

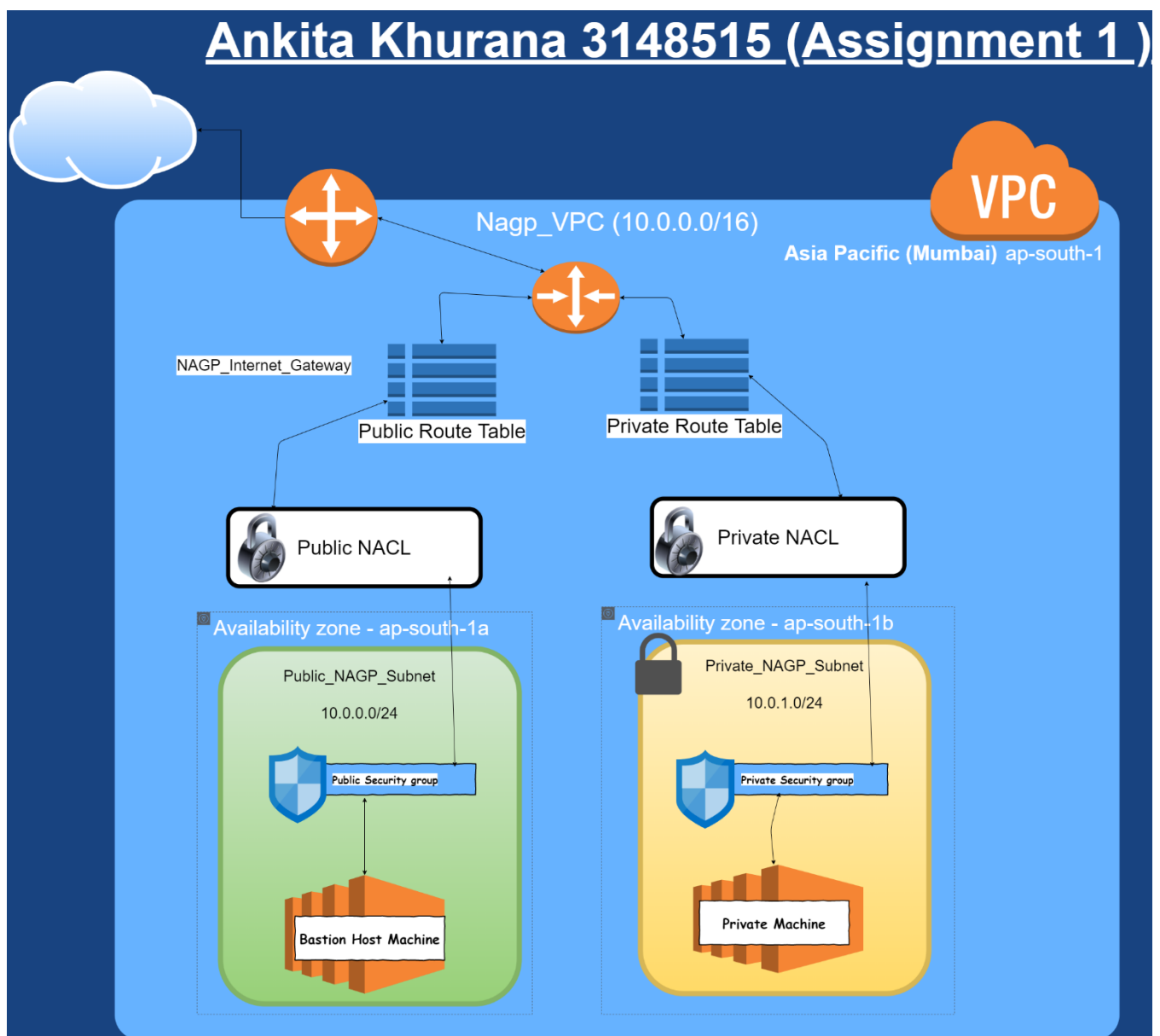
CLOUD COMPUTING ASSIGNMENT 1

- Ankita Khurana

- 3148515

Note:

1. As mentioned in the group (No NAT Gateway/Instance) is supposed to be added to the architecture, hence only one Public subnet is made for the Bastion Host. And one private subnet for the private machine.
2. S3 Bucket was not added to any Subnet from CLI, hence not included in the architecture provided.



