Assessment Task
Portfolio of Evidence

ICTCLD506_AT1_PE_TQM_v1

Student Name		**Student Number**	
Unit Code/s & Name/s	ICTCLD506 Implement virtual network in cloud environments		
Cluster Name *If applicable*	N/A		
Assessment Name	Portfolio of Evidence	**Assessment Task No.**	1 of 2
Assessment Due Date	Week 8	**Date Submitted**	/ /
Assessor Name			

Student Declaration: I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature.

Student Signature		**Date**	/ /

PRIVACY STATEMENT: TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at https://tafeqld.edu.au/global/privacy-policy.html) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at privacy@tafeqld.edu.au

Instructions to Student	**General Instructions:** This written assessment contains three (3) parts: • Section A – Design a virtual network • Section B – Configure a virtual network and peering • Section C – Configure virtual network peering The answers required for these tasks shall be written in plain English, using language that is understandable by a person of a technical level suitable for the case study.

Materials to be supplied:

For the student to successfully complete this assessment they will need to acquire:

- a computer system installed with a current desktop operating system with appropriate internet browser, and office suite able to save in Microsoft Word .docx format, and current industry standard file formats
- Internet access
- Uptown IT documentation, located in Connect.

Work, Health and Safety:

TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules, specifically as they relate to progress of study and assessment guidelines.

Student rules: http://tafeqld.edu.au/current-students/student-rules/

Assessment Criteria:

To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard:

- deploy and configure at least 6 of the following different types of cloud resources, including but not limited to

– virtual machines

– container services

– load balancers and autoscaling

– serverless functions

– API gateways

– block or object storage

– managed databases

– DNS

– content delivery networks

	● use cloud management console, cloud software development kits or command line tools ● develop and execute test plans and demonstrate successful task completion ● consider procedural improvements to produce repeatable and automated deployments by reducing manual processes ● monitor and manage inventory, changes and lifecycle of at least one cloud resource ● use cloud management console, cloud software development kits or command line tools ● collect and analyse cloud and system data and adjust resources accordingly ● summarise ways system operations in cloud environments can be automated to minimise manual intervention.
Submission details (if relevant)	**Due:** Week 8 as per the unit study guide. Insert your details on page 1 and sign the Student Declaration. Include this form with your submission. Submit the listed files below as per the instructions in the Connect online learning system stated on the Assessment Task 2 page. You are to submit the following files: 1. ICTCLD506_AT2_Design_*yourname*.docx 2. ICTCLD506_AT2_Configuration_*yourname*.docx 3. ICTCLD506_AT2_Peering_*yourname*.docx Assessment to be submitted via: ● TAFE Queensland Learning Management System (Connect): *https://connect.tafeqld.edu.au/d2l/login* ● **Username:** 9 digit student number ● **For Password:** Reset password go to: *https://passwordreset.tafeqld.edu.au/default.aspx*
Instructions to Assessor	Student will require: ● computer applications currently used in industry ● support resources, including online, manuals and training booklets ● a computer system with a suitable current OS and access to the internet ● information and data sources required to design and implement cloud infrastructure ● specific requirements and industry standards, organisational procedures and legislative requirements, including business and

	functionality requirements as well as retention/lifecycle business policy, as required ● retention/lifecycle policy example as it relates to managing cloud infrastructure ● data to gather information from to determine output and user requirements, including user access and business protocols. **Work, Health and Safety:** TAFE Queensland student rules are designed to ensure that learners are aware of their rights as well as their responsibilities. All learners are encouraged to familiarise themselves with the TAFE Queensland student rules, specifically as they relate to progress of study and assessment guidelines. **Student rules:** http://tafeqld.edu.au/current-students/student-rules/ **Level of Assistance:** Teachers and tutors should be available in class, and accessible by email for students working from home. Staff cannot directly show students answers but guide them to where to go to complete tasks individually. The teacher will make reasonable adjustment for students, as and when appropriate, after consultation with the Disability and Counselling team. **Assessment Criteria:** See Marking Criteria on Connect. Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards. Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.
Note to Student	*An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.*

© TAFE Queensland. Uncontrolled copy if printed. Refer to TAFE Queensland intranet for current version of document.

Case study: Daydreams Travel Agency

Mission statement

Daydreams offer value for money holidays you dream about through a large range of destinations, helpful agents and a smooth booking process that will get you up and away enjoying life quickly.

Description of the business

Daydreams Travel Agency employs eight staff members and operates on a $2,000,000 annual budget. At present, they operate out of a single small building in a suburban neighbourhood.

They have had success in the first three years of operation and now would like to expand by increasing the size of the physical location to accommodate 12 on-site employees.

Furthermore, understanding the modern businesses profiles, Daydreams Travel Agency perfectly adopt the idea of remote workers. This would save lots of resources and expenses, as well as achieving more exposure to clients nationwide. This is why the strategic plan proposes hiring 10 work-from-home sales personnel.

The CEO understands that their future success depends on their ability to capitalise on emerging technologies to satisfy their clients, but she knows very little about technology herself.

She has been advised by her IT consultant that the company's computers, servers, and network are outdated and prone to failure. The team has been asked to write a report outlining what the company will need to do to expand.

In order to keep up with the competition, and stay abreast of emerging technologies, the CEO is in favour of retiring the company's old servers and transitioning to a cloud-based network which would support all of the company's current and future business needs. This would require a comprehensive plan to develop a virtual network solution in partnership with a cloud service provider. This solution will include the design and configuration of a virtual network, and appropriate peering connections to support the company's operations.

Current configuration:

- Gigabit ethernet network cards on all computers and the servers.
- Cat 6 cables connecting the computers and server via L2 switch.
- Cisco Switches: Catalyst 2940.
- One server providing file services, DNS, DHCP and email. OS: Windows Server 2016.
- The server storage capacity does not adequately support the existing staff.
- VPN is in place to support remote access functionality.
- BackupExec hardware and software is used to maintain a 3/2/1 backup plan.
- Many staff members complain that the network is too slow.

Business concerns:

Daydreams systems need to become more secure with more redundancy, security elements, system monitoring and maintenance schedules. It would be good to keep a log of all staff system access and usage, plus access to data should be on need-to-know basis according to business role. Data should be accessible to staff as and when they need it from their location.

Strategic plan:

- Increase number of on-site employees from 8 to 20.
- Hire 10 work-from-home sales representatives that need 24/7 access to company's resources and limited physical existence in the company's premises (around 4 hours a week pp).
- Implement new and innovative approaches to selecting travel destinations/recreation and bookings.
- Make creative use of emerging technologies to meet the needs of our staff and therefore our clients.
- Extend markets to surrounding suburbs and interstate.
- A budget for the new technologies is set at $135,000.

Organisational policies and procedures

- Data privacy of staff and clients is to be maintained at all times.
- Copyright and Intellectual Property rights are to be respected at all times, for our own property and others.
- Transactions made in/by our business will have the clients' best interest at heart.
- Negligence will not be tolerated, particularly around loss of information and breach of legislation. Staff must be aware and follow process.
- Honesty and respect are expected in all business dealings.

Your role

As a Senior System Administrator, and a member of the IT team, management has requested you to design and configure a virtual network for the company and fully document the process. Your plan should provide a reasonable approach to the next stage of the transition away from on-site operations and towards virtual/cloud-based operations.

© TAFE Queensland. Uncontrolled copy if printed. Refer to TAFE Queensland intranet for current version of document.

Section A – Design a Virtual Network

(ICTCLD506_AT2_Design_*yourname*.docx)

NOTE: *In Part 2 question 2.1 you will develop a topology for the virtual network. You may want to return to the initial questions once you have completed that topology as it will be helpful in developing these solutions.*

Part 1 – Prepare to Design and Configure the Virtual Network

In preparation, research cloud vendor service providers to identify sources of information that will be helpful in designing and configuring a virtual network in a cloud platform, including business and legislative requirements. In particular, focus on AWS as one of the industry leaders, to locate industry standards, procedures, and guidelines.

1.1 List all of the networking requirements for Daydreams Travel Agency based on the business needs in the case study. List the cloud resources needed to meet these requirements.

Business Needs	Cloud Resource	Comments
Increased Storage	Amazon S3	S3 standard single bucket in the local AWS region
Scalable Computing Resources	Amazon EC2	Elastic Compute Cloud for flexible, scalable computing power
Network Security and Redundancy	AWS Shield & AWS Route 53	Advanced protection against DDoS attacks; DNS service
Remote Access for Work-from-Home	AWS VPN	Secure and private connection for remote employees
High Availability and Disaster Recovery	Amazon RDS & AWS Backup	Managed database service for resilience; backup solutions
Data Privacy and Compliance	AWS Identity and Access Management (IAM) & AWS Key Management Service (KMS)	Manage user access and encryption keys
System Monitoring and Maintenance	Amazon CloudWatch & AWS Systems Manager	Monitoring and management of cloud resources and applications
Email Services	Amazon WorkMail	Secure, managed business email and calendaring service
File Sharing and Collaboration	Amazon WorkDocs	Fully managed, secure content creation, storage, and collaboration service

1.2 Identify business and industry requirements. To do this, you will need to conduct research to investigate travel industry standards and guidelines, and state and Commonwealth legislation and frameworks. Also look at tourism industry associations e.g. Tourism Australia, Business Queensland, Australian Federation of Travel agents, etc.

a. Australian Travel Accreditation Scheme (ATAS): ATAS is an industry accreditation scheme setting the quality benchmark for the Australian travel industry. It's a voluntary membership scheme open to all travel intermediaries, focusing on elevating industry standards and increasing consumer awareness of the benefits of booking travel through an ATAS accredited agent. Those meeting the requirements receive national accreditation and the right to use the 'ATAS - travel accredited' branding, symbolizing quality and professionalism.

b. Australian Consumer Law (ACL) for Travel and Accommodation Businesses: The ACL covers key aspects such as refunds, cancellations, and consumer guarantees. This guide is particularly relevant for travel and accommodation businesses, addressing issues where consumers frequently report problems and where industry bodies have requested detailed guidance. It includes information on what constitutes a major failure to comply with a consumer guarantee and changes to the definition of 'consumer'.

c. Quality Tourism Framework: This framework, developed by the Australian Tourism Industry Council (ATIC), combines multiple tourism accreditation, business development, and awards programs into a single, user-friendly online tool. It aims to develop businesses from start-up through to niche markets and international trade channels, promoting high-quality tourism businesses and providing modern branding to promote the status as a Quality Tourism Accredited Business

1.3 Identify security options for the virtual network based on AWS tools. The table below will provide a basic framework for this task. Provide enough information that this table could be used as a guide for implementation of security tools.

Security tool	**Applied to …**	**Comments**
Amazon IAM	To control and monitor access and identity for all components	Identify users and roles before configuring IAM
AWS Identity and Access Management (IAM)	Manage user access and permissions	Create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.
AWS Key Management Service (KMS)	Manage encryption keys	Create and control the encryption keys used to encrypt your data, and use AWS KMS to manage them.
AWS Shield	Protection against DDoS attacks	Enable AWS Shield Standard for automatic protection or upgrade to AWS Shield

© TAFE Queensland. Uncontrolled copy if printed. Refer to TAFE Queensland intranet for current version of document.

