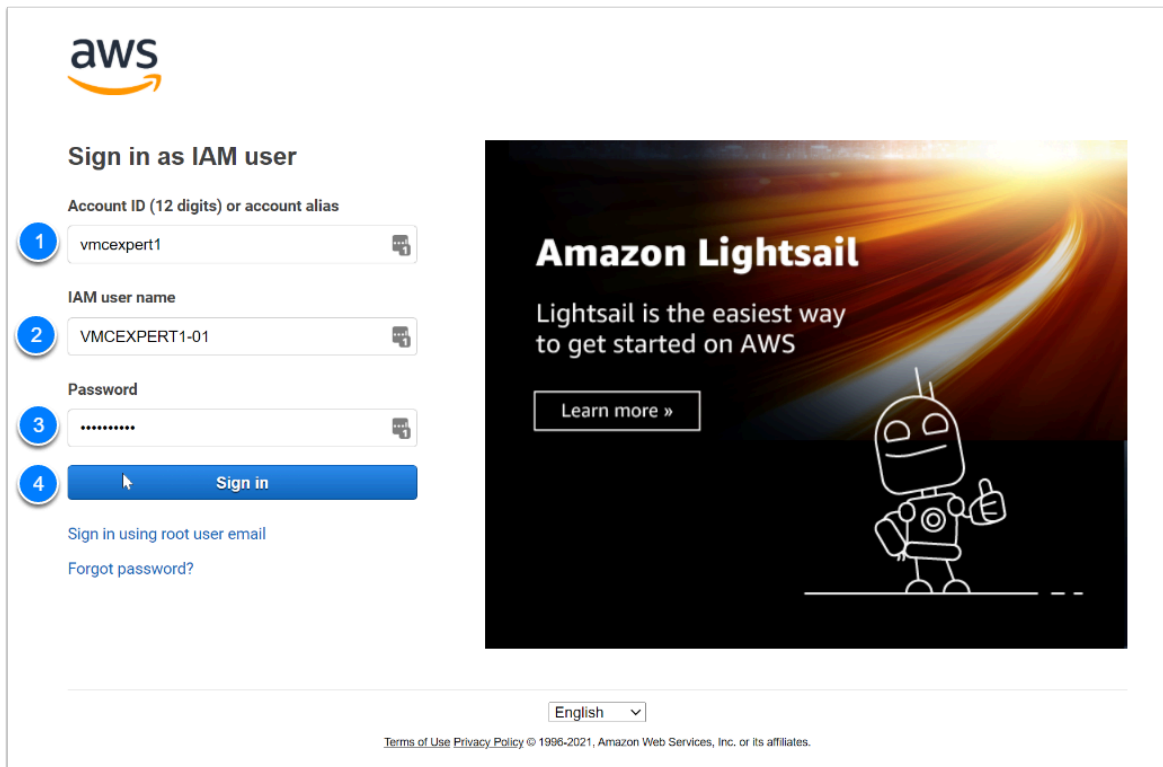
### Task 3.1 - View AWS RDS Instance

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)

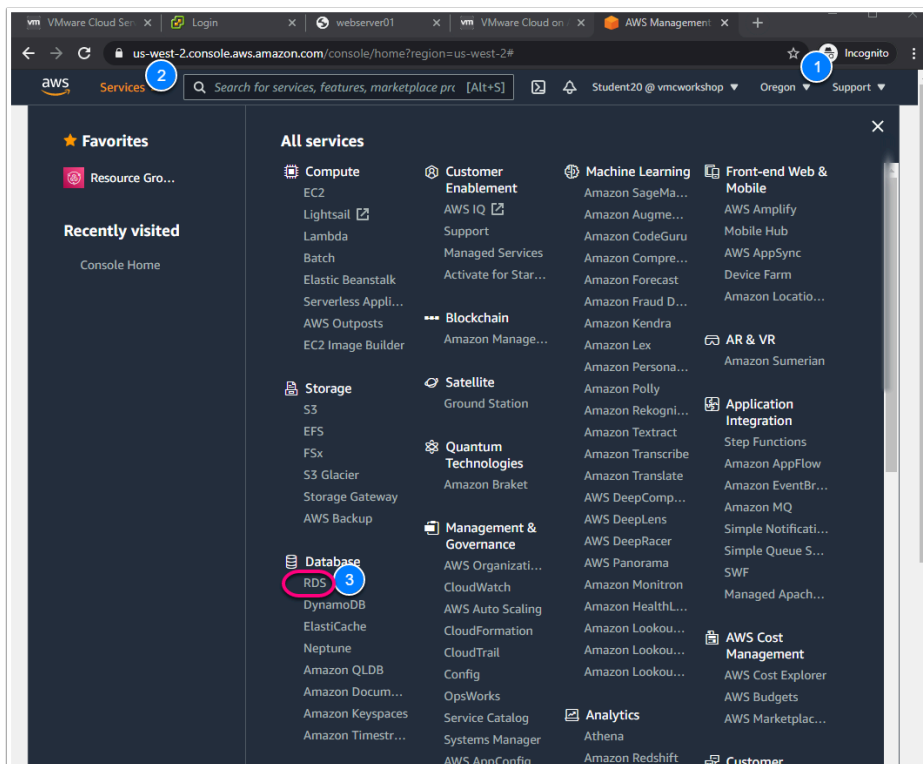
The Credentials below are from the AWS Console portion of your student lab assignment sheet

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>**

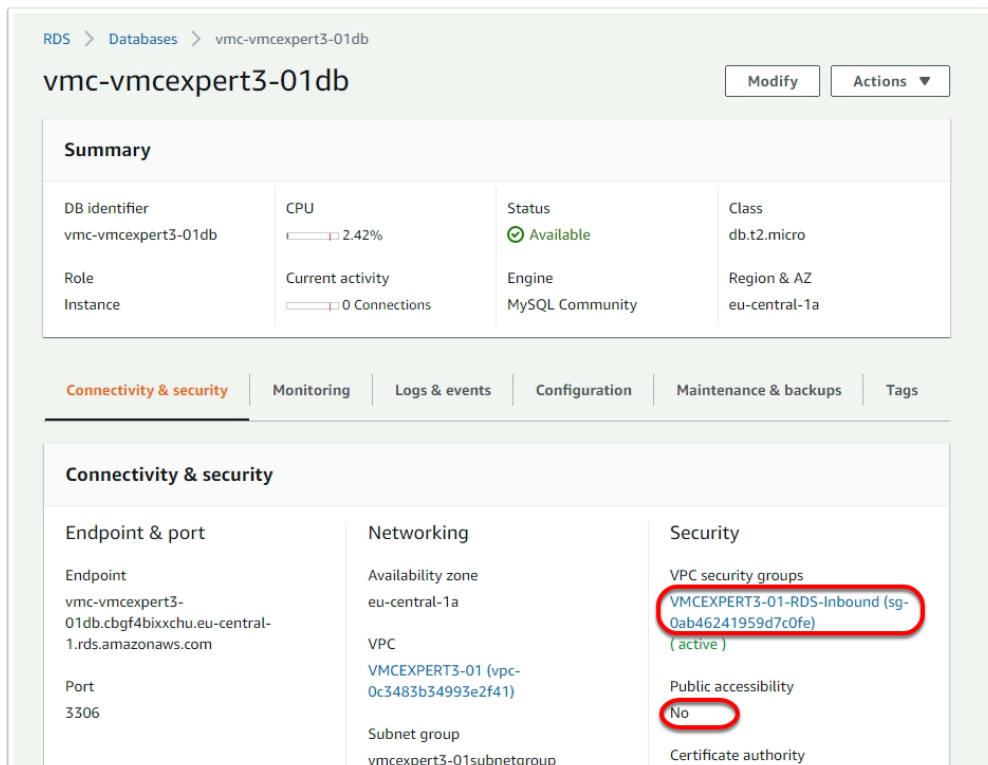
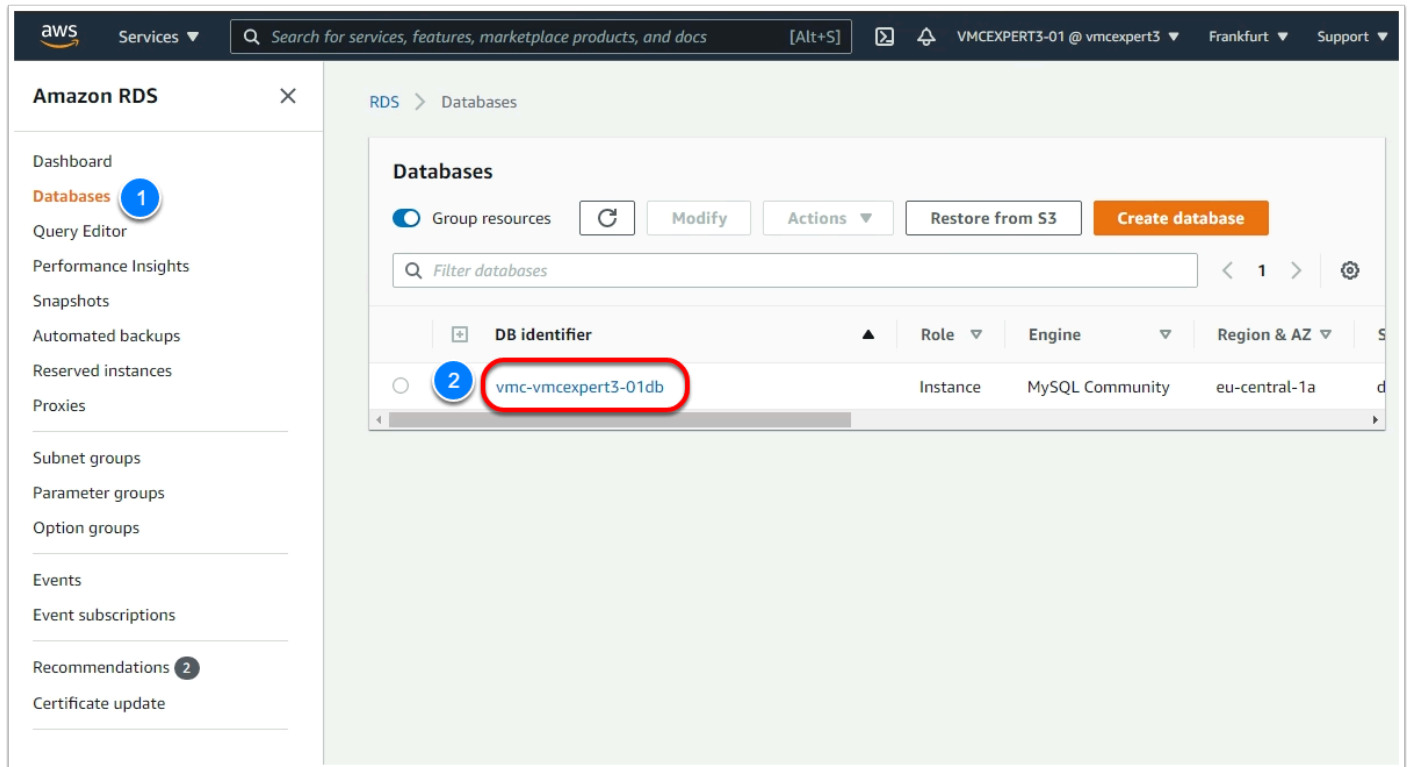
Click **Sign In**



1. You are now signed into the AWS console. 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 you are using **vmcexpert3**
2. Expand the **All Services** drop down then select the **RDS** service under the **Database** group



4. In the **Amazon RDS** left pane click on **Databases**
5. Search for your student number (**i.e. 01 through 31**) Click the text under the **DB Identifier** column into the RDS instance that corresponds to your designated student number
6. Ensure that you are on the **Connectivity & Security** Tab, Scroll down to the **Connectivity & Security** section, look inside the **Security** subsection at the **Public Accessibility** details.  
**Notice** the RDS instance is not publicly accessible, meaning this instance can only be accessed from within AWS.



## Task 3.2 - View the AWS RDS pre-configured Security Policy settings

1. Click on the blue hyperlink corresponding to your Student##-RDS underneath the **VPC Security groups** text
2. Check / Select the **Student##-RDS-Inbound** RDS Security group corresponding to you (may not match your student number).
3. After highlighting the appropriate security group click on the **Inbound** tab in the pane below
4. Review the Inbound rules, and note that your PhotoAppVM should be allowed access to TCP Port 3306
5. Click **Outbound** tab
6. You can see All traffic (internal to AWS) is allowed; this includes your VMware Cloud on AWS SDDC logical networks.

