2023 Cornell AWS Direct Connect Architecture Migration

This page is being retained for historical purposes, but is no longer maintained. All relevant Direct Connect information about the current (2023 and after) Direct Connect architecture has been migrated to primary customer Direct Connect documentation, Cornell AWS Direct Connect.

Executive Summary

- Cornell AWS accounts using Direct Connect will be migrated to a new network architecture in January 2023.
- This new architecture simplifies Direct Connect configuration and management, and improves Direct Connect bandwidth and flexibility.
- The migration process is designed to avoid interruption of Direct Connect connectivity, how brief interruptions may occur.
- Cornell AWS account owners/administrators will be solicited for feedback directly via email several times throughout this process. But, in most cases, this input is not required for the migration to proceed.
    - AWS accounts having VPCs using Direct Connect and with numerous subnets and route tables, or where network resources are configured by infrastructure-as-code *will* need to provide input to complete this migration.
- While line items for charges to Cornell AWS accounts will change between the old and new Direct Connect architectures, the overall change in cost is negligible.
    - CIT will be paying for new costs of ~$36/mo for each customer VPC connected the new Direct Connect architecture.

Introduction

This document provides details about the Direct Connect architecture migration Cornell will be executing in early 2023.

Rationale

Cornell AWS accounts using Direct Connect for private access to Cornell networks will be transitioned to using Internet 2 Cloud Connect (I2CC) as the Direct Connect provider.

The Internet 2 Direct Connect provider offers several benefits:

- Consolidating and simplifying configuration and management of Direct Connect for Cornell AWS accounts
- Improving flexibility and bandwidth of Direct Connect connectivity
- Allows private Cornell network traffic in AWS and Azure to flow between those clouds without transiting campus

Scope

As of 29 Nov 2022, 65 Cornell AWS accounts were configured to use Direct Connect. During this migration, all those AWS accounts will have their existing Direct Connect connectivity updated to use new pathways and AWS resources to connect the Cornell campus network to AWS.

Within those 65 Cornell AWS accounts, only the network resources within VPCs using Direct Connect will be affected. Other VPCs in those Cornell AWS accounts will not be affected.

For VPCs using Direct connect, the following table identifies the impact of this migration on specific types of network traffic

Connectivity	Changing?
VPC connectivity to the Internet	not changing
VPC-to-VPC peering	not changing
VPC to campus addresses via the Direct Connect	• architecture changes • overall connectivity not changing
VPC to campus addresses via the Internet	not changing

Terminology

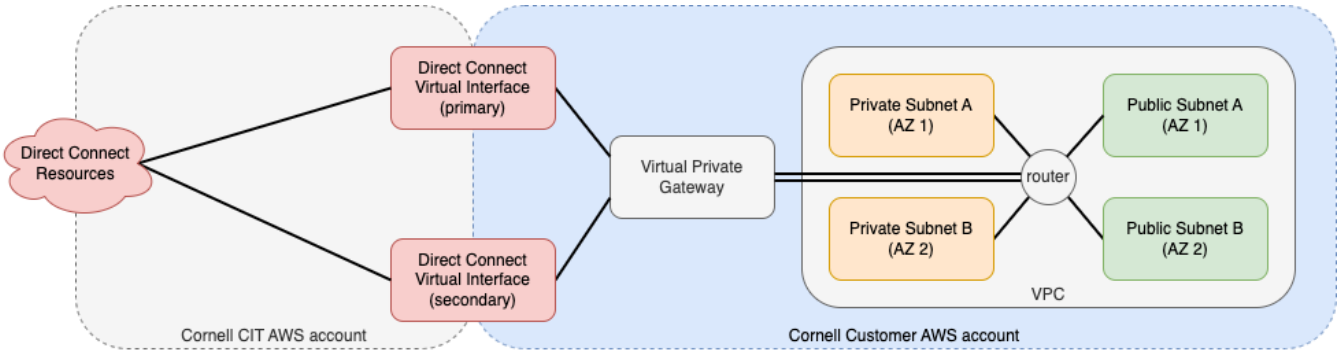
We use the following terminology in this document:

- customer – Cornell AWS account owners/administrators
- Version 1 (v1) architecture – This is the network architecture used by Cornell AWS Direct Connect networking prior to the 2023 migration.
- Version 2 (v2) architecture – This is the network architecture used by Cornell AWS Direct Connect networking after the 2023 migration.
- VPC – Virtual Private Cloud
- DC – Direct Connect
- TGW – Transit Gateway
- VGW – Virtual Private Gateway

Architectures

These diagrams show the network resources within Cornell AWS accounts that connect a VPC to the Cornell campus network via Direct Connect.