		Advanced for additional protection layers.
AWS WAF (Web Application Firewall)	Protect web applications from common web exploits	Create a set of rules that define the conditions that AWS WAF searches for in web requests to block or allow traffic.
Amazon VPC (Virtual Private Cloud)	Isolate network infrastructure	Set up a VPC to define a virtual network in your own logically isolated area within the AWS cloud.
Amazon CloudWatch	Monitor and log security and operational activity	Use CloudWatch to collect and track metrics, collect and monitor log files, and set alarms.
AWS Systems Manager	Manage and secure infrastructure	Use Systems Manager for a unified user interface to view operational data from multiple AWS services and automate operational tasks across AWS resources.
AWS Config	Track resource configurations and changes	Use AWS Config to assess, audit, and evaluate the configurations of your AWS resources.
AWS VPN	Secure connection to AWS network	Establish a secure and private tunnel from your network or device to the AWS global network.
Amazon Inspector	Automated security assessment service	Use Amazon Inspector to automatically assess applications for exposure, vulnerabilities, and deviations from best practices.

Part 2 – Design and Configure the Virtual Network

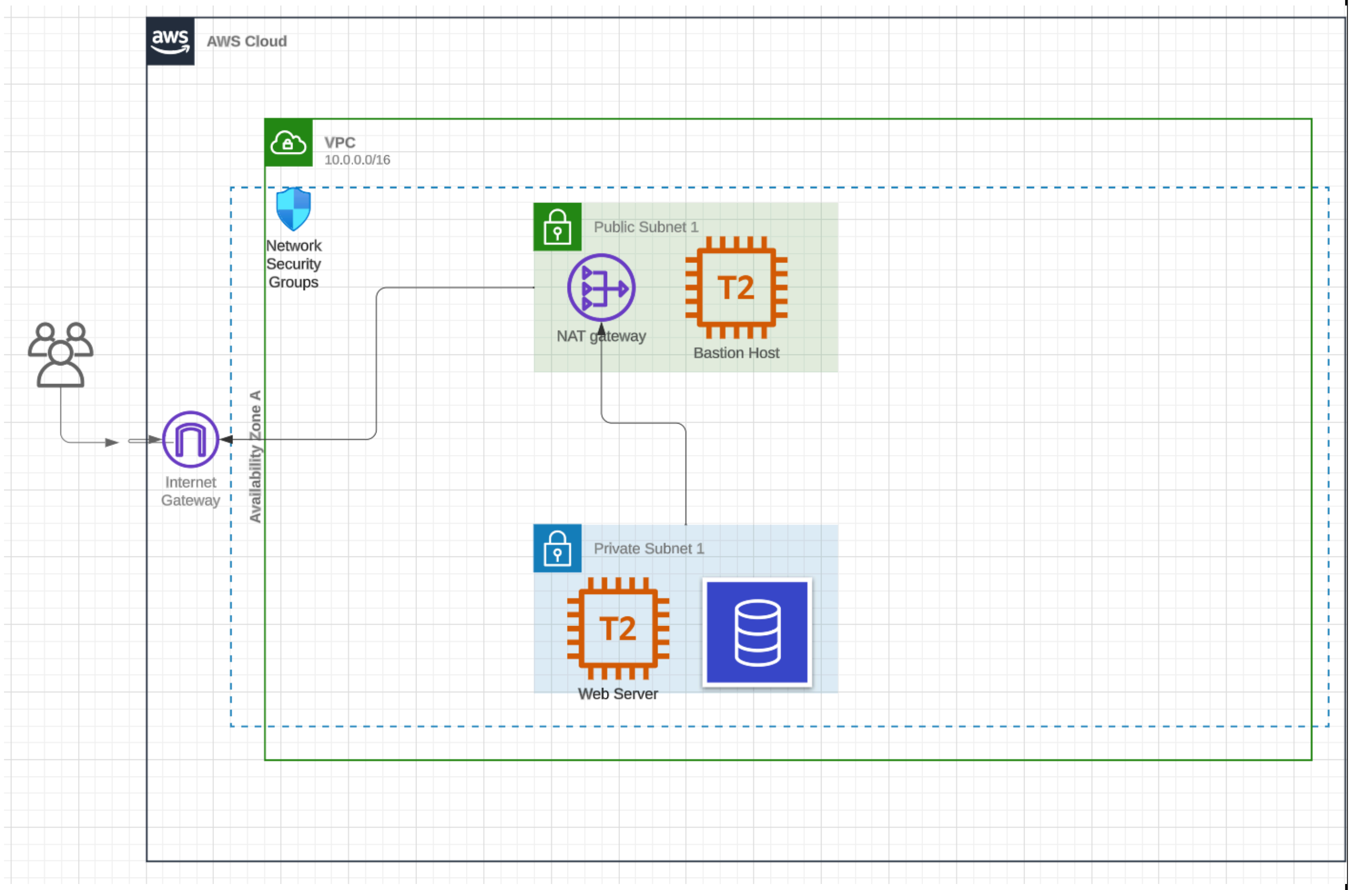
2.1 List and describe the AWS tools, resources, gateways, and services required to build a multi-tier solution for the case study company. Use the table below as a framework. Use the third column to indicate the procedure or command you might use to achieve the implementation. You may add rows and columns as needed. Your completed table must address how you would use SSH and VPN to support the network.

Tools/Resources Gateways/Services	Applied to …	How will you implement
Amazon S3	Will provide storage for all DTA operations in the local geographical area	https://s3.region code.amazonaws.com.bucketname
Amazon EC2	Hosting web servers, application servers	Launch EC2 instances via AWS Management Console or AWS CLI: `aws ec2 run-instances --image-id [ami-id] --count [number] --instance-type [type]`
Amazon RDS	Database services for DTA	Create RDS instances in AWS Management Console or via AWS CLI: `aws rds create-db-instance --db-instance-identifier [identifier] --db-instance-class [class] --engine [engine]`
AWS VPN	Secure connection for remote workers	Set up via AWS Virtual Private Network Console, create a Customer Gateway and a Virtual Private Gateway, then connect them
AWS Direct Connect	Dedicated network connection to AWS	Set up via AWS Management Console, create a Direct Connect connection and configure your router
Amazon VPC	Network isolation and security	Create a VPC via AWS Management Console or AWS CLI: `aws ec2 create-vpc --cidr-block [block]`
AWS IAM	Manage user access and permissions	Use AWS Management Console or AWS CLI to create users, groups, and roles: `aws iam create-user --user-name [name]`
AWS CloudFront	Content delivery network service	Set up a distribution via AWS Management Console or AWS CLI: `aws cloudfront create-distribution --origin-domain-name [domain-name]`
AWS Elastic Load Balancing	Distribute incoming application traffic	Create a load balancer via AWS Management Console or AWS CLI: `aws elb create-load-balancer --name [name] --subnets [subnet-ids]`
AWS Route 53	DNS and domain name management	Use AWS Management Console to configure DNS settings, register domain names

AWS Shield & WAF	Protection against DDoS attacks and web application firewall	Enable AWS Shield Standard via AWS Management Console and set up WAF rules
Amazon CloudWatch	Monitoring and logging	Use AWS Management Console or AWS CLI to set up monitoring: `aws cloudwatch put-metric-alarm --alarm-name [name] --metric-name [metric]`
SSH (Secure Shell)	Secure access to cloud resources	Use SSH keys for secure access to EC2 instances: `ssh -i /path/to/key.pem ec2-user@[instance-ip]`

2.2 Create a logical topology for your virtual network. Show your subnet scheme using the table below as a template. Add rows as needed.

TOPOLOGY

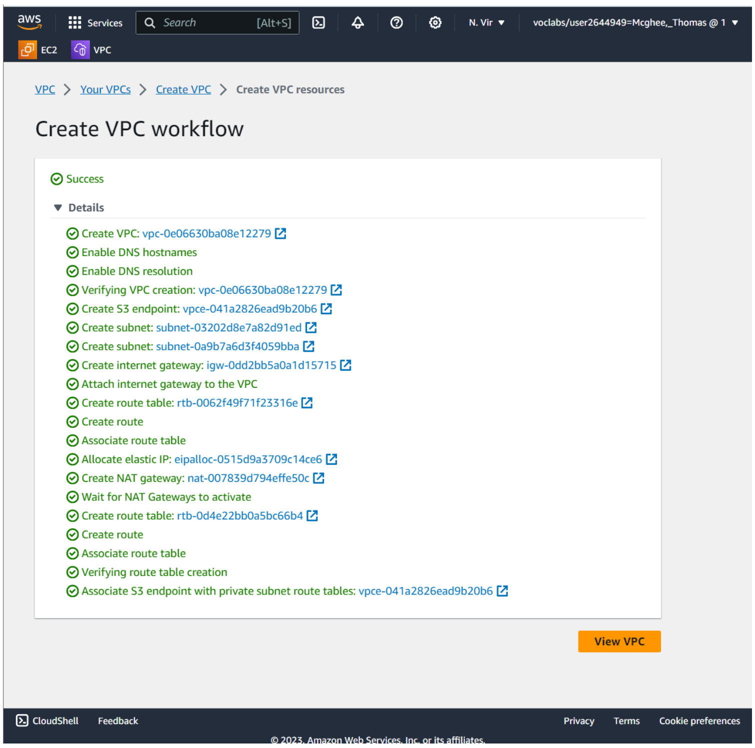


Components requiring IP addresses (including instances and gateways)	**IP address**	**Subnet mask**
Amazon S3	192.168.0.20	255.255.255.0
NAT Gateway	192.168.0.10	255.255.255.0
Amazon EC2 (Webserver)	192.168.1.3	255.255.255.0
Amazon EC2 (Bastion)	192.168.0.3	255.255.255.0
VPC	192.167.0.0	255.255.0.0

Section B – Configure a virtual network and peering

(ICTCLD506_AT2_Configuration_*yourname*.docx)

2.3 Insert screen shots to show how you have enabled the gateways and services according to the table in question 2.1. These can include dialog boxes from the AWS management console showing each activity, and/or operations taken at the command line interface. You may also show code fragments if you are using code in your development.


aws
Services
Search
[Alt+S]
N. Vir
voclabs/user2644949=Mcghee,_Thomas @ 1
EC2
VPC
VPC > Your VPCs > Create VPC > Create VPC resources
View VPC
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.

