Shared AWS VPC for Cornell AWS Accounts

Introduction

Cornell AWS customers now have two new options for easy access to the private Cornell network in AWS.

- The first option, opting into to use the Shared AWS VPC, is the simplest. As the name suggests, the Shared VPC gives Cornell AWS customers access to a set of large private subnets in us-east-1. These subnets reside on the private Cornell network and their use is shared with other Cornell AWS customers. We call this option the **Multitenant Subnets** option.
- The second option offers exclusive access to a set of private subnets that are customized for your use. These subnets in us-east-1 can be customized with respect to size and Availability Zone location and also reside on the private Cornell network. They can also be shared with other Cornell AWS accounts that you specify. We call this option the **Exclusive Use Subnets** option within the Shared VPC offering.

Resources deployed to subnets in either offering have network access to other Cornell network resources, specifically:

- all Cornell Standard VPCs in AWS, via Transit Gateway
- on-campus Cornell networks, via Direct Connect
- private Cornell VNETs in Azure, via Internet2 Cloud Connect

In the past, each Cornell AWS customer that required access to the private Cornell network in AWS received their own Cornell Standard VPC that provided an AWS VPC for their exclusive use. In contrast, the **Multitenant Subnets** option described in this document provides similar network connectivity in a set of AWS subnets shared among many Cornell AWS customers. The **Exclusive Use Subnets** option offers the same network connectivity but sharing is amongst a set of Cornell AWS customers that you specify.

> The initial options of the Shared VPC deployment supplies only **private** subnets to opted-in Cornell AWS accounts. This means that neither option can be used to host a public web site or public APIs, for example. Please contact Cloud Support with feedback about your needs to access to public subnets in the Shared VPC.

Features and Benefits

> See also Shared AWS VPC FAQs.

The following table compares the new Shared VPC options with the traditional Cornell Standard VPC.

Benefit	Feature	Description	Cornell Standard VPC	Shared VPC	
				Multitenant Subnets	Exclusive Use Subnets
Ease of use	AWS Account integration	Subnets are visible directly from your AWS account, via the web console or API.	✓	✓	✓
	No VPC management	Customers do not have to worry about managing a VPC. Subnet, route table, NAT gateway, endpoint, and network ACL management is performed by the CIT Cloud Team.	✗	✓	✓
Fault-tolerance and Flexibility	AZ flexibility	Use subnets in any **us-east-1** Availability Zone.	not by default	✓	✓

	Fault-tolerant internet access	Each subnet uses a NAT Gateway in the same Availability Zone as the subnet to route outgoing traffic to the public internet. A NAT Gateway failure in one zone won't affect subnets in other zones.	not by default	✅	✅
Privileged network access	Private Cornell addressing	Resources are assigned IP addresses from the private Cornell network. As such, they reside on the Cornell network and can reach other resources on the Cornell network.	✅	✅	✅
	Public subnets	Ability to deploy resources to public subnets, directly accessible from the internet.	✅	❌	❌
	Access to on-campus Cornell networks	Subnets have private network connectivity to the on-campus Cornell network.	✅	✅	✅
	Access to Cornell networks in Azure	Subnet have private network connectivity to private Cornell networks (VNETs) in Azure.	✅	✅	✅
	Access to on-campus Cornell networks	Subnets have private network connectivity to the on-campus Cornell network.	✅	✅	✅
	S3 and DynamoDB gateway endpoints	Gateway endpoints for S3 and Dynamo DB in the VPC make communication with those services quick and private.	not by default	✅	✅
	VPC Peering	Peer to arbitrary AWS VPCs	✅	❌	❌
Security	Baseline network security	Subnets use the Cornell Baseline AWS Network ACL, managed by the CIT Cloud Team.	❌	✅	✅
	Customer-defined security groups	Customers manage and control the Security Groups applied to their resources. Thus, they have the final say about what network connectivity is allowed.	✅	✅	✅
	CIDR-based access control	Subnet size allows subnet CIDR blocks to be used for meaningful network access control by your collaborators.	✅	❌	✅
	Known peers	Subnets are used only by teams you know.	✅	❌	✅
Cost	"Free" NAT Gateways	NAT Gateways are managed and paid for by CIT. NAT Gateways run by customers typically cost at least $1/day.	❌	✅	✅
	"Free" VPC Flow Logs	VPC Flow Logs are managed and paid for by CIT.	❌	✅	✅
	Pay for what you use	Customers pay for resources deployed to the Shared VPC as if they were using their own VPC. There are no additional charges for opting into either Shared VPC option.	✅	✅	✅