Architecture

RESOURCES AND SERVICES used till date for XYZ project

1. S3 Buckets list

Archive all of your long-term data into Amazon S3 Glacier Deep Archive to save costs. [Learn more »](#) [Documentation](#)

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. [Switch to the new console.](#)

S3 buckets [Discover the console](#)

Search for buckets All access types

+ Create bucket Edit public access settings Empty Delete 1 Buckets 1 Regions

| <input type="checkbox"/> Bucket name | Access | Region | Date created |
|---|-------------------------------|-----------------------|-----------------------------------|
| <input type="checkbox"/> ankita-nagp-bucket | Bucket and objects not public | Asia Pacific (Mumbai) | Jun 16, 2020 11:11:24 AM GMT+0530 |

2. EC2 Machines : (Bastion host on Public subnet + Private Ec2 on private subnet)

a. Logging into Public Bastion Host

```
ankitakhurana@Ankita3148515 MINGW64 ~/Desktop
$ ssh -i "nagppublic.pem" ec2-user@13.234.136.193
Last login: Tue Jun 16 03:29:09 2020 from 106.215.82.111

 _ _ | _ _ | _ _ )
 _ | ( _ _ | _ _ /   Amazon Linux AMI
 _ _ | \ _ _ | _ _ |

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
```

b. Logging into Private Machine from Bastion Host

```
[ec2-user@ip-10-0-0-139 ~]$ chmod 400 key.pem
[ec2-user@ip-10-0-0-139 ~]$ ssh -i "key.pem" ec2-user@10.0.1.53

 _ _ | _ _ | _ _ )
 _ | ( _ _ | _ _ /   Amazon Linux AMI
 _ _ | \ _ _ | _ _ |

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
[ec2-user@ip-10-0-1-53 ~]$ |
```

POLICIES

1. Policy for **DEVELOPERS** (R/W on S3 Buckets + Full access (Create etc) on EC2)

The screenshot shows the AWS IAM Policy console for the policy 'nagp_developers_group_policy'. The 'Permissions' tab is selected, showing a table of permissions. The table has columns for Service, Access level, Resource, and Request condition. Two permissions are listed: EC2 with Full access, and S3 with Full: List, Read, Write. A red circle highlights the 'S3' entry in the original image.

| Service | Access level | Resource | Request condition |
|---------|-------------------------|---------------|-------------------|
| EC2 | Full access | All resources | None |
| S3 | Full: List, Read, Write | All resources | None |

Example: On logging from a user in developer group (Writing in Bucket)

The screenshot shows the Amazon S3 console for the bucket 'ankita-nagp-bucket'. The 'Overview' tab is selected. A search bar is at the top. Below it are buttons for Upload, Create folder, Download, and Actions. A table lists the contents of the bucket. One entry is visible: 'folderMadebyDeveloper'. A red circle highlights this entry in the original image.

| Name | Last modified | Size | Storage class |
|-----------------------|---------------|------|---------------|
| folderMadebyDeveloper | -- | -- | -- |

2. Policy for roles/users who wants to have min permissions (Assignment checkers)

Policies > Nagp_Assignment_Checkers

Summary Delete policy

Policy ARN arn:aws:iam::495336230329:policy/Nagp_Assignment_Checkers

Description Nagp_Assignment_Checkers Permissions

Permissions Policy usage Policy versions Access Advisor

Policy summary { } JSON Edit policy ?

| Service ▾ | Access level | Resource | Request condition |
|--|------------------|---------------|-------------------|
| Allow (2 of 232 services) Show remaining 230 | | | |
| EC2 | Full: List, Read | All resources | None |
| S3 | Full: List, Read | All resources | None |

GROUPS

1. **Developer group** (For giving access to Services for development, two users made under this group)

IAM > Groups > nagp_developers

▼ Summary

Group ARN: arn:aws:iam::495336230329:group/nagp_developers

Users (in this group): 2

Path: /

Creation Time: 2020-06-14 12:52 UTC+0530

Users | **Permissions** | Access Advisor

Managed Policies

The following managed policies are attached to this group. You can attach up to 10 managed policies.