Version 1 (pre-2023)



Example Public VPC Route Table
0.0.0.0/0 → Internet Gateway
10.92.xx.yy → local
10.0.0.0/8 → VGW

Example Private VPC Route Table
0.0.0.0/0 → NAT Gateway
10.92.xx.yy → local
10.0.0.0/8 → VGW
128.84.0.0/16 → VGW
128.253.0.0/16 → VGW
132.236.0.0/16 → VGW
192.35.82.0/24 → VGW
192.122.235.0/24 → VGW
192.122.236.0/24 → VGW

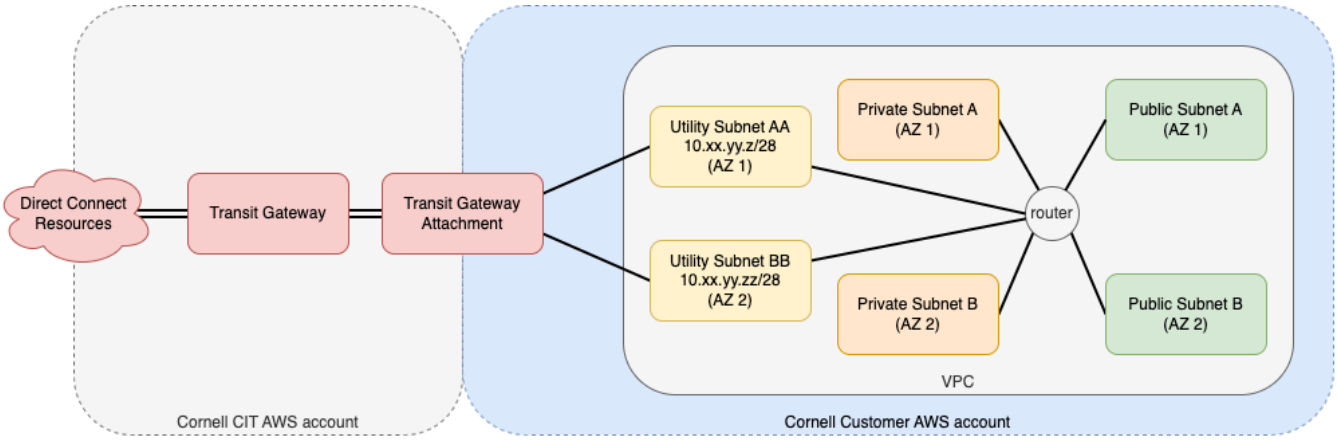
draw.io source: dc-arch-legacy.customer.v2.drawio

Paths and Traffic Filtering in Version 1 Architecture

Inbound Traffic – From Direct Connect to EC2 Instance

	Resource	Filtering
Source	Direct Connect Virtual Interface	—
	Virtual Private Gateway	—
	NACL of Subnet containing EC2 instance	inbound rules of NACL
	EC2 Instance Security Group	inbound rules of SG
	EC2 Instance Elastic Network Interface	—
Destination	EC2 Instance	—

Version 2 (2023)



Example Public VPC Route Table
0.0.0.0/0 → Internet Gateway
10.92.aa.bb/22 → local (primary subnets)
10.xx.yy.z/28 → local (utility)
10.xx.yy.zz/28 → local (utility)
10.0.0.0/8 → TGW Attachment

Example Private VPC Route Table
0.0.0.0/0 → NAT Gateway
10.92.aa.bb/22 → local (primary subnets)
10.xx.yy.z/28 → local (utility)
10.xx.yy.zz/28 → local (utility)
10.0.0.0/8 → TGW Attachment
128.84.0.0/16 → TGW Attachment
128.253.0.0/16 → TGW Attachment
132.236.0.0/16 → TGW Attachment
192.35.82.0/24 → TGW Attachment
192.122.235.0/24 → TGW Attachment
192.122.236.0/24 → TGW Attachment

dc-arch-2023.customer.ALTERNATE.10-8.v2.drawio

Paths and Traffic Filtering in Version 2 Architecture

Inbound Traffic – From TGW to EC2 Instance NOT Residing in a Subnet Attached to TGW

