

# Shared VPC

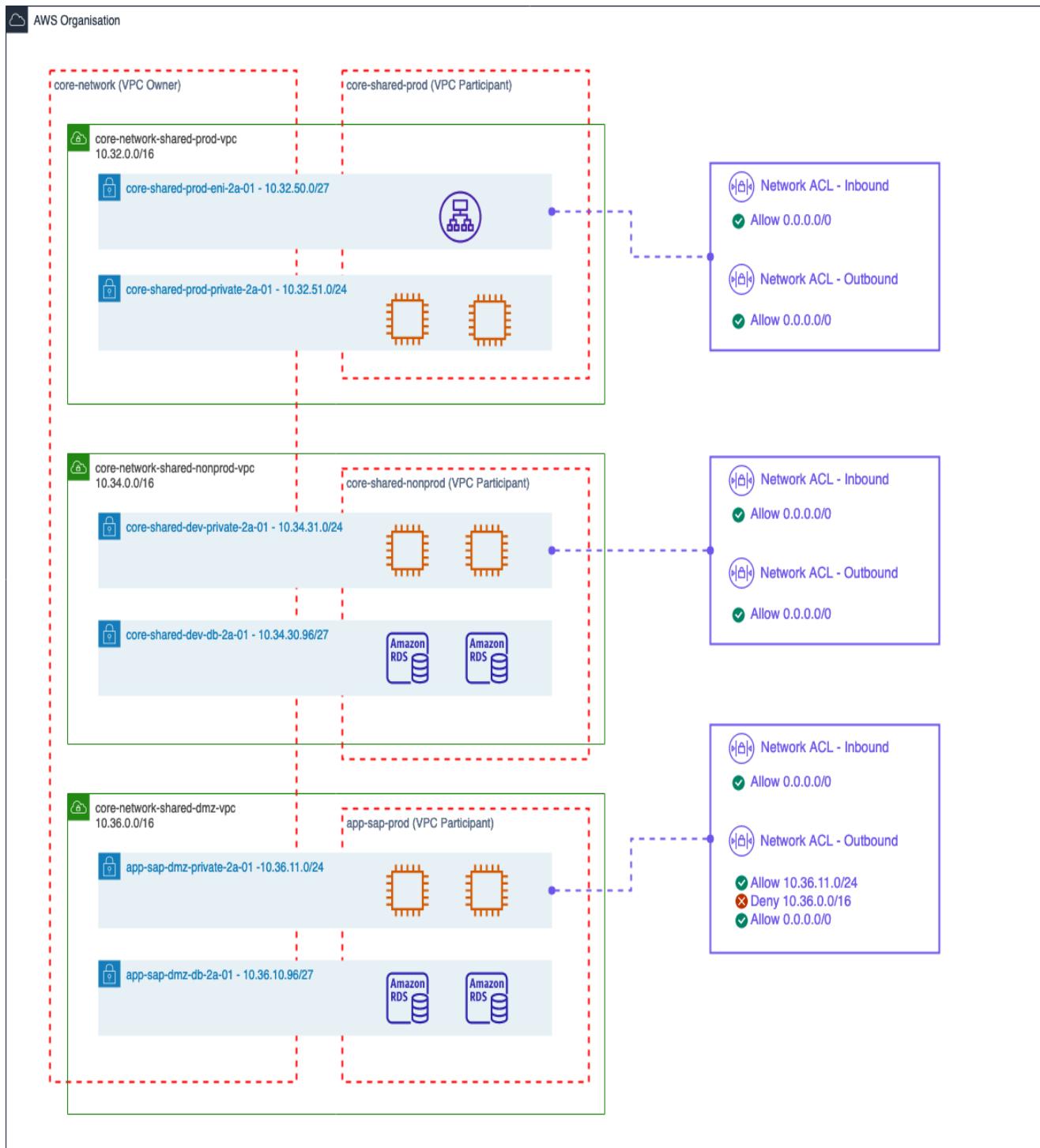
- [Overview](#)
- [Traditional VPC's](#)
- [Shared VPC's](#)
  - [VPC Route Tables](#)
- [Centralised Inspection](#)
  - [Principles](#)
  - [TGW Route Tables](#)
  - [Routing Logic Examples](#)
- [Centralised Endpoints](#)
- [Shared Subnets](#)
- [Shared Subnet Table](#)
  - [Prod Subnets](#)
    - [Prod Subnet Allocation Table](#)
  - [Nonprod Subnets](#)
    - [Nonprod Subnet Allocation Table](#)
  - [DMZ Subnets](#)
    - [Default DMZ NACL](#)
    - [Default DMZ NACL - Outbound Rules](#)
    - [Default DMZ NACL - Inbound Rules](#)
    - [DMZ Subnet Allocation Table](#)

## Overview

With the use of Shared VPC's, accounts can now be de-coupled from the underlying VPC. Where previously there was a one-to-one mapping of accounts to VPC, there is now a one-to-many relationship between accounts and VPC's; that is, a single VPC can serve multiple accounts. In doing so, we can now have fewer, larger, centrally managed VPC's as opposed to many smaller, de-centralised VPC's. The benefits of a shared VPC model are;

- Separation of duties; network constructs such as IP addressing, routing etc; are centrally managed
- Efficient use of subnets
- Simplified operations
- Cost optimisation; reduction in hourly transit gateway (TGW) attachment charges and potential inter-AZ traffic charge

The diagram below outlines a high-level overview of a shared VPC topology.



## Traditional VPC's

Whilst there will be accounts that contain their own VPC, especially those that are housing applications in a more cloud-native manner, the majority of workloads are expected to live on the shared VPC's. The following table lists those VPC's which are not on the shared VPC.

VPC Name	Purpose	Owner Account	VPC CIDR	Reserved CIDR Ranges	Number of usable	Region

					<b>addresses</b>	
core-security-fw-vpc	Security gateway VPC	core-security	10.44.0.0/20	N/A	4094	ap-southeast-2
app-metering-nonprod-ieemts-fsx-ontap	Tertiary VPC required for FSx OnTap	app-metering-nonprod	10.45.0.0/27	N/A	30	ap-southeast-2
app-metering-prod-ieemts-fsx-ontap	Tertiary VPC required for FSx OnTap	app-metering-prod	10.45.1.0/27	N/A	30	ap-southeast-2
app-dataplatform-dev-vpc	Dataplatform dev	app-dataplatform-irm-dev	172.32.0.0/16	N/A	65,534	ap-southeast-2
app-dataplatform-devops-vpc	Dataplatform devops	app-dataplatform-irm-devops	172.33.0.0/16	N/A	65,534	ap-southeast-2
app-dataplatform-prod-vpc	Dataplatform prod	app-dataplatform-latfo	172.36.0.0/16	N/A	65,534	ap-southeast-2

		rm- prod				
app- dataplatform- qa-vpc	Dataplatform prod	app- dataplatfo rm-qa	172.35.0. 0/16	N/A	65,534	ap-southeast-2

## Shared VPC's

The following table lists the shared VPC's that have been created. All VPC's are created in the **core-network** account, referred to as the **owner account**. The first 10 subnets are reserved for the VPC itself and will be used for any centralised resources in the **core-network** account such as the **eni** subnets.