[Attach Policy](#)

| Policy Name | Actions |
|------------------------------|---|
| nagp_developers_group_policy | Show Policy Detach Policy Simulate Policy |

USERS

1. Developers user accounts made for the development team

[Add user](#) [Delete user](#)

Find users by username or access key Showing 2 results

| <input type="checkbox"/> | User name ▼ | Groups | Access key age | Password age | Last activity | MFA |
|--------------------------|-------------|---------------------------------|----------------|--------------|---------------|-------------|
| <input type="checkbox"/> | User1 | nagp_developers | None | Yesterday | Yesterday | Not enabled |
| <input type="checkbox"/> | User2 | nagp_developers | None | Yesterday | Today | Not enabled |

1. Single checker user account made for temp access

Users > Checker

Summary

User ARN arn:aws:iam::495336230329:user/Checker

Path /

Creation time 2020-06-16 13:02 UTC+0530

Permissions | **Groups** | Tags (1) | Security credentials | Access Advisor

▼ Permissions policies (1 policy applied)

[Add permissions](#)

| Policy name ▼ | Policy type ▼ |
|--|----------------|
| Attached directly | |
| ▶ Nagp_Assignment_Checkers | Managed policy |

VPC COMPONENTS

1. Nagp_VPC : 10.0.0.0/16

The screenshot shows the AWS VPC console with a table of VPCs. The first VPC, 'Nagp_VPC', is selected and highlighted in blue. A red arrow points to the selection checkbox. Below the table, the details for 'Nagp_VPC' are displayed.

| Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | DHCP options set | Main Route 1 |
|----------|-----------------------|-----------|-------------|-----------|------------------|---------------|
| Nagp_VPC | vpc-094f864a85fe52c9f | available | 10.0.0.0/16 | - | dopt-687b8103 | rtb-030eb8... |

VPC: vpc-094f864a85fe52c9f

Description

| | | | |
|------------------|-----------------------|----------------|-----------------------|
| VPC ID | vpc-094f864a85fe52c9f | Tenancy | default |
| State | available | Default VPC | No |
| IPv4 CIDR | 10.0.0.0/16 | IPv6 CIDR | - |
| IPv6 Pool | - | DNS resolution | Enabled |
| Network ACL | acl-0df32dca26aad6123 | DNS hostnames | Disabled |
| DHCP options set | dopt-687b8103 | Route table | rtb-030eb8292851b3ce5 |
| Owner | 495336230329 | | |

2. Public_Nagp_Subnet : 10.0.0.0/24

The screenshot shows the AWS VPC console with a table of subnets. The first subnet, 'Public_NA...', is selected and highlighted in blue. Below the table, the details for 'Public_Nagp_Subnet' are displayed.

| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 CIDR | Availability Zone |
|---------------|--------------------------|-----------|-----------------------------|-------------|----------------|-----------|-------------------|
| Public_NA... | subnet-04c9ee257c6ef6422 | available | vpc-094f864a85fe52c9f ... | 10.0.0.0/24 | 250 | - | ap-south-1a |
| Private_Na... | subnet-07a193036e44836b1 | available | vpc-094f864a85fe52c9f ... | 10.0.1.0/24 | 250 | - | ap-south-1b |

Subnet: subnet-04c9ee257c6ef6422

Description

| | | | |
|---------------------------------|--|--------------------------|--|
| Subnet ID | subnet-04c9ee257c6ef6422 | State | available |
| VPC | vpc-094f864a85fe52c9f Nagp_VPC | IPv4 CIDR | 10.0.0.0/24 |
| Available IPv4 Addresses | 250 | IPv6 CIDR | - |
| Availability Zone | ap-south-1a (aps1-az1) | Route Table | rtb-03d4c03443cd0e764 Public_Nagp_RT |
| Network ACL | acl-0c8659473a55ddea6 Public_nagp_NACL | Default subnet | No |
| Auto-assign public IPv4 address | No | Auto-assign IPv6 address | No |
| Owner | 495336230329 | | |

3. Private_Nagp_Subnet: 10.0.1.0/24

The screenshot shows the AWS VPC console with a table of subnets. The second subnet, 'Private_Na...', is selected and highlighted in blue. Below the table, the details for 'Private_Nagp_Subnet' are displayed.

| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 CIDR | Availability Zone |
|---------------|--------------------------|-----------|-----------------------------|-------------|----------------|-----------|-------------------|
| Public_NA... | subnet-04c9ee257c6ef6422 | available | vpc-094f864a85fe52c9f ... | 10.0.0.0/24 | 250 | - | ap-south-1a |
| Private_Na... | subnet-07a193036e44836b1 | available | vpc-094f864a85fe52c9f ... | 10.0.1.0/24 | 250 | - | ap-south-1b |