Security Groups (1/1) Info

Filter security groups

search: sg-0ab46241959d7c0fe X Clear filters

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-0ab46241959d7c0fe	VMCEXP3-01-RDS-Inbound	vpc-0c3483b34993e2f41	VMCEXP3-01-RDS-Inbound	8244C...

sg-0ab46241959d7c0fe - VMCEXP3-01-RDS-Inbound

Details Inbound rules Outbound rules Tags

Inbound rules (2)

Filter security group rules

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-0e6c11e0f0bf82e82	IPv4	MySQL/Aurora	TCP	3306	67.198.12.121/32
-	sgr-0bf029b8c6223771b	IPv4	MySQL/Aurora	TCP	3306	10.10.0.0/16

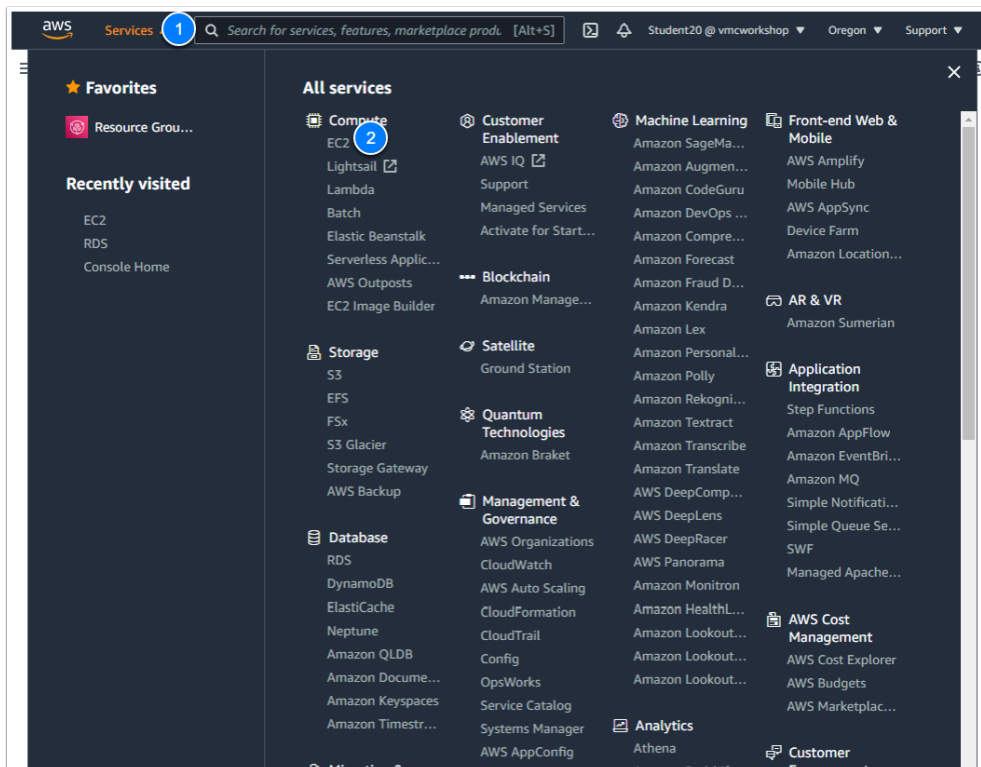
**Note:** VMware Cloud on AWS establishes routing in the default VPC Security Group, only RDS can leverage this or create its own

### Task 3.2.1 - 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

- Click on **EC2** under **Compute**
- In the upper left-hand corner move the **slider left** to close the New EC2 Experience page  
If you get the Feedback to EC2 dialog, click **Cancel**



- From the EC2 Dashboard navigate to the **Network & Security** menu in the left panel then click **Network Interfaces**.
- All Student environments belong to the same AWS account, therefore, hundreds of ENI's may exist.  
In order to minimize the view type **RDS** in the search area and press Enter to add a filter
- Expand the **Security Group** column to see the names or the **Primary Private IPv4** column (the 2nd and 3rd number in the 2nd octet corresponding to your student number) and to find your **VMCEXPERT#-XX-RDS-Inbound** security group corresponding to your student number.
- Check the box to your corresponding RDS SG as found in the steps above  
**Note: In the screenshot below <vmcexpert3-01-RDS-Inbound>**
- Once selected, look in the details pane below to find the **Primary private IPv4 IP**. Copy this address to your notes for the next step



**Network interfaces (1/3)** Info

search: 3-01 X Clear filters

	Name	Network inter...	Subnet ID	VPC ID	Avai...	Security groups	Description
<input checked="" type="checkbox"/>	-	eni-01e004b96ce...	subnet-00e67a7...	vpc-0c3483b34...	eu-cent...	VMCEXP3-01-RDS-Inbound	RDSNetwork
<input type="checkbox"/>	-	eni-0d5aac5f85d...	subnet-00e67a7...	vpc-0c3483b34...	eu-cent...	VMCEXP3-01-EFS-SG	EFS mount t
<input type="checkbox"/>	-	eni-03a22c5e3a8...	subnet-00e67a7...	vpc-0c3483b34...	eu-cent...	VMCEXP3-01-ALB-SG	ELB app/VM

Source/dest. check: True

IP addresses

Private IPv4 address	Private IPv4 DNS	Elastic Fabric Adapter
172.101.5.47	ip-172-101-5-47.eu-central-1.compute.internal	False
Public IPv4 address	Public IPv4 DNS	IPv6 addresses
-	-	-
Secondary private IPv4 addresses	Association ID	Elastic IP address owner
-	-	-
MAC address		
02:7e:c8:69:d4:68		
Instance details		

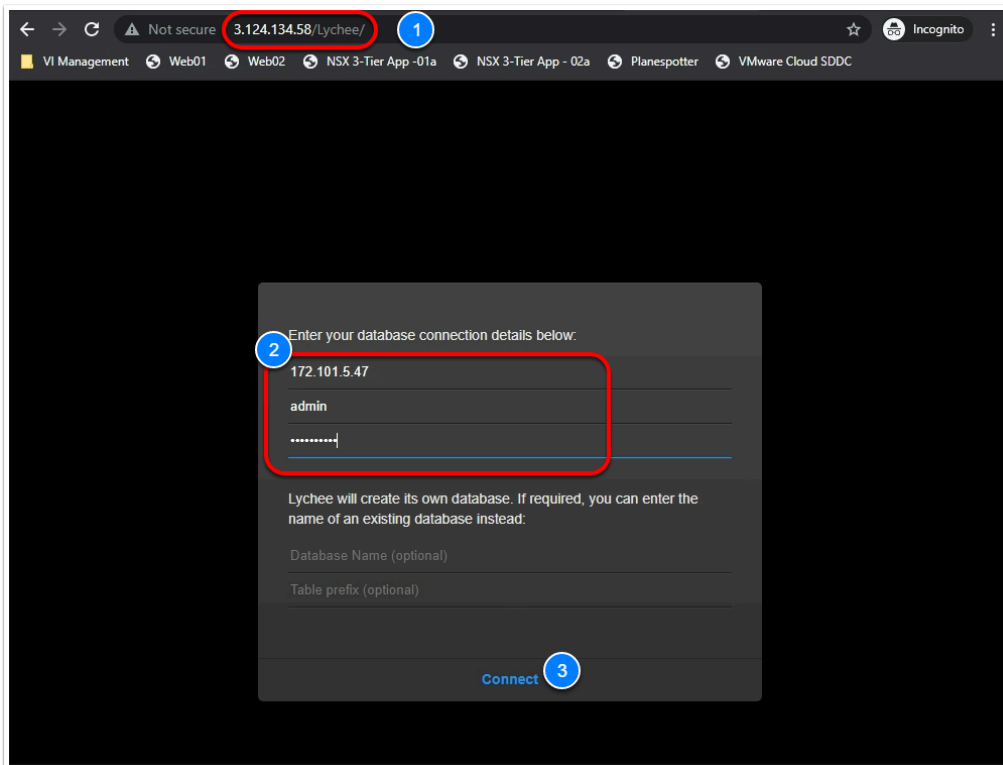
## Task 3.3 - Configure & Test the PhotoApp against the AWS RDS

You will now access the PhotoApp and update its 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.

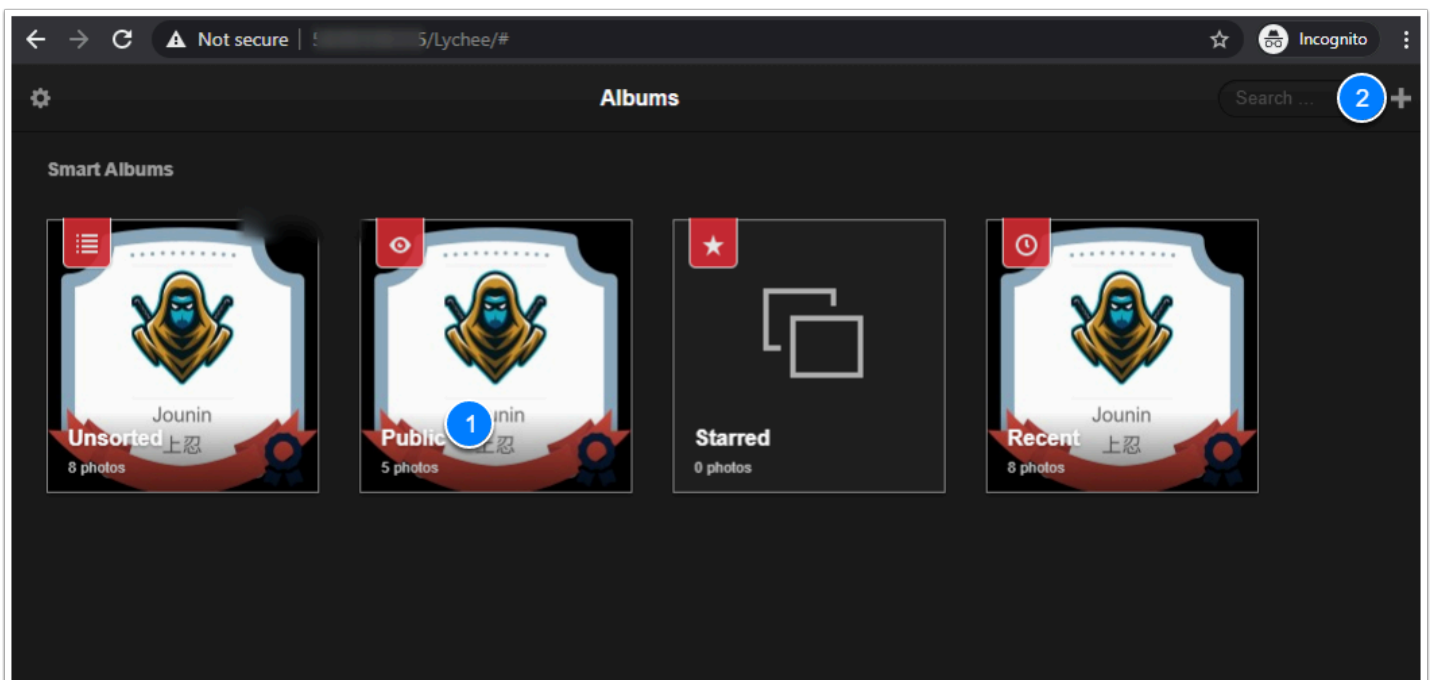
1. On your smart phone (tablet or personal computer), open up a browser and type your public IP address you requested in the VMware Cloud on AWS portal in the browser address bar followed by /Lychee (case sensitive) ie: **1.2.3.4/Lychee**

**NOTE:** This is the IP You used to setup the NAT Rule for webserver01 (Task 2.1.1, Steps 3 - 6). See your worksheet, if you recorded it there.

2. Enter the database connection information below (**case sensitive**), using the IP address (Primary Private IP) you noted in the previous task from the RDS ENI:
  - Database Host: **x.x.x.x**
  - Database Username: **admin**
  - Database Password: **<AWS Console PW provided By your instructor>**
3. Click **connect** (Username and Password are Case-Sensitive)



4. In the 'Enter a username and password for your installation dialog type
  - **admin**
  - **AWS Console PW provided By your instructor (you will use this PW to login in the upcoming lab tasks so ensure you set it with appropriate case)**
5. Click **Create Login**
6. Upload a few images into the Public folder



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.

## 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.

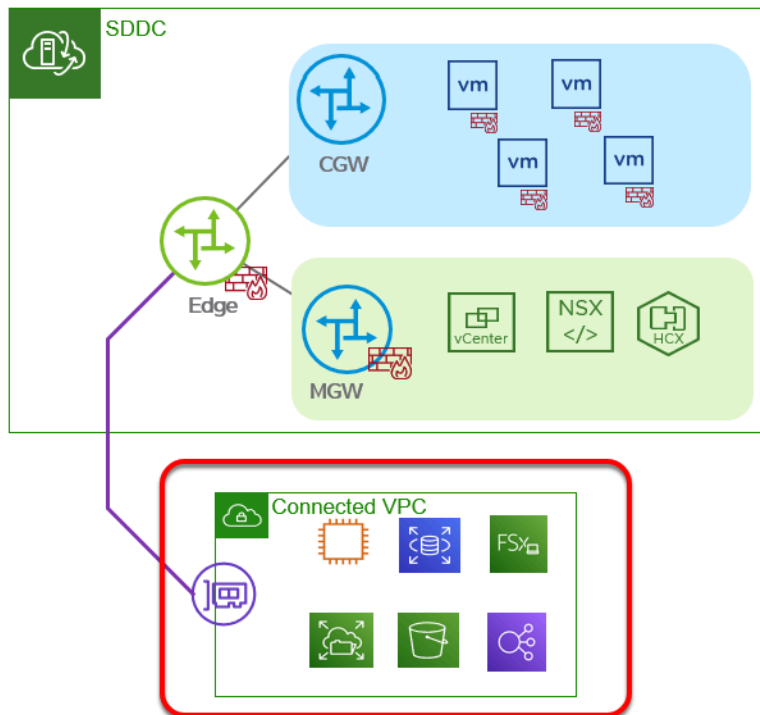
## OPTIONAL LABS

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)



- i** 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.

