Virtual Private Cloud

Each AWS region that hosts POS services requires creation of a VPC to host those services. Kensium uses standard naming and configuration to make maintenance and operations easier. The steps described below to configure a VPC must be repeated for each AWS region that Kensium uses to host POS.

a) AWS Documentation

Ensure that you review and understand the Amazon documenation for AWS's Virtual Private Cloud (VPC) services. VPC is used for communications between other AWS services such as RDS and EC2. Documentation includes:

- General documentation:
  - https://aws.amazon.com/vpc
  - https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
- RDS and VPCs:
  - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.WorkingWithRDSInstanceinaVPC.html
- Scenarios:
  - Thorough description of typical scenarios involved with VPCs.
  - https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_VPC.Scenarios.html

In particular, read the following article as it describes the subnet arrangement we follow:

> https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Tutorials.WebServerDB.CreateVPC.html

This topic expands on the steps described in the article.

b) Create VPC

Using Amazon's VPC Dashboard, click the Create VPC button. We will use the ensuing screen to create a VPC with both public and private subnets.

Kensium uses public and private subnets for future flexibility. While POS databases currently need to be publicly accessible to support legacy sync communications, future versions of POS will perform sync exclusively through the POS server. When supported, this approach to communications will enable databases to be migrated to the private subnet for additional security.

The AWS screen for creating VPCs has changed as of 2023. The screen now automates the creation of the VPC and its related subnets, route tables, and network connections.

In the Create VPC screen, specify the following values:

Field	Value/Example	Notes
Resources to Create	VPC and more	
Name tag auto-generation	Uncheck	Disable automatic generation – we'll manually name VPC entities.
IPv4 CIDR block	10.0.0.0/16	
IPv6 CIDR block	None	
Tenancy	Default	
Number of Availability zones	2	We'll be using a primary and secondary (backup) AZ.
Customize Availability Zones	*	Choose the primary and secondary AZs that you want to use in the region. Multiple AZs are useful for AWS services that support Multi-AZ replication. The first AZ is the primary AZ, and the second AZ is the backup AZ.
Number of public subnets	2	We want a public subnet for each availability zone.
Number of private subnets	2	We want a private subnet for each availability zone.
Customize subnets CIDR blocks	–	Use the AWS defaults.
NAT Gateways	none	

Field	Value/Example	Notes
VPC Endpoints	S3 Gateway	
Enable DNS hostnames	Yes	
Enable DNS resolution	Yes	

c) Specify VPC Names

The next step is to enter names for the VPC and related entity names. We don't use the AWS standard naming scheme, but rather use our own simplified scheme.

The following table provides the names that should be used. Ensure that you correctly match subnet names with route table names (the AWS page will show you the matches).

In our example, we'll assume the following:

- The VPC has been created in the us-west-2 region
- The primary Availability zone is us-west-2c
- The secondary Availability zone is us-west-2d

Type Name Notes VPC VPC-POS VPC name Subnets SN-POS-PUB-1C Public subnet: 1 is primary, C is the AZ SN-POS-PRIV-1C Private subnet: 1 is primary, C is the AZ SN-POS-PUB-2D Public subnet: 2 is secondary, D is the AZ SN-POS-PRIV-2D Private subnet: 2 is secondary, D is the AZ Route tables RTB-POS-PUB Public routing table RTB-POS-PRIV-C Private routing table for subnet in C AZ RTB-POS-PRIV-D Private routing table for subnet in D AZ Network connections IGW-POS Public internet gateway VPCE-POS-S3 VPC endpoint for S3

d) Default Security Group

The Create VPC screen will create a default security group. This group does not have a name assigned.

Edit the name of this default security group, and rename it to SG-POS-DEFAULT.

e) Web Security Group

Create a new security group that represents the web servers that host Kensium POS. This security group

allows the public to access the POS servers through standard web protocols.

- Security group name: SG-POS-WEB
- Description: Public web access to POS servers
- VPC: VPC-POS

Add the following inbound rules.

- HTTP (port 80) from anywhere (0.0.0.0/0)
- HTTPS (port 443) from anywhere (0.0.0.0/0)

After the security group is created, edit the Name so that it is the same as Security group name.

f) Database Security Group

Create a new security group that represents the RDS instances that will host Kensium POS databases. This security group permits access to databases from POS web servers, as well as direct organization communications (e.g. Kensium Comm Services).

- Security group name: SG-POS-DB
- Description: POS server & organization access to POS databases
- VPC: VPC-POS

Add the following inbound rules.

- MSSQL (port 1433) from security group rms-sg-web, with a description of POS server access to MSSQL databases

After the security group is created, edit the Name so that it is the same as Security group name.

> When creating rules for direct organization communications, always enter the organization ID in the rule description. This will make it easier to update or delete rules if the organization's IP addresses change.

g) Operations Security Group

Create a new security group that represents any access required by Kensium operations personnel to

configure and maintain EC2 and RDS instances.

- Security group name: SG-POS-OPS
- Description: Kensium operations access to POS servers and databases
- VPC: VPC-POS

No inbound rules need to be added at this time. These will be added as required to permit Kensium personnel to access the POS servers and databases. Typical open ports include:

- Port 3389 (RDP) to manage EC2 instances via Remote Desktop
- Port 1433 (MSSQL) to manage SQL Server databases using SQL Server Management Studio

> When creating operator rules, always enter the person's name in the rule description. This will make it easier to update or delete rules if the person's IP address changes.

After the security group is created, edit the Name so that it is the same as Security group name.

h) DB Subnet Group

Open the Amazon RDS console, navigate to Subnet groups, then choose Create DB Subnet Group. Enter the following fields:

>Field	Value/Example	Notes
Name	DBSNG-POS	
Description	DB Subnet group for POS	
VPC	VPC-POS	RDS instances should be placed within the POS VPC.
Availability Zones	us-west2c and us-west-2d (example)	Set to the primary and backup AZs we've chosen for the AWS region.
Subnets	…	Select the subnets that you created above.

i) ElastiCache Subnet Group

Open the Amazon ElastiCache console, navigate to Subnet groups, then choose Create DB Subnet Group. Enter the following fields:

>Field	Value/Example	Notes
Name	`ELCSNG-POS`	
Description	`ElastiCache Subnet group for POS`	
VPC	`VPC-POS`	ELC instances should be placed within the POS VPC.
AZ & Subnets	Add all	Use the `Add All` link to add all of the VPC subnets to the subnet group. Verify that this includes (and only includes) the subnets added above.

j) Review Configuration

Once completed, review the configuration of all entities created above with this document. Correct any problems before using the configuration to host POS servers and databases.