VPC Name	Purpose	Owner Account	VPC CIDR	Reserved CIDR Ranges	Number of usable addresses	Region
core-network-shared-prod-vpc	Production workload	core-network	10.32.0.0/16	10.32.0.0/24 - 10.32.9.0/24	65,534	ap-southeast-2
core-network-shared-nonprod-vpc	Non-production workload	core-network	10.34.0.0/16	10.34.0.0/24 - 10.34.9.0/24	65,534	ap-southeast-2
core-network-shared-dmz-vpc	DMZ workload (production and non-	core-network	10.36.0.0/16	10.36.0.0/24 - 10.36.9.0/24	65,534	ap-southeast-2

	producti on)				
--	-----------------	--	--	--	--

## VPC Route Tables

Each shared VPC contains 2 route tables. The table below lists the purpose of each using the **core-network-shared-prod** VPC as an example.

Route Table Name	Main Route Table	Purpose	Routes
<b>core-network-shared-prod-vpc-rt</b>	Yes	All non-TGW subnets are assigned to this route table by default. This route table contains a default route via the TGW to access any resources outside of the local VPC.	0.0.0.0 via TGW
<b>core-network-shared-prod-tgw-rt</b>	No	All TGW subnets are assigned to this route table by explicit association. This allows for NACL's towards the TGW to remain open, whilst being able to apply NACL's to workload subnets.	N/A

## Centralised Inspection

Each shared VPC corresponds to a route table on the TGW. This is to control the flow of routing to ensure that any inter-VPC traffic is first sent to the inspection VPC in the **core-security** account before being sent to the destination VPC. The **core-security** account contains a set of Palo Alto VM-series firewalls which control the flow of traffic between VPC's. Any communication between shared VPC's must be explicitly defined and allowed in the security policy.

**⚠** Traffic within the VPC is contained to the VPC; it does not traverse the firewalls.

## Principles

The principle for network segmentation is as follows:

- Traffic between environments ( `prod` , `nonprod` and `dmz` ) **in AWS to AWS** networks is to be inspected and controlled by the AWS VM-series firewalls.
- Traffic from environments ( `prod` , `nonprod` and `dmz` ) in **AWS to on-premises** networks is to be inspected and controlled by the on-premises PA firewalls.

## TGW Route Tables

Based on the above principles, the route tables are configured as per the table below.

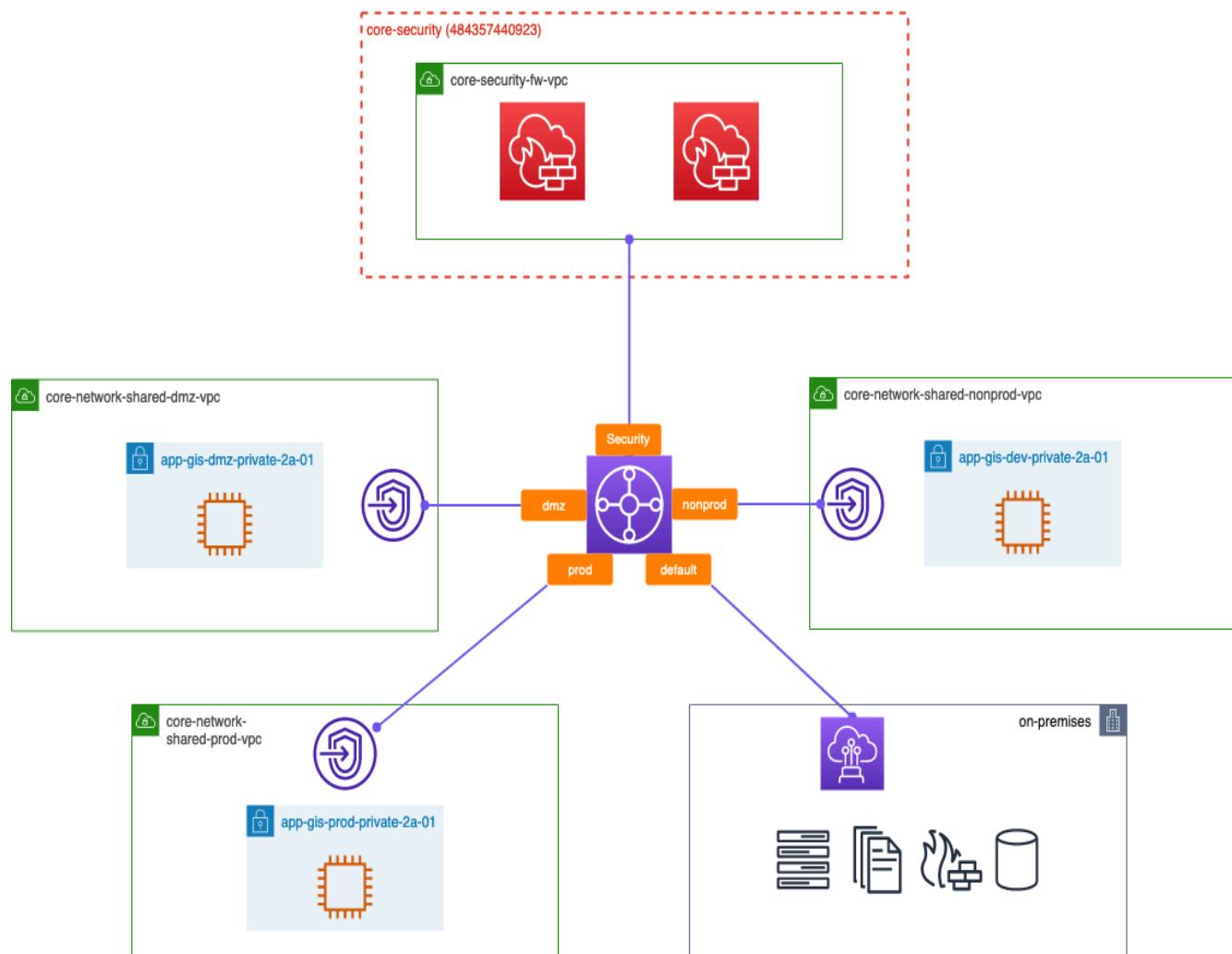
**💡** The propagation rules may change to prevent unnecessary tromboning of traffic through the VM-series firewalls.

Route Table Name	Association (the VPC attachment to associate with this route table)	Propagation (the routes to propagate to this route table)	Static Routes
prod	<code>core-network-shared-prod-vpc</code>	<ul style="list-style-type: none"><li>local VPC</li><li><code>core-security-fw-vpc</code> - for default route</li><li>non-shared VPCs - to allow direct reachability to non-shared VPC's (such as dataplatform etc;)</li><li>DX Gateway - to allow direct reachability to on-prem networks that are advertised over BGP</li><li>AWS VMC - to allow direct reachability to VMC networks (DFW being used)</li></ul>	<ul style="list-style-type: none"><li>0.0.0.0/0 via <code>core-security-fw-vpc</code> - to force internet path through VM-series firewalls.</li><li>10.0.0.0/8 via DX gateway -</li><li>10.34.0.0/16 via <code>core-security-fw-vpc</code> - to force internet path through VM-series firewalls</li><li>10.36.0.0/16 via <code>core-security-fw-vpc</code> - to force internet path through VM-series firewalls</li></ul>

nonprod	<code>core-network-shared-nonprod-vpc</code>	<ul style="list-style-type: none"> <li>local VPC</li> <li><code>core-security-fw-vpc</code> - for default route</li> <li>non-shared VPCs - to allow direct reachability to non-shared VPC's (such as dataplatform etc;)</li> <li>DX Gateway - to allow direct reachability to on-prem networks that are advertised over BGP</li> <li>AWS VMC - to allow direct reachability to VMC networks (DFW being used)</li> </ul>	<ul style="list-style-type: none"> <li>0.0.0.0/0 via <code>core-security-fw-vpc</code> - to force internet path through VM-series firewalls.</li> </ul>
dmz	<code>core-network-shared-dmz-vpc</code>	<ul style="list-style-type: none"> <li>local VPC</li> <li><code>core-security-fw-vpc</code> - for default route</li> <li>non-shared VPCs - to allow direct reachability to non-shared VPC's (such as dataplatform etc;)</li> <li>DX Gateway - to allow direct reachability to on-prem networks that are advertised over BGP</li> <li>AWS VMC - to allow direct reachability to VMC networks (DFW being used)</li> </ul>	<ul style="list-style-type: none"> <li>0.0.0.0/0 via <code>core-security-fw-vpc</code> - to force internet path through VM-series firewalls</li> </ul>

security	<b>core-security-fw-vpc</b>	<ul style="list-style-type: none"> <li>All VPC's - to allow return traffic</li> </ul>	N/A - all routes to be learnt via propagation
default	<ul style="list-style-type: none"> <li>non-shared VPCs</li> <li>DX Gateway (on-premises networks)</li> <li>AWS VMC (VMC networks)</li> </ul>	<ul style="list-style-type: none"> <li>All VPC's</li> </ul>	N/A - all routes to be learnt via propagation

The below diagram provides an overview of the route tables and their relationship to the various environments.