	Resource	Filtering	Notes
Source	TGW	—	
	TGW Attachment	—	
	TGW Attachment Elastic Network Interface	—	
	NACL of Subnet attached to TGW	outbound rules of NACL attached to utility subnet	The NACL bound to the utility subnets will allow all traffic in and out.
	Route Table of Subnet attached to TGW	—	
	NACL of Subnet containing EC2 instance	inbound rules of NACL for destination subnet	
	EC2 Instance Security Group	inbound rules of SG	
Destination	EC2 Instance Elastic Network Interface	—	

What Is Changing?

Before the migration is executed, a set of resources in Cornell AWS accounts will be tagged with details about the migration. In addition, a small set of new resources that support the v2 architecture will be created in Cornell AWS accounts. After the migration is complete, a few resources not used in the v1 architecture will be deleted.

Cornell AWS customers will have the opportunity to provide feedback before migration and any resource deletion that affects their AWS accounts.

Tagging

For this migration, we are tagging AWS resources to provide information about how the each resource is involved in the migration itself, the v1 architecture, and the v2 architecture.

Tag Key	Tag Values	Description	VPC	Subnets	Route Tables	NACLs ‡	Transit Gateway Attachments	Virtual Private Gateways	Direct Connect Virtual Interfaces
cit:dc-arch-migration-target	yes/no	Will this resource itself be affected as part of the migration?	✓	✓	✓	✓	✓	✓	✓
cit:dc-arch-migration-description	prose	Description of planned changes to this resource	✓	✓	✓	✓	✓	✓	✓
cit:dc-arch-version	v1/v2	Is this a v1 or v2 architecture resource? After migration, v1 resources utilized in the v2 architecture will be relabeled as v2 resources.	✓	✓	✓	✓	✓	✓	✓
cit:dc-arch-migration-new-resource	yes/no	Is this a new resource specifically created for the v2 architecture?	n/a	n/a	✓	✓	✓	n/a	n/a
cit:dc-arch-migration-replaces	resource ID	If this v2 resource will be replacing a v1 resource, this ID references the resource that will be replaced.	n/a	n/a	✓	n/a	n/a	n/a	n/a
cit:subnet-type	public /private /utility	Is this a private or public subnet? Public subnets are those with a route to an Internet Gateway. Utility subnets will be created specifically to use for TGW Attachments. Private subnets are all subnets that are not public and are not utility subnets.	n/a	✓	n/a	n/a	n/a	n/a	n/a
cit:tgw-attachment-target	yes/no	Will a Transit Gateway be attached to this subnet?	n/a	✓	n/a	n/a	n/a	n/a	n/a
cit:dc-arch-exclude-tgw-routes	yes/no	This tag is applied only to the new Route Table that is created for use by the TGW Attachment utility subnets	n/a	n/a	✓	n/a	n/a	n/a	n/a
cit:dc-vgw	yes/no	Does this Route Table contain rules referencing a VGW?	n/a	n/a	✓	n/a	n/a	n/a	n/a
Cost Center	R524755	This tag added to TGW Attachments will result in CIT paying for the $0.05/hr cost of attaching a VPC to a TGW.	n/a	n/a	n/a	n/a	✓	n/a	n/a

‡ Only the NACL created for use by utility subnets will be tagged.

ℹ Direct Connect Gateways are also involved in the migration but cannot be tagged.

New Resources

A few new resources will be created as part of this migration.

- New Resource Groups are an easy way to see the lists of affected resources.
- New Route Tables will have routes that replace Virtual Private Gateway destinations with Transit Gateway Attachments destinations.
- New utility Subnets, one for each AZ where the VPC is active.
- New permissive Network ACL to be used only by the new utility Subnets.
- Transit Gateway Attachments will connect VPCs to the v2 architecture.

If you use Terraform or other infrastructure-as-code tools to manage your VPC, let us know. We can work directly with you to allow your tools to create or import these new resources.

Resource Groups

New AWS resource groups collect references to relevant AWS account resources in one place (per Cornell AWS account) for easy reference and review:

ℹ Resources can and will appear in multiple resource groups!