Subnet: subnet-07a193036e44836b1

Description

| | | | |
|---------------------------------|---|--------------------------|---|
| Subnet ID | subnet-07a193036e44836b1 | State | available |
| VPC | vpc-094f864a85fe52c9f Nagp_VPC | IPv4 CIDR | 10.0.1.0/24 |
| Available IPv4 Addresses | 250 | IPv6 CIDR | - |
| Availability Zone | ap-south-1b (aps1-az3) | Route Table | rtb-0f2bc0c480711a6de Private_Nagp_RT |
| Network ACL | acl-0433a1727a6b22dac Private_Nagp_NACL | Default subnet | No |
| Auto-assign public IPv4 address | No | Auto-assign IPv6 address | No |
| Owner | 495336230329 | | |

4. Public_nagp_RT (Route table)

Filter by tags and attributes or search by keyword

1 to 4 of 4

| Name | Route Table ID | Explicit subnet association | Edge associations | Main |
|-----------------|-----------------------|-----------------------------|-------------------|------|
| Public_Nagp_RT | rtb-03d4c03443cd0e764 | subnet-04c9ee257c6ef6422 | - | No |
| Private_Nagp_RT | rtb-0f2bc0c480711a6de | subnet-07a193036e44836b1 | - | No |

Route Table: rtb-03d4c03443cd0e764

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status | Propagated |
|-------------|------------------------------|--------|------------|
| 10.0.0.0/16 | local | active | No |
| 0.0.0.0/0 | <u>igw-0432df096eae556b2</u> | active | No |

5. Private_nagp_RT (Route table)

Filter by tags and attributes or search by keyword

1 to 4 of 4

| Name | Route Table ID | Explicit subnet association | Edge associations | Main |
|-----------------|-----------------------|-----------------------------|-------------------|------|
| Public_Nagp_RT | rtb-03d4c03443cd0e764 | subnet-04c9ee257c6ef6422 | - | No |
| Private_Nagp_RT | rtb-0f2bc0c480711a6de | subnet-07a193036e44836b1 | - | No |

Route Table: rtb-0f2bc0c480711a6de

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status | Propagated |
|-------------|--------|--------|------------|
| 10.0.0.0/16 | local | active | No |

6. Private_nagp_NACL : inbound rules

Filter by tags and attributes or search by keyword

1 to 4 of 4

| Name | Network ACL ID | Associated with | Default | VPC | Owner |
|---------------|---------------------|---------------------|---------|----------------------------------|--------------|
| Private_Na... | acl-0433a1727a6b... | subnet-07a19303... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| Public_nag... | acl-0c8659473a55... | subnet-04c9ee257... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |

Details Inbound Rules Outbound Rules Subnet associations Tags

Edit inbound rules

View All rules

| Rule # | Type | Protocol | Port Range | Source | Allow / Deny |
|--------|-----------------|----------|--------------|-------------|--------------|
| 100 | SSH (22) | TCP (6) | 22 | 10.0.0.0/24 | ALLOW |
| 110 | Custom TCP Rule | TCP (6) | 1024 - 65535 | 0.0.0.0/0 | ALLOW |
| * | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

7. Private_nagp_NACL : outbound rules

Filter by tags and attributes or search by keyword

1 to 4 of 4

| Name | Network ACL ID | Associated with | Default | VPC | Owner |
|---------------------|---------------------|---------------------|---------|----------------------------------|--------------|
| Private_Na... | acl-0433a1727a6b... | subnet-07a19303... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| Public_nag... | acl-0c8659473a55... | subnet-04c9ee257... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| acl-0df32dca26aa... | | | Yes | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |

Network ACL: acl-0433a1727a6b22dac

Details Inbound Rules **Outbound Rules** Subnet associations Tags

Edit outbound rules

View All rules

| Rule # | Type | Protocol | Port Range | Destination | Allow / Deny |
|--------|-----------------|----------|--------------|-------------|--------------|
| 100 | Custom TCP Rule | TCP (6) | 1024 - 65535 | 0.0.0.0/0 | ALLOW |
| * | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

8. Public_nagp_NACL : inbound rules

Filter by tags and attributes or search by keyword

1 to 4 of 4

| Name | Network ACL ID | Associated with | Default | VPC | Owner |
|---------------------|---------------------|---------------------|---------|----------------------------------|--------------|
| Private_Na... | acl-0433a1727a6b... | subnet-07a19303... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| Public_nag... | acl-0c8659473a55... | subnet-04c9ee257... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| acl-0df32dca26aa... | | | Yes | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |