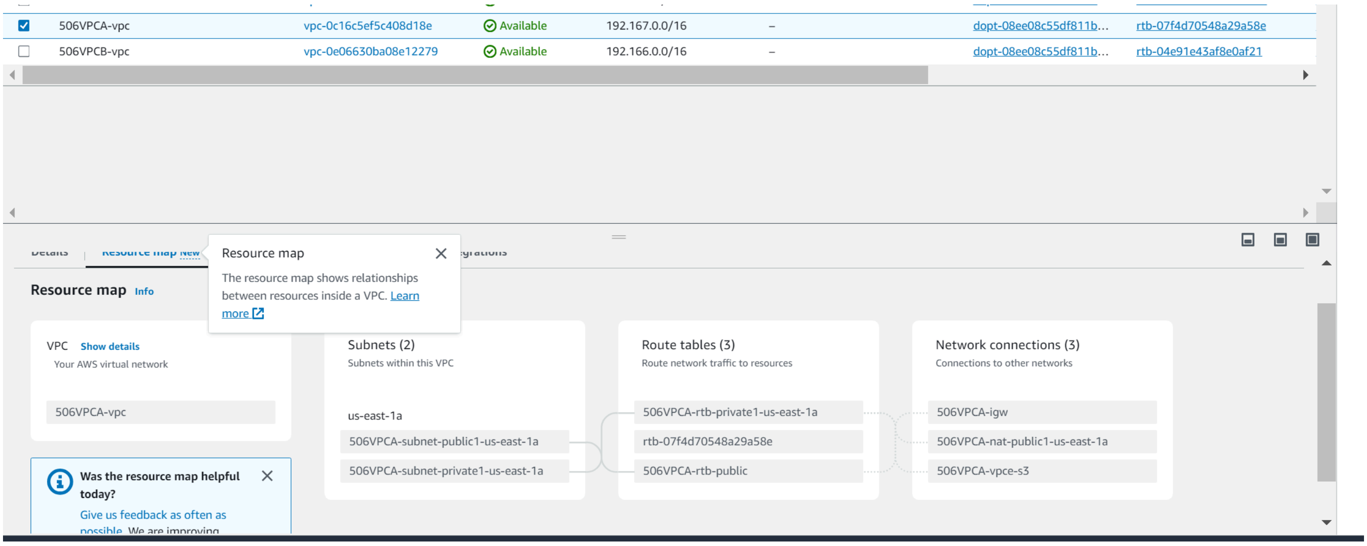
Create VPC workflow

✓ Success

▼ Details

- ✓ Create VPC: vpc-0e06630ba08e12279
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-0e06630ba08e12279
- ✓ Create S3 endpoint: vpce-041a2826ead9b20b6
- ✓ Create subnet: subnet-03202d8e7a82d91ed
- ✓ Create subnet: subnet-0a9b7a6d3f4059bba
- ✓ Create internet gateway: igw-0dd2bb5a0a1d15715
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-0062f49f71f23316e
- ✓ Create route
- ✓ Associate route table
- ✓ Allocate elastic IP: eipalloc-0515d9a3709c14ce6
- ✓ Create NAT gateway: nat-007839d794effe50c
- ✓ Wait for NAT Gateways to activate
- ✓ Create route table: rtb-0d4e22bb0a5bc66b4
- ✓ Create route
- ✓ Associate route table
- ✓ Verifying route table creation
- ✓ Associate S3 endpoint with private subnet route tables: vpce-041a2826ead9b20b6

VPC



☑	506VPCA-vpc	vpc-0c16c5ef5c408d18e	✓ Available	192.167.0.0/16	–	dopt-08ee08c55df811b...	rtb-07f4d70548a29a58e
□	506VPCB-vpc	vpc-0e06630ba08e12279	✓ Available	192.166.0.0/16	–	dopt-08ee08c55df811b...	rtb-04e91e43af8e0af21

Resource map

The resource map shows relationships between resources inside a VPC. Learn more

VPC: Your AWS virtual network
506VPCA-vpc

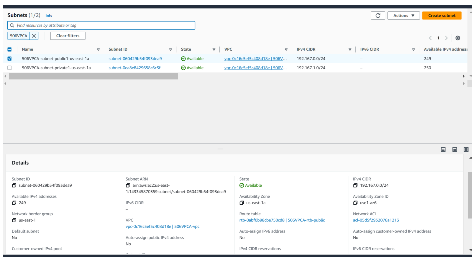
Subnets (2): Subnets within this VPC
us-east-1a
506VPCA-subnet-public1-us-east-1a
506VPCA-subnet-private1-us-east-1a

Route tables (3): Route network traffic to resources
506VPCA-rtb-private1-us-east-1a
rtb-07f4d70548a29a58e
506VPCA-rtb-public

Network connections (3): Connections to other networks
506VPCA-igw
506VPCA-nat-public1-us-east-1a
506VPCA-vpce-s3

Was the resource map helpful today?
Give us feedback as often as possible. We are improving

Public Subnet:



Subnets (1/2) Info

Find resources by attribute or tag

506VPCA ✕ | Clear filters

☐	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresse
☑	506VPCA-subnet-public1-us-east-1a	subnet-060429b54f093dea9	✓ Available	vpc-0c16c5ef5c408d18e | 506V...	192.167.0.0/24	–	249
☐	506VPCA-subnet-private1-us-east-1a	subnet-0ea8e8429658c6c3f	✓ Available	vpc-0c16c5ef5c408d18e | 506V...	192.167.1.0/24	–	250

Details

Subnet ID
subnet-060429b54f093dea9

Available IPv4 addresses
249

Network border group
us-east-1

Default subnet
No

Customer-owned IPv4 pool

Subnet ARN
arn:aws:ec2:us-east-1:143345870359:subnet/subnet-060429b54f093dea9

IPv6 CIDR
–

VPC
vpc-0c16c5ef5c408d18e | 506VPCA-vpc

Auto-assign public IPv4 address
No

State
✓ Available

Availability Zone
us-east-1a

Route table
rtb-0abf0b98cbe750cd8 | 506VPCA-rtb-public

Auto-assign IPv6 address
No

IPv4 CIDR reservations

IPv4 CIDR
192.167.0.0/24

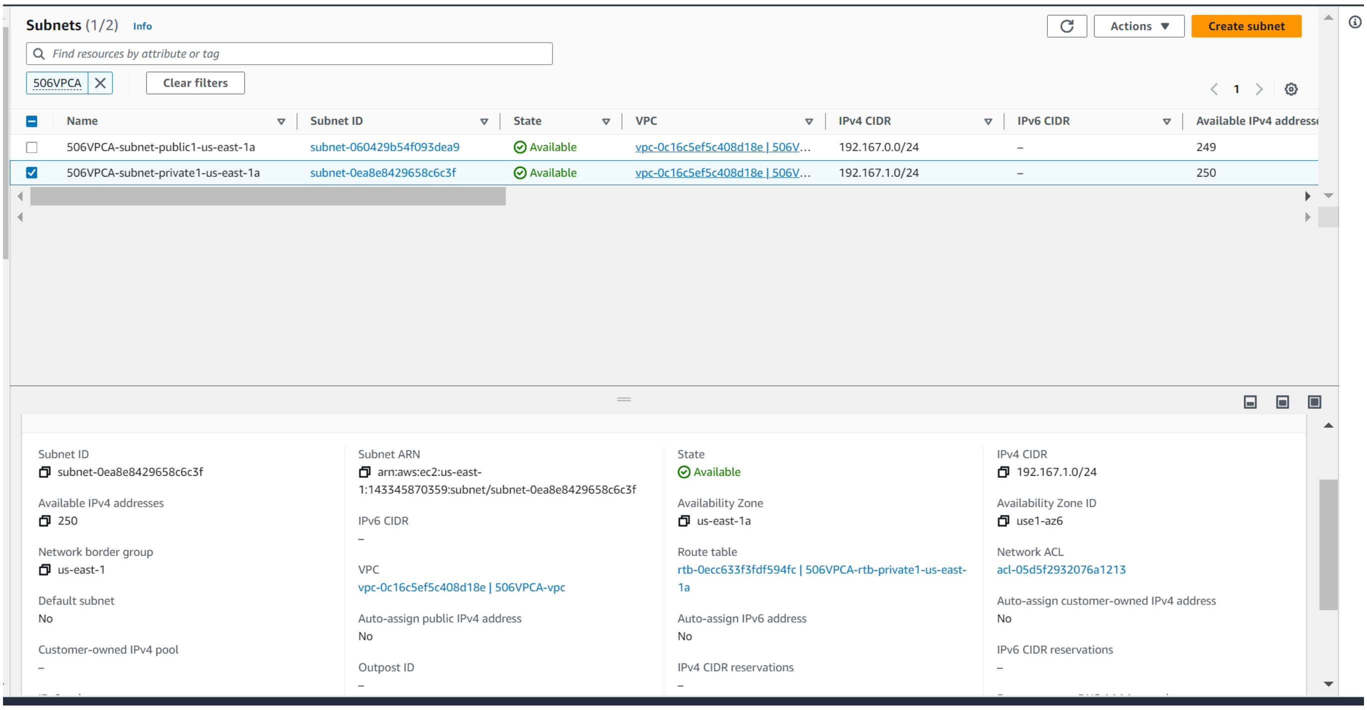
Availability Zone ID
use1-az6

Network ACL
acl-05d5f2932076a1213

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations

Private Subnet:



Subnets (1/2) Info

Find resources by attribute or tag

506VPCA ✕ | Clear filters

☐	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresse
☐	506VPCA-subnet-public1-us-east-1a	subnet-060429b54f093dea9	✓ Available	vpc-0c16c5ef5c408d18e | 506V...	192.167.0.0/24	–	249
☑	506VPCA-subnet-private1-us-east-1a	subnet-0ea8e8429658c6c3f	✓ Available	vpc-0c16c5ef5c408d18e | 506V...	192.167.1.0/24	–	250

Subnet ID
subnet-0ea8e8429658c6c3f

Available IPv4 addresses
250

Network border group
us-east-1

Default subnet
No

Customer-owned IPv4 pool
–

Subnet ARN
arn:aws:ec2:us-east-1:143345870359:subnet/subnet-0ea8e8429658c6c3f

IPv6 CIDR
–

VPC
vpc-0c16c5ef5c408d18e | 506VPCA-vpc

Auto-assign public IPv4 address
No

Outpost ID
–

State
✓ Available

Availability Zone
us-east-1a

Route table
rtb-0ecc633f3fdf594fc | 506VPCA-rtb-private1-us-east-1a

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

IPv4 CIDR
192.167.1.0/24

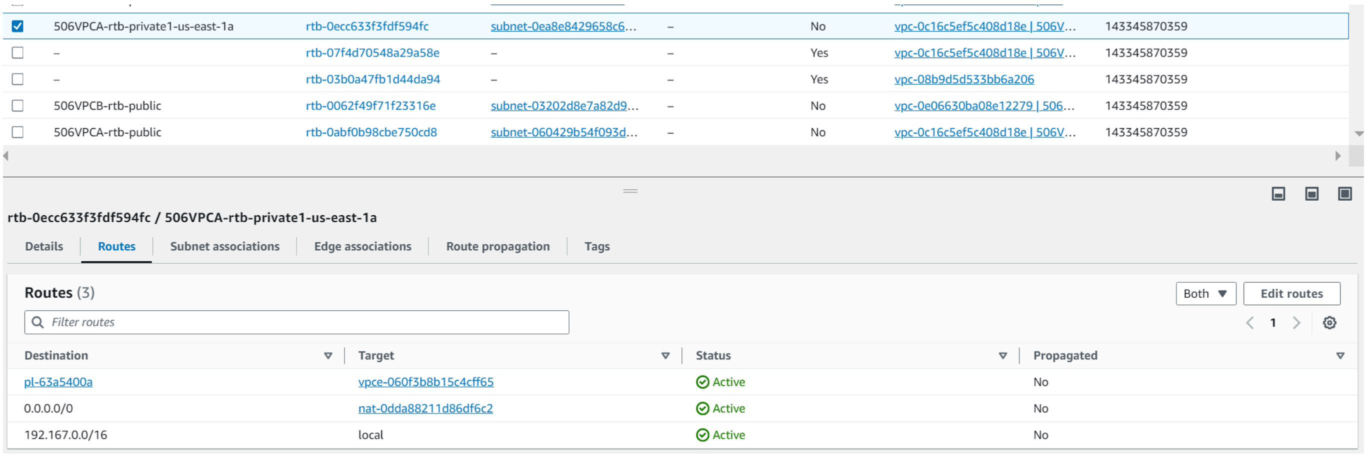
Availability Zone ID
use1-az6

Network ACL
acl-05d5f2932076a1213

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Route Table for private subnet:



☑	506VPCA-rtb-private1-us-east-1a	rtb-0ecc633f3fdf594fc	subnet-0ea8e8429658c6...	–	No	vpc-0c16c5ef5c408d18e | 506V...	143345870359
☐	–	rtb-07f4d70548a29a58e	–	–	Yes	vpc-0c16c5ef5c408d18e | 506V...	143345870359
☐	–	rtb-03b0a47fb1d44da94	–	–	Yes	vpc-08b9d5d533bb6a206	143345870359
☐	506VPCB-rtb-public	rtb-0062f49f71f23316e	subnet-03202d8e7a82d9...	–	No	vpc-0e06630ba08e12279 | 506...	143345870359
☐	506VPCA-rtb-public	rtb-0abf0b98cbe750cd8	subnet-060429b54f093d...	–	No	vpc-0c16c5ef5c408d18e | 506V...	143345870359

rtb-0ecc633f3fdf594fc / 506VPCA-rtb-private1-us-east-1a

Details | **Routes** | Subnet associations | Edge associations | Route propagation | Tags

Routes (3)

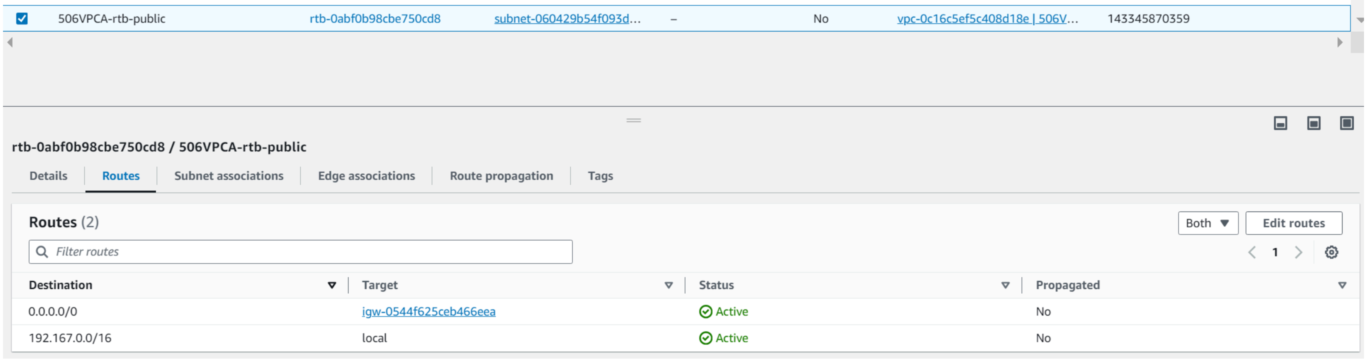
Both ▼ | Edit routes

Filter routes

Destination	Target	Status	Propagated
pl-63a5400a	vpce-060f3b8b15c4cff65	✓ Active	No
0.0.0.0/0	nat-0dda88211d86df6c2	✓ Active	No
192.167.0.0/16	local	✓ Active	No

Route table for public subnet:

© TAFE Queensland. Uncontrolled copy if printed. Refer to TAFE Queensland intranet for current version of document.



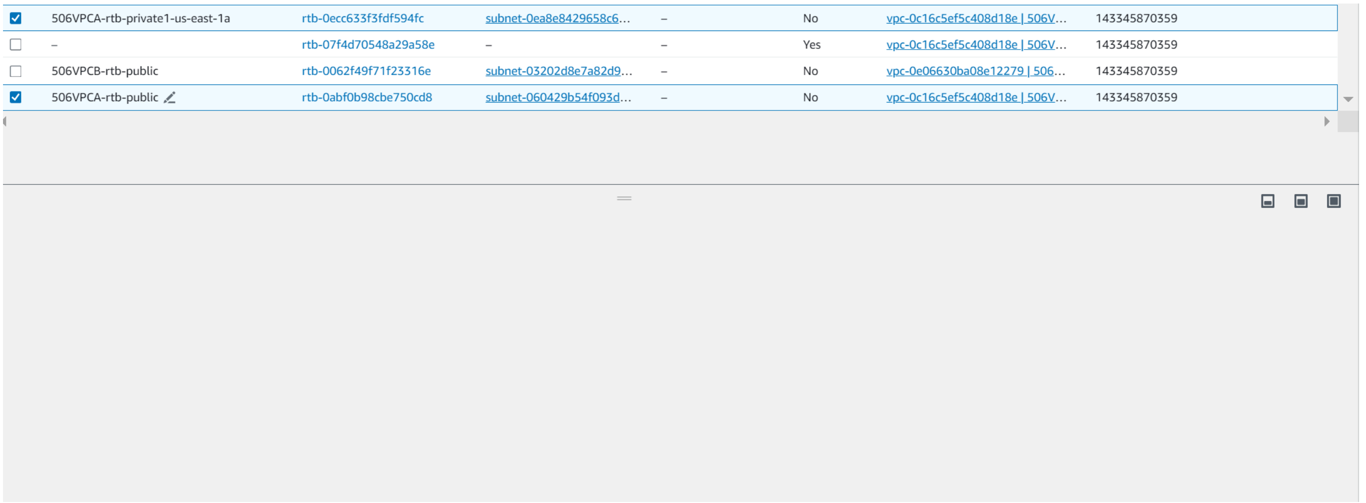
☑	506VPCA-rtb-public	rtb-0abf0b98cbe750cd8	subnet-060429b54f093d...	–	No	vpc-0c16c5ef5c408d18e | 506V...	143345870359

rtb-0abf0b98cbe750cd8 / 506VPCA-rtb-public

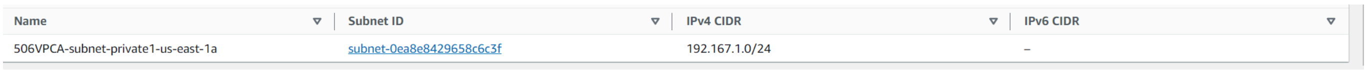
Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0544f625ceb466eea	Active	No
192.167.0.0/16	local	Active	No

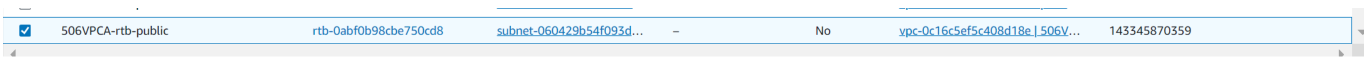
All subnets: for VPC



☑	506VPCA-rtb-private1-us-east-1a	rtb-0ecc633f3fdf594fc	subnet-0ea8e8429658c6...	–	No	vpc-0c16c5ef5c408d18e | 506V...	143345870359
☐	–	rtb-07f4d70548a29a58e	–	–	Yes	vpc-0c16c5ef5c408d18e | 506V...	143345870359
☐	506VPCB-rtb-public	rtb-0062f49f71f23316e	subnet-03202d8e7a82d9...	–	No	vpc-0e06630ba08e12279 | 506...	143345870359
☑	506VPCA-rtb-public	rtb-0abf0b98cbe750cd8	subnet-060429b54f093d...	–	No	vpc-0c16c5ef5c408d18e | 506V...	143345870359

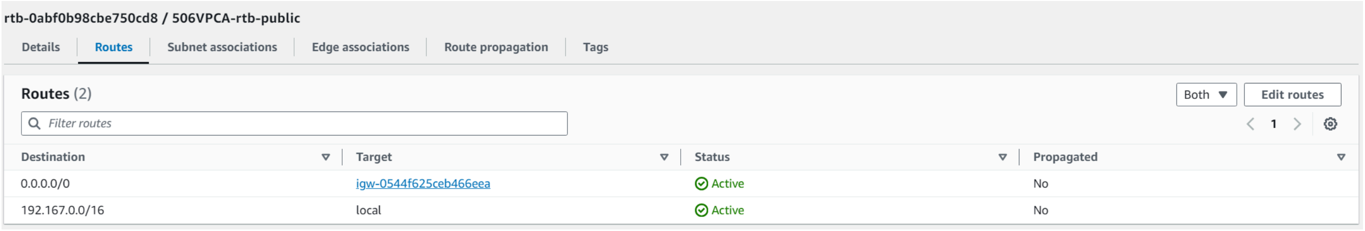


Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
506VPCA-subnet-private1-us-east-1a	subnet-0ea8e8429658c6c3f	192.167.1.0/24	–



☑	506VPCA-rtb-public	rtb-0abf0b98cbe750cd8	subnet-060429b54f093d...	–	No	vpc-0c16c5ef5c408d18e | 506V...	143345870359

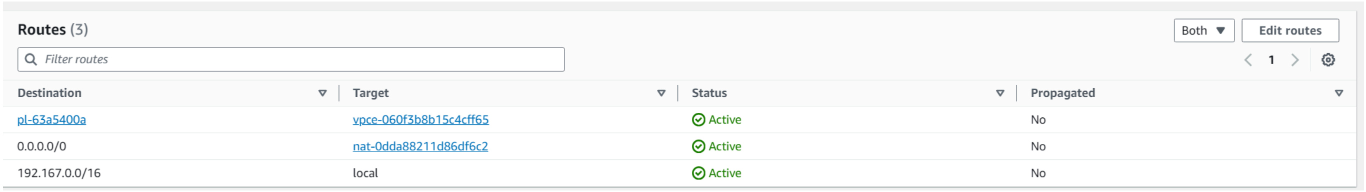
2.4 Include screen shots to show how you have configured route tables and routing targets. This should align to the topology in question 2.1 and your subnetting scheme in question 2.2.



rtb-0abf0b98cbe750cd8 / 506VPCA-rtb-public

Routes (2)

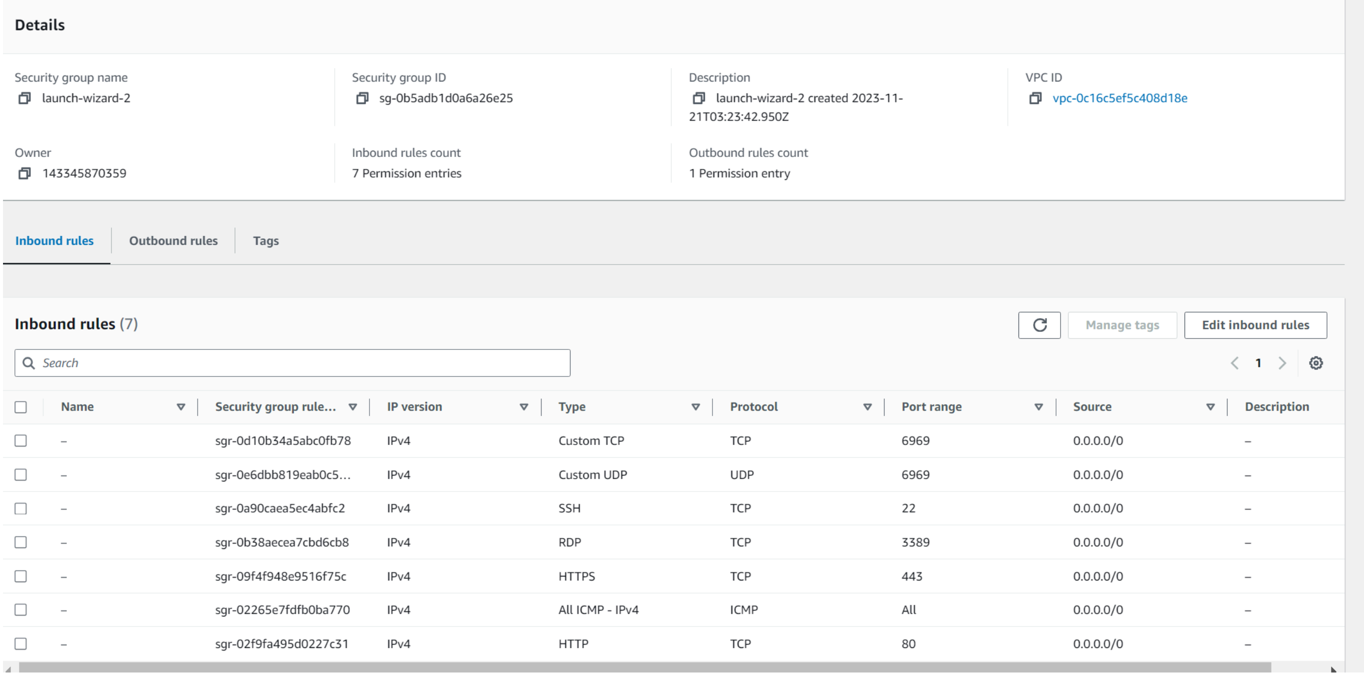
Destination	Target	Status	Propagated
0.0.0.0/0	igw-0544f625ceb466eea	Active	No
192.167.0.0/16	local	Active	No



Routes (3)

Destination	Target	Status	Propagated
pl-63a5400a	vpce-060f3b8b15c4cff65	Active	No
0.0.0.0/0	nat-0dda88211d86df6c2	Active	No
192.167.0.0/16	local	Active	No

2.5 Include screen shots to show how you have configured security controls to support your virtual network. The configuration should align to the security controls that you listed in the table in question 1.3.



