An Introduction to AWS Direct Connect

Julien Simon, Principal Technical Evangelist, AWS

julsimon@amazon.fr
@julsimon

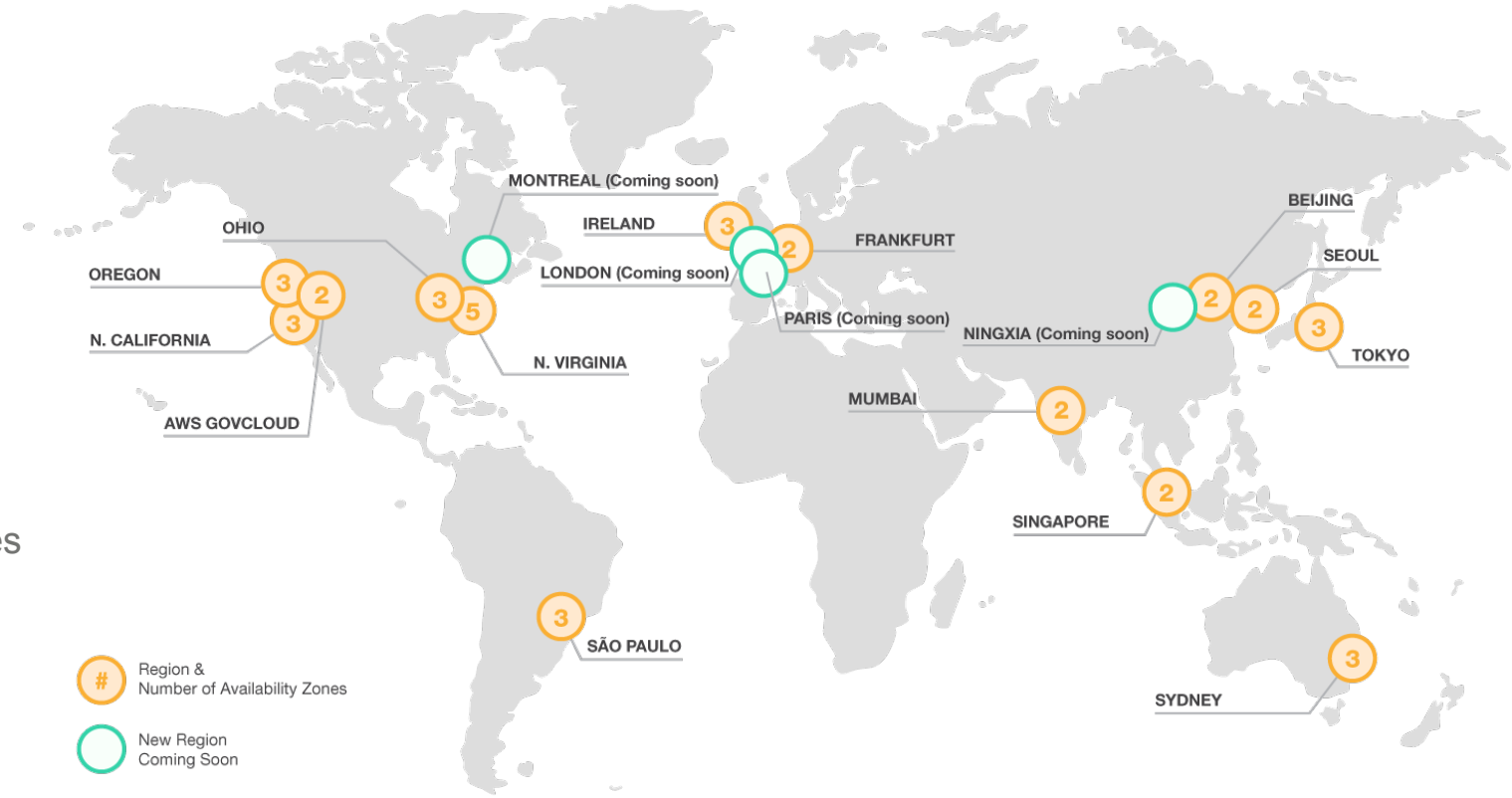
amazon web services

AWS Global Infrastructure

14 Regions

38 Availability Zones

63 Edge Locations



Moving data in and out of the cloud

- Backup and archive to Amazon S3 / Glacier
- Replicate server data & databases for Disaster Recovery
- Load analytical data into Amazon Redshift or EMR
- Build a hybrid architecture
- Migrate applications to AWS

https://en.wikipedia.org/wiki/Wildebeest

What is AWS Direct Connect (DX) ?

- Private dedicated link to an AWS Region, 1G or 10G (lower speeds available through partners)
- At least one DX location for each AWS Region
- Each DX location provides connectivity to one AWS region (**)
- Homogeneous network performance (speed & throughput)
- Incoming traffic is free, outgoing traffic is cheaper
- Uses BGP (Border Gateway Protocol) for routing

