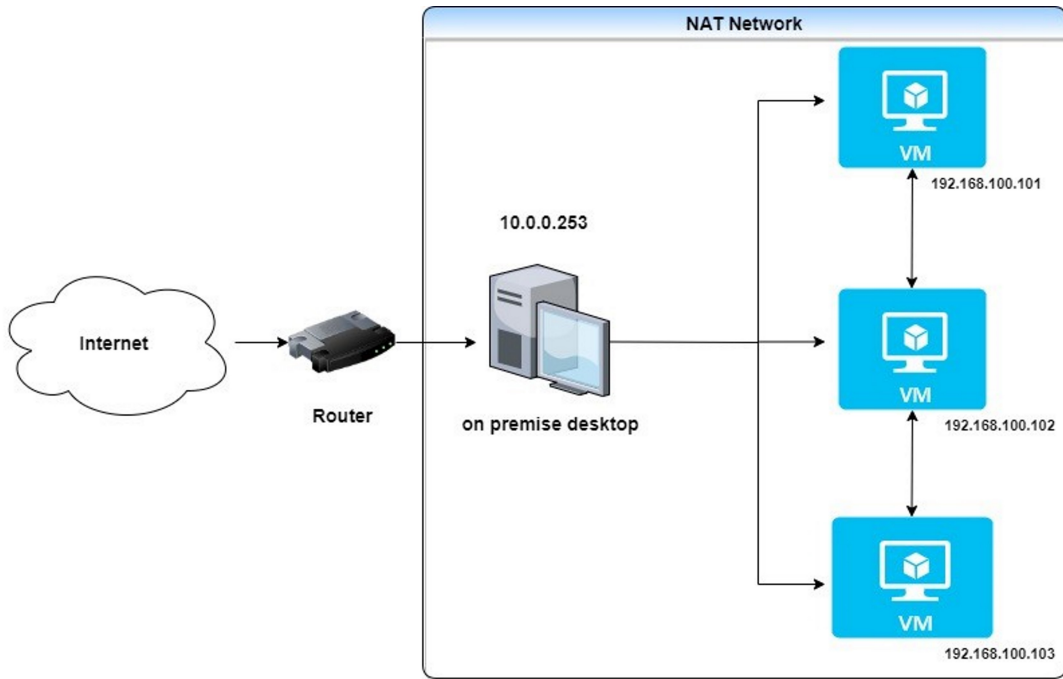


AWS Capstone Project

Monday, November 29, 2021 9:47 AM

Super Pear is a new tech startup that is looking to convert their current network infrastructure to the cloud using Amazon's AWS. Their current network consists of one router, one physical desktop PC, and 3 laptops running VM software. what would be the most cost effective way to migrate the Super Pear team to AWS? Provide screenshots of the network prior to, during, and after the conversion.



Before we begin discussing the actual process of converting their network to the cloud, it's best to see how the move would financially impact this company.

aws pricing calculator

Feedback English Contact Sales

Successfully added Amazon EC2 estimate.

AWS Pricing Calculator > My Estimate

My Estimate [Edit](#)

[Add service](#) [Add support](#) [Add group](#) [Clear estimate](#) [Export estimate](#) [Share](#)

Estimate summary [Info](#)

Upfront cost 0.00 USD	Monthly cost 69.61 USD	Total 12 months cost 835.32 USD
--------------------------	---------------------------	---

Getting Started with AWS

[Contact Us](#) [Sign in to the Console](#)

Services (1)

Amazon EC2 [Edit](#) [Action](#)

Description: Super Pear lift and shift
Region: US East (Ohio)

Quick estimate

Operating system (Linux), Quantity (4), Pricing strategy (EC2 Instance Savings Plans 1 Year No Upfront), Storage amount (20 GB), Instance type (t4g.medium)