- cit-dc-arch-migration-affected-resources – These resources will be directly affected by this migration. These resources include:
  - new resources that support the v2 architecture
  - resources that support the v1 architecture and will no longer be needed for the v2 architecture
  - resources that will remain, but will have their configuration changed to support the v2 architecture
- cit-dc-arch-version-1-resources – All network resources that support or utilize the v1 architecture

    - After the v1 v2 migration is complete, v1 resources will either be deleted (if they are not used in the v2 architecture) or relabeled as v2 resources (if they continue to be used in the v2 architecture).
- cit-dc-arch-version-2-resources – All newly-created resources that support the v2 architecture

These Resource Groups will be created during the **Preparation** phase of the migration. See Migration Process.

If you use Terraform or other infrastructure-as-code tools to manage your VPC, you may need to add configuration to instruct those tools to ignore these new tags. For example, we have specific guidance for Terraform: Terraform Configuration Guidance for 2023 Direct Connect Architecture Migration.

Some resources that belong in these Resource Groups will not be present because of limitations in the the resource types that Resource Groups can handle. These resource types are:

- Transit Gateway Attachments
- Direct Connect Virtual Interfaces
- Direct Connect Connections

Route Tables

The AWS Transit Gateways used in the v2 architecture require different routing rules than the Virtual Private Gateways (VGW) used in the v1 architecture. Each VPC Route Table that references a Virtual Private Gateway will be duplicated and, in the new Route Table, rules referencing a VGW will be replaced with rules referencing a TGW Attachment. The new Route Tables will *not* include "blackhole" routes (i.e. routes to resources, like old peering connections, that no longer exist) from the original Route Tables.

These new Route Tables will be created prior to the migration, but will not actually be utilized until the migration is executed. When migration is executed, subnets associated with the v1 Route Tables will be re-associated to the corresponding v2 Route Tables. Similarly, if the "main" Route Table for the VPC references a VGW, the corresponding v2 Route Table will be set as the "main" Route Table for the VPC.

These Route Tables will be created during the **Migration** phase of the migration. See Migration Process.

Utility Subnets

New "utility" subnets will be created in each VPC. The sole purpose for these subnets is to be used to make TGW Attachments. One new subnet will be created for each AZ where the VPC has private or public subnets. (This provides the best resiliency for the Direct Connect connectivity through the TGW.)

In order to create these subnets, VPCs will have an additional CIDR block associated with it. The new subnets will be created with /28 CIDR blocks from the new CIDR attached to the VPC. These tiny subnets (~16 IPv4 addresses) should not be used for anything else. The Route Tables and NACLs associated with these subnets make them unsuitable for general use.

Network ACL

The Network ACLs already in customer VPCs will not be affected by this migration. However, a new NACL will be created in each VPC and associated with the new utility subnets. The NACL will be permissive (allowing all traffic in and out) and named in such a way to discourage use for other purposes.

Transit Gateway Attachments

Transit Gateway Attachments are the mechanism that VPCs connect to Transit Gateways. The Transit Gateways we use in the v2 architecture reside in a central AWS account, and a TGW Attachment is what links the VPC in a Cornell AWS account to those central TGWs.

Unlike Virtual Private Gateways, TGW Attachments connect to specific subnets in a VPC. We will be making these TGW Attachments to the utility subnets in VPCs which were specifically created for this purpose.

TGW Attachments will be created during the **Migration** phase of the migration. See Migration Process.

Resource Deletion

After migration is complete, a few resources will be deleted during the **Cleanup** phase of the migration. These are:

- Virtual Private Gateways (VGWs)
- Direct Connect Virtual Private Interfaces (DCVIFs)
- Direct Connect Gateways that supported the v1 architecture.

Neither VGWs nor DCVIFs have a role in the v2 architecture.

V1 Route Tables will *not* be deleted, but will not be used in the v2 architecture. Cornell AWS account owners can delete the v1 Route Tables if they wish. Once the VGWs are deleted, those v1 Route Tables will not be all that functional.

Costs

The management and routing simplification offered by the v2 architecture comes with a shift in costs seen by Cornell AWS accounts using Direct Connect, but the overall impact to Cornell AWS account costs should be negligible.