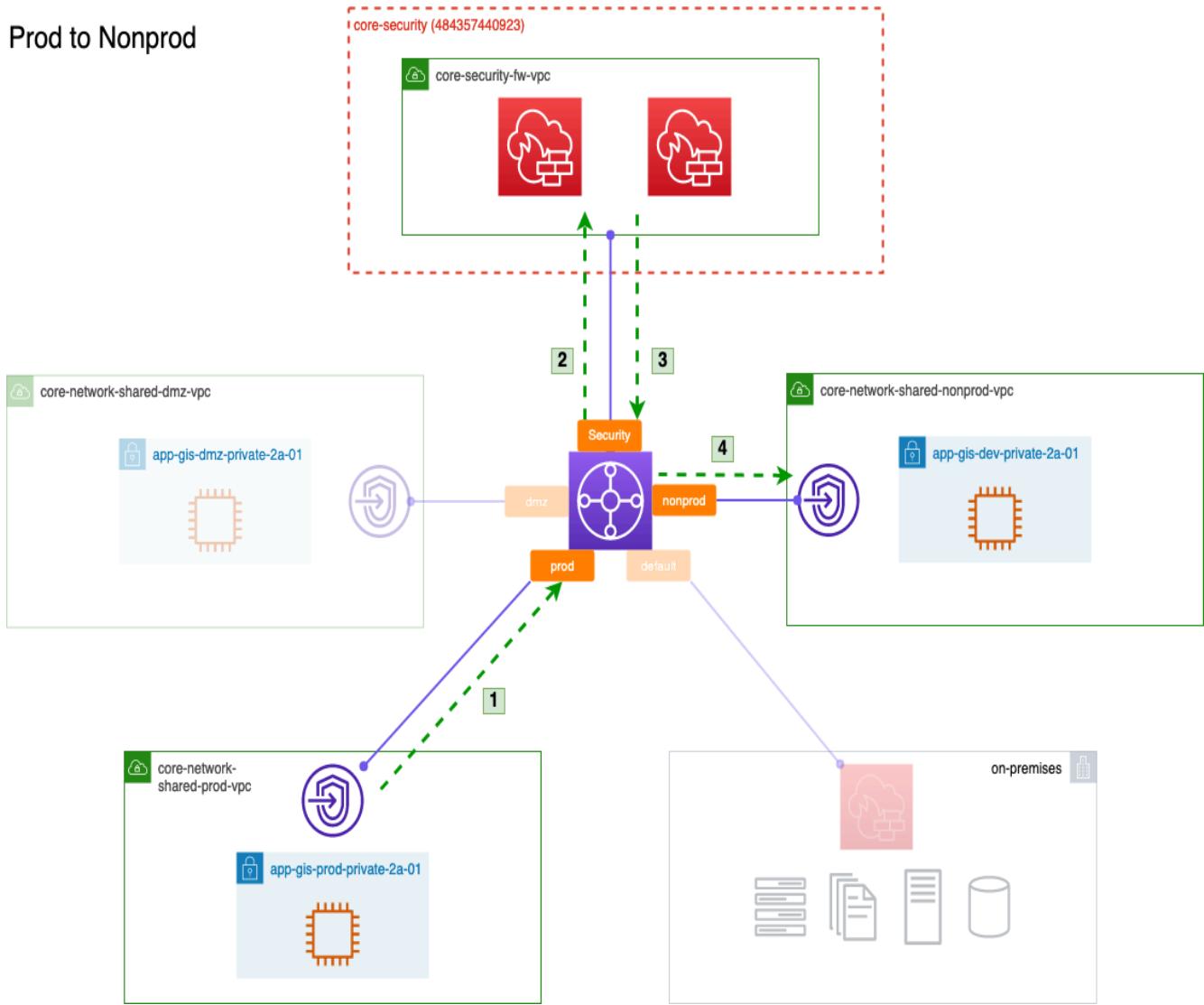
### Routing Logic Examples

The following drawings will detail some of the flows to give readers a better understanding of the routing logic.



For simplicity, environments attached to the `default` route table are shown as on-premises networks. In reality, these include VMC and non-shared VPC's ( `mobileapps` and `dataplatform` VPC's as examples).