Details

Security group name
launch-wizard-2

Security group ID
sg-0b5adb1d0a6a26e25

Description
launch-wizard-2 created 2023-11-21T03:23:42.950Z

VPC ID
vpc-0c16c5ef5c408d18e

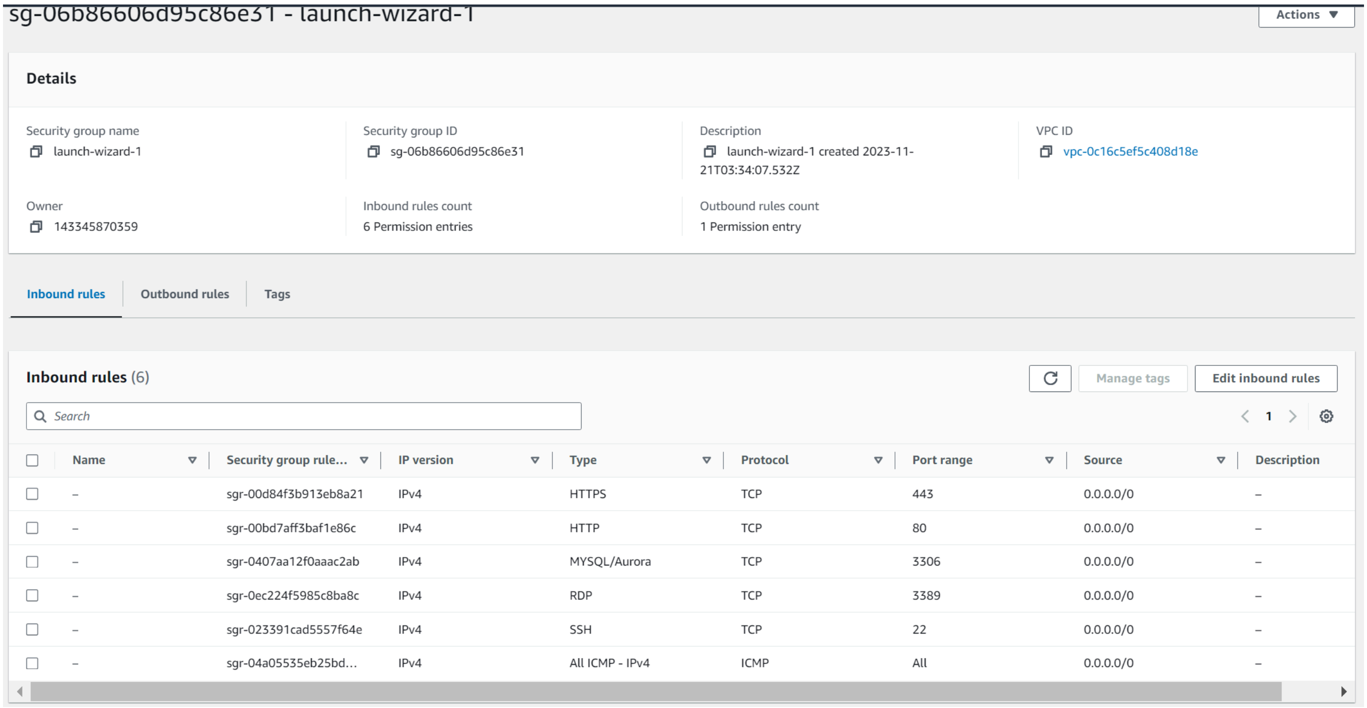
Owner
143345870359

Inbound rules count
7 Permission entries

Outbound rules count
1 Permission entry

Inbound rules (7)

☐	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☐	–	sgr-0d10b34a5abc0fb78	IPv4	Custom TCP	TCP	6969	0.0.0.0/0	–
☐	–	sgr-0e6dbb819eab0c5…	IPv4	Custom UDP	UDP	6969	0.0.0.0/0	–
☐	–	sgr-0a90caea5ec4abfc2	IPv4	SSH	TCP	22	0.0.0.0/0	–
☐	–	sgr-0b38aecea7cbd6cb8	IPv4	RDP	TCP	3389	0.0.0.0/0	–
☐	–	sgr-09f4f948e9516f75c	IPv4	HTTPS	TCP	443	0.0.0.0/0	–
☐	–	sgr-02265e7fdfb0ba770	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	–
☐	–	sgr-02f9fa495d0227c31	IPv4	HTTP	TCP	80	0.0.0.0/0	–



sg-06b86606d95c86e31 - launch-wizard-1

Details

Security group name
launch-wizard-1

Security group ID
sg-06b86606d95c86e31

Description
launch-wizard-1 created 2023-11-21T03:34:07.532Z

VPC ID
vpc-0c16c5ef5c408d18e

Owner
143345870359

Inbound rules count
6 Permission entries

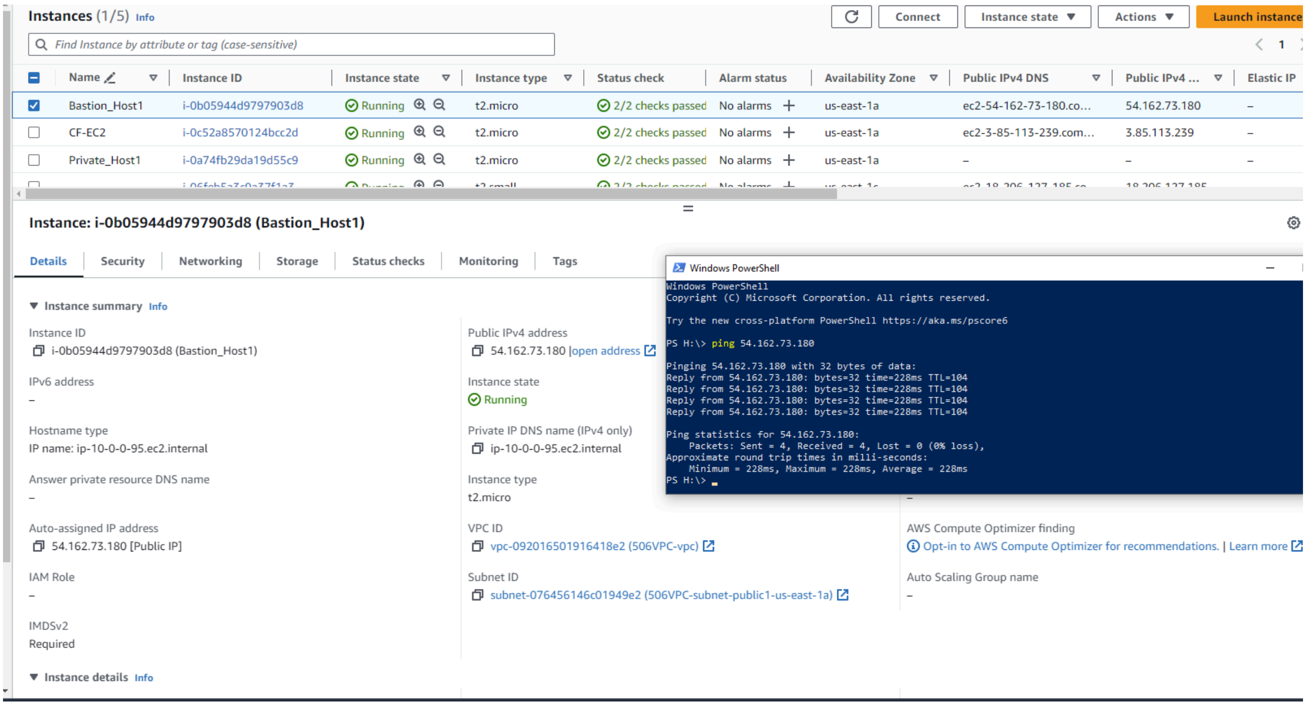
Outbound rules count
1 Permission entry

Inbound rules (6)

☐	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☐	–	sgr-00d84f3b913eb8a21	IPv4	HTTPS	TCP	443	0.0.0.0/0	–
☐	–	sgr-00bd7aff3baf1e86c	IPv4	HTTP	TCP	80	0.0.0.0/0	–
☐	–	sgr-0407aa12f0aaac2ab	IPv4	MYSQL/Aurora	TCP	3306	0.0.0.0/0	–
☐	–	sgr-0ec224f5985c8ba8c	IPv4	RDP	TCP	3389	0.0.0.0/0	–
☐	–	sgr-023391cad5557f64e	IPv4	SSH	TCP	22	0.0.0.0/0	–
☐	–	sgr-04a05535eb25bd…	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	–

2.6 Include screen shots to show how you have confirmed the expected flow of traffic through the virtual network.

2.6.1 Confirm network traffic is permitted to enter into the virtual network



☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	Bastion_Host1	i-0b05944d9797903d8	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-162-73-180.co...	54.162.73.180	–
☐	CF-EC2	i-0c52a8570124bcc2d	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-85-113-239.com...	3.85.113.239	–
☐	Private_Host1	i-0a74fb29da19d55c9	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	–	–	–

Instance: i-0b05944d9797903d8 (Bastion_Host1)

▼ Instance summary Info

Instance ID
i-0b05944d9797903d8 (Bastion_Host1)

IPv6 address
–

Hostname type
IP name: ip-10-0-0-95.ec2.internal

Answer private resource DNS name
–

Auto-assigned IP address
54.162.73.180 [Public IP]

IAM Role
–

IMDSv2
Required

Public IPv4 address
54.162.73.180 | open address

Instance state
Running

Private IP DNS name (IPv4 only)
ip-10-0-0-95.ec2.internal

Instance type
t2.micro

VPC ID
vpc-092016501916418e2 (506VPC-vpc)

Subnet ID
subnet-076456146c01949e2 (506VPC-subnet-public1-us-east-1a)