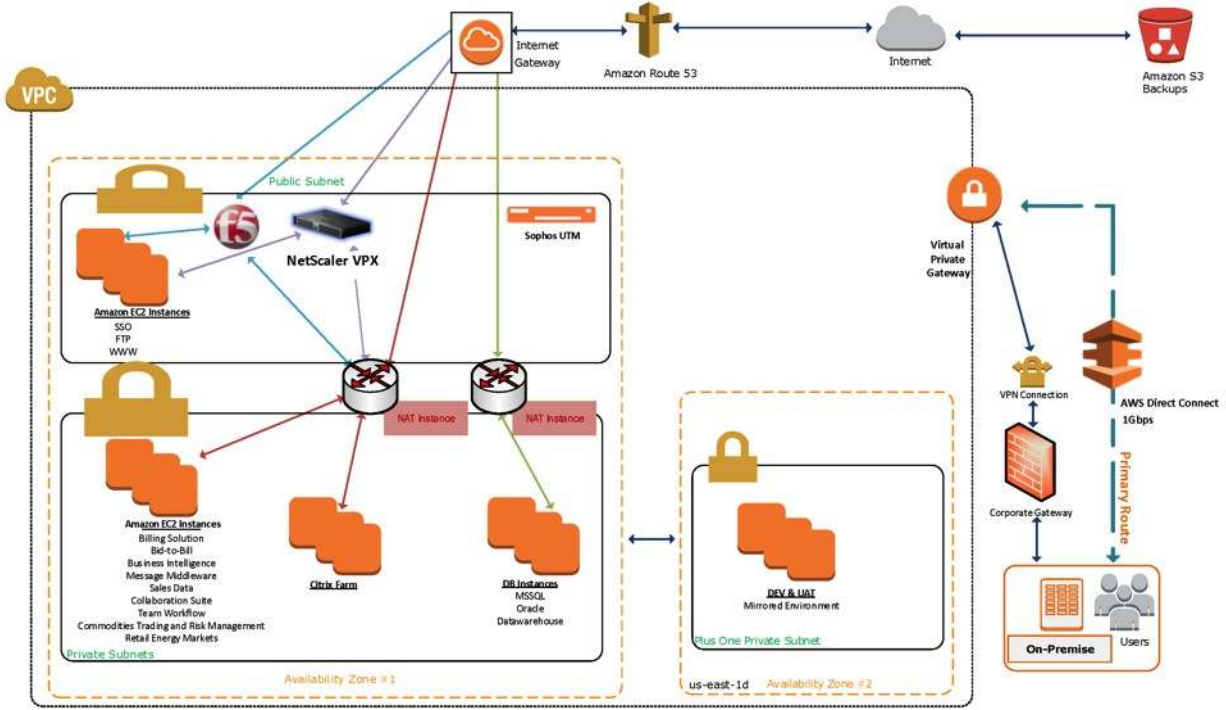
How much does DX cost?

Port Speed	Port-Hour Rate	Port-Hour Rate in Japan
50M	$0.03/hour	$0.029/hour
100M	$0.06/hour	$0.057/hour
200M	$0.12/hour	$0.114/hour
300M	$0.18/hour	$0.171/hour
400M	$0.24/hour	$0.228/hour
500M	$0.30/hour	$0.285/hour
1G	$0.30/hour ($216 / month)	$0.285/hour
10G	$2.25/hour ($1620 / month)	$2.142/hour

Incoming traffic : free
Outgoing traffic : $0.02-$0.03 / GB (depending on region)

Case study: Hess Corporation

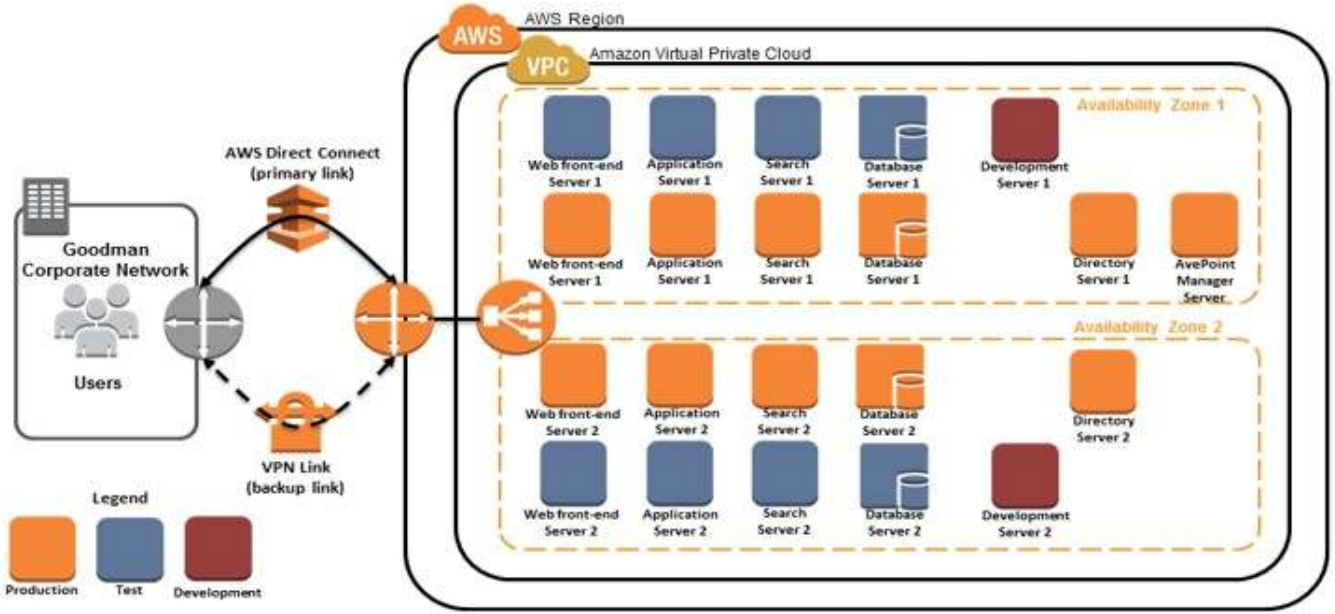
https://aws.amazon.com/solutions/case-studies/hess-corporation/



"We had some fairly complex data replication requirements during the migration. Everything worked as expected and our support teams could use the same tools to manage servers that they had grown accustomed to in our data center. The cloud was basically an extension of our network."