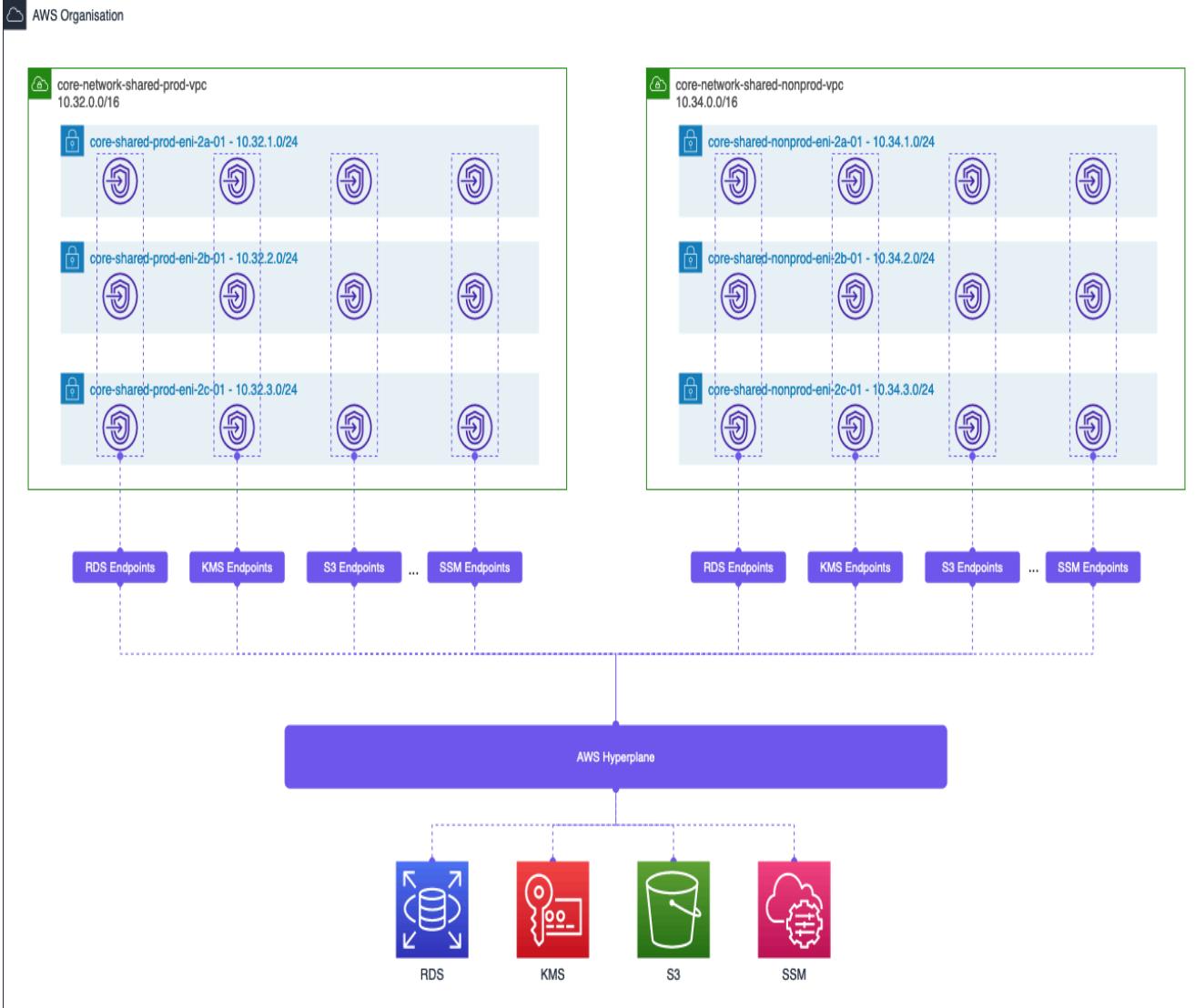
### Prod to Nonprod



### Centralised Endpoints

It's good practice to access AWS services using PrivateLink, which allows for private connectivity between your VPC and the AWS service. For e.g. by using an endpoint for the `rds` service, VPC's (and even on-premises networks) can access an RDS instance without going over the public internet. This is achieved by deploying an ENI (elastic network interface) for the relevant service into the account. These endpoints are centralised in the `core-network` account to provide a central location to configure, monitor and apply policy.

The diagram below illustrates the endpoints created in the `core-network` account for private access to the relevant AWS service.



For each service ENI, there will be a `prod` and a `nonprod` variant to ensure that access to the AWS service from either environment doesn't need to trombone through the security VPC.

For example, the `rds` endpoint in the `core-network-shared-nonprod-vpc` ensures that a `nonprod` workload can access the service without being forced through the inspection VPC.

The service endpoints will be created across at least 3 availability-zones (AZ) on the `eni` subnet in the `core-network` account.

The following table outlines the ENI subnets created for each of the shared VPC's.

- Whilst there are ENI subnets for the shared DMZ VPC, these are not expected to be used.

Shared VPC	Account	ENI Subnets	CIDR
------------	---------	-------------	------

core-network-shared-prod-vpc	core-network	core-network-shared-prod-eni-2a-01 core-network-shared-prod-eni-2b-01 core-network-shared-prod-eni-2c-01	10.32.1.0/24 10.32.2.0/24 10.32.3.0/24
core-network-shared-nonprod-vpc	core-network	core-network-shared-nonprod-eni-2a-01 core-network-shared-nonprod-eni-2b-01 core-network-shared-nonprod-eni-2c-01	10.34.1.0/24 10.34.2.0/24 10.34.3.0/24

## Shared Subnets

The default subnet design for all **new AWS WORKLOAD** accounts is based on a 3-tier design. This applies mostly to **prod** and **nonprod** environments, whereas with **dmz**, it may not be necessary to have an **eni**, **db** and **private** subnet.

The table below outlines the purpose of each subnet. Each account will be allocated 4 x **/24** subnets and distributed in the following manner. All subnets are to be available in at least 2 AZ's; where a third AZ exist, a subnet is to be available in that AZ.

Subnet Name	CIDR	Example	Purpose
<b>{{{account_name}}}-{{{environment}}}-eni-{{{AZ ID}}}-{{{counter}}}</b>	3 x <b>/27</b> subnets	app-gis-prod-eni-az1-01	The <b>eni</b> subnet can be used for any services that require an interface endpoint, such an ALB/ELB.

<code>{{account_name}}-{{environment}}-db-{{AZ ID}}-{{counter}}</code>	3 x /27 subnets	app-gis-dev-db-az2-01	The <b>db</b> subnet can be used for any database or back-end services, such as RDS.
<code>{{account_name}}-{{environment}}-private-{{AZ ID}}-{{counter}}</code>	3 x /24 subnets	app-gis-qa-private-az3-01	The <b>private</b> subnet can be used for any workloads, such as EC2 instances, ECS clusters etc;

- i** Subnets can be renamed or re-purposed as required. For e.g. in the database subnet, whilst the application may not require an RDS instance, the same subnet could be used to run a managed key/value store.

## Shared Subnet Table

The following section outlines each of the subnet allocations per account.

### Prod Subnets

Prod subnets are to be created on the prod shared VPC range ( `10.34.0.0/16` ). The following environment names can be used to differentiate between the different non-prod environments (if required).

- `prod`

### Prod Subnet Allocation Table

<b>Account</b>	<b>Subnet Name</b>	<b>Subnet CIDR</b>	<b>Description</b>
app-general-prod ( 707986513376 )	app-general-prod-eni-az3-01	10.32.10.0/27	ALB/ELB ENI's etc;
	app-general-prod-eni-az1-01	10.32.10.32/27	ALB/ELB ENI's etc;
	app-general-prod-eni-az2-01	10.32.10.64/27	ALB/ELB ENI's etc;
	app-general-prod-db-az3-01	10.32.64.0/25	Database subnet - AZ A
	app-general-prod-db-az1-01	10.32.64.128/25	Database subnet - AZ B
	app-general-prod-db-az2-01	10.32.65.0/25	Database subnet - AZ C
	app-general-prod-private-az3-01	10.32.11.0/24	Workload subnet - AZ A
	app-general-prod-private-az1-01	10.32.12.0/24	Workload subnet - AZ B
	app-general-prod-private-az2-01	10.32.13.0/24	Workload subnet - AZ C
app-gis-prod ( 730257151575 )	app-gis-prod-eni-az3-01	10.32.14.0/27	ALB/ELB ENI's etc;
	app-gis-prod-eni-az1-01	10.32.14.32/27	ALB/ELB ENI's etc;
	app-gis-prod-eni-az2-01	10.32.14.64/27	ALB/ELB ENI's etc;
	app-gis-prod-db-az3-01	10.32.14.96/27	Database subnet - AZ A
	app-gis-prod-db-az1-01	10.32.14.128/27	Database subnet - AZ B
	app-gis-prod-db-az2-01	10.32.14.160/27	Database subnet - AZ C
	app-gis-prod-private-az3-01	10.32.15.0/24	Workload subnet - AZ A
	app-gis-prod-private-az1-01	10.32.16.0/24	Workload subnet - AZ B
	app-gis-prod-private-az2-01	10.32.17.0/24	Workload subnet - AZ C
app-integration-prod ( 986097159693 )	app-integration-prod-eni-az3-01	10.32.18.0/27	ALB/ELB ENI's etc;
	app-integration-prod-eni-az1-01	10.32.18.32/27	ALB/ELB ENI's etc;
	app-integration-prod-eni-az2-01	10.32.18.64/27	ALB/ELB ENI's etc;
	app-integration-prod-db-az3-01	10.32.18.96/27	Database subnet - AZ A
	app-integration-prod-db-az1-01	10.32.18.128/27	Database subnet - AZ B
	app-integration-prod-db-az2-01	10.32.18.160/27	Database subnet - AZ C
	app-integration-prod-private-az3-01	10.32.19.0/24	Workload subnet - AZ A
	app-integration-prod-private-az1-01	10.32.20.0/24	Workload subnet - AZ B
	app-integration-prod-private-az2-01	10.32.21.0/24	Workload subnet - AZ C
app-metering-prod ( 933981731246 )	app-metering-prod-eni-az3-01	10.32.22.0/27	ALB/ELB ENI's etc;
	app-metering-prod-eni-az1-01	10.32.22.32/27	ALB/ELB ENI's etc;
	app-metering-prod-eni-az2-01	10.32.22.64/27	ALB/ELB ENI's etc;
	app-metering-prod-db-az3-01	10.32.22.96/27	Database subnet - AZ A