V1 Architecture

Cornell AWS accounts using Direct Connect saw these Direct Connect-related charges:

- Bandwidth charges for traffic from VPCs to campus using the Direct Connect is charged at $0.02/GB.
    - This cost is born by each Cornell AWS account using Direct Connect in the v1 architecture. This cost will no longer be present using the v2 architecture.
- Bandwidth charges from traffic TO VPCs from campus is free.

V2 Architecture

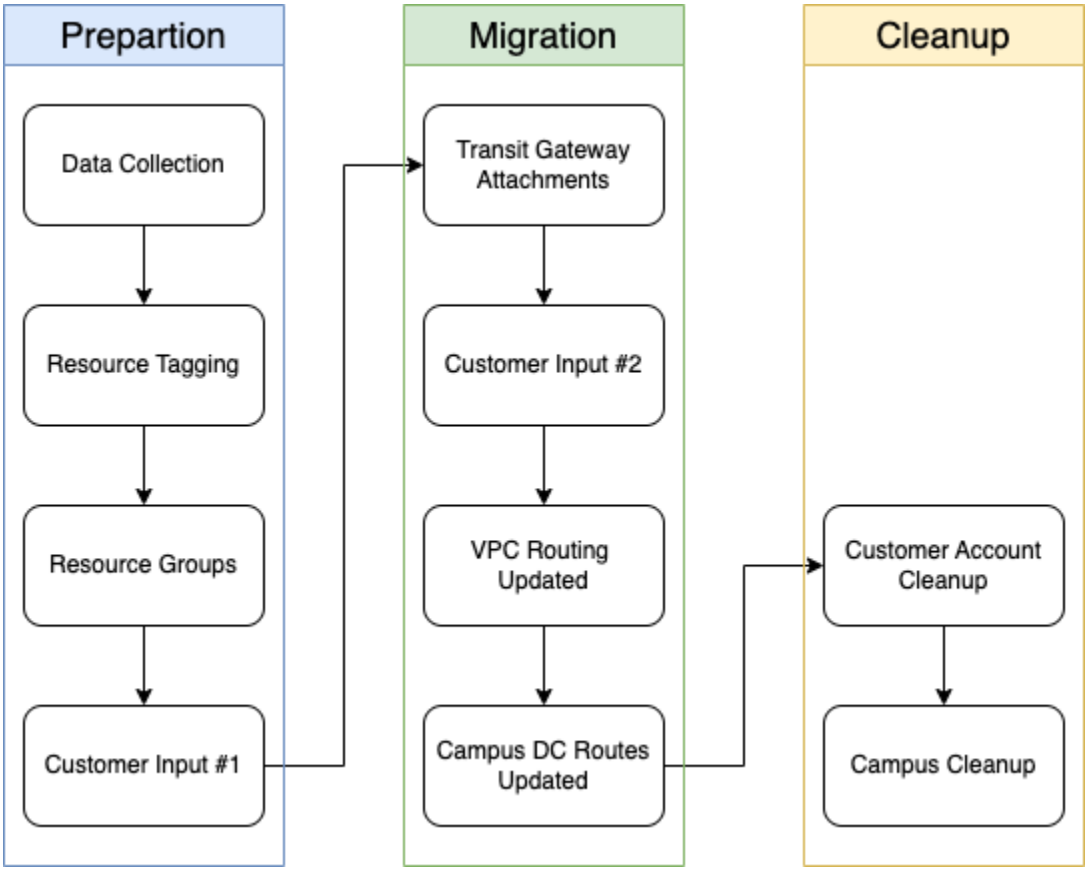
These charges are involved in the v2 architecture:

- Every VPC connected to the Transit Gateway is charged $0.05/hr by AWS. These charges will appear in customer AWS account invoices, **but** the charges will be paid for by CIT since a **Cost Center** tag on the TGW attachment automatically will automatically direct those charges to a CIT KFS account.
- Bandwidth charges for traffic from the VPC *to the TGW* is $0.02/GB. This cost is born by the customer and the magnitude of the charge will be similar to the Direct Connect egress charges born by the customer in the v1 architecture.
- Bandwidth for traffic *from the TGW* to the VPC is free.