## Optional 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

### 💡 Prerequisites:

- Configure Compute Gateway Firewall Rules for Elastic Network Interface (ENI) traffic
- Configure AWS Security Groups to allow traffic to/from VMware Cloud on AWS (VMC)
- Amazon supports this for Linux operating systems only at this time.

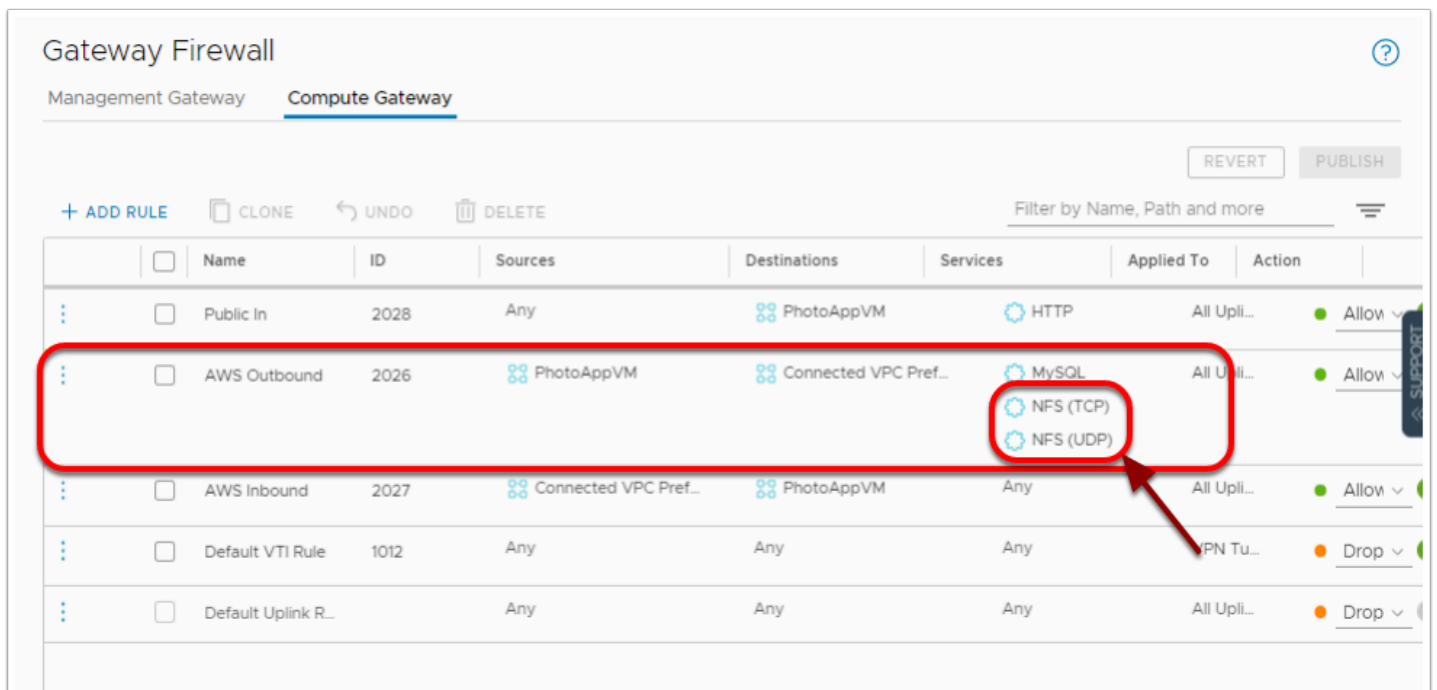
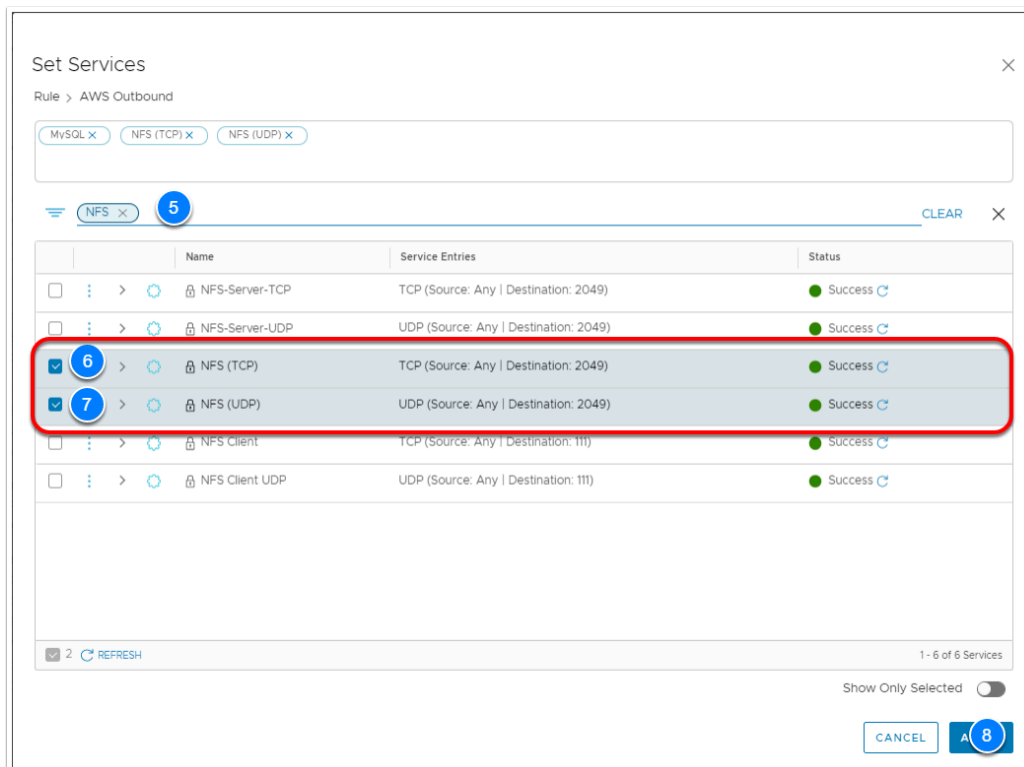
## Task 1 - Configure VMC on AWS Gateway Firewall Rules

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. In the VMC on AWS Console Click the **Networking & Security** tab
2. Click **Gateway Firewall**
3. Click **Compute Gateway**
4. Hover over the **Services** field of the **"AWS Outbound"** Rule and Click the **Edit** (Pencil Icon)
5. In the Search field of the Set Services Dialog Type **NFS** & Press Enter
6. Select **NFS(TCP)** & **NFS(UDP)**
7. Click **Apply**
8. Click **Publish**

The screenshot shows the VMware Cloud on AWS console interface. The left sidebar contains navigation tabs: Summary, Networking & Security (selected), Add Ons, Maintenance, Troubleshooting, Settings, and Support. Under Networking & Security, there are sub-tabs: Overview, Network (Segments, VPN, NAT, Tier-1 Gateways, Transit Connect), Security (Gateway Firewall (selected), Distributed Firewall), Inventory (Groups, Services, Virtual Machines), Tools (IPFIX, Port Mirroring), and System (DNS, DHCP, Global Configuration). The main content area is titled 'Gateway Firewall' and has two sub-tabs: Management Gateway and Compute Gateway (selected). Below the sub-tabs are buttons for '+ ADD RULE', 'CLONE', 'UNDO', and 'DELETE'. A table lists the firewall rules. The 'AWS Outbound' rule is highlighted, and the 'Services' field is being edited to add NFS.

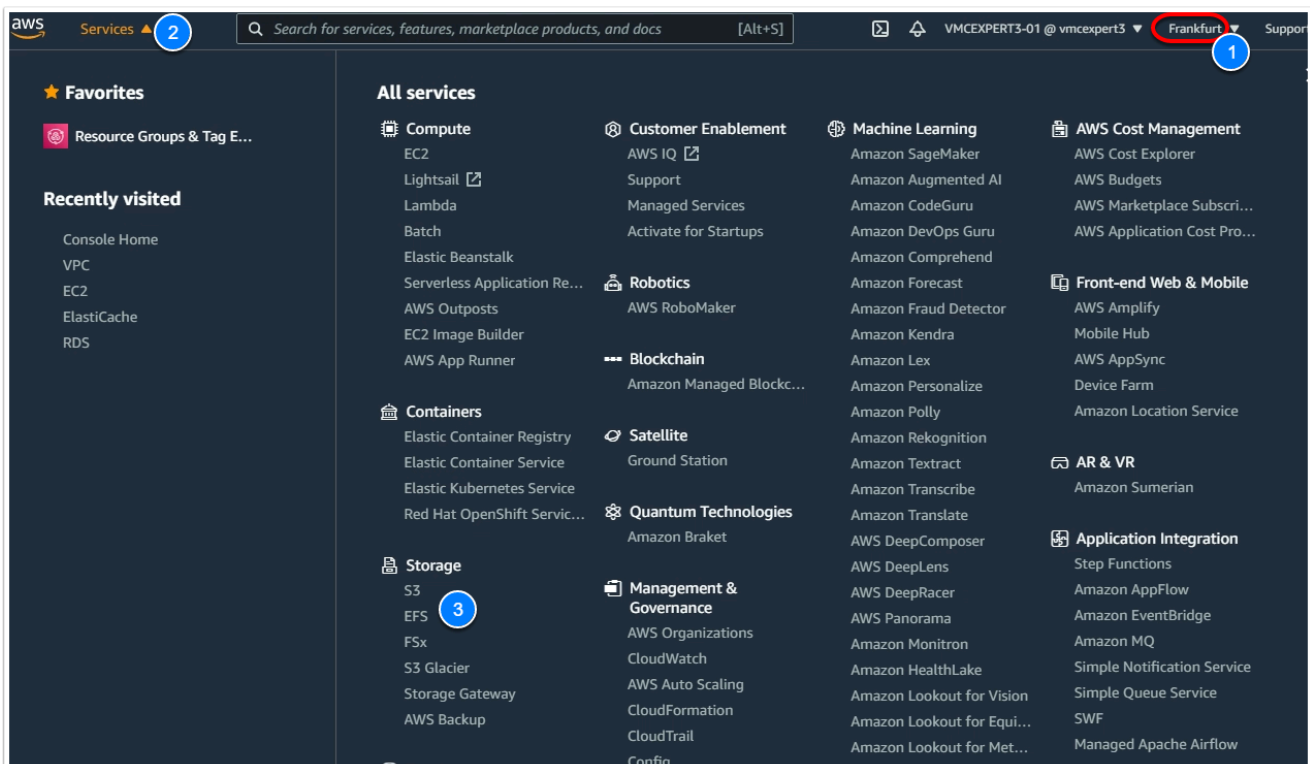
	Name	ID	Sources	Destinations	Services	Applied To	Action
<input type="checkbox"/>	Public In	2028	Any	PhotoAppVM	HTTP	All Upli...	Allow
<input type="checkbox"/>	AWS Outbound	2026	PhotoAppVM	Connected VPC Pref...	MySQL	All Upli...	Allow
<input type="checkbox"/>	AWS Inbound	2027	Connected VPC Pref...	PhotoAppVM	Any	All Upli...	Allow
<input type="checkbox"/>	Default VTI Rule	1012	Any	Any	Any	VPN Tu...	Drop
<input type="checkbox"/>	Default Uplink R...		Any	Any	Any	All Upli...	Drop



## 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 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 then select **Storage > EFS**
5. In the list of file systems find your EFS (**VMCExpert#-xx**, where **#** is the Environment ID, and **xx** is your student number)
6. Click **<your EFS Instance> vmcexpert#-xx** text to view its details
7. Click the **Network** tab
8. Record the IP address of your EFS (e.g. **172.120.14.147**)
9. **Note: You will need this IP to mount the share in your Webserver01 VM**



Amazon EFS > File systems > fs-776cdf2c

## VMCEXP3-01 (fs-776cdf2c)

[Delete](#) [Attach](#)

**General** [Edit](#)

Performance mode	Automatic backups
General Purpose	⊖ Disabled
Throughput mode	Encrypted
Bursting	b5a38020-0d60-457f-afab-9c6a9a3a83a9 (aws/elasticfilesystem)
Lifecycle policy	File system state
30 days since last access	✔ Available
Availability zone	
Regional	

Metered size | Monitoring | Tags | File system policy | Access points | **Network** <sup>4</sup>