	app-metering-prod-db-az1-01	10.32.22.128/27	Database subnet - AZ B
	app-metering-prod-db-az2-01	10.32.22.160/27	Database subnet - AZ C
	app-metering-prod-private-az3-01	10.32.23.0/24	Workload subnet - AZ A
	app-metering-prod-private-az1-01	10.32.24.0/24	Workload subnet - AZ B
	app-metering-prod-private-az2-01	10.32.25.0/24	Workload subnet - AZ C
{{ Placeholder }}	{{ Placeholder }}-prod-eni-az3-01	10.32.26.0/27	ALB/ELB ENI's etc;
	{{ Placeholder }}-prod-eni-az1-01	10.32.26.32/27	ALB/ELB ENI's etc;
	{{ Placeholder }}-prod-eni-az2-01	10.32.26.64/27	ALB/ELB ENI's etc;
	{{ Placeholder }}-prod-db-az3-01	10.32.26.96/27	Database subnet - AZ A
	{{ Placeholder }}-prod-db-az1-01	10.32.26.128/27	Database subnet - AZ B
	{{ Placeholder }}-prod-db-az2-01	10.32.26.160/27	Database subnet - AZ C
	{{ Placeholder }}-prod-private-az3-01	10.32.27.0/24	Workload subnet - AZ A
	{{ Placeholder }}-prod-private-az1-01	10.32.28.0/24	Workload subnet - AZ B
	{{ Placeholder }}-prod-private-az2-01	10.32.29.0/24	Workload subnet - AZ C
core-devops ( 378066971077 )	core-devops-prod-eni-az1-01	10.32.30.0/27	ALB/ELB ENI's etc;
	core-devops-prod-eni-az2-01	10.32.30.32/27	ALB/ELB ENI's etc;
	core-devops-prod-eni-az3-01	10.32.30.64/27	ALB/ELB ENI's etc;
	core-devops-prod-db-az1-01	10.32.30.96/27	Database subnet - AZ A
	core-devops-prod-db-az2-01	10.32.30.128/27	Database subnet - AZ B
	core-devops-prod-db-az3-01	10.32.30.160/27	Database subnet - AZ C
	core-devops-prod-private-az1-01	10.32.31.0/24	Workload subnet - AZ A
	core-devops-prod-private-az2-01	10.32.32.0/24	Workload subnet - AZ B
	core-devops-prod-private-az3-01	10.32.33.0/24	Workload subnet - AZ C
core-backup ( 234268347951 )	core-backup-prod-eni-az3-01	10.32.34.0/27	ALB/ELB ENI's etc;
	core-backup-prod-eni-az1-01	10.32.34.32/27	ALB/ELB ENI's etc;
	core-backup-prod-eni-az2-01	10.32.34.64/27	ALB/ELB ENI's etc;
	core-backup-prod-db-az3-01	10.32.34.96/27	Database subnet - AZ A
	core-backup-prod-db-az1-01	10.32.34.128/27	Database subnet - AZ B
	core-backup-prod-db-az2-01	10.32.34.160/27	Database subnet - AZ C
	core-backup-prod-private-az3-01	10.32.35.0/24	Workload subnet - AZ A
	core-backup-prod-private-az1-01	10.32.36.0/24	Workload subnet - AZ B

	core-backup-prod-private-az2-01	10.32.37.0/24	Workload subnet - AZ C
core-logging ( 720112911739 )	core-logging-prod-eni-az3-01	10.32.38.0/27	ALB/ELB ENI's etc;
	core-logging-prod-eni-az1-01	10.32.38.32/27	ALB/ELB ENI's etc;
	core-logging-prod-eni-az2-01	10.32.38.64/27	ALB/ELB ENI's etc;
	core-logging-prod-db-az3-01	10.32.38.96/27	Database subnet - AZ A
	core-logging-prod-db-az1-01	10.32.38.128/27	Database subnet - AZ B
	core-logging-prod-db-az2-01	10.32.38.160/27	Database subnet - AZ C
	core-logging-prod-private-az3-01	10.32.39.0/24	Workload subnet - AZ A
	core-logging-prod-private-az1-01	10.32.40.0/24	Workload subnet - AZ B
	core-logging-prod-private-az2-01	10.32.41.0/24	Workload subnet - AZ C
core-network ( 234268347951 )	core-network-prod-eni-az3-01	10.32.42.0/27	ALB/ELB ENI's etc;
	core-network-prod-eni-az1-01	10.32.42.32/27	ALB/ELB ENI's etc;
	core-network-prod-eni-az2-01	10.32.42.64/27	ALB/ELB ENI's etc;
	core-network-prod-db-az3-01	10.32.42.96/27	Database subnet - AZ A
	core-network-prod-db-az1-01	10.32.42.128/27	Database subnet - AZ B
	core-network-prod-db-az2-01	10.32.42.160/27	Database subnet - AZ C
	core-network-prod-private-az3-01	10.32.43.0/24	Workload subnet - AZ A
	core-network-prod-private-az1-01	10.32.44.0/24	Workload subnet - AZ B
	core-network-prod-private-az2-01	10.32.45.0/24	Workload subnet - AZ C
core-security ( 484357440923 )	core-security-prod-eni-az3-01	10.32.46.0/27	ALB/ELB ENI's etc;
	core-security-prod-eni-az1-01	10.32.46.32/27	ALB/ELB ENI's etc;
	core-security-prod-eni-az2-01	10.32.46.64/27	ALB/ELB ENI's etc;
	core-security-prod-db-az3-01	10.32.46.96/27	Database subnet - AZ A
	core-security-prod-db-az1-01	10.32.46.128/27	Database subnet - AZ B
	core-security-prod-db-az2-01	10.32.46.160/27	Database subnet - AZ C
	core-security-prod-private-az3-01	10.32.47.0/24	Workload subnet - AZ A
	core-security-prod-private-az1-01	10.32.48.0/24	Workload subnet - AZ B
	core-security-prod-private-az2-01	10.32.49.0/24	Workload subnet - AZ C
core-shared-prod ( 581446142335 )	core-shared-prod-eni-az3-01	10.32.50.0/27	ALB/ELB ENI's etc;
	core-shared-prod-eni-az1-01	10.32.50.32/27	ALB/ELB ENI's etc;
	core-shared-prod-eni-az2-01	10.32.50.64/27	ALB/ELB ENI's etc;
	core-shared-prod-db-az3-01	10.32.50.96/27	Database subnet - AZ A