Summary

In total, Cornell AWS accounts using Direct Connect should not experience any significant change in charges for using the v2 Direct Connect architecture. The one new cost that customers will see on invoices is being paid by CIT through the use of a **Cost Center** tag on the relevant resources.

Migration Process and Schedule



draw.io source: direct-connect-migration-process.v2.drawio

Phase	Stage	Timeframe	Status	Activity	Impact on Cornell AWS Account VPC Networks

Preparation	Data Collection	November 2022	✅	• Gather information about Direct Connect resources and connected VPCs in Cornell AWS accounts	none
	Resource Tagging	14 Dec 2022	✅	• Add tags to existing resources in customer accounts to assist with targeting, identification, status, intended disposition	none
	Resource Groups		✅	• Create Transit Gateway in CIT AWS account • Create Resource Groups for resources involved in the migration in customer accounts	none
	Customer Input #1	15 Dec 2022 - 02 Jan 2023	✅	• Cornell AWS account owner/admin review • Cornell AWS account owner/admin feedback solicited	none
Migration	Transit Gateway Attachments	03 Jan 2023 - 06 Jan 2023	✅	• Utility Subnets • Transit Gateway Attachments created in customer accounts • v2 Route Tables created in customer accounts • NACLs for Utility Subnets	none
	Customer Input #2	09 Jan 2023 - 13 Jan 2023	✅	• Cornell AWS account owner/admin review • Cornell AWS account owner/admin feedback solicited • Route Table and/or TGW Attachments adjusted according to customer input	none
	v2 BGP Updated	17 Jan 2023 7am	✅	• v2 Direct Connect infrastructure will have BGP configuration changed to begin advertising new routes via I2CC	Azure-to-AWS-VPC traffic may begin to use the v2 architecture (in just the one direction). This is limited only to Azure-to-AWS-VPC traffic due to Cornell's network architecture.
	VPC Routing Updated	17 Jan 2023 9am	✅	• v2 Route Tables activated • v1 Route Tables deactivated	• VPC-to-campus traffic will be routed through the v2 architecture • Azure-to-AWS-VPC traffic may use the v2 architecture.
	Campus Direct Connect Routes Updated	18 Jan 2023 9am	✅	• Direct Connect Virtual Interfaces in customer accounts will be disabled. This causes DC traffic to begin using the v2 architecture for campus-to-AWS traffic	• campus-to-VPC traffic will be routed through the V2 architecture • all Azure-to-AWS-VPC traffic will be routed through the v2 architecture
Cleanup	Customer Account Cleanup	23 Jan 2023 - 31 Jan 2023	✅	• VGWs and DC VIFs in customer accounts deleted	none
	Campus Direct Connect Cleanup		✅	• Campus Direct Connect resources deleted or decommissioned	none

Alternate Migration Days

Customers have the option to request that migration for their VPC(s) occur during the week of Jan 9-13 instead of the default migration dates of January 17 and 18. This is especially encouraged for customers that have a separate sandbox or development VPC that needs to be migrated. We can also support taking both migration steps on the same alternate day, but we'd like to leave a 1-4 hour gap between migration steps to confirm that the "VPC Routing Updated" step was successful before continuing to the "Campus Direct Connect Routes Updates" step.

Rollback

Both the "VPC Routing Updated" and the "Campus Direct Connect Routes Updated" steps have simple rollback mechanism. If you discover problems with networking in your VPC after either step and think the change needs to be rolled back, send an email to cloud-incident@cornell.edu and ping Paul Allen (pea1) on Teams.

- The rollback for the "VPC Routing Updated" step is to reassign the original Route Tables to the public and private subnets. This will rollback takes effect immediately.

- The rollback for the "Campus Direct Connect Routes Updated" step is to the cancel the failover of the Direct Connect Virtual Interfaces that we triggered to initial the campus routing updates. This rollback takes 5-20 minutes to complete.

FAQs

How do I tell if my AWS account will be affected by this change?

The list of AWS accounts affected by this migration is here: Cornell AWS Accounts Affected by 2023 Direct Connect Architecture Migration

You will receive multiple emails to the email address associated with the root user of your Cornell AWS account. These emails will make announcements and ask for your input during the migration process.

Will there be any interruption in Direct Connect connectivity during this migration?