Monthly: 69.61 USD

Acknowledgement

Using the AWS Pricing calculator, we can get an estimate of how much it'll be to virtualize Super Pear's network. Since the company needs constant and consistent performance, it would be more beneficial to sign up using the 1 year savings plan option. This will provide a decent sized discount! Also, since this company is expecting to expand in size in the near future, moving to the cloud will provide the necessary elasticity to expand resources without worrying about Capital expenditure.

```
Trey's Notebook
Administrator: Windows PowerShell

Suggestion [3,General]: The command AwsReplicationWindowsInstaller.exe was not found, but does exist in the current location. Windows PowerShell does not load commands from the current location by default. If you trust this command, instead type: ".\AwsReplicationWindowsInstaller.exe". See "get-help about_Command_Precedence" for more details.
PS C:\users\Trey0\downloads> .\AwsReplicationWindowsInstaller.exe --region us-east-2 --aws-access-key-id AKIA3N6QBQPEDZGGAH22 --aws-secret-access-key [REDACTED]
The installation of the AWS Replication Agent has started.
Verifying that the source server has enough free disk space to install the AWS Replication Agent.
(a minimum of 2 GB of free disk space is required)
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: c:
To replicate some of the disks, type the path of the disks, separated with a comma (for example, C:,D:). To replicate all disks, press Enter:C:
Disk to replicate identified: c:\ of size 954 GiB
All volumes for replication were successfully identified.
Downloading the AWS Replication Agent onto the source server... Finished.
Installing the AWS Replication Agent onto the source server... Finished.
Syncing the source server with the Application Migration Service Console... Finished.
The following is the source server ID: s-43a9a9293cce98e3c.
The AWS Replication Agent was successfully installed.
Press Enter to close...
PS C:\users\Trey0\downloads> aws --version
aws-cli/2.4.0 Python/3.8.8 Windows/10 exe/AMD64 prompt/off
PS C:\users\Trey0\downloads> aws iam create-role --role-name vmimport --assume-role-policy-document "file://C:\Users\Trey0\VirtualBoxVMs\trust-policy.json"

Unable to locate credentials. You can configure credentials by running "aws configure".
PS C:\users\Trey0\downloads> aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [None]:
Default output format [None]:
PS C:\users\Trey0\downloads> aws configure
AWS Access Key ID [None]: AKIA3N6QBQPEJN7HLH63
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-2
Default output format [None]: json
PS C:\users\Trey0\downloads> aws iam create-role --role-name vmimport --assume-role-policy-document "file://C:\Users\Trey0\VirtualBoxVMs\trust-policy.json"

An error occurred (AccessDenied) when calling the CreateRole operation: User: arn:aws:iam::785878451144:user/SMS is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::785878451144:role/vmimport
PS C:\users\Trey0\downloads> aws configure
AWS Access Key ID [*****]LH63]: AKIA3N6QBQPEJN7HLH63
AWS Secret Access Key [*****]wXw1]: [REDACTED]
Default region name [us-east-2]: us-east-2
Default output format [json]:
PS C:\users\Trey0\downloads> aws iam create-role --role-name vmimport --assume-role-policy-document "file://C:\Users\Trey0\VirtualBoxVMs\trust-policy.json"

An error occurred (AccessDenied) when calling the CreateRole operation: User: arn:aws:iam::785878451144:user/MGN is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::785878451144:role/vmimport
```

To begin the process, instead of using Amazon migration services which is better for larger operations, it was easier to use Windows PowerShell to run the AWS replication installer to prep the transfer of VMs to AWS. This is the starting process of a lift and shift.

Once the .ova files were imported and formed into AMIs, they were then launched into instances and were able to be seen in the EC2 instance library.

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a search bar, and service links for Resource Groups & Tag Editor, VPC, CloudFront, EC2, and Elastic Beanstalk. The left sidebar contains a navigation menu with categories like VPC Dashboard, EC2 Global View, Filter by VPC, and sections for Virtual Private Cloud, Security, and Reachability. The main content area displays the details for VPC vpc-089b271b4a5d81801, titled "vpc-089b271b4a5d81801 / Super Pear AWS Capstone".

VPC Details:

Property	Value
VPC ID	vpc-089b271b4a5d81801
State	Available
Tenancy	Default
Default VPC	No
Route 53 Resolver DNS Firewall rule groups	-
DHCP options set	dopt-8a6c27e1
IPV4 CIDR	10.0.0.0/16
Owner ID	785878451144
DNS hostnames	Disabled
DNS resolution	Enabled
Main route table	rtb-0c66967164fc8621d / SuperPear Public
Main network ACL	acl-05e371867c45aba46
IPv6 pool	-
IPv6 CIDR	-

IPv4 CIDRs:

CIDR	Status
10.0.0.0/16	Associated

IPv6 CIDRs:

CIDR	Status
------	--------

Once we have created the EC2 instances, the Virtual Private Cloud can be established. It was set up with the IPv4 CIDR range of 10.0.0.0/16

The screenshot shows the AWS Management Console interface with a green notification banner at the top stating "Internet gateway igw-00c3d835077b5d168 successfully attached to vpc-09f0fe0eb4f385332". The main content area displays the details for Internet Gateway igw-00c3d835077b5d168, titled "igw-00c3d835077b5d168 / IG-SuperPear".