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. | Learn more

Auto Scaling Group name
–

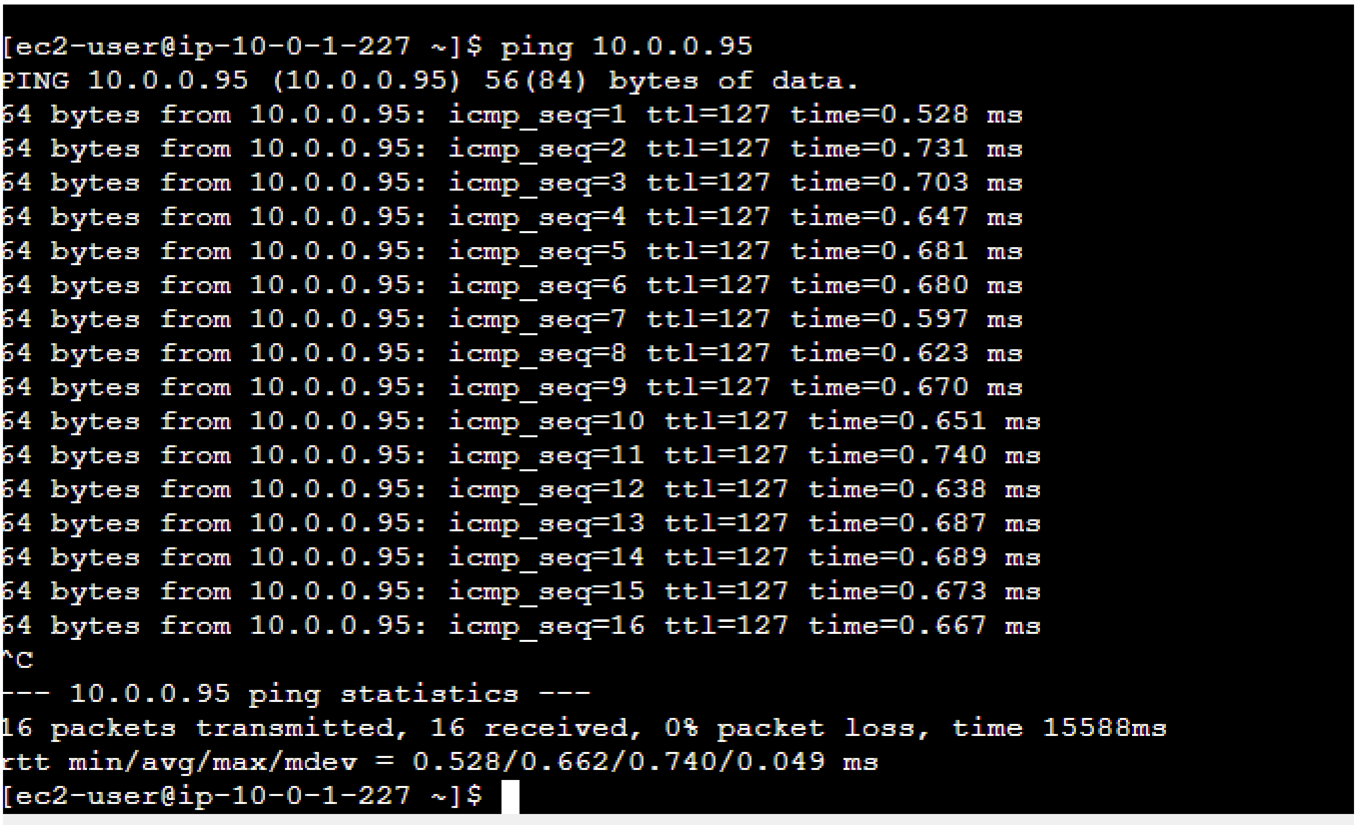
▼ Instance details Info

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS H:\> ping 54.162.73.180

Pinging 54.162.73.180 with 32 bytes of data:
Reply from 54.162.73.180: bytes=32 time=228ms TTL=104
Reply from 54.162.73.180: bytes=32 time=228ms TTL=104
Reply from 54.162.73.180: bytes=32 time=228ms TTL=104
Reply from 54.162.73.180: bytes=32 time=228ms TTL=104

Ping statistics for 54.162.73.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 228ms, Maximum = 228ms, Average = 228ms
PS H:\>
```

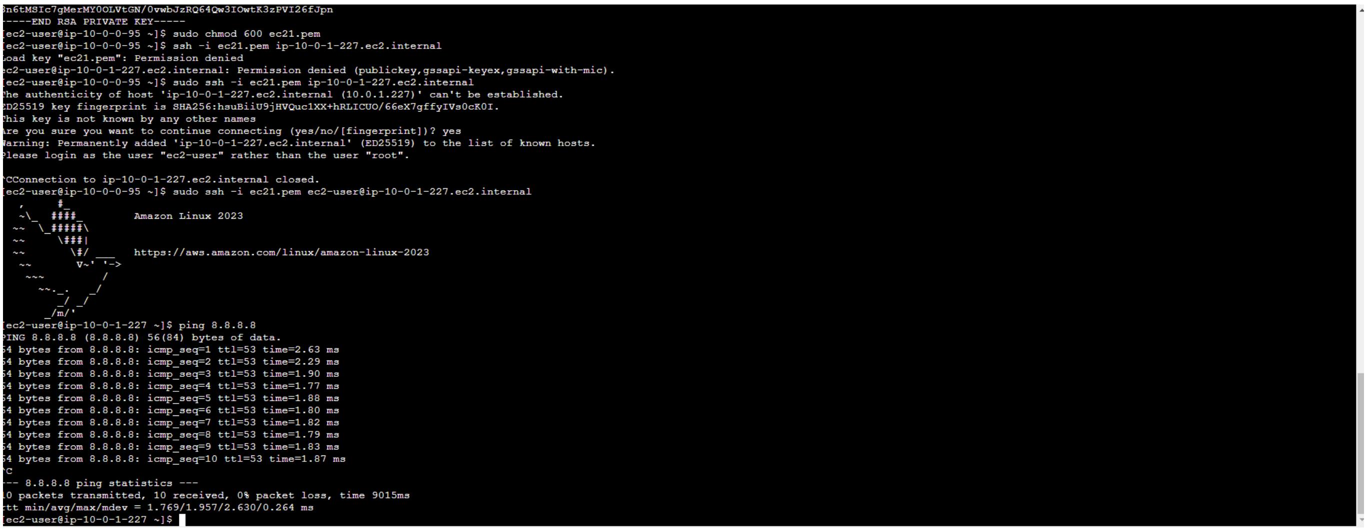
Pinging from tafe network to public ec2 ip

2.6.2 Confirm network traffic is permitted to travel through the virtual network

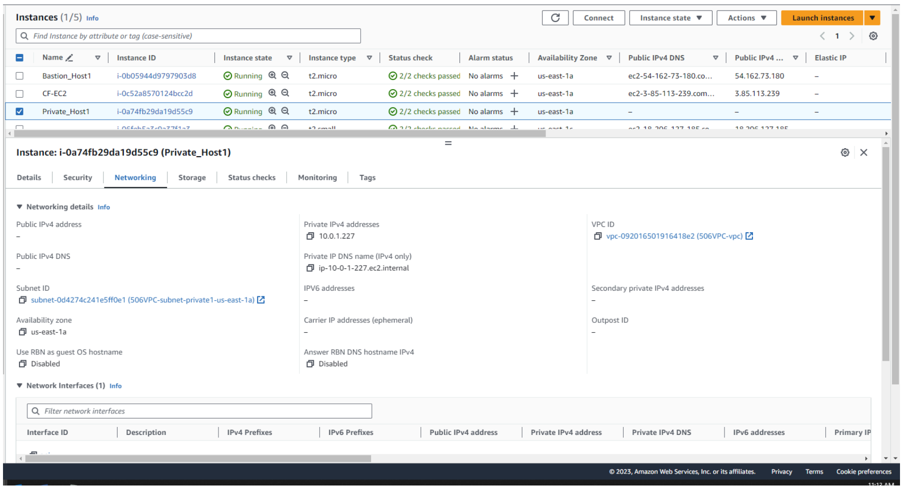


```
[ec2-user@ip-10-0-1-227 ~]$ ping 10.0.0.95
PING 10.0.0.95 (10.0.0.95) 56(84) bytes of data.
64 bytes from 10.0.0.95: icmp_seq=1 ttl=127 time=0.528 ms
64 bytes from 10.0.0.95: icmp_seq=2 ttl=127 time=0.731 ms
64 bytes from 10.0.0.95: icmp_seq=3 ttl=127 time=0.703 ms
64 bytes from 10.0.0.95: icmp_seq=4 ttl=127 time=0.647 ms
64 bytes from 10.0.0.95: icmp_seq=5 ttl=127 time=0.681 ms
64 bytes from 10.0.0.95: icmp_seq=6 ttl=127 time=0.680 ms
64 bytes from 10.0.0.95: icmp_seq=7 ttl=127 time=0.597 ms
64 bytes from 10.0.0.95: icmp_seq=8 ttl=127 time=0.623 ms
64 bytes from 10.0.0.95: icmp_seq=9 ttl=127 time=0.670 ms
64 bytes from 10.0.0.95: icmp_seq=10 ttl=127 time=0.651 ms
64 bytes from 10.0.0.95: icmp_seq=11 ttl=127 time=0.740 ms
64 bytes from 10.0.0.95: icmp_seq=12 ttl=127 time=0.638 ms
64 bytes from 10.0.0.95: icmp_seq=13 ttl=127 time=0.687 ms
64 bytes from 10.0.0.95: icmp_seq=14 ttl=127 time=0.689 ms
64 bytes from 10.0.0.95: icmp_seq=15 ttl=127 time=0.673 ms
64 bytes from 10.0.0.95: icmp_seq=16 ttl=127 time=0.667 ms
^C
--- 10.0.0.95 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15588ms
rtt min/avg/max/mdev = 0.528/0.662/0.740/0.049 ms
[ec2-user@ip-10-0-1-227 ~]$
```

2.6.3 Confirm network traffic is permitted to travel out of the virtual network



```
3n6tMSIc7gMerMY0OLVtGN/0vwbJzRQ64Qw3IOwtK3zPVI26fJpn
-----END RSA PRIVATE KEY-----
[ec2-user@ip-10-0-0-95 ~]$ sudo chmod 600 ec21.pem
[ec2-user@ip-10-0-0-95 ~]$ ssh -i ec21.pem ip-10-0-1-227.ec2.internal
Load key "ec21.pem": Permission denied
ec2-user@ip-10-0-1-227.ec2.internal: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[ec2-user@ip-10-0-0-95 ~]$ sudo ssh -i ec21.pem ip-10-0-1-227.ec2.internal
The authenticity of host 'ip-10-0-1-227.ec2.internal (10.0.1.227)' can't be established.
ED25519 key fingerprint is SHA256:hsuBiiU9jHVQuc1XX+hRLICUO/66eX7gffyIVs0cK0I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ip-10-0-1-227.ec2.internal' (ED25519) to the list of known hosts.
Please login as the user "ec2-user" rather than the user "root".