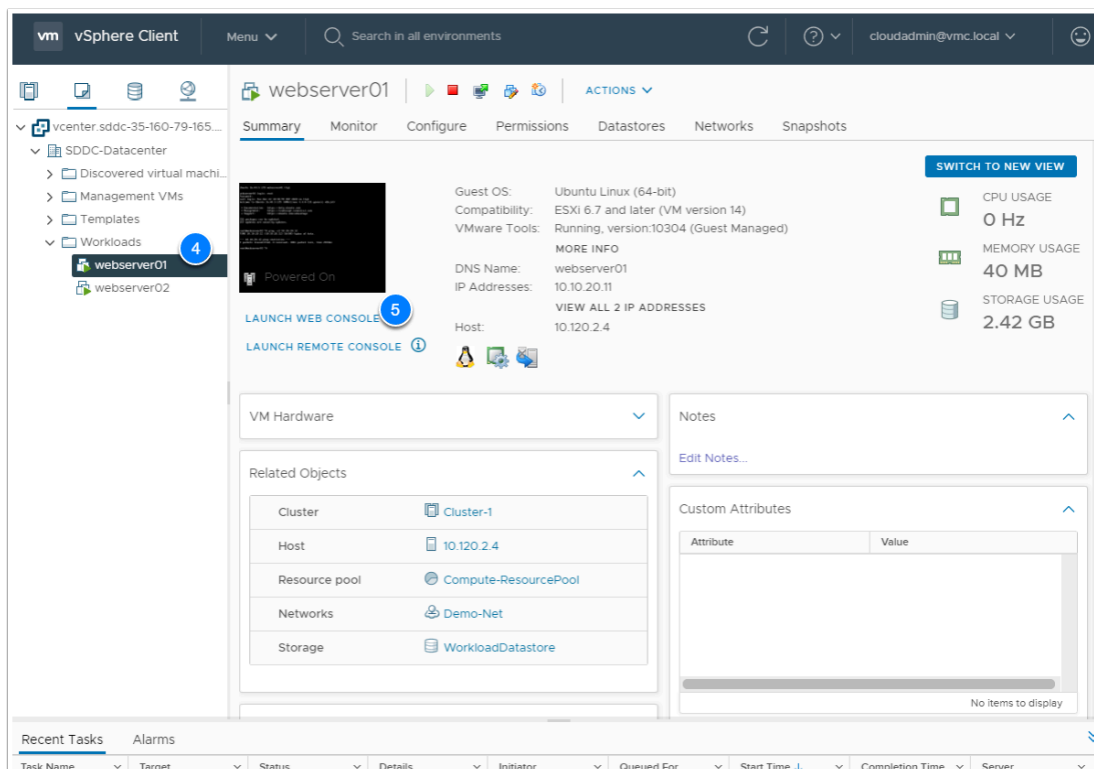
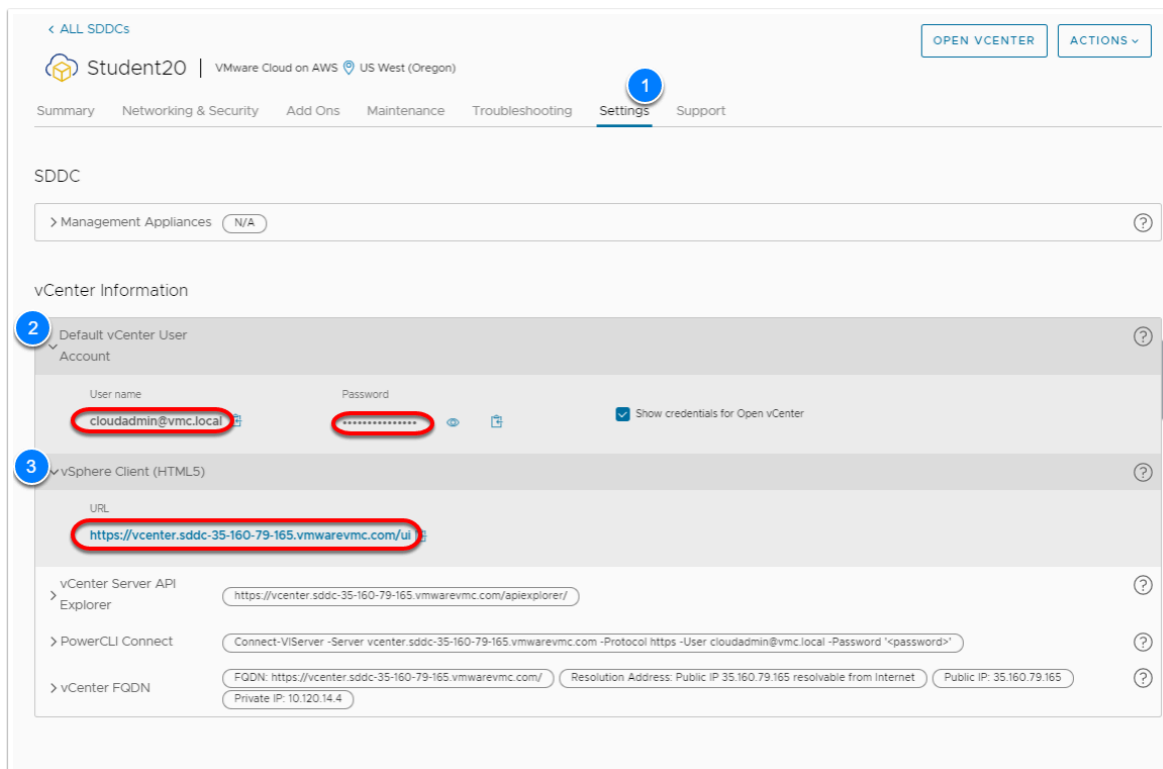
**Network** [Manage](#)

Availability zone ▲	Mount target ID ▼	Subnet ID ▼	Mount target state ▼	IP address ▼	Network interface ID ▼	Security groups ▼
eu-central-1a	fsmt-d1b15489	subnet-0b62de2afd74c5e8d	✔ Available	172.101.2.86 <sup>5</sup>	eni-0cc170312765b2ae0	sg-0669905d742f1513f (VMCEXP3-01-EFS-SG)

## 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. **NOTE: You can access the vCenter Information and login details from the settings tab of the VMC on AWS Console**
3. Select **webserver01**
4. Click **LAUNCH WEB CONSOLE**
5. In the browser tab for webserver01. if needed, Log in as
6. login: **root**
7. password: **VMware1!**

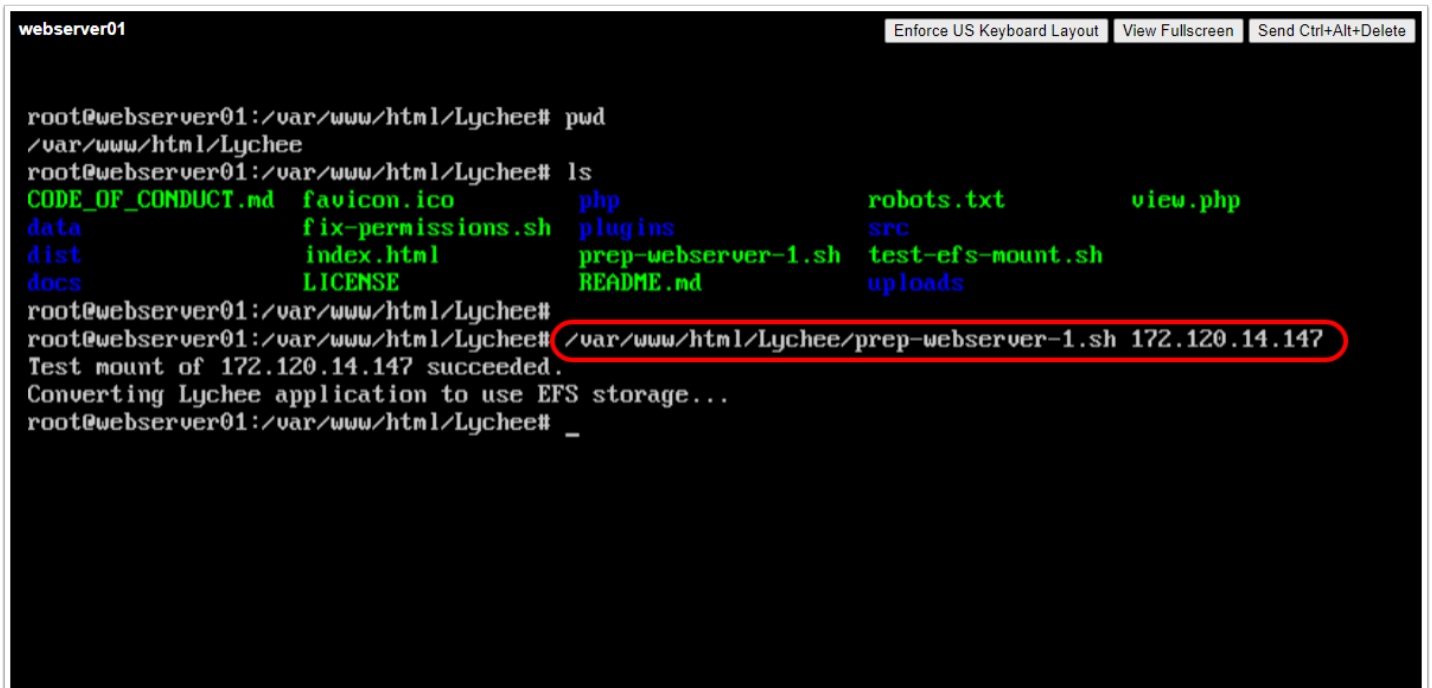




8. At the shell prompt enter the following commands (note, your current directory **must** be /var/www/html/Lychee for the prep-webserver-1.sh script to work correctly - make sure to run the cd command as shown):

```
<p>cd /var/www/html/Lychee  
./prep-webserver-1.sh <your_efs_ip></your_efs_ip></p>
```

📄 Click to copy



```
webserver01
root@webserver01:/var/www/html/Lychee# pwd
/var/www/html/Lychee
root@webserver01:/var/www/html/Lychee# ls
CODE_OF_CONDUCT.md  favicon.ico      php              robots.txt      view.php
data                fix-permissions.sh  plugins          src
dist                index.html       prep-webserver-1.sh  test-efs-mount.sh
docs                LICENSE          README.md          uploads
root@webserver01:/var/www/html/Lychee# /var/www/html/Lychee/prep-webserver-1.sh 172.120.14.147
Test mount of 172.120.14.147 succeeded.
Converting Lychee application to use EFS storage...
root@webserver01:/var/www/html/Lychee# _
```

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

to view the operations performed by the script let's take a look at the script

```
<p>cat /var/www/html/Lychee/prep-webserver-1.sh</p>
```

📄 Click to copy

```
webserver01
Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

root@webserver01:/var/www/html/Lychee# ls
CODE_OF_CONDUCT.md  favicon.ico  php  robots.txt  uploads-bak
data                fix-permissions.sh  plugins  src  view.php
dist                index.html  prep-webserver-1.sh  test-efs-mount.sh
docs                LICENSE  README.md  uploads

root@webserver01:/var/www/html/Lychee#
root@webserver01:/var/www/html/Lychee# cat /var/www/html/Lychee/prep-webserver-1.sh
#!/bin/bash
if [ $# == 0 ]; then
    echo "Usage: $0 [EFS IP Address]"
    exit 0
fi
mount -t nfs4 $1:/ /mnt
if [ $? == 0 ]; then
    echo "Test mount of $1 succeeded."
    umount /mnt
    echo "Converting Lychee application to use EFS storage..."
    mv uploads uploads-bak
    mkdir uploads
    mount -t nfs4 $1:/ uploads
    chown www-data:www-data uploads
    chmod 775 uploads
    cd uploads-bak
    cp -rp * ../uploads
    echo "$1:/var/www/html/Lychee/uploads nfs4 rw 0 0" >> /etc/fstab
else
    echo "Mount $1 failed."
fi
root@webserver01:/var/www/html/Lychee#
```

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

```
<p>ls /var/www/html/Lychee/uploads/big</p>
```