	core-shared-prod-db-az1-01	10.32.50.128/27	Database subnet - AZ B
	core-shared-prod-db-az2-01	10.32.50.160/27	Database subnet - AZ C
	core-shared-prod-private-az3-01	10.32.51.0/24	Workload subnet - AZ A
	core-shared-prod-private-az1-01	10.32.52.0/24	Workload subnet - AZ B
	core-shared-prod-private-az2-01	10.32.53.0/24	Workload subnet - AZ C
app-sap-prod ( 389778594784 )	app-sap-prod-eni-az3-01	10.32.54.0/27	ALB/ELB ENI's etc;
	app-sap-prod-eni-az1-01	10.32.54.32/27	ALB/ELB ENI's etc;
	app-sap-prc	-a	ALB/ELB ENI's etc;
	app-sap-prod-db-az3-01	10.32.55.0/25	Database subnet - AZ A
	app-sap-prod-db-az1-01	10.32.55.128/25	Database subnet - AZ B
	app-sap-prod-db-az2-01	10.32.56.0/25	Database subnet - AZ C
	app-sap-prod-private-az3-01	10.32.57.0/24	Workload subnet - AZ A
	app-sap-prod-private-az1-01	10.32.58.0/24	Workload subnet - AZ B
	app-sap-prod-private-az2-01	10.32.59.0/24	Workload subnet - AZ C
app-mobileapps-prod ( 017555196640 )	app-mobileapps-prod-eni-az1-01	10.32.60.0/27	ALB/ELB ENI's etc;
	app-mobileapps-prod-eni-az2-01	10.32.60.32/27	ALB/ELB ENI's etc;
	app-mobileapps-prod-eni-az3-01	10.32.60.64/27	ALB/ELB ENI's etc;
	app-mobileapps-prod-db-az1-01	10.32.60.96/27	Database subnet - AZ A
	app-mobileapps-prod-db-az2-01	10.32.60.128/27	Database subnet - AZ B
	app-mobileapps-prod-db-az3-01	10.32.60.160/27	Database subnet - AZ C
	app-mobileapps-prod-private-az1-01	10.32.61.0/24	Workload subnet - AZ A
	app-mobileapps-prod-private-az2-01	10.32.62.0/24	Workload subnet - AZ B
	app-mobileapps-prod-private-az3-01	10.32.63.0/24	Workload subnet - AZ C
app-eventstreaming-prod ( 792792536048 )	app-eventstreaming-prod-eni-az1-01	10.32.66.0/27	ALB/ELB ENI's etc;
	app-eventstreaming-prod-eni-az2-01	10.32.66.32/27	ALB/ELB ENI's etc;
	app-eventstreaming-prod-eni-az3-01	10.32.66.64/27	ALB/ELB ENI's etc;
	app-eventstreaming-prod-eni-az1-02	10.32.107.0/27	ALB/ELB ENI's etc;
	app-eventstreaming-prod-eni-az1-02	10.32.107.32/27	ALB/ELB ENI's etc;
	app-eventstreaming-prod-eni-az1-02	10.32.107.64/27	ALB/ELB ENI's etc;
	app-eventstreaming-prod-db-az1-01	10.32.66.96/27	Database subnet - AZ A
	app-eventstreaming-prod-db-az2-01	10.32.66.128/27	Database subnet - AZ B
	app-eventstreaming-prod-db-az3-01	10.32.66.160/27	Database subnet - AZ C

	app-eventstreaming-prod-private-az1-01	10.32.67.0/24	Workload subnet - AZ A
	app-eventstreaming-prod-private-az2-01	10.32.68.0/24	Workload subnet - AZ B
	app-eventstreaming-prod-private-az3-01	10.32.69.0/24	Workload subnet - AZ C
app-cx-prod ( 490941487530 )	app-cx-prod-eni-az1-01	10.32.70.0/27	ALB/ELB ENI's etc;
	app-cx-prod-eni-az2-01	10.32.70.32/27	ALB/ELB ENI's etc;
	app-cx-prod-eni-az3-01	10.32.70.64/27	ALB/ELB ENI's etc;
	app-cx-prod-db-az1-01	10.32.70.96/27	Database subnet - AZ A
	app-cx-prod-db-az2-01	10.32.70.128/27	Database subnet - AZ B
	app-cx-prod-db-az3-01	10.32.70.160/27	Database subnet - AZ C
	app-cx-prod-private-az1-01	10.32.71.0/24	Workload subnet - AZ A
	app-cx-prod-private-az2-01	10.32.72.0/24	Workload subnet - AZ B
	app-cx-prod-private-az3-01	10.32.73.0/24	Workload subnet - AZ C
app-outagesapi-prod ( 905418108896 )	app-outagesapi-prod-eni-az1-01	10.32.74.0/27	ALB/ELB ENI's etc;
	app-outagesapi-prod-eni-az2-01	10.32.74.32/27	ALB/ELB ENI's etc;
	app-outagesapi-prod-eni-az3-01	10.32.74.64/27	ALB/ELB ENI's etc;
	app-outagesapi-prod-db-az1-01	10.32.74.96/27	Database subnet - AZ A
	app-outagesapi-prod-db-az2-01	10.32.74.128/27	Database subnet - AZ B
	app-outagesapi-prod-db-az3-01	10.32.74.160/27	Database subnet - AZ C
	app-outagesapi-prod-private-az1-01	10.32.75.0/24	Workload subnet - AZ A
	app-outagesapi-prod-private-az2-01	10.32.76.0/24	Workload subnet - AZ B
	app-outagesapi-prod-private-az3-01	10.32.77.0/24	Workload subnet - AZ C
app-datahub-prod ( 339712836516 )	app-datahub-prod-eni-az1-01	10.32.78.0/27	ALB/ELB ENI's etc;
	app-datahub-prod-eni-az2-01	10.32.78.32/27	ALB/ELB ENI's etc;
	app-datahub-prod-eni-az3-01	10.32.78.64/27	ALB/ELB ENI's etc;
	app-datahub-prod-db-az1-01	10.32.78.96/27	Database subnet - AZ A
	app-datahub-prod-db-az2-01	10.32.78.128/27	Database subnet - AZ B
	app-datahub-prod-db-az3-01	10.32.78.160/27	Database subnet - AZ C
	app-datahub-prod-private-az1-01	10.32.79.0/24	Workload subnet - AZ A
	app-datahub-prod-private-az2-01	10.32.80.0/24	Workload subnet - AZ B
	app-datahub-prod-private-az3-01	10.32.81.0/24	Workload subnet - AZ C
	app-datahub-prod-private-az1-02	10.32.82.0/24	Databricks Tenant 1 Workgroup 1