As of 09 Dec 2022, our testing indicates that we should be able to complete this migration without any interruption in overall Direct Connect connectivity. However we cannot guarantee this for individual VPCs. If interruptions occur, they should be brief (minutes, not hours).

How will this change affect my AWS account costs?

Cornell AWS accounts will not experience substantive differences in charges between v1 and v2 architecture. A new $36/mo charge for each VPC connected to the v2 architecture is billed directly to a CIT KFS account.

For more details, please see the Costs section above.

Does this change affect VPC peering?

VPC peering is not affected by this change.

Future Peering Changes

Since the Transit Gateway in the v2 architecture is configured to fully interconnect attached VPCs, most VPC peering among Cornell AWS VPCs could be removed eventually. When VPC peering is removed, VPC-to-VPC traffic that formerly used a peering connection would use the Transit Gateway instead. All traffic would remain in AWS, and the traffic would take two (2) hops to reach the target VPC instead of the one (1) hop that the peering connections support.

⚠️ There are two cases where VPC peering would need to remain in place:

1. When Security Groups in one VPC reference Security Groups in a peered VPC, that peering cannot be removed without adjusting the security group to use CIDR blocks instead of the referenced Security Group. TGW Attachments do not support this type of cross-VPC Security Group referencing.
2. Peering between VPCs where one of the VPCs is not using Cornell Direct Connect. VPCs not using Direct Connect cannot replace peering with the TGW Attachment in the v2 architecture.

Reducing the amount of peering amongst Cornell AWS VPCs will take place later and customers will be contacted separately about that. No peering changes are planned as part of the Direct Connect architecture migration.

Does this change affect which campus network CIDR blocks are routed to/from my private and public subnets?

Our goal with this migration is that the routing of traffic between your VPC and Cornell public and private CIDR blocks will remain effectively unchanged between the v1 and v2 architectures. I.e. the Direct Connect routing option that you chose when your Direct Connect connectivity was established will remain in place. Those routing options are "private network extension", "hybrid", and "all campus" routing. For details on those options see Cornell AWS Direct Connect Routing Diagrams.

The exact pathways that Direct Connect traffic takes will change between the v1 and v2 architectures. But, the starting point (e.g., your VPC) and endpoint (e.g. a campus VLAN) of this traffic will constant.

When, specifically, will this migration occur?

See detailed schedule above.

Is there any flexibility in migration dates?

Yes. See Alternate Migration Days above.

Can the migration be rolled back?

Yes. Each of the two active migration steps ("VPC Routing Updated" and "Campus Direct Connect Routes Updated") can be individually rolled back for each migrating AWS VPC. See Rollback above.

What if I use Terraform or a similar tool to manage the network resources in my AWS account?

If you use Terraform or a similar tool to manage your VPCs, please inform the Cloud Team during the **Customer Input #1** stage. You would have several options to update your infrastructure-as-code configuration to support this migration. You could import the new Route Tables and TGW Attachments, or you could create your own Route Tables and TGW Attachments.

During the **Preparation** phase, you can tell Terraform to ignore the "cit:" tags that have been added to your network resources. This guide shows how: Terraform Configuration Guidance for 2023 Direct Connect Architecture Migration.

I don't really use the Direct Connect in my AWS account. Can I remove that feature?

Yes, you can. Just contact cloud-support@cornell.edu. Depending on the timing of things, we may need to migrate your Direct Connect connectivity to the v2 architecture before removing Direct Connect from your account entirely.

References

- Cornell Documentation
  - Cornell AWS Accounts Affected by 2023 Direct Connect Architecture Migration
  - Terraform Configuration Guidance for 2023 Direct Connect Architecture Migration
  - Cornell AWS Direct Connect Routing Diagrams
  - Announcements
    - 2023-01-16 AWS Direct Connect Architecture Migration Execution
    - 2023-01-10 AWS Direct Connect Architecture Migration Customer Review and Feedback #2
    - 2022-12-20 AWS Direct Connect Architecture Design Update
    - 2022-12-15 AWS Direct Connect Architecture Migration Customer Review and Feedback
    - 2022-12-09 AWS Direct Connect Architecture Migration Preparation Continues
    - 2022-11-02 Upcoming AWS Direct Connect Changes
- External Documentation
  - AWS Direct Connect
  - AWS Transit Gateway
  - Internet 2 Cloud Connect