 Click to copy

```
webserver01
Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

root@webserver01:/var/www/html/Lychee# ls
CODE_OF_CONDUCT.md  favicon.ico  php  robots.txt  uploads-bak
data                fix-permissions.sh  plugins  src  view.php
dist                index.html  prep-webserver-1.sh  test-efs-mount.sh
docs                LICENSE  README.md  uploads

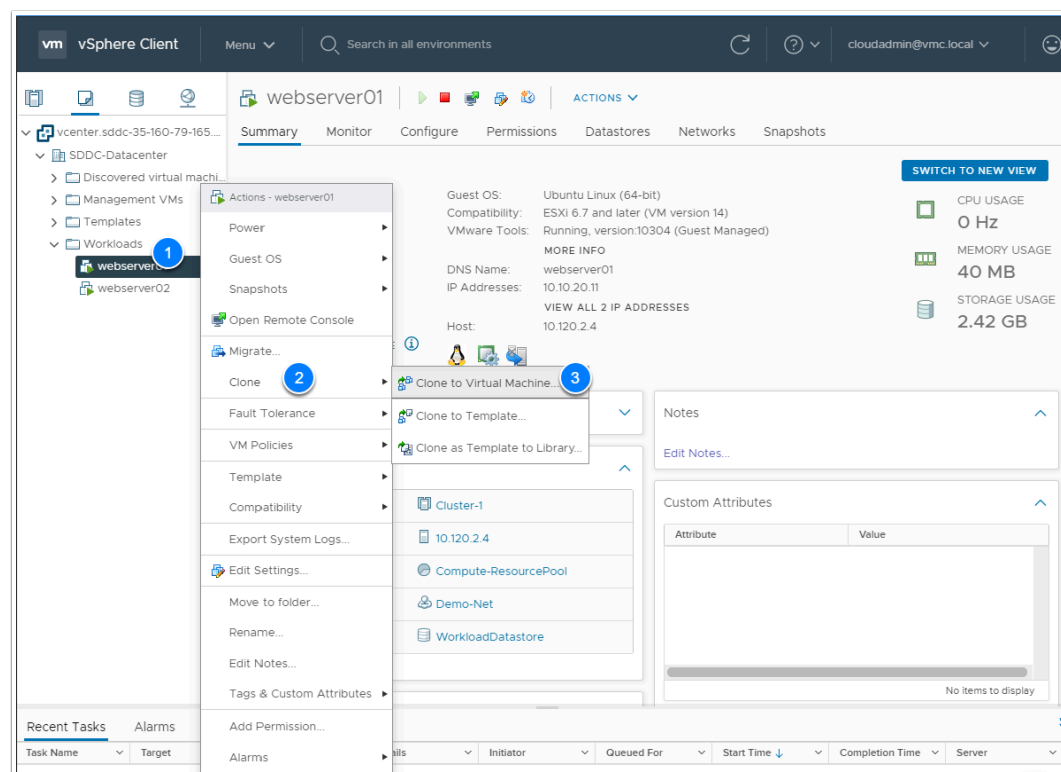
root@webserver01:/var/www/html/Lychee#
root@webserver01:/var/www/html/Lychee# ls /var/www/html/Lychee/uploads/big/
70d59d954dd7975d6e2c7772f1b1797c.jpg  a1cad9c9d16dbb47c373bbeb8377c3d4.png  index.html
87a27fb640da93a9744f6af4bdc1598a.png  d30d4e4148775338ef4d6b541a248d6d.jpg

root@webserver01:/var/www/html/Lychee#
```

## 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 central repository as webserver01.

1. In the vSphere Client Select and right-click **webserver01**
2. Select **clone --> Clone to Virtual Machine**
3. On the **Select a Name and Folder** page name the **virtual machine name** enter **webserver03**
4. Expand the SDDC > SDDC DC > and highlight Workloads
5. Click Next
6. On the **Select a Compute Resource** page select the **Compute-ResourcePool**
7. Click Next
8. On the **Select Storage** page select the **WorkloadDatastore**
9. Click next
10. On the **Select Clone Options** page click the following check-boxes
  - **Customize the operating system**
  - **Do not Select Power on virtual machine after creation**
11. Click **Next** to continue.
12. On the **Customize Guest OS** page select the **LinuxSpec** customization specification.
13. Click **Next** to continue.
14. Review the information for accuracy and click **Finish** to clone the virtual machine.



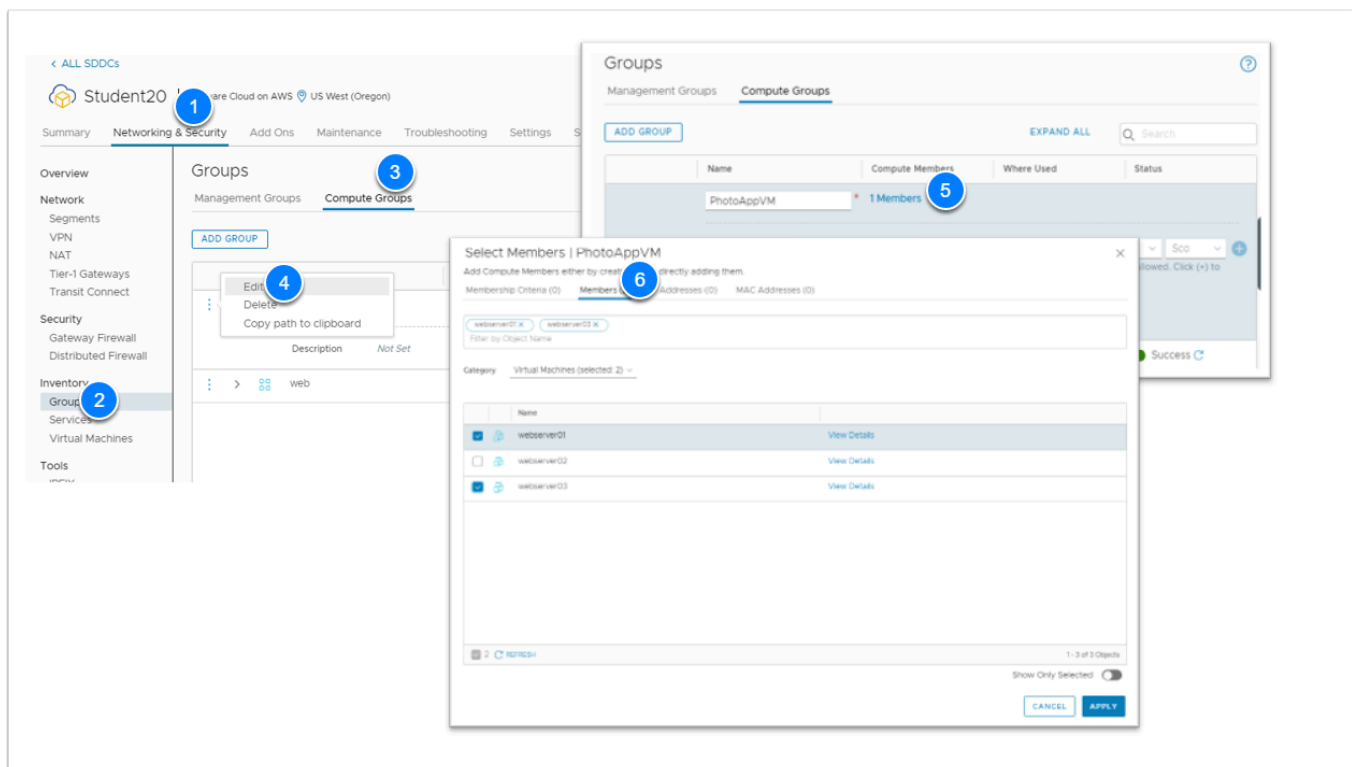
**i** It should take a couple of minutes for the virtual machine to clone. While this happens upload a couple of additional images to the Public Gallery from webserver01

## 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 VMC on AWS SDDC Console click the **Networking & Security** 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**

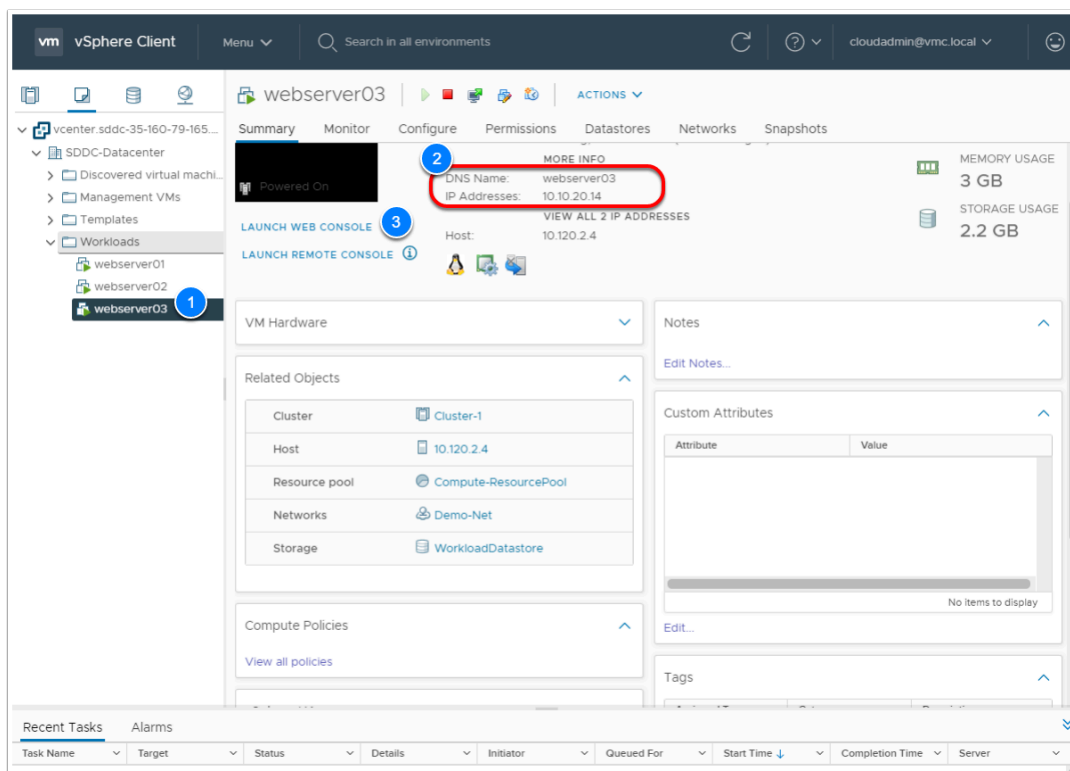
The clone of webserver03 should be complete by now. In the vSphere Client select **webserver03** and power it on (or reboot it if it's already powered on).



❗ **NOTE:** If the VM powered-on before you modified the group in the steps above, you'll need to reboot it before proceeding

## Task 4.2 - Verify Access to NFS from webserver03

1. Select **webserver03**
2. Review and record **webserver03 IP address** (You'll need this IP when creating a NAT rule for webserver03)
3. Click **LAUNCH WEB CONSOLE**
4. In the browser tab for webserver03. Log in as
5. login: **root**
6. password: **VMware1!**



6. At the shell prompt enter the following commands

```
<p>mount | grep nfs</p>
```

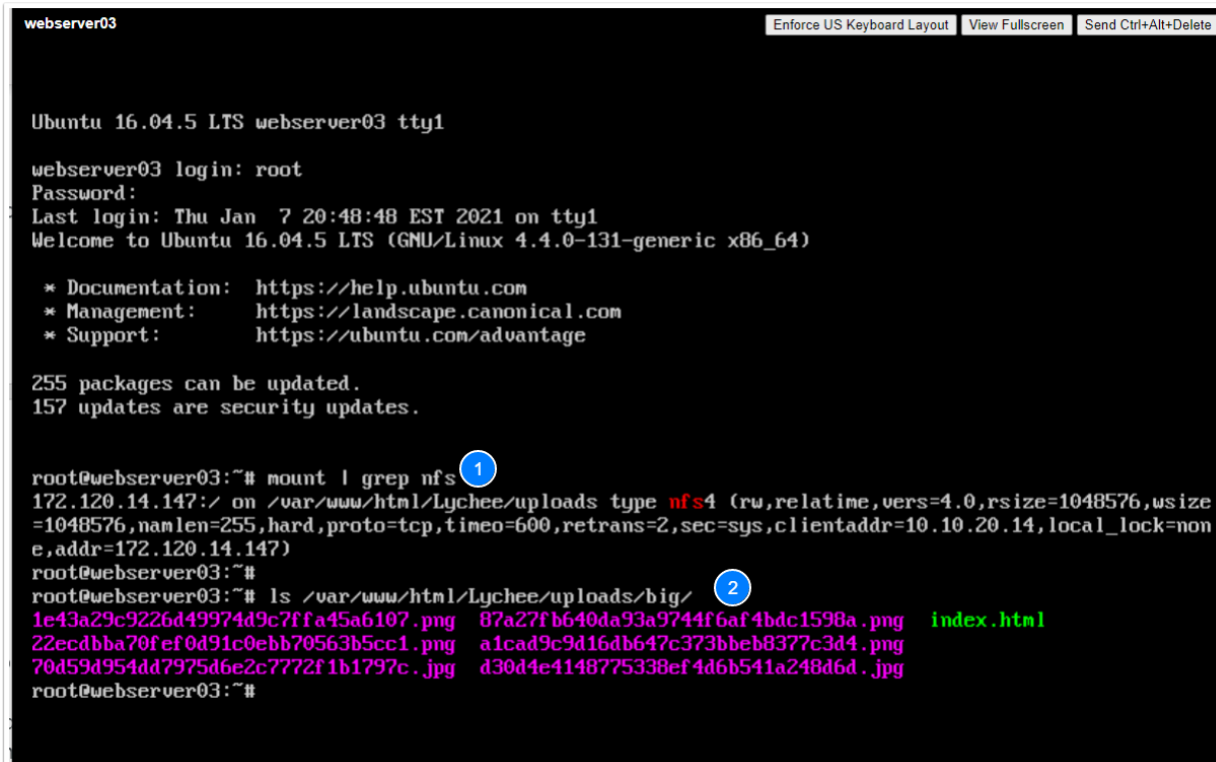
 Click to copy

You should see a mount point at **/var/www/html/Lychee/uploads**

```
<p>ls /var/www/html/Lychee/uploads/big/</p>
```