	app-databricks-prod-private-az1-02	10.32.82.0/24	Databricks Tenant 1 Workspace 1
	app-databricks-prod-private-az2-02	10.32.83.0/24	Databricks Tenant 1 Workspace 1
	app-databricks-prod-private-az3-02	10.32.84.0/24	Databricks Tenant 1 Workspace 1
	app-databricks-prod-private-az1-03	10.32.85.0/24	Databricks Tenant 1 Workspace 2
	app-databricks-prod-private-az2-03	10.32.86.0/24	Databricks Tenant 1 Workspace 2
	app-databricks-prod-private-az3-03	10.32.87.0/24	Databricks Tenant 1 Workspace 2
	app-databricks-prod-private-az1-04	10.32.88.0/24	Databricks Tenant 2 Workspace 1
	app-databricks-prod-private-az2-04	10.32.89.0/24	Databricks Tenant 2 Workspace 1
	app-databricks-prod-private-az3-04	10.32.90.0/24	Databricks Tenant 2 Workspace 1
	app-databricks-prod-private-az1-05	10.32.91.0/24	Databricks Tenant 2 Workspace 2
	app-databricks-prod-private-az2-05	10.32.92.0/24	Databricks Tenant 2 Workspace 2
	app-databricks-prod-private-az3-05	10.32.93.0/24	Databricks Tenant 2 Workspace 2
app-rancher-prod ( 060795945711 )	app-rancher-prod-eni-az1-01	10.32.94.0/27	ALB/ELB ENI's etc;
	app-rancher-prod-eni-az2-01	10.32.94.32/27	ALB/ELB ENI's etc;
	app-rancher-prod-eni-az3-01	10.32.94.64/27	ALB/ELB ENI's etc;
	app-rancher-prod-db-az1-01	10.32.94.96/27	Database subnet - AZ A
	app-rancher-prod-db-az2-01	10.32.94.128/27	Database subnet - AZ B
	app-rancher-prod-db-az3-01	10.32.94.160/27	Database subnet - AZ C
	app-rancher-prod-private-az1-01	10.32.95.0/24	Workload subnet - AZ A
	app-rancher-prod-private-az2-01	10.32.96.0/24	Workload subnet - AZ B
	app-rancher-prod-private-az3-01	10.32.97.0/24	Workload subnet - AZ C
	app-rancher-prod-private-az1-02	10.32.104.0/24	Workload subnet - AZ A
	app-rancher-prod-private-az2-02	10.32.105.0/24	Workload subnet - AZ B
	app-rancher-prod-private-az3-02	10.32.106.0/24	Workload subnet - AZ C
app-databricks-prod ( 339712836516 )	app-databricks-prod-private-az1-06	10.32.98.0/24	Databricks Tenant 3 Workspace 1
	app-databricks-prod-private-az2-06	10.32.99.0/24	Databricks Tenant 3 Workspace 1
	app-databricks-prod-private-az3-06	10.32.100.0/24	Databricks Tenant 3 Workspace 1
	app-databricks-prod-private-az1-07	10.32.101.0/24	Databricks Tenant 3 Workspace 2
	app-databricks-prod-private-az2-07	10.32.102.0/24	Databricks Tenant 3 Workspace 2
	app-databricks-prod-private-az3-07	10.32.103.0/24	Databricks Tenant 3 Workspace 2
app-eventstreaming-dr ( 182066453630 )	app-eventstreaming-dr-eni-az1-01	10.32.108.0/27	ALB/ELB ENI's etc;
	app-eventstreaming-dr-eni-az2-01	10.32.108.32/27	ALB/ELB ENI's etc;

app-eventstreaming-dr-eni-az3-01	10.32.108.64/27	ALB/ELB ENI's etc;
app-eventstreaming-dr-db-az1-01	10.32.108.96/27	Database subnet - AZ A
app-eventstreaming-dr-db-az2-01	10.32.108.128/27	Database subnet - AZ B
app-eventstreaming-dr-db-az3-01	10.32.108.160/27	Database subnet - AZ C
app-eventstreaming-dr-private-az1-01	10.32.109.0/24	Workload subnet - AZ A
app-eventstreaming-dr-private-az2-01	10.32.110.0/24	Workload subnet - AZ B
app-eventstreaming-dr-private-az3-01	10.32.111.0/24	Workload subnet - AZ C

⚠ Please double-check the subnet allocations. The last row in the list may not represent the final subnet range to be used.

## Nonprod Subnets

Nonprod subnets are to be created on the nonprod shared VPC range ( `10.34.0.0/16` ).

The following environment names can be used to differentiate between the different non-prod environments (if required).

- `nonprod`
- `dev`
- `qa`
- `test`
- `sbx`

## Nonprod Subnet Allocation Table

## DMZ Subnets

DMZ subnets are to be created on the DMZ shared VPC range ( `10.36.0.0/16` ). All DMZ subnets are created with a default NACL that is associated with the subnet grouping. At the time of writing (06/07/2022), the subnet grouping will be based on the last-octet descriptor. The table shows an example.

#### Default DMZ NACL

Subnet Name	Subnet CIDR	NACL Name
app-gis-dmz-prod-private-az1-internal	10.36.22.0/27	app-giz-dmz-prod-private-internal
app-gis-dmz-prod-private-az2-internal	10.36.22.32/27	
app-gis-dmz-prod-private-az3-internal	10.36.22.64/27	
app-gis-dmz-prod-private-az1-external	10.36.23.0/27	app-giz-dmz-prod-private-external
app-gis-dmz-prod-private-az2-external	10.36.23.32/27	
app-gis-dmz-prod-private-az3-external	10.36.23.64/27	

The following table outlines the default NACL applied to every DMZ subnet. Values from the previous table is used for completeness.

#### Default DMZ NACL - Outbound Rules

Rule Number	Type	Protocol	Port Range	Destination	Action	Note
100	All traffic	ALL	ALL	10.36.23.0/27	Allow <span style="color: green;">✓</span>	Allows intra-subnet reachability
101	All traffic	ALL	ALL	10.36.23.32/27	Allow <span style="color: green;">✓</span>	Allows intra-subnet reachability
102	All traffic	ALL	ALL	10.36.23.64/27	Allow <span style="color: green;">✓</span>	Allows intra-

						subnet reachability
110	DNS (TCP) 53	TCP (6)	53	10.36.0.2	Allow	Allow DNS to VPC resolver
111	DNS (UDP) 53	UDP (17)	53	10.36.0.2	Allow	Allow DNS to VPC resolver
112	HTTPS (443)	TCP (6)	443	10.36.1.0/24	Allow	Allow HTTPS to VPC endpoints (for PrivateLink)
113	HTTPS (443)	TCP (6)	443	10.36.2.0/24	Allow	Allow HTTPS to VPC endpoints (for PrivateLink)
114	HTTPS (443)	TCP (6)	443	10.36.3.0/24	Allow	Allow HTTPS to VPC endpoints (for PrivateLink)
115-149	Custom rules					
150	All traffic	ALL	ALL	10.36.0.0/16	Deny	Deny intra-VPC traffic (prevents DMZ workloads in other

						DMZ subnets)
200	All traffic	ALL	ALL	0.0.0.0/0	Allow <span style="color: green;">✓</span>	Allow Outbound to anywhere (will be captured by the AWS firewalls)
*	All traffic	ALL	ALL	0.0.0.0/0	Deny <span style="color: red;">✗</span>	Default implicit Deny

---

#### Default DMZ NACL - Inbound Rules

Rule Number	Type	Protocol	Port Range	Destination	Action	Note
100	All traffic	ALL	ALL	0.0.0.0/0	Allow <span style="color: green;">✓</span>	Allows Inbound from anywhere (would have been captured by the AWS firewalls)
*	All traffic	ALL	ALL	0.0.0.0/0	Deny <span style="color: red;">✗</span>	Default implicit Deny

