Using the AWS Shared VPC Offerings

Introduction

This document provides practical information about using either the **Multitenant Subnets** or **Exclusive Use Subnets** options of the Shared VPC offering once its has been provisioned to your Cornell AWS account.

Best Practices

- Use Security Groups applied to resources deployed in the Shared VPC to restrict ingress to those resources, even by traffic from the local VPC and subnets. You don't want to be affected by something dumb another team does when they are using the Shared VPC.
- When deploying replicas of a specific resource, be sure to spread them out across multiple subnets (and thus multiple AZs).
- Be especially careful about configuring resources that automatically scale up (e.g., EC2 Auto Scaling Groups).
- If you are managing Elastic Network Interfaces directly, be sure to delete them once they are no longer needed.
- Don't change the tags that "come with" the shared resources. But, feel free to add additional tags as you see fit. See Tagging below for more information.

What You'll See

Tagging

The resources shared in the context of the Shared VPC offerings are extensively tagged in order to provide helpful information to users. This tagging is maintained by a process that regularly resets the tag values if they are changed.

Except for the "Name" tag, all other tags used by the Shared VPC offerings are prefixed by "cit:". Any tags that you add will remain unchanged.

Tags Added to Most Shared Resources

Tag Key	Tag Value	Description
Name	*varies*	Across the Shared VPC offerings, resource names are constructed to be clear and have uniform structure.
cit:contact-email	cloud-support@cornell.edu	Where to direct questions about the resource.
cit:description	*varies*	Prose description of the resource
cit:documentation-url	https://confluence.cornell.edu/x/Go8xHQ	Where the resource is more completely documented.
cit:deployment	shared-vpc	This tag identifies the resource as being part of the Shared VPC offering.
cit:name	*varies*	Generally duplicates the value of the "Name" tag.

Multitenant Subnet Resources

VPC

Name	cornell-shared-vpc

Subnets

There is one private Subnet for each AZ.

Name **cit:Name**	cornell-shared-vpc/private-use1-az**N**	Identifies the subnet as belonging to the cornell-shared-vpc and further in which AZ it resides. Note the use of AZ IDs (which are consistent across accounts) not AZ names (which are not consistent across accounts).
cit:nat-gateway-public-ipv4-address	*see below*	This is the public IP address that is attached to the NAT Gateway servicing this private subnet. This Public IP address will remain unchanged for the life of the subnet.
cit:subnet-type	private-mulitenant	Identifies the subnet as belonging to the **Multitenant Subnets** offering.

Route Tables

There is one Route Table for each AZ.

Name **cit:name**	cornell-shared-vpc/private-use1-az**N**	Identifies the route table as belonging to the cornell-shared-vpc and further the AZ which it serves. Note the use of AZ IDs (which are consistent across accounts) not AZ names (which are not consistent across accounts).
cit:az-id	use1-az**N**	AZ served by the route table.

Network ACLs

A single Network ACL serves all the subnets.

Name **cit:name**	cornell-shared-vpc/baseline	Identifies the Network ACL as the Cornell baseline NACL. See Baseline AWS Network ACL.

Exclusive Use Subnet Resources

Exclusive Subnets live in the same VPC as the **Multitenant Subnets.** They also use the same Network ACLs, Route Tables, and NAT Gateways.

If customer AWS account uses only the **Exclusive Use Subnets** offering and not the **Multitenant Subnets** offering, only the relevant Network ACLs and route tables will be visible in the customer account. The multitenant subnets will not be visible.

Subnets

There will be one private subnet per AZ configured for each specific set of exclusive subnets.

Name **cit:Name**	LABEL/private-use1-az**N**	Each subnet contains the LABEL configured for the set and the ID of the AZ where the subnet resides.
cit:nat-gateway-public-ipv4-address	*see below*	This is the public IP address that is attached to the NAT Gateway servicing this private subnet. This Public IP address will remain unchanged for the life of the subnet.
cit:tenant-account-ids	*varies*	This is a comma-separated list of the AWS account IDs with which the subnet is shared. E.g., "123456789012,111222333444"
cit:subnet-type	private-exclusive	Identifies the subnet as belonging to the **Exclusive Use Subnets** offering.

What You Won't See

NAT Gateways

The NAT Gateways used by the Shared VPC offerings are not visible from customer AWS accounts. However, the Route Tables that are visible do properly show which NAT Gateway they use. Due to this lack of visibility, we have provided tagging on private subnets that shows the public IP address for the NAT Gateway used by that subnet. Traffic to the internet from a subnet will appear to be coming from that IP address.

These are the the NAT Gateway public IP addresses used by the Shared VPC offerings. These will remain fixed.

Availability Zone	NAT Gateway Public IP Address
use1-az1	75.101.192.203
use1-az2	34.230.123.26
use1-az3	54.205.225.30
use1-az4	35.173.86.238
use1-az5	44.211.111.35
use1-az6	18.210.42.171

References

- Cornell
  - Shared AWS VPC for Cornell AWS Accounts
  - Shared AWS VPC FAQs
  - Cornell AWS Direct Connect
  - The Cornell Standard VPC
- AWS
  - AWS Resource Access Manager
  - AWS Systems Manager Parameter Store