📄 Click to copy

You should see the two additional files you uploaded in the previous task



The terminal window shows the following commands and output:

```
webserver03 login: root
Password:
Last login: Thu Jan  7 20:48:48 EST 2021 on tty1
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

255 packages can be updated.
157 updates are security updates.

root@webserver03:~# mount | grep nfs ①
172.120.14.147:/ on /var/www/html/Lychee/uploads type nfs4 (rw,relatime,vers=4.0,rsz=1048576,wsz=1048576,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=10.10.20.14,local_lock=none,addr=172.120.14.147)
root@webserver03:~#
root@webserver03:~# ls /var/www/html/Lychee/uploads/big/ ②
1e43a29c9226d49974d9c7ffa45a6107.png  87a27fb640da93a9744f6af4bdc1598a.png  index.html
22ecdbba70fef0d91c0ebb70563b5cc1.png  a1cad9c9d16db647c373bbeb8377c3d4.png
70d59d954dd7975d6e2c7772f1b1797c.jpg  d30d4e4148775338ef4d6b541a248d6d.jpg
root@webserver03:~#
```

## Optional 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.

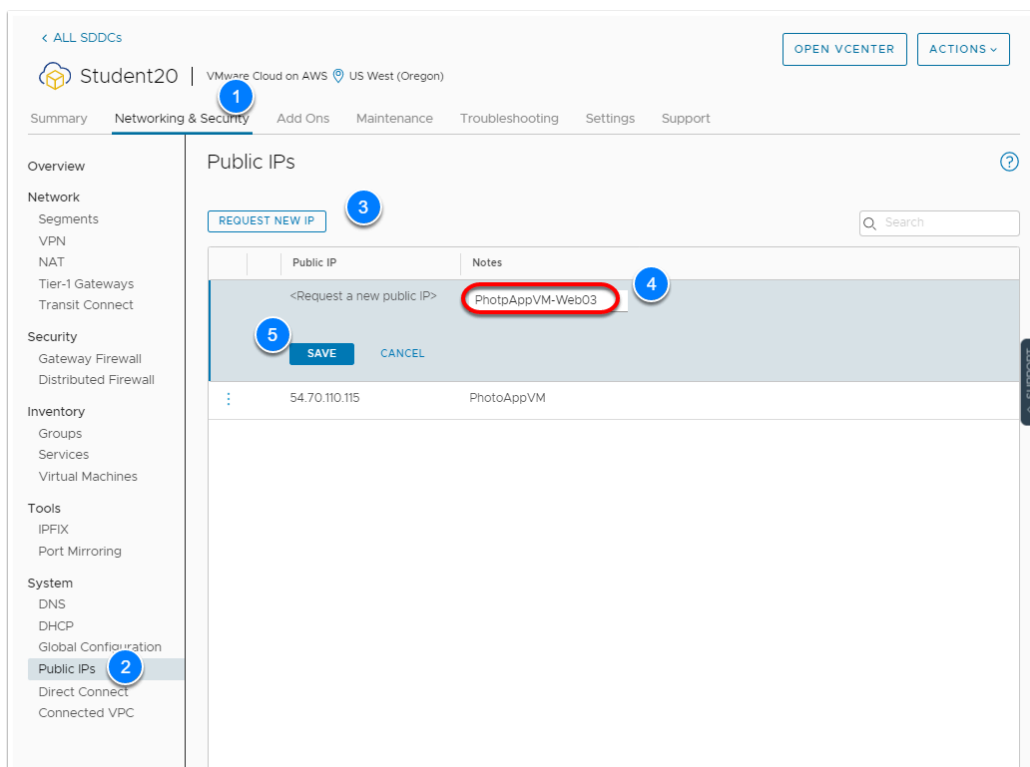
In this session we will load balance webserver01 and webserver03 (PhotoAppVM). We will then test connectivity to the PhotoVMApp via the Amazon Application Load-Balancer.

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 - Request a public IP for Webserver03

Make sure you're logged into the VMC on AWS Console, and viewing the details of your SDDC (VMCEXPERT#-XX)

1. Click the **Networking and Security** Tab
2. Click **Public IPs**
3. Click **REQUEST NEW IP**
4. In the Noted Field type **PhotoAppVM-Web03**
5. Click **Save**
6. Record the Newly requested Public IP, you will use it to Configure the NAT rule for webserver03





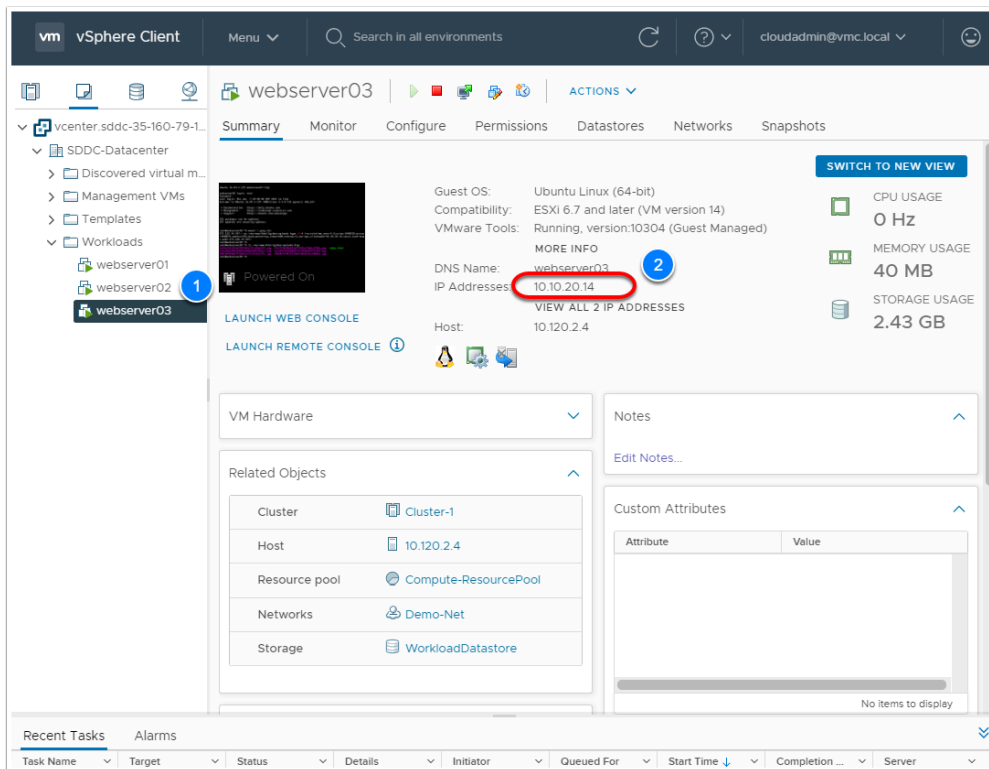
The screenshot shows the VMware Cloud on AWS console interface. The top navigation bar includes a link to 'ALL SDDCs', the 'Student20' logo, and the text 'VMware Cloud on AWS US West (Oregon)'. There are buttons for 'OPEN VCENTER' and 'ACTIONS'. The main navigation menu on the left includes 'Summary', 'Networking & Security' (selected), 'Add Ons', 'Maintenance', 'Troubleshooting', 'Settings', and 'Support'. Under 'Networking & Security', there are sub-menus for 'Overview', 'Network' (with 'Segments', 'VPN', 'NAT', 'Tier-1 Gateways', and 'Transit Connect'), 'Security' (with 'Gateway Firewall' and 'Distributed Firewall'), and 'Inventory' (with 'Groups', 'Services', and 'Virtual Machines'). The main content area is titled 'Public IPs' and features a 'REQUEST NEW IP' button and a search bar. A table lists public IP addresses with columns for 'Public IP' and 'Notes'. The first row shows a public IP ending in '.87' with the note 'PhotpAppVM-Web03', which is highlighted by a red circle. A blue circle with the number '6' is positioned to the left of this row. The second row shows a public IP ending in '.115' with the note 'PhotoAppVM'. A 'SUPPORT' button is visible on the right side of the table.

Public IP	Notes
...87	PhotpAppVM-Web03
...0.115	PhotoAppVM

## Task 2 - Setup a NAT rule for Webserver03

To setup a NAT rule we need the Public IP (which you already requested and recorded in the previous task) and the Private IP of webserver03. We will begin this task by confirming the IP address of webserver03

1. In the vSphere Client Click **webserver03**
2. From the summary screen view and record the **IP address** of Webserver03
3. On the Networking and Security tab Click **NAT**
4. Click **ADD NAT RULE**
  1. Type **PhotoApp-Web03 NAT** in the Name field
  2. Select **<your Newly requested Public IP>** in the Drop-down field for Public IP
  3. Type the **<Private IP for webserver03>** in the Internal IP field (10.10.x.x)
  4. Click **Save**.



If needed, you can access the vSphere Client URL and cloudadmin username and password from the Settings tab of the VMC on AWS Console

< ALL SDDCs

Student20 | VMware Cloud on AWS US West (Oregon)

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Overview

Network

Segments

VPN

NAT

Tier-1 Gateways

Transit Connect

Security

Gateway Firewall

Distributed Firewall

Inventory

Groups

Services

Virtual Machines

Tools

IPFIX

Port Mirroring

System

DNS

## NAT

Internet

ADD NAT RULE

EXPAND ALL

Search

Name	Public IP	Service	Public Port	Internal IP	Internal Port	Firewall	Status
PhotoApp-1	54.70.110.115	All Traffic	Any	10.10.20.14	Any	Match Internal Address	Success

Logging: No

Rule Enabled: Yes

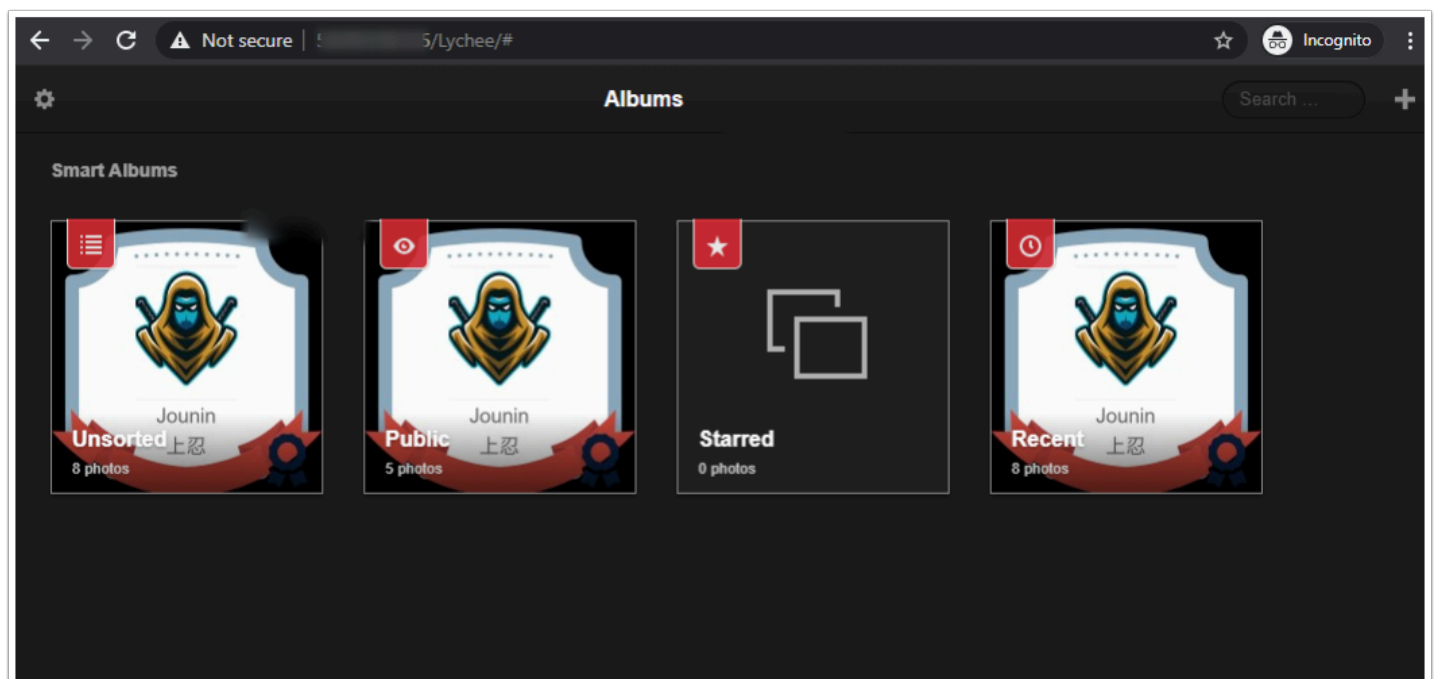
SAVE CANCEL

PhotoApp NAT 54.70.110.115 Any Any 10.10.20.11 Any Match Internal Address Success

On your Phone or Computer access the PhotoApp on webserver03 by typing **http://<Public ip>/Lychee** in your browser.