^CConnection to ip-10-0-1-227.ec2.internal closed.
[ec2-user@ip-10-0-0-95 ~]$ sudo ssh -i ec21.pem ec2-user@ip-10-0-1-227.ec2.internal
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-1-227 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=53 time=2.63 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=53 time=2.29 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=53 time=1.90 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=53 time=1.77 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=53 time=1.88 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=53 time=1.80 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=53 time=1.82 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=53 time=1.79 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=53 time=1.83 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=53 time=1.87 ms
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 1.769/1.957/2.630/0.264 ms
[ec2-user@ip-10-0-1-227 ~]$
```



Instances (1/5) Info

Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
□	Bastion_Host1	i-0b05944d9797903d8	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-54-162-73-180.co...	54.162.73.180	–
□	CF-EC2	i-0c52a8570124bcc2d	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	ec2-3-85-113-239.com...	3.85.113.239	–
☑	Private_Host1	i-0a74fb29da19d55c9	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	–	–	–

Instance: i-0a74fb29da19d55c9 (Private_Host1)

Networking details Info

Public IPv4 address
–

Private IPv4 addresses
10.0.1.227

VPC ID
vpc-092016501916418e2 (506VPC-vpc)

Public IPv4 DNS
–

Private IP DNS name (IPv4 only)
ip-10-0-1-227.ec2.internal

Subnet ID
subnet-0d4274c241e5ff0e1 (506VPC-subnet-private1-us-east-1a)

IPV6 addresses
–

Secondary private IPv4 addresses
–

Availability zone
us-east-1a

Carrier IP addresses (ephemeral)
–

Outpost ID
–

Use RBN as guest OS hostname
Disabled

Answer RBN DNS hostname IPv4
Disabled

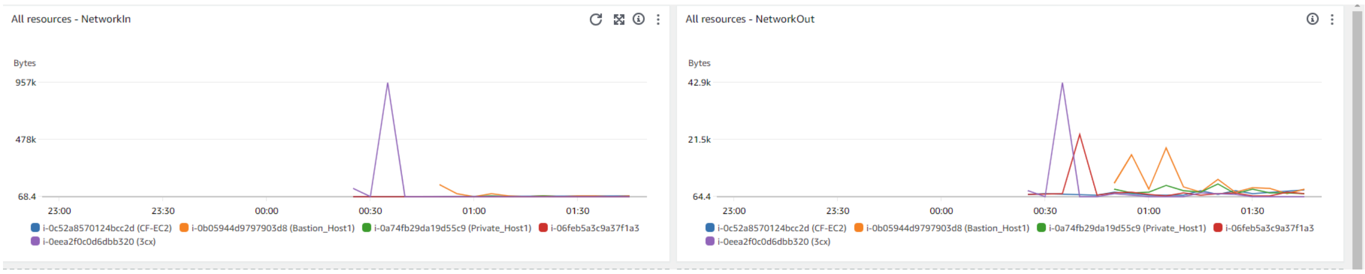
Network Interfaces (1) Info

Filter network interfaces

Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address	Private IPv4 DNS	IPv6 addresses	Primary IP

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

2.7 Include screen shots to show how you collected and monitored network traffic logs and other metrics. This can focus on collection and monitoring tasks using the AWS Cloudwatch tools that are available to you in the learning environment.



2.8 Referring to your findings in question 2.6: explain how the testing that you completed has confirmed external connectivity to resources within the virtual network, and how only permitted traffic was able to access that resource.

Testing completed showed that logging the network usage via bandwidth showed successful flow of network traffic alongside positive ping (icmp) packets being sent to and from the private ec2 instance behind the bastion host. Ontop of this, security groups were put in place to only allow specific protocols to access the vpc and subsequently the ec2 instances. There is an implicit deny all traffic unless a security group is added therefore only allowing network traffic that I added, which was http, https,rdp, mysql and icmpv4.

2.9 Referring again to question 2.6:

a) Describe one of the major problems that you encountered.

Multiple problems occurred, as you can tell by the different naming of instances i had to constantly retry and set the whole system from scratch continuously until i got it right. The first time there was an issue with assigning a public ip address to the ec2 bastion host on vpc1 which i redid entirely because there were issues with routing tables were misconfigured. I tried manually adding the ip address.

b) Describe the process you used to solve that problem.

I made sure that the correct configurations were enabled inside both the vpc and ec2 security groups and routing tables were successfully configured to allow routing traffic through the NAT gateway to the outside.

c) What tools did you use?

dependencies used: yum nano chmod aws cloudshell, powershell, external network interface device, ping command, icmp packets, aws management gui shell, vpc eni configuration shell inside aws

d) What was the step-by step-procedure that you followed (option to use a flow-chart)?

Identify the Problem: No SSH access to EC2 instances.

Review Security Groups: Adjust inbound and outbound rules.

Check NACLs: Ensure they allow necessary traffic.

Test SSH Access: Attempt to connect after each change.

Monitor VPC Flow Logs: Analyze traffic flow for blocked connections.

Repeat Steps 2-5: Until successful connection is established.

e) What did you learn from that problem solving experience?

From this experience, I learned the importance of a systematic approach to troubleshooting network issues in a cloud environment. It highlighted the need for a thorough understanding of how different components like security groups and NACLs interact and affect network connectivity. Additionally, it underscored the value of patience and careful analysis of logs and settings in diagnosing and resolving complex network issues. This experience also reinforced the importance of following best practices in network configuration to prevent such issues from occurring in the first place.

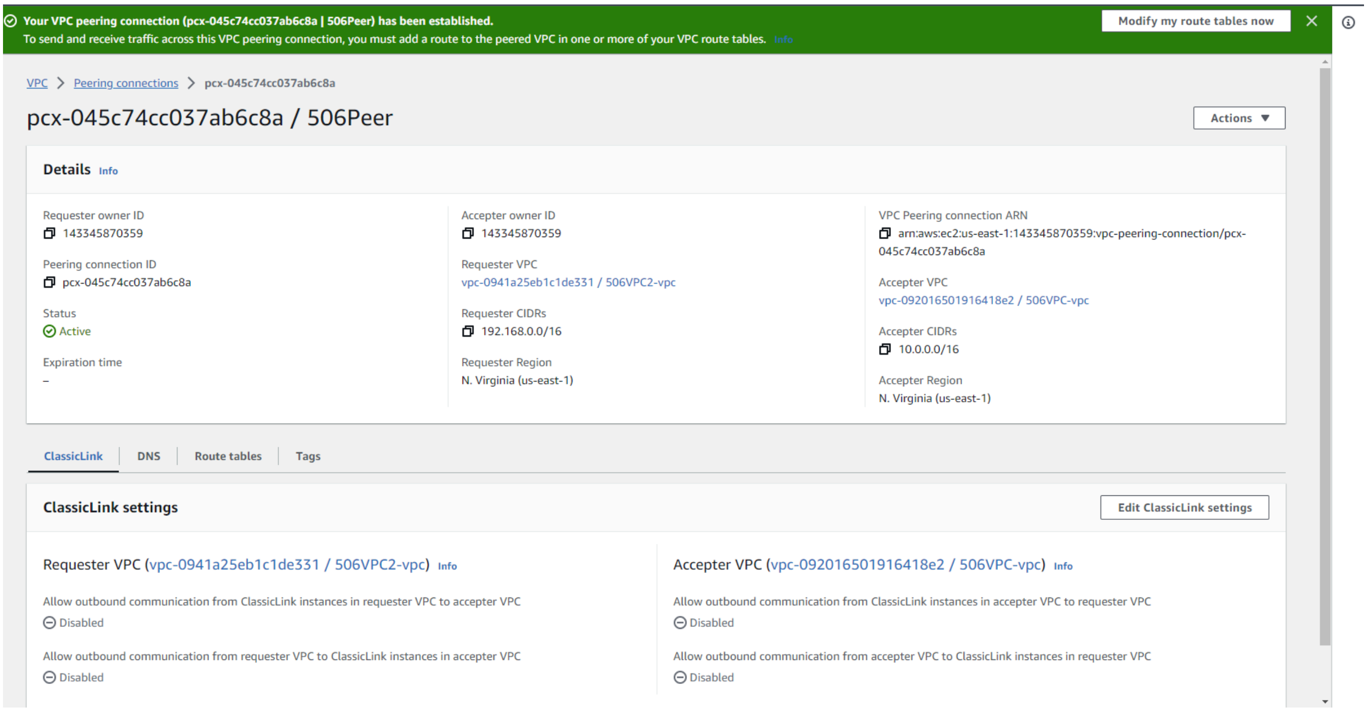
Section C – Configure Virtual Network Peering

(ICTCLD506_AT2_Peering_*yourname*.docx)

Part 3 – Establish Peering Connection between Two Virtual Networks

3.1 Include screen shots to show how you established a VPC peering connection between two VPCs.

Your peering connection should allow routing of traffic between the two VPCs using private IPv4 addresses.



Your VPC peering connection (pcx-045c74cc037ab6c8a | 506Peer) has been established.
To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. Info

VPC > Peering connections > pcx-045c74cc037ab6c8a

pcx-045c74cc037ab6c8a / 506Peer

Details Info

Requester owner ID
143345870359

Peering connection ID
pcx-045c74cc037ab6c8a

Status
Active

Expiration time
–

Accepter owner ID
143345870359

Requester VPC
vpc-0941a25eb1c1de331 / 506VPC2-vpc

Requester CIDRs
192.168.0.0/16

Requester Region
N. Virginia (us-east-1)

VPC Peering connection ARN
arn:aws:ec2:us-east-1:143345870359:vpc-peering-connection/pcx-045c74cc037ab6c8a

Accepter VPC
vpc-092016501916418e2 / 506VPC-vpc

Accepter CIDRs
10.0.0.0/16

Accepter Region
N. Virginia (us-east-1)

ClassicLink settings

Requester VPC (vpc-0941a25eb1c1de331 / 506VPC2-vpc) Info

Allow outbound communication from ClassicLink instances in requester VPC to accepter VPC
Disabled

Allow outbound communication from requester VPC to ClassicLink instances in accepter VPC
Disabled

Accepter VPC (vpc-092016501916418e2 / 506VPC-vpc) Info

Allow outbound communication from ClassicLink instances in accepter VPC to requester VPC
Disabled

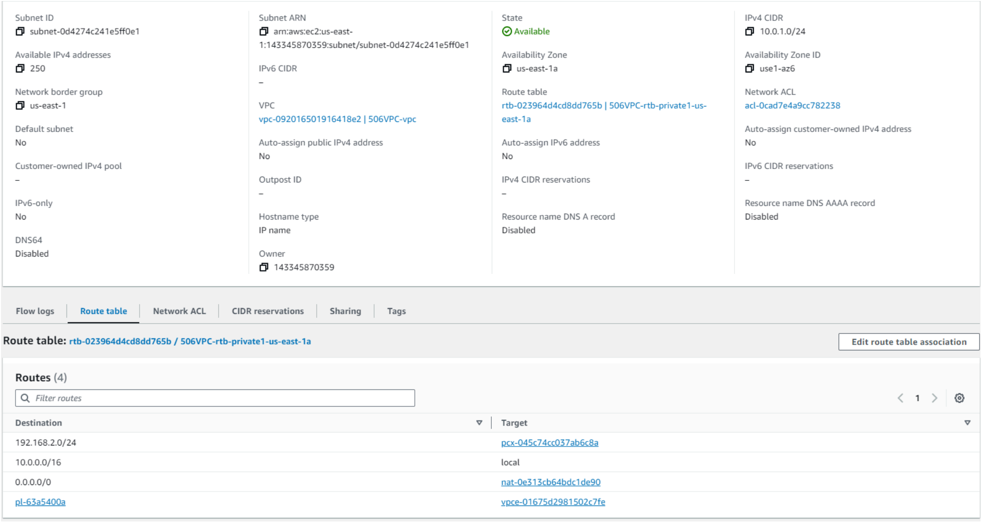
Allow outbound communication from accepter VPC to ClassicLink instances in requester VPC
Disabled

3.2 Include screen shots to show how you adjusted routing tables to allow traffic between the two VPCs.

Your peering connection should allow routing of traffic between the two VPCs using private IPv4 addresses. The route should point to the CIDR block (or portion of the CIDR block) of the peer VPC in the VPC peering connection and specify the VPC peering connection as the target.

I adjusted the VPC tables to route the others private subnet through the VPC peering connection. I was able to do this by editing the Route tables of each private subnet respectively, here you can see what I've changed:

This is the private host in the Bastion ec2 network group (506VPC), and here is the route table i edited, its the first entry in the table itself.



Subnet ID
subnet-0d4274c241e5ff0e1

Available IPv4 addresses
250

Network border group
us-east-1

Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

Subnet ARN
arn:aws:ec2:us-east-1:143345870359:subnet/subnet-0d4274c241e5ff0e1

IPv6 CIDR
–

VPC
vpc-092016501916418e2 | 506VPC-vpc

Auto-assign public IPv4 address
No

Outpost ID
–

Hostname type
IP name

Owner
143345870359

State
Available

Availability Zone
us-east-1a

Route table
rtb-023964d4cd8dd765b | 506VPC-rtb-private1-us-east-1a

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

Resource name DNS A record
Disabled

IPv4 CIDR
10.0.1.0/24

Availability Zone ID
use1-az6

Network ACL
acl-0cad7e4a9cc782238

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Resource name DNS AAAA record
Disabled

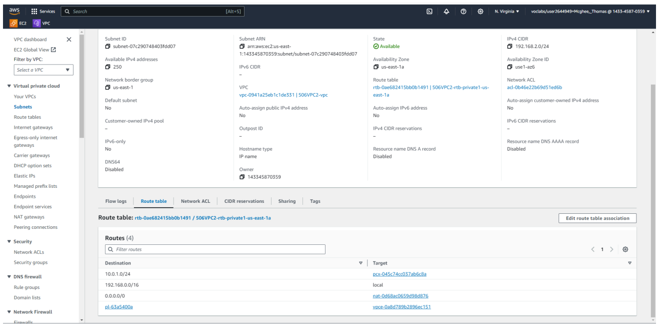
Route table: rtb-023964d4cd8dd765b / 506VPC-rtb-private1-us-east-1a

Routes (4)

Destination	Target
192.168.2.0/24	pcx-045c74cc037ab6c8a
10.0.0.0/16	local
0.0.0.0/0	nat-0e313cb64bdc1de90
pl-63a5400a	vpce-01675d2981502c7fe

© TAFE Queensland. Uncontrolled copy if printed. Refer to TAFE Queensland intranet for current version of document.

For 506VPC2 I did the exact same.



Subnet ID
subnet-07c290748403fdd07

Available IPv4 addresses
250

Network border group
us-east-1

Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

Subnet ARN
arn:aws:ec2:us-east-1:143345870359:subnet/subnet-07c290748403fdd07

IPv6 CIDR
–

VPC
vpc-0941a25eb1c1de331 | 506VPC2-vpc

Auto-assign public IPv4 address
No

Outpost ID
–

Hostname type
IP name

Owner
143345870359

State
Available

Availability Zone
us-east-1a

Route table
rtb-0ae682415bb0b1491 | 506VPC2-rtb-private1-us-east-1a

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

Resource name DNS A record
Disabled

IPv4 CIDR
192.168.2.0/24

Availability Zone ID
use1-az6

Network ACL
acl-0b46e22b69d51ed6b

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

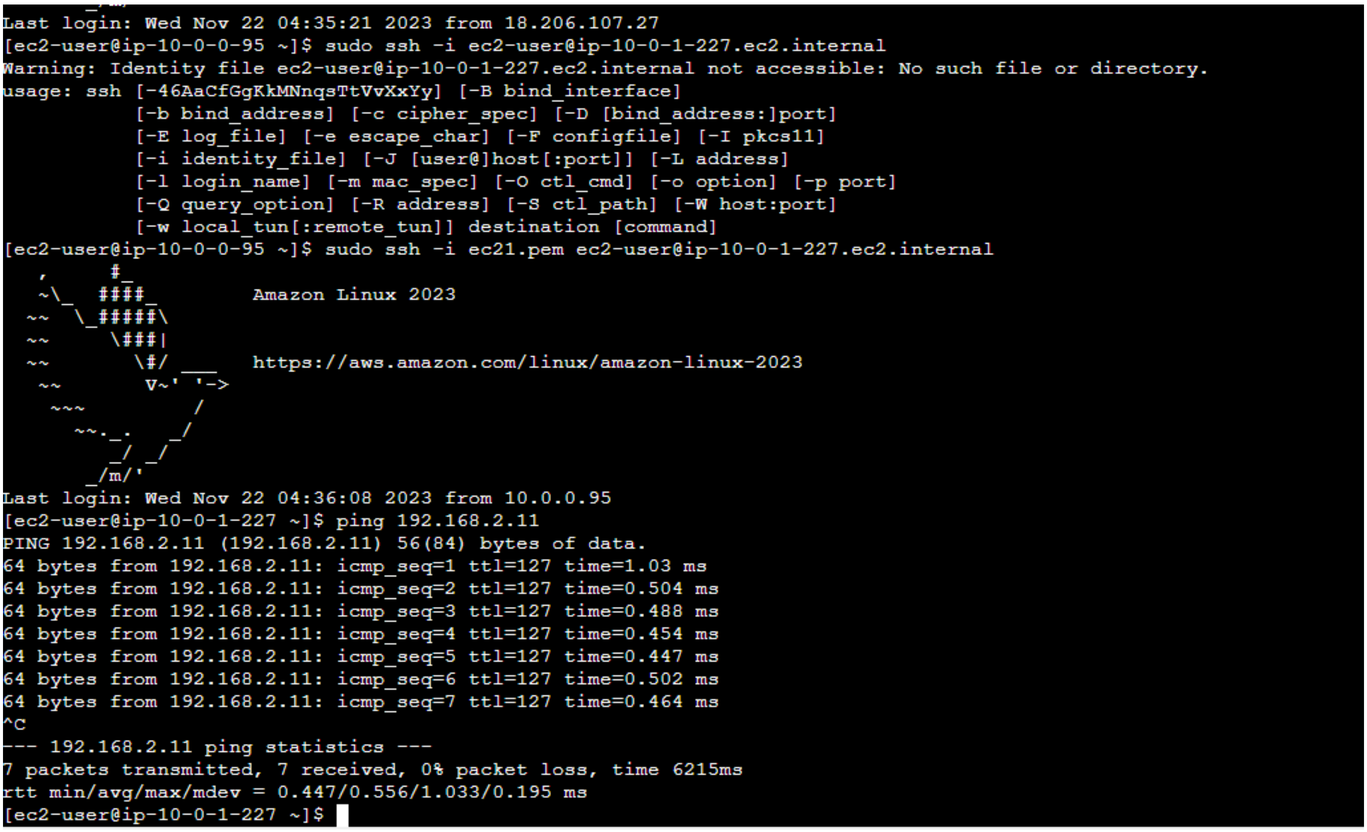
Resource name DNS AAAA record
Disabled

Route table: rtb-0ae682415bb0b1491 / 506VPC2-rtb-private1-us-east-1a

Routes (4)

Destination	Target
10.0.1.0/24	pcx-045c74cc037ab6c8a
192.168.0.0/16	local
0.0.0.0/0	nat-0d68ac0659d98d876
pl-63a5400a	vpce-0a8d789b2896ec151

I initially confused myself thinking the VPC network address was the destination between each peer however that doesn't work due to the fact it is unable to find the connection as it will always be the lowest subnet range that it searches for a connection with and will not make the connection work.