---

#### DMZ Subnet Allocation Table

<b>Account</b>	<b>Subnet Name</b>	<b>Subnet CIDR</b>	<b>Description</b>
app-sap-prod ( 389778594784 )	app-sap-dmz-prod-az1-01	10.36.10.0/27	DMZ prod workloads
	app-sap-dmz-prod-az2-01	10.36.10.32/27	DMZ prod workloads
	app-sap-dmz-prod-az3-01	10.36.10.64/27	DMZ prod workloads
app-sap-nonprod ( 259379897532 )	app-sap-dmz-nonprod-az3-01	10.36.11.0/27	DMZ nonprod workloads
	app-sap-dmz-nonprod-az1-01	10.36.11.32/27	DMZ nonprod workloads
	app-sap-dmz-nonprod-az3-01	10.36.11.64/27	DMZ nonprod workloads
core-test(569052024257)	core-test-dmz-eni-az3-01	10.36.14.0/27	ALB/ELB ENI's etc;
	core-test-dmz-eni-az1-01	10.36.14.32/27	ALB/ELB ENI's etc;
	core-test-dmz-eni-az3-01	10.36.14.64/27	ALB/ELB ENI's etc;
	core-test-dmz-db-az3-01	10.36.14.96/27	Database subnet - AZ A
	core-test-dmz-db-az1-01	10.36.14.128/27	Database subnet - AZ B
	core-test-dmz-db-az3-01	10.36.14.160/27	Database subnet - AZ C
	core-test-dmz-private-az3-01	10.36.15.0/24	Workload subnet - AZ A
	core-test-dmz-private-az1-01	10.36.16.0/24	Workload subnet - AZ B
	core-test-dmz-private-az3-01	10.36.17.0/24	Workload subnet - AZ C
app-integration-nonprod	app-integration-dmz-nonprod-private-az1-01	10.36.18.0/27	Integration Nonprod DMZ workloads
	app-integration-dmz-nonprod-private-az1-02	10.36.18.32/27	Integration Nonprod DMZ workloads
	app-integration-dmz-nonprod-private-az1-03	10.36.18.64/27	Integration Nonprod DMZ workloads
	app-integration-dmz-nonprod-eni-az1-01	10.36.19.0/27	Integration Nonprod DMZ ALB ENIs
	app-integration-dmz-nonprod-eni-az1-02	10.36.19.32/27	Integration Nonprod DMZ ALB ENIs
	app-integration-dmz-nonprod-eni-az1-03	10.36.19.64/27	Integration Nonprod DMZ ALB ENIs
app-integration-prod	app-integration-dmz-prod-private-az1-01	10.36.20.0/27	Integration Prod DMZ workloads
	app-integration-dmz-prod-private-az1-02	10.36.20.32/27	Integration Prod DMZ workloads
	app-integration-dmz-prod-private-az1-03	10.36.20.64/27	Integration Prod DMZ workloads
	app-integration-dmz-prod-eni-az1-01	10.36.21.0/27	Integration Prod DMZ ALB ENIs
	app-integration-dmz-prod-eni-az1-02	10.36.21.32/27	Integration Prod DMZ ALB ENIs

	app-integration-dmz-prod-eni-az1-03	10.36.21.64/27	Integration Prod DMZ ALB ENIs
app-gis-prod	app-gis-dmz-prod-private-az1-internal	10.36.22.0/27	GIS Nonprod DMZ Internal workloads
	app-gis-dmz-prod-private-az2-internal	10.36.22.32/27	GIS Nonprod DMZ Internal workloads
	app-gis-dmz-prod-private-az3-internal	10.36.22.64/27	GIS Nonprod DMZ Internal workloads
	app-gis-dmz-prod-private-az1-external	10.36.23.0/27	GIS Nonprod DMZ Public workloads
	app-gis-dmz-prod-private-az2-external	10.36.23.32/27	GIS Nonprod DMZ Public workloads
	app-gis-dmz-prod-private-az3-external	10.36.23.64/27	GIS Nonprod DMZ Public workloads
app-general-nonprod	app-general-dmz-nonprod-private-az1-01	10.36.24.0/27	General NonProd DMZ workloads
	app-general-dmz-nonprod-private-az1-02	10.36.24.32/27	General NonProd DMZ workloads
	app-general-dmz-nonprod-private-az1-03	10.36.24.64/27	General NonProd DMZ workloads
	app-general-dmz-nonprod-private-az1-external	10.36.32.0/27	General Nonprod DMZ Public workloads
	app-general-dmz-nonprod-private-az2-external	10.36.32.32/27	General Nonprod DMZ Public workloads
	app-general-dmz-nonprod-private-az3-external	10.36.32.64/27	General Nonprod DMZ Public workloads
	app-general-dmz-nonprod-eni-az1-01		General NonProd DMZ ALB ENIs
	app-general-dmz-nonprod-eni-az1-02	10.36.25.32/27	General NonProd DMZ ALB ENIs
	app-general-dmz-nonprod-eni-az1-03	10.36.25.64/27	General NonProd DMZ ALB ENIs
app-general-prod	app-general-dmz-prod-private-az1-01	10.36.26.0/27	General Prod DMZ workloads
	app-general-dmz-prod-private-az1-02	10.36.26.32/27	General Prod DMZ workloads
	app-general-dmz-prod-private-az1-03	10.36.26.64/27	General Prod DMZ workloads
	app-general-dmz-prod-eni-az1-01	10.36.27.0/27	General Prod DMZ ALB ENIs
	app-general-dmz-prod-eni-az1-02	10.36.27.32/27	General Prod DMZ ALB ENIs

	app-general-dmz-prod-eni-az1-03	10.36.27.64/27	General Prod DMZ ALB ENIs
core-shared-nonprod	core-shared-dmz-nonprod-private-az1-01	10.36.28.0/27	Core Shared Nonprod DMZ workloads
	core-shared-dmz-nonprod-private-az1-02	10.36.28.32/27	Core Shared Nonprod DMZ workloads
	core-shared-dmz-nonprod-private-az1-03	10.36.28.64/27	Core Shared Nonprod DMZ workloads
	core-shared-dmz-nonprod-eni-az1-01	10.36.29.0/27	Core Shared Nonprod DMZ ALB ENIs
	core-shared-dmz-nonprod-eni-az1-02	10.36.29.32/27	Core Shared Nonprod DMZ ALB ENIs
	core-shared-dmz-nonprod-eni-az1-03	10.36.29.64/27	Core Shared Nonprod DMZ ALB ENIs
	core-shared-dmz-nonprod-db-az1-01	10.36.29.96/27	Core Shared Nonprod DMZ DB
	core-shared-dmz-nonprod-db-az2-01	10.36.29.128/27	Core Shared Nonprod DMZ DB
	core-shared-dmz-nonprod-db-az3-01	10.36.29.160/27	Core Shared Nonprod DMZ DB
core-shared-prod	core-shared-dmz-prod-private-az1-01	10.36.30.0/27	Core Shared Prod DMZ workloads
	core-shared-dmz-prod-private-az1-02	10.36.30.32/27	Core Shared Prod DMZ workloads
	core-shared-dmz-prod-private-az1-03	10.36.30.64/27	Core Shared Prod DMZ workloads
	core-shared-dmz-prod-eni-az1-01	10.36.31.0/27	Core Shared Prod DMZ ALB ENIs
	core-shared-dmz-prod-eni-az1-02	10.36.31.32/27	Core Shared Prod DMZ ALB ENIs
	core-shared-dmz-prod-eni-az1-03	10.36.31.64/27	Core Shared Prod DMZ ALB ENIs
	core-shared-dmz-prod-db-az1-01	10.36.31.96/27	Core Shared Prod DMZ DB
	core-shared-dmz-prod-db-az1-02	10.36.31.128/27	Core Shared Prod DMZ DB
	core-shared-dmz-prod-db-az1-03	10.36.31.160/27	Core Shared Prod DMZ DB
core-security	core-security-dmz-prod-private-az1-01	10.36.33.0/27	Core Security Prod DMZ workloads
	core-security-dmz-prod-private-az2-01	10.36.33.32/27	Core Security Prod DMZ workloads
	core-security-dmz-prod-private-az3-01	10.36.33.64/27	Core Security Prod DMZ workloads
	core-security-dmz-prod-eni-az1-01	10.36.34.0/27	Core Security Prod DMZ ALB ENIs
	core-security-dmz-prod-eni-az2-01	10.36.34.32/27	Core Security Prod DMZ ALB ENIs
	core-security-dmz-prod-eni-az3-01	10.36.34.64/27	Core Security Prod DMZ ALB ENIs
	core-security-dmz-prod-db-az1-01	10.36.34.96/27	Core Security Prod DMZ DB

core-security-dmz-prod-db-az2-01	10.36.34.128/27	Core Security Prod DMZ DB
core-security-dmz-prod-db-az3-01	10.36.34.160/27	Core Security Prod DMZ DB