Use Cases

Both the **Multitenant Subnets** and the **Exclusive Use Subnets** options of the Shared VPC offering support many, many use cases. A few of those are:

- Manual deployment of a few resources that require access to the Cornell private network
- Using Infrastructure as Code to create and manage AWS resources in the Shared VPC
- Standing up an RDS instance in the private Cornell network
- Deploying an API Gateway API or Lambda function with access to the Cornell network
- Deployment of resources which will be accessed only by users on the Cornell VPN

Misuse Cases

Misuse cases are situations where the **Multitenant Subnets** and the **Exclusive Use Subnets** option should not or cannot be used. Some of those are:

- Deploying a public web site or API. (Public subnets would be required to deploy a publicly accessible web site, but the initial release of the Shared VPC offers only private subnets.)
- Cornell private network access in regions other than us-east-1 (N. Virginia)
- Need to customize Network ACLs, Route Tables, or other VPC configuration
- Peering to non-Cornell AWS VPCs
- Ability to use a large number of private Cornell IP addresses in AWS
- Deploying Kubernetes or using EKS (Kubernetes consumes vast numbers of IP addresses, which is incompatible with the Shared VPC model)

Requesting Access to Shared VPC Offerings

By requesting and using any Shared VPC offering, you are consenting to follow the Guidelines for Use.

Multitenant Subnets

Send a note to Cloud Support with the following information:

- Your AWS account ID. The **Multitenant Subnets** will be shared to this account.
- Whether you have existing VPCs (especially Cornell Standard VPCs) in your AWS account that you will be trying to retire after you begin using the Shared VPC offerings.
- Any questions you have about using the Shared VPC offering.

Exclusive Use Subnets

Before provisioning **Exclusive Use Subnets** we will probably need a short meeting to discuss details. But, get the process started by sending a note to Cloud Support with the following information:

- Your AWS account ID.
- Specifics about the subnets you wish:
  - What other AWS accounts should have access to the subnets?
  - A list of AZs where the subnets should reside. We provision one subnet per AZ.
  - The size of the subnets.
  - A label to use as a prefix for names of the subnets and related resources.
- A list of people that should be invited to a brief meeting to confirm the subnet parameters.
- Whether you have existing VPCs (especially Cornell Standard VPCs) in your AWS account that you will be trying to retire after you begin using the Shared VPC offerings.
- Any questions you have about using the Shared VPC offering.

Guidelines

Customers using the Shared VPC offerings must agree to abide by the following guidelines:

- Customers cannot use the Shared VPC to deploy systems that utilize large quantities of IPv4 addresses.

  > If you configure a deployment that consumes vast quantities of IP addresses in the **Multitenant Subnets**, and it is negatively affecting other **Multitenant Subnets** customers, the resources created by the deployment may, in an urgent situation, be destroyed in order to remove or reduce the impact to other customers.

  Examples of services that could use lots of IPs from a subnet:

  - Kubernetes clusters and the Amazon Elastic Kubernetes Service (EKS) both use large numbers of IP addresses, even for trivial deployments, and so should not be deployed to the Shared VPC.
  - Large AWS EMR deployments. (EMR clusters with a handful of nodes are OK.)

- If you need to move extremely large amounts of data (e.g, more than a TB) into or out of any Shared VPC offering, please contact Cloud Support so that we can assist in plotting the most time- and cost-efficient way to accomplish this.
- We cannot customize the Network ACL used by the Shared VPC offerings for arbitrary customer needs.
  - However, since the Shared VPC is a new offering, there may be adjustments needed to accommodate reasonable use-cases we had not envisioned. Please contact Cloud Support to discuss.
- We cannot peer the Shared VPC with arbitrary AWS VPCs, whether or not those VPCs are owned by Cornell AWS accounts. All Cornell VPCs on the private Cornell network are already accessible to the Shared VPC via the Direct Connect Transit Gateway architecture.
  - If you have a use case where massive quantities of data are being passed between the Shared VPC and a Cornell Standard VPC, contact Cloud Support to discuss whether a direct peering would be beneficial for cost or latency efficiencies.