```
Last login: Wed Nov 22 04:35:21 2023 from 18.206.107.27
[ec2-user@ip-10-0-0-95 ~]$ sudo ssh -i ec2-user@ip-10-0-1-227.ec2.internal
Warning: Identity file ec2-user@ip-10-0-1-227.ec2.internal not accessible: No such file or directory.
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]
[ec2-user@ip-10-0-0-95 ~]$ sudo ssh -i ec21.pem ec2-user@ip-10-0-1-227.ec2.internal
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Wed Nov 22 04:36:08 2023 from 10.0.0.95
[ec2-user@ip-10-0-1-227 ~]$ ping 192.168.2.11
PING 192.168.2.11 (192.168.2.11) 56(84) bytes of data.
64 bytes from 192.168.2.11: icmp_seq=1 ttl=127 time=1.03 ms
64 bytes from 192.168.2.11: icmp_seq=2 ttl=127 time=0.504 ms
64 bytes from 192.168.2.11: icmp_seq=3 ttl=127 time=0.488 ms
64 bytes from 192.168.2.11: icmp_seq=4 ttl=127 time=0.454 ms
64 bytes from 192.168.2.11: icmp_seq=5 ttl=127 time=0.447 ms
64 bytes from 192.168.2.11: icmp_seq=6 ttl=127 time=0.502 ms
64 bytes from 192.168.2.11: icmp_seq=7 ttl=127 time=0.464 ms
^C
--- 192.168.2.11 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6215ms
rtt min/avg/max/mdev = 0.447/0.556/1.033/0.195 ms
[ec2-user@ip-10-0-1-227 ~]$
```

3.3 Create task sign-off letter which summarises the contents of the portfolio and presents your documents for review and approval. Your sign-off sheet should be addressed to the Manager of the IT team for comment and/or approval.

Task Sign-Off Letter

Name: Tom McGhee
Instructor: Cloud Manager

Date: 20/10/2023

Dear Cloud Manager, I have designed a cloud network which provides and fulfills the business concerns of DayDream Travel agency in terms of redundancy, (using Multiple EC2 instances), Security Elements (SSH keys, Security groups that only allow specific traffic required and a bastion host which protects inside network from active threats. System Monitoring (Cloudwatch services), maintenance schedules. The strategic plan is what I'll be talking about in this sign off letter. This Report has delved into the vast arrays of how to setup the network. From the topological diagram, to evaluating the AWS needs with multiple services explained, and then the implementation of the overall cloud network focusing on Peering connections inside AWS as the cornerstone of the design itself. Plan to transition: Move all instances into their respective fields, Amazon S3, Amazon EC2, AWS Shield & AWS Route 53, AWS VPN, Amazon RDS & AWS Backup, AWS Identity and Access Management (IAM) & AWS Key, Management Service (KMS), Amazon CloudWatch & AWS Systems Manager, Amazon WorkMail, Amazon WorkDocs. All these services enable the company to transition to a cloud based network which would support the companies current and future business needs. This plan provides a solution, and as Manager I need your permission to implement this.

Sign Below if you agree to the above changes that will be implemented into your business:

Signature:

~~Completion and Submission~~

~~Check all three of your portfolio documents:~~

~~1. ICTCLD506_AT2_Design_*yourname*.docx~~

~~2. ICTCLD506_AT2_Configuration_*yourname*.docx~~

~~3. ICTCLD506_AT2_Peering_*yourname*.docx~~

~~for consistency and accuracy. Proofread and edit the text as needed to assure proper sentence and paragraph structure. Check that the filenames are correct according to the list above.~~

~~At the end of the third document, check your task sign-off letter which should summarise the contents of the portfolio and present your documents for review and approval. Your sign-off sheet should be addressed to the Manager of the IT team for comment and/or approval.~~

Ignore above, concatenated all parts as single file.

© TAFE Queensland. Uncontrolled copy if printed. Refer to TAFE Queensland intranet for current version of document.

Submit all three documents into the Connect folder designated by your instructor.

End of Assessment