When prompted to login, enter (if not prompted select the arrow at the top left)

1. **admin**
2. **<AWS Console Password Provided by your instructor>** for Password
3. Click **Sign In**



## Task 3 - Configure AWS Native ALB to load balance PhotoApp

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)

Account ID or alias: **vmcexpert{#} i.e vmcexpert1**

IAM user name: **VMCEXPERT#-XX**(where # is the Environment ID and xx is the number assigned to you)

Password: **<AWS Console PW provided By your instructor>**

Click **Sign In**

### Task 3.1 - Add Web Servers to the Amazon Application Load Balancer

1. In the upper left-hand Click **Services** then **EC2**
2. In the upper left-hand corner move the **slider Right** to enable the **New EC2 Experience** page

**NOTE:** In the previous lab, we disabled "New EC2 Experience" dashboard. This steps reverts back to the "New EC2 Experience". Not enabling this mode will cause a mismatch between the lab steps and your interface.

2. In the Left pane under Load Balancing, Click **Target Groups**
3. Find and click the text for your target group <vmcexpert#-xx-default> (where **XX** is your student number)

The screenshot shows the AWS Management Console interface. In the left-hand navigation pane, under the 'Load Balancing' section, 'Target Groups' is selected and marked with a blue circle containing the number '1'. The main content area displays the 'Target groups (1/2)' page. A table lists the target groups, with the first row, 'VMCEXP3-01-default', highlighted by a red circle and a blue circle containing the number '2'. The table columns include Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. Below the table, the details for the selected target group 'VMCEXP3-01-default' are shown, including its ARN, target type (IP), protocol (HTTP), and VPC ID.

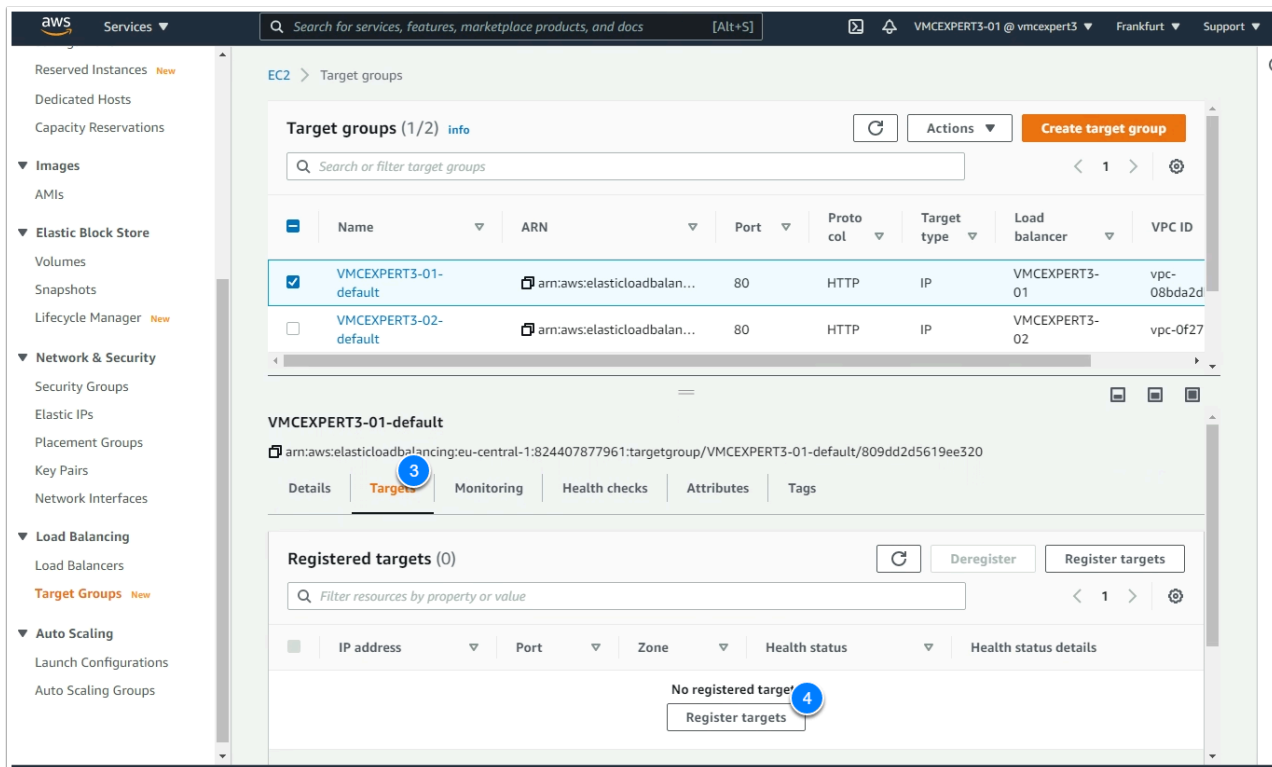
Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
VMCEXP3-01-default	arn:aws:elasticloadbalancing:eu-central-1:824407877961:targetgroup/VMCEXP3-01-default/809dd2d5619ee320	80	HTTP	IP	VMCEXP3-01	vpc-08bda2db
VMCEXP3-02-default	arn:aws:elasticloadbalancing:eu-central-1:824407877961:targetgroup/VMCEXP3-02-default/809dd2d5619ee320	80	HTTP	IP	VMCEXP3-02	vpc-0f27...

**VMCEXP3-01-default**  
arn:aws:elasticloadbalancing:eu-central-1:824407877961:targetgroup/VMCEXP3-01-default/809dd2d5619ee320

**Details**

Target type IP	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-08bda2db256077d7d
Load balancer VMCEXP3-01			

3. Click the **Targets** tab
4. Click **Register targets**



5. In the Network Drop-Down list, select **Other Private IP address**
6. In the IP Field Enter the **<Private IP address of Webserver01>**
7. Click **Include as pending below**
8. Repeat steps 6 & 7, this time using the **<Private IP for webserver03>**
9. Click **Register pending targets**
10. Wait 10-20 seconds, click the refresh circle, the status should turn from **'initial'** to **'healthy'**

aws Services Search for services, features, marketplace products, and docs [Alt+S] Student20 @ vmcworkshop Oregon Support

EC2 > Target groups > Student20-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 and ports to the list of pending targets. Once you are satisfied with your selections, click Register pending targets.

**IP addresses**  
Specify IP addresses from a network VPC or outside the VPC to register as targets.

Network  
Other private IP address 5

Availability Zone  
all

IP  
Enter a private IP address.  
10.10.20.11 6

Ports  
Ports for routing to this target.  
80

Allowed ranges  
.....

1-65535 (separate multiple ports with commas)

Include as pending below 7

2 selections are now pending below. Include more or register targets when ready.

**Targets (2)** Remove all pending

All Filter resources by property or value

Remove	Status	IP address	Port	Zone
X	Pending	10.10.20.14	80	all
X	Pending	10.10.20.11	80	all

2 pending Cancel Register pending targets

## Task 3.2 - Validate the Application Load Balancing

1. Click Load Balancers
2. Type <VMCEXPERT#-XX> in the Search field to Find your load balance, Where XX = your student number. i.e. VMCEXPERT3-01
3. Select the Load Balancer
4. From the Description tab copy the DNS name <VMCEXPERT#-XX-UID.(region).elb.amazonaws.com>

The screenshot shows the AWS Management Console interface for an Elastic Load Balancing (ELB) instance. At the top, there's a 'Create Load Balancer' button and an 'Actions' dropdown. Below this is a table listing ELB instances. The first instance, VMCEXP3-01, is selected. Below the table, the 'Load balancer: VMCEXP3-01' section is visible, with tabs for 'Description', 'Listeners', 'Monitoring', 'Integrated services', and 'Tags'. The 'Description' tab is active, showing the 'Basic Configuration' section. The 'DNS name' field is highlighted with a red circle, showing the value: VMCEXP3-01-888644610.eu-central-1.elb.amazonaws.com (A Record). Other fields include Name (VMCEXP3-01), ARN, State (Active), Type (application), Scheme (internet-facing), IP address type (ipv4), and VPC (vpc-08bda2db256077d7d).

Name	DNS name	State	VPC ID	Availability Zones	Type
VMCEXP3-01	VMCEXP3-01-888644610.eu-central-1.elb.amazonaws.com	Active	vpc-08bda2db256077d7d	eu-central-1b, eu-central-1a	application
VMCEXP3-02	VMCEXP3-02-407248310.eu-central-1.elb.amazonaws.com	Active	vpc-0f27782e03caa1f62	eu-central-1a, eu-central-1b	application

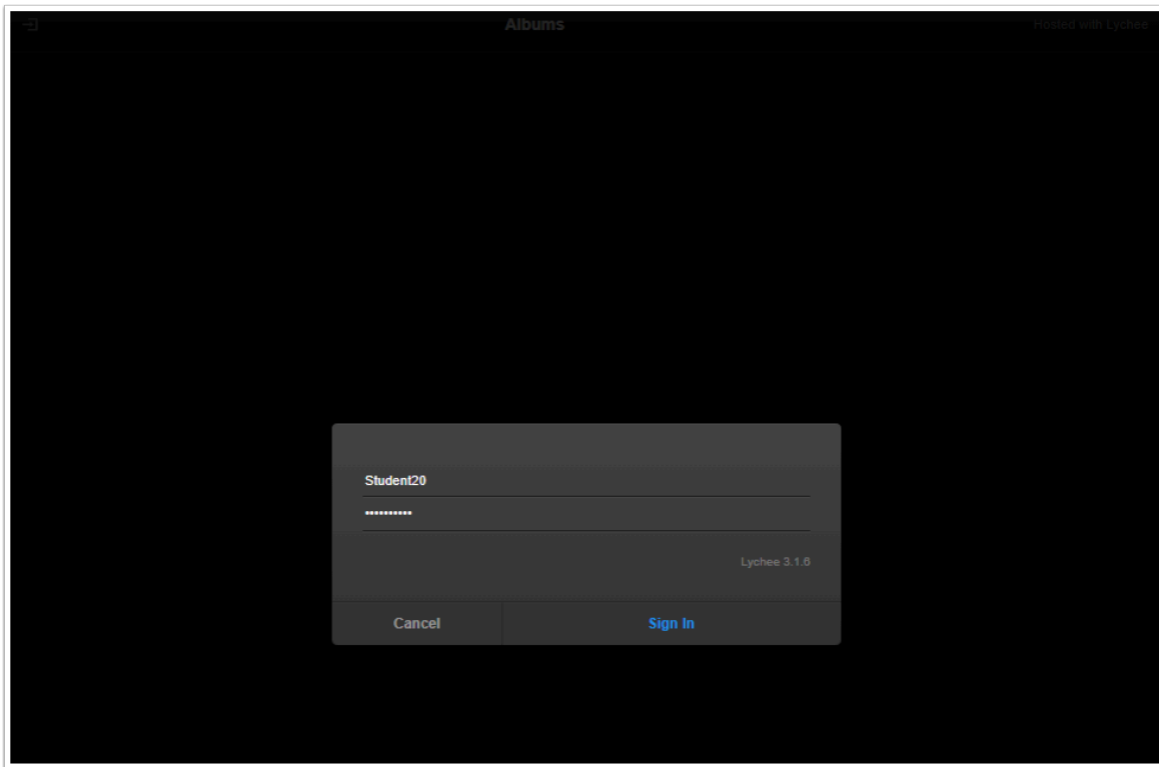
**Load balancer: VMCEXP3-01**

**Basic Configuration**

- Name:** VMCEXP3-01
- ARN:** arn:aws:elasticloadbalancing:eu-central-1:824407877961:loadbalancer/app/VMCEXP3-01/d89486a1b29fbd12
- DNS name:** VMCEXP3-01-888644610.eu-central-1.elb.amazonaws.com (A Record)
- State:** Active
- Type:** application
- Scheme:** internet-facing
- IP address type:** ipv4
- VPC:** vpc-08bda2db256077d7d