Internet Gateway Details:

Property	Value
Internet gateway ID	igw-00c3d835077b5d168
State	Attached
VPC ID	vpc-09f0fe0eb4f385332 Super Pear AWS Capstone
Owner	785878451144

Tags:

Key	Value
Name	IG-SuperPear

Next, we have to set up an internet gateway for the VPC, which is basically the virtual router that allows internet connectivity to the cloud. Once it is created, it has to be attached to the Super Pear VPC.

The screenshot shows the AWS Management Console interface for a private subnet. The breadcrumb navigation indicates the path: VPC > Subnets > subnet-0a7f070258596e195. The title of the page is "subnet-0a7f070258596e195 / SuperPear PrivateSN". The "Details" tab is selected, displaying a table of subnet properties.

Subnet ID	Subnet ARN	State	IPv4 CIDR
subnet-0a7f070258596e195	arn:aws:ec2:us-east-2:785878451144:subnet/subnet-0a7f070258596e195	Available	10.0.1.0/24
Available IPv4 addresses	IPv6 CIDR	Availability Zone	Availability Zone ID
248	-	us-east-2a	use2-az1
VPC	Route table	Network ACL	Default subnet
vpc-089b271b4a5d81801 Super Pear AWS Capstone	rtb-020b585edd8578214 SuperPear Private	acl-05e371867c45aba46	No
Auto-assign public IPv4 address	Auto-assign customer-owned IPv4 address	Auto-assign customer-owned IPv4 address	Customer-owned IPv4 pool
No	No	No	-
Outpost ID	IPv6 CIDR reservations	IPv6 CIDR reservations	IPv6-only
-	-	-	No
Hostname type	Resource name DNS AAAA record	Resource name DNS AAAA record	Owner
IP name	Disabled	Disabled	785878451144

Below the details table, there are tabs for "Flow logs", "Route table", "Network ACL", "CIDR reservations", "Sharing", and "Tags". The "Flow logs" tab is currently selected.

The screenshot shows the AWS Management Console interface for a public subnet. The breadcrumb navigation indicates the path: VPC > Subnets > subnet-0cc11ae272059955f. The title of the page is "subnet-0cc11ae272059955f / SuperPear PublicSN". The "Details" tab is selected, displaying a table of subnet properties.

Subnet ID	Subnet ARN	State	IPv4 CIDR
subnet-0cc11ae272059955f	arn:aws:ec2:us-east-2:785878451144:subnet/subnet-0cc11ae272059955f	Available	10.0.0.0/24
Available IPv4 addresses	IPv6 CIDR	Availability Zone	Availability Zone ID
250	-	us-east-2a	use2-az1
VPC	Route table	Network ACL	Default subnet
vpc-089b271b4a5d81801 Super Pear AWS Capstone	rtb-0c66967164fc8621d SuperPear Public	acl-05e371867c45aba46	No
Auto-assign public IPv4 address	Auto-assign customer-owned IPv4 address	Auto-assign customer-owned IPv4 address	Customer-owned IPv4 pool
No	No	No	-
Outpost ID	IPv6 CIDR reservations	IPv6 CIDR reservations	IPv6-only
-	-	-	No
Hostname type	Resource name DNS AAAA record	Resource name DNS AAAA record	Owner
IP name	Disabled	Disabled	785878451144

Below the details table, there are tabs for "Flow logs", "Route table", "Network ACL", "CIDR reservations", "Sharing", and "Tags". The "Flow logs" tab is currently selected.