Edit inbound rules

View All rules

| Rule # | Type | Protocol | Port Range | Source | Allow / Deny |
|--------|-----------------|----------|--------------|-----------|--------------|
| 100 | HTTP* (8080) | TCP (6) | 8080 | 0.0.0.0/0 | ALLOW |
| 110 | HTTPS* (8443) | TCP (6) | 8443 | 0.0.0.0/0 | ALLOW |
| 120 | SSH (22) | TCP (6) | 22 | 0.0.0.0/0 | ALLOW |
| 130 | Custom TCP Rule | TCP (6) | 1024 - 65535 | 0.0.0.0/0 | ALLOW |
| * | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

9. Public_nagp_NACL : outbound rules

Filter by tags and attributes or search by keyword

1 to 4 of 4

| Name | Network ACL ID | Associated with | Default | VPC | Owner |
|---------------------|---------------------|---------------------|---------|----------------------------------|--------------|
| Private_Na... | acl-0433a1727a6b... | subnet-07a19303... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| Public_nag... | acl-0c8659473a55... | subnet-04c9ee257... | No | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |
| acl-0df32dca26aa... | | | Yes | vpc-094f864a85fe52c9f Nagp_VPC | 495336230329 |

Details Inbound Rules **Outbound Rules** Subnet associations Tags

Edit outbound rules

View All rules

| Rule # | Type | Protocol | Port Range | Destination | Allow / Deny |
|--------|-----------------|----------|--------------|-------------|--------------|
| 100 | Custom TCP Rule | TCP (6) | 1024 - 65535 | 0.0.0.0/0 | ALLOW |
| 110 | SSH (22) | TCP (6) | 22 | 0.0.0.0/0 | ALLOW |
| * | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

10. Private_Nagp_SG (Security Group) : inbound rules

Security Groups (1/4) Info

Filter security groups

| Name | Security group ID | Security group name | VPC ID |
|------|----------------------|---------------------|-----------------------|
| - | sg-09dc45e95e214306e | Private_Nagp_SG | vpc-094f864a85fe52c9f |

Details | **Inbound rules** | Outbound rules | Tags

Inbound rules Edit inbound rules

| Type | Protocol | Port range | Source | Description - optional |
|------|----------|------------|---------------------------------------|------------------------|
| SSH | TCP | 22 | sg-0fd3d0501f74c911d (Public_Nagp_SG) | - |

11. Private_Nagp_SG (Security Group) : outbound rules

Security Groups (1/4) Info

Filter security groups

| Name | Security group ID | Security group name | VPC ID |
|------|----------------------|---------------------|-----------------------|
| - | sg-09dc45e95e214306e | Private_Nagp_SG | vpc-094f864a85fe52c9f |

Details | Inbound rules | **Outbound rules** | Tags

Outbound rules Edit outbound rules

| Type | Protocol | Port range | Destination | Description - optional |
|-------------|----------|------------|-------------|------------------------|
| All traffic | All | All | 0.0.0.0/0 | - |

12. Public_Nagp_SG (Security Group) : inbound rules

Security Groups (1/4) Info

Filter security groups

| Name | Security group ID | Security group name | VPC ID |
|------|----------------------|---------------------|-----------------------|
| - | sg-0fd3d0501f74c911d | Public_Nagp_SG | vpc-094f864a85fe52c9f |

Details | **Inbound rules** | Outbound rules | Tags

Inbound rules Edit inbound rules

| Type | Protocol | Port range | Source | Description - optional |
|------|----------|------------|-----------|------------------------|
| SSH | TCP | 22 | 0.0.0.0/0 | - |

13. Public_Nagp_SG (Security Group) : outbound rules

VPC > Security Groups

Security Groups (1/4) Info

Filter security groups

< 1 >

Name

Security group ID

Security group name

VPC ID

☒

-

sg-0fd3d0501f74c911d

Public_Nagp_SG

vpc-094f864a85fe52c9f

Outbound rules

Edit outbound rules

| Type | Protocol | Port range | Destination | Description - optional |
|-------------|----------|------------|-------------|------------------------|
| All traffic | All | All | 0.0.0.0/0 | - |

14. Internet Gateway

VPC > Internet gateways

Internet gateways (1/2) Info

Filter internet gateways

< 1 >

Name

Internet gateway ID

State

VPC ID

☒

NAGP_Internet_Gat...

igw-0432df096eae556b2

Attached

vpc-094f864a85fe52c9f | Na

Key

Value

NameNAGP_Internet_Gateway