See also Best Practices.

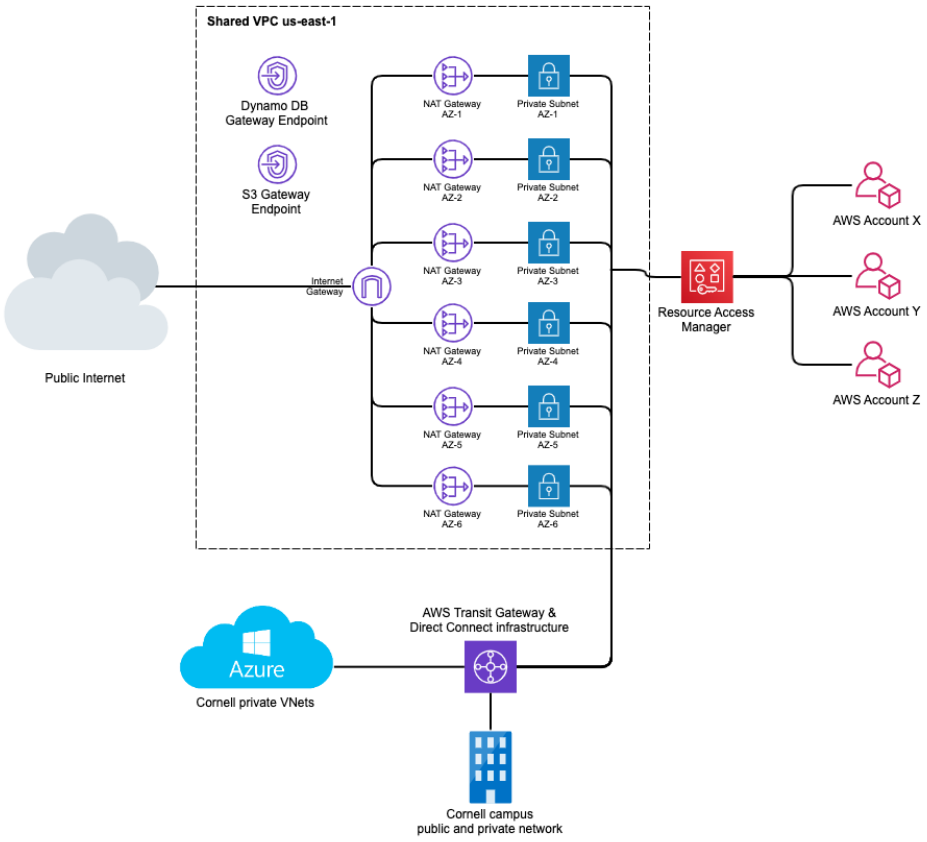
Roadmap — Potential Features for Future Releases

> These features are being considered for the future. Weigh in on them or suggest others by sending a note to Cloud Support.

- Specifics about the Share VPC resources (e.g., VPC id, subnet ids, etc.) could be created in the Systems Manager Parameter Store in customer accounts. These details could them easily be referenced from CloudFormation templates; see Using dynamic references to specify template values.
- Indirect access to shared public subnets, allowing only deployment of Application or Network Load Balancers routing to targets in any Shared VPC offering.
- Direct access to public subnets for deploying arbitrary resources that can be made public.

Appendix

Architecture



Usable IP Addresses in Subnets

AWS reserves 5 addresses in each subnet for its own use. See Subnet Sizing.

CIDR Notation	Subnet Bits	Total Addresses	Useable Addresses
/28	28	16	11
/27	27	32	27
/26	26	64	59
/25	25	128	123
/24	24	256	251

References

- Cornell
  - Shared AWS VPC FAQs
  - Using the AWS Shared VPC Offerings
  - Cornell AWS Direct Connect
  - The Cornell Standard VPC
- AWS
  - AWS Resource Access Manager
  - AWS Systems Manager Parameter Store
  - Subnet Sizing