Created a public subnet (10.0.0.0/24) and linked it to the Super Pear public route table which will allow incoming and outgoing web traffic for the master VM. Also created a private subnet (10.0.1.0/24) which will allow the other 3 VMs to only communicate with each other.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor VPC CloudFront EC2 Elastic Beanstalk

New VPC Experience Tell us what you think

VPC Dashboard
EC2 Global View **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables **New**
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Endpoint Services
NAT Gateways
Peering Connections

SECURITY
Network ACLs
Security Groups

REACHABILITY
Reachability Analyzer

VPC > NAT gateways > nat-03edfffd2a70cdfdc

nat-03edfffd2a70cdfdc / SuperPearNGW

Delete

Details Info

NAT gateway ID nat-03edfffd2a70cdfdc	Connectivity type Public	State Available	State message Info
Elastic IP address 18.116.207.49	Private IP address 10.0.0.233	Network interface ID eni-079aa12af9067e2a4	VPC vpc-089b271b4a5d81801 / Super Pear AWS Capstone
Subnet subnet-0cc11ae272059955f / SuperPear PublicSN	Created 2021/11/30 08:14 GMT-5	Deleted -	

Monitoring Tags

Monitoring

1h 3h 12h 1d 3d 1w Add to dashboard

Packets out to destination (Count) Packets out to source (Count) Bytes out to destination (Bytes)

1 1 1

No data available. No data available. No data available.

Created and attached a NAT Gateway to the public SuperPear subnet and gave it an Elastic IP address . We will then to adjust the Route table connected to the private subnet so that it can communicate with the NAT Gateway. This will allow the 3 connected VMs to access the web for software updates/patches.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor VPC CloudFront EC2 Elastic Beanstalk

New VPC Experience Tell us what you think

VPC Dashboard
EC2 Global View **New**

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD
Your VPCs
Subnets
Route Tables **New**
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Managed Prefix Lists
Endpoints
Endpoint Services
NAT Gateways
Peering Connections

SECURITY
Network ACLs
Security Groups

REACHABILITY
Reachability Analyzer

VPC > Route tables > rtb-020b585edd8578214

rtb-020b585edd8578214 / SuperPear Private

Actions

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Details Info

Route table ID rtb-020b585edd8578214	Main No	Explicit subnet associations subnet-0a7f070258596e195 / SuperPear PrivateSN	Edge associations -
VPC vpc-089b271b4a5d81801 Super Pear AWS Capstone	Owner ID 785878451144		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Edit routes

Filter routes Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-03edfffd2a70cdfdc	Active	No

Feedback English (US) © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie pre

Here is the beforementioned Private route table with an added route that links it to the NAT Gateway

and allows internet access to the VMs in the private subnet.

The screenshot shows the AWS Management Console interface for a VPC. The left sidebar contains navigation links for VPC, CloudFront, EC2, and Elastic Beanstalk. The main content area displays the details for a route table named 'rtb-0c66967164fc8621d / SuperPear Public'. A notification banner at the top indicates that network connectivity can be checked using the Reachability Analyzer. Below this, the 'Details' tab is active, showing the route table ID, VPC, main status (Yes), owner ID, explicit subnet associations (subnet-0cc11ae272059955f / SuperPear PublicSN), and edge associations. The 'Routes' tab is also visible, showing a single route with destination 10.0.0.0/16, target 'local', and status 'Active'.

rtb-0c66967164fc8621d / SuperPear Public

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0c66967164fc8621d	Yes	subnet-0cc11ae272059955f / SuperPear PublicSN	-
VPC	Owner ID		
vpc-089b271b4a5d81801 Super Pear AWS Capstone	785878451144		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Public route table with an explicit association to the Super Pear public subnet

The screenshot shows the AWS Management Console interface for Security Groups. The left sidebar contains navigation links for EC2, Images, Elastic Block Store, and Network & Security. The main content area displays a list of security groups. The 'SuperPearRoot' security group is selected. Below the list, the 'Inbound rules' tab is active, showing a single rule with name '-', security group rule 'sgr-0c8a0d9a6fa7ab274', IP version 'IPv4', type 'SSH', protocol 'TCP', and port range '22'.