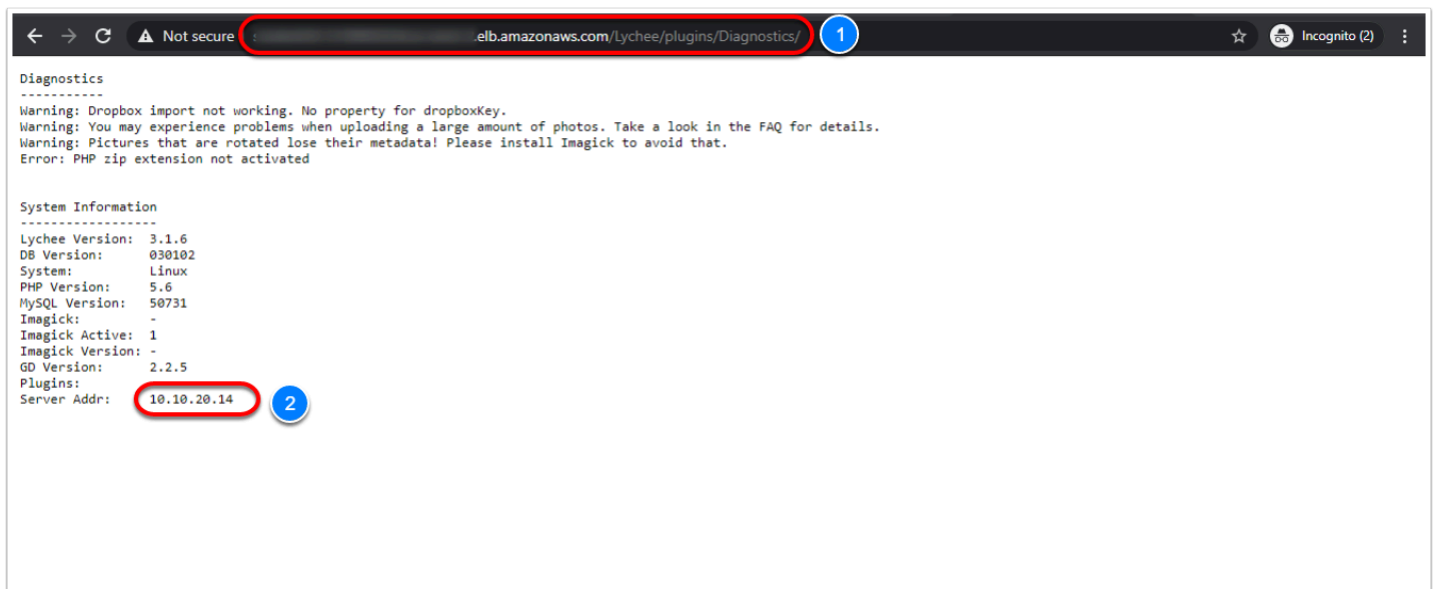
- Paste the **DNS Name** in your browser and append **/Lychee** to access the PhotoApp via ALB i.e. vmcexpert3-01-888644610.eu-central-1.elb.amazonaws.com/Lychee
- If you aren't prompted for a login, Click the exit icon in the upper-right hand of the application page
- When prompted to login in use the following:
  - admin** for Username (where XX is your student number)
  - <Password Provided by your instructor>** for Password
  - Click **Sign In**



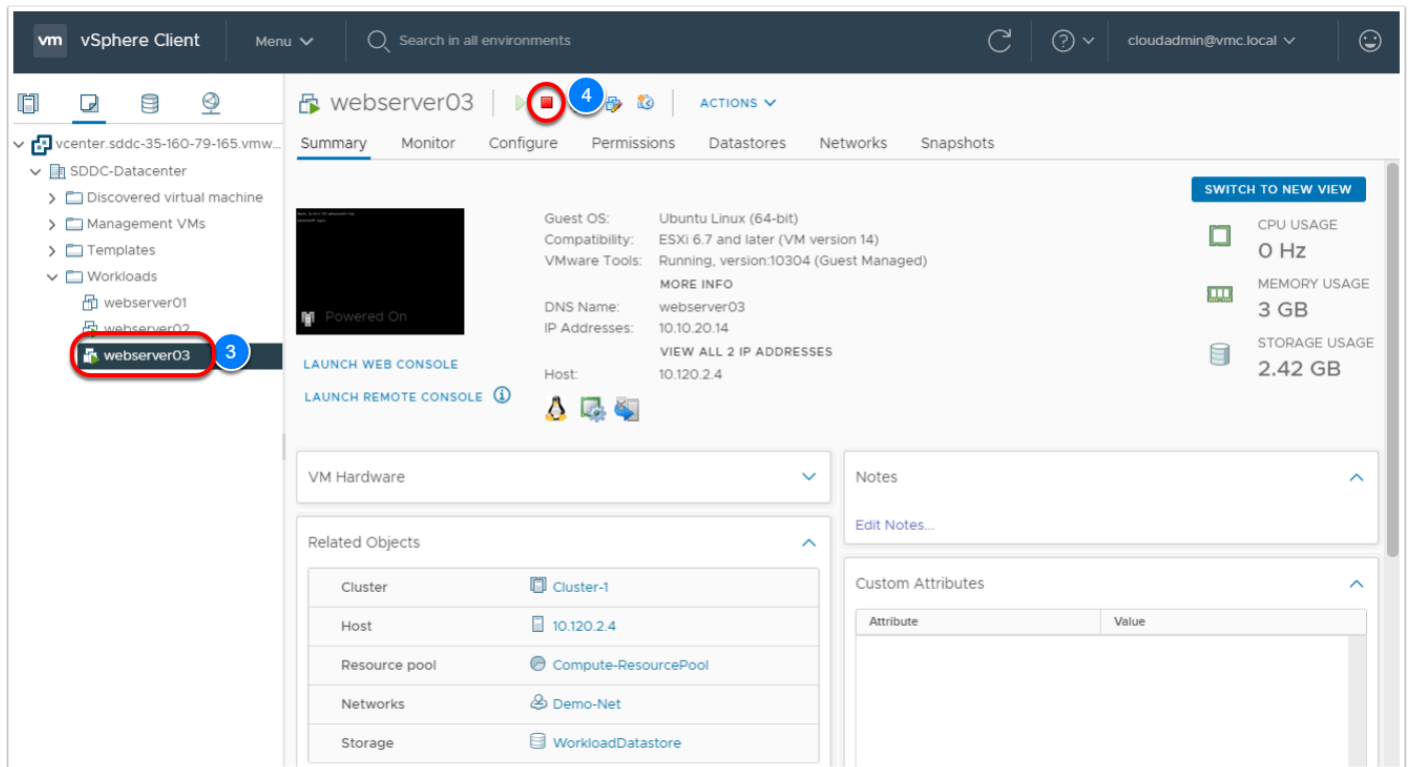


### Task 3.2.1 - Test Load Balancer functionality

1. In your browser type **<your ALB DNSName>/Lychee/plugins/Diagnostics** (Note Case-sensitivity)
2. i.e. student20-1218955224.us-west-2.elb.amazonaws.com/Lychee/plugins/Diagnostics/  
The output should report to you the server currently displaying the page



3. In the vSphere Client select the <**webserver VM**> reported above
4. Click Power-off to Power-off the <**webserver VM**>



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

EC2 > Target groups > Student20-default

**Student20-default** Delete

arn:aws:elasticloadbalancing:us-west-2:750192297402:targetgroup/Student20-default/5380e66e3b62e855

### Basic configuration

Target type IP	Protocol : Port HTTP : 80  Protocol version HTTP1	VPC vpc-051cd8dc828fb6c41 <a href="#">↗</a>	Load balancer Student20 <a href="#">↗</a>
-------------------	---	--	--

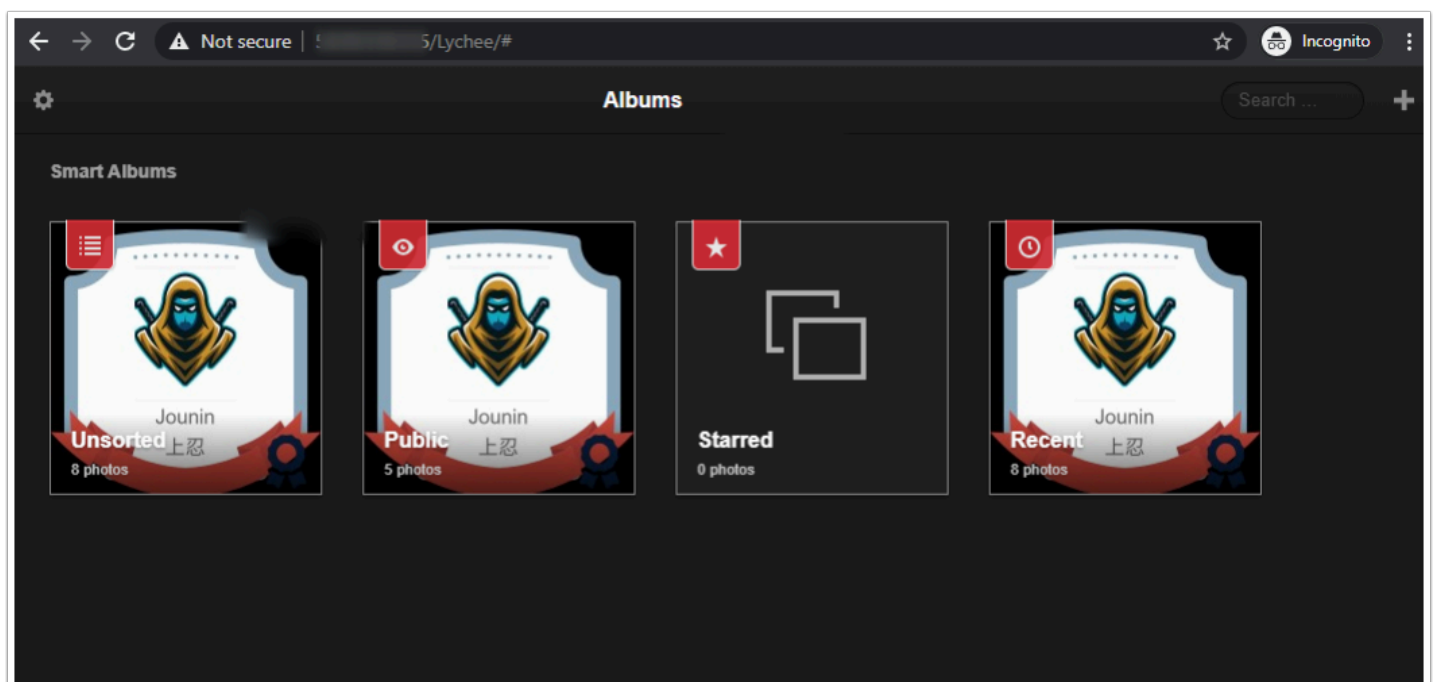
Group details | **Targets** <sup>8</sup> | Monitoring | Tags

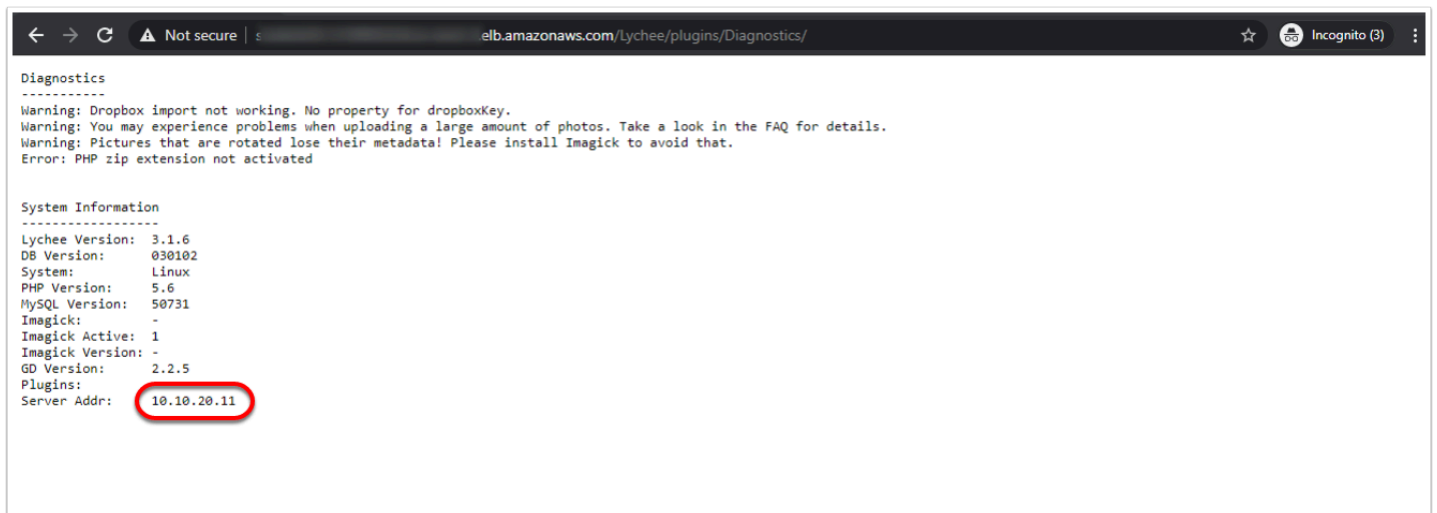
**Registered targets (2)** ↻ Deregister Register targets

< 1 > ⚙

<input type="checkbox"/>	IP address	Port	Zone	Status	Status details
<input type="checkbox"/>	10.10.20.11	80	all	🟢 healthy	
<input type="checkbox"/>	10.10.20.14	80	all	🔴 unhealthy	Request timed out

10. In a new Google Chrome incognito window type **<your ALB DNSName>/Lychee**  
i.e. vmcexpert3-01-1218955224.eu-central-1.elb.amazonaws.com/Lychee
11. You can repeat step one to confirm your load-balancer is directing request to your other web server
12. Power-on your previously powered-off vm in step 2






```
Diagnostics
-----
Warning: Dropbox import not working. No property for dropboxKey.
Warning: You may experience problems when uploading a large amount of photos. Take a look in the FAQ for details.
Warning: Pictures that are rotated lose their metadata! Please install Imagick to avoid that.
Error: PHP zip extension not activated

System Information
-----
Lychee Version: 3.1.6
DB Version: 030102
System: Linux
PHP Version: 5.6
MySQL Version: 50731
Imagick: -
Imagick Active: 1
Imagick Version: -
GD Version: 2.2.5
Plugins:
Server Addr: 10.10.20.11
```

## 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.