Security Groups (1/10) Info

Filter security groups

Name	Security group ID	Security group name	VPC ID	Description	Owner
AWSTest	sg-00397e59d89d8cc69	launch-wizard-2	vpc-04ca4beac947013a	launch-wizard-2 create...	78587845114
-	sg-01a139ce996a19564	default	vpc-089b271b4a5d81801 ...	default VPC security gr...	78587845114
-	sg-02c6e94e	default	vpc-d0cabcb	default VPC security gr...	78587845114
SuperPearRoot	sg-03e4324d953375ede	SPMaster	vpc-089b271b4a5d81801 ...	ssh to root ip	78587845114
-	sg-054ccf59589d84608	launch-wizard-4	vpc-089b271b4a5d81801 ...	launch-wizard-4 create...	78587845114
-	sg-0594db94bb41a49ef	launch-wizard-3	vpc-089b271b4a5d81801 ...	launch-wizard-3 create...	78587845114
-	sg-09855c9e62ea8a603	launch-wizard-1	vpc-d0cabcb	launch-wizard-1 create...	78587845114
AWS Application Mi...	sg-0c5a410c7348c41fe	AWS Application Migra...	vpc-d0cabcb	Security group with th...	78587845114
SuperPear Master	sg-0f35db0a30d36a57e	only me	vpc-d0cabcb	root user ssh	78587845114

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (1/1)

Filter security group rules

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-0c8a0d9a6fa7ab274	IPv4	SSH	TCP	22

Security group set up for each EC2 instance that allows all outgoing traffic, but only allows incoming SSH

access to only the root user's IP address.

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Resource Groups & Tag Editor

VPC

CloudFront

EC2

Elastic Beanstalk

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
 - Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

IAM dashboard

Security recommendations

- Root user has MFA
 - Having multi-factor authentication (MFA) for the root user improves security for this account.
- Root user has no active access keys
 - Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

- User groups2
- Users6
- Roles9
- Policies0
- Identity providers0

What's new

- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 50 services. 3 months ago
- IAM Access Analyzer helps you generate IAM policies based on access activity found in your organization trail. 3 months ago
- IAM Access Analyzer adds new policy checks to help validate conditions during IAM policy authoring. 5 months ago
- AWS Amplify announces support for IAM permissions boundaries on Amplify-generated IAM roles. 6 months ago

AWS Account

- Account ID
 - 785878451144
- Account Alias
 - 785878451144
 - Create
- Sign-in URL for IAM users in this account
 - https://785878451144.signin.aws.amazon.com/console

Quick Links

- My security credentials
 - Manage your access keys, multi-factor authentication (MFA) and other credentials.

Tools

- Policy simulator
 - The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.
- Web identity federation playground
 - Authenticate yourself to any of the supported web identity providers, see the requests and responses, obtain a set of temporary security credentials.

https://console.aws.amazon.com/iamv2/home?#/roles

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor VPC CloudFront EC2 Elastic Beanstalk

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
 - Archive rules
- Analizers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

IAM > Users

Users (6) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

	User name	Groups	Last activity	MFA	Password a...	Active key age
☐	master	None	-	None	None	-
☐	MGN	None	-	None	None	-
☐	Ron	EC2Read	-	None	None	-
☐	SMS	None	-	None	None	-
☐	Timmy	EC2Admin	-	None	None	-
☐	tmunroe	EC2Admin	-	None	31 days ago	-

aws

Services

Search for services, features, blogs, docs, and more

[Alt+S]

Global

trey0

Resource Groups & Tag Editor

VPC

CloudFront

EC2

Elastic Beanstalk

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analizers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Introducing the new Roles list experience

We've redesigned the Roles list experience to make it easier to use. [Let us know what you think.](#)

IAM > Roles

Roles (9) info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

Role name

Trusted entities

Last activity

AWSApplicationMigrationConversionServerRole

AWS Service: ec2

-

AWSApplicationMigrationMGNRole

AWS Service: mgn

3 days ago

AWSApplicationMigrationReplicationServerRole

AWS Service: ec2

3 days ago

AWSServiceRoleForApplicationMigrationService

AWS Service: mgn (Service-Linked Role)

16 minutes ago

AWSServiceRoleForSupport

AWS Service: support (Service-Linked Role)

23 days ago

AWSServiceRoleForTrustedAdvisor

AWS Service: trustedadvisor (Service-Linked Role)

-

EC2readonly

AWS Service: ec2

-

master

AWS Service: ec2

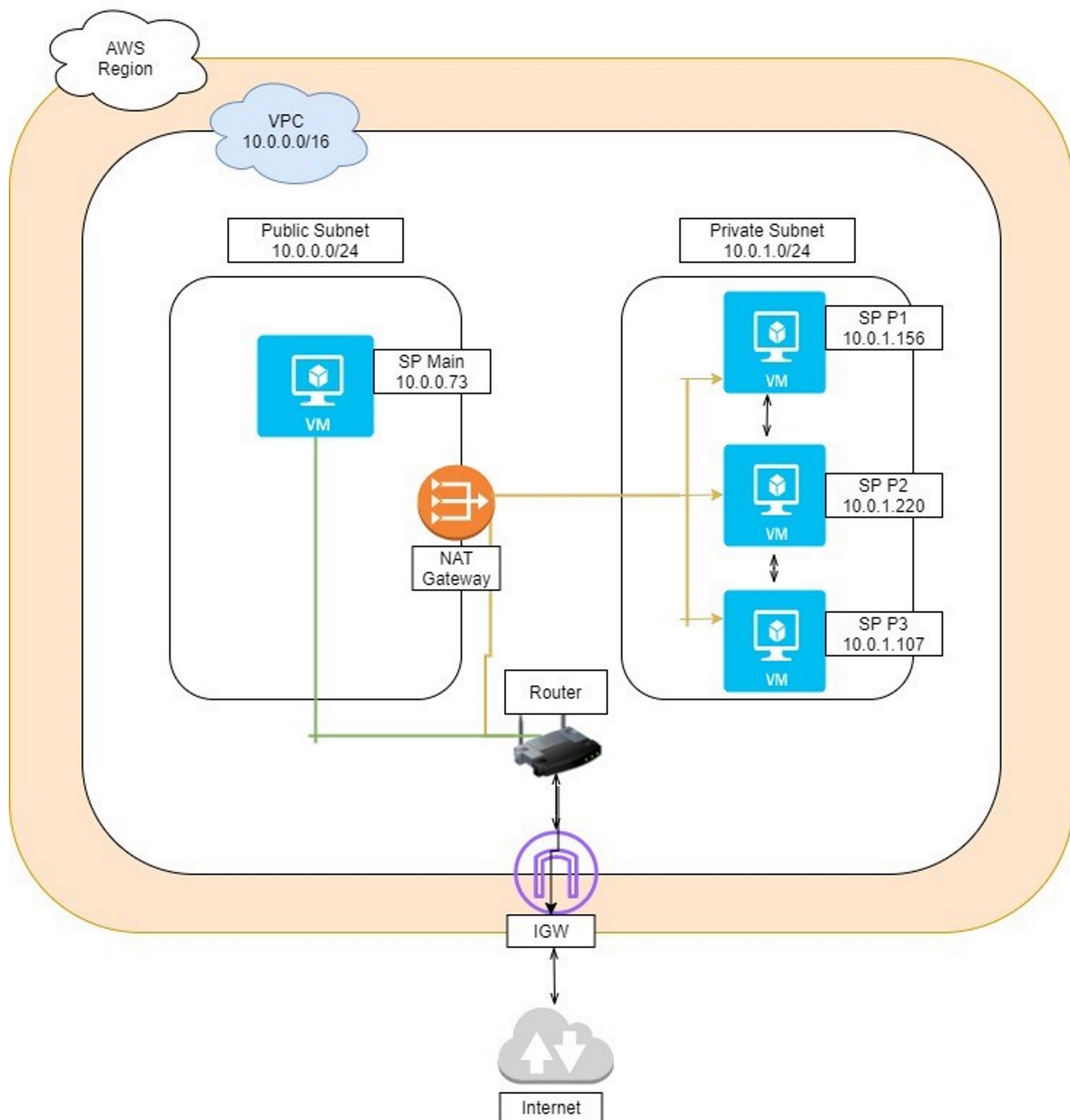
27 days ago

vmimport

AWS Service: vmie

5 days ago

A display of the IAM dashboard. The SuperPear Main VM has root access with MFA set up for extra security. The main VM also has full EC2 admin access. The other 3 VMs on the private subnet only have programmatic access via AWS CLI and secret key and access code. They also only have EC2 read only access.



After completion of the "lift and shift", this is how the network will look and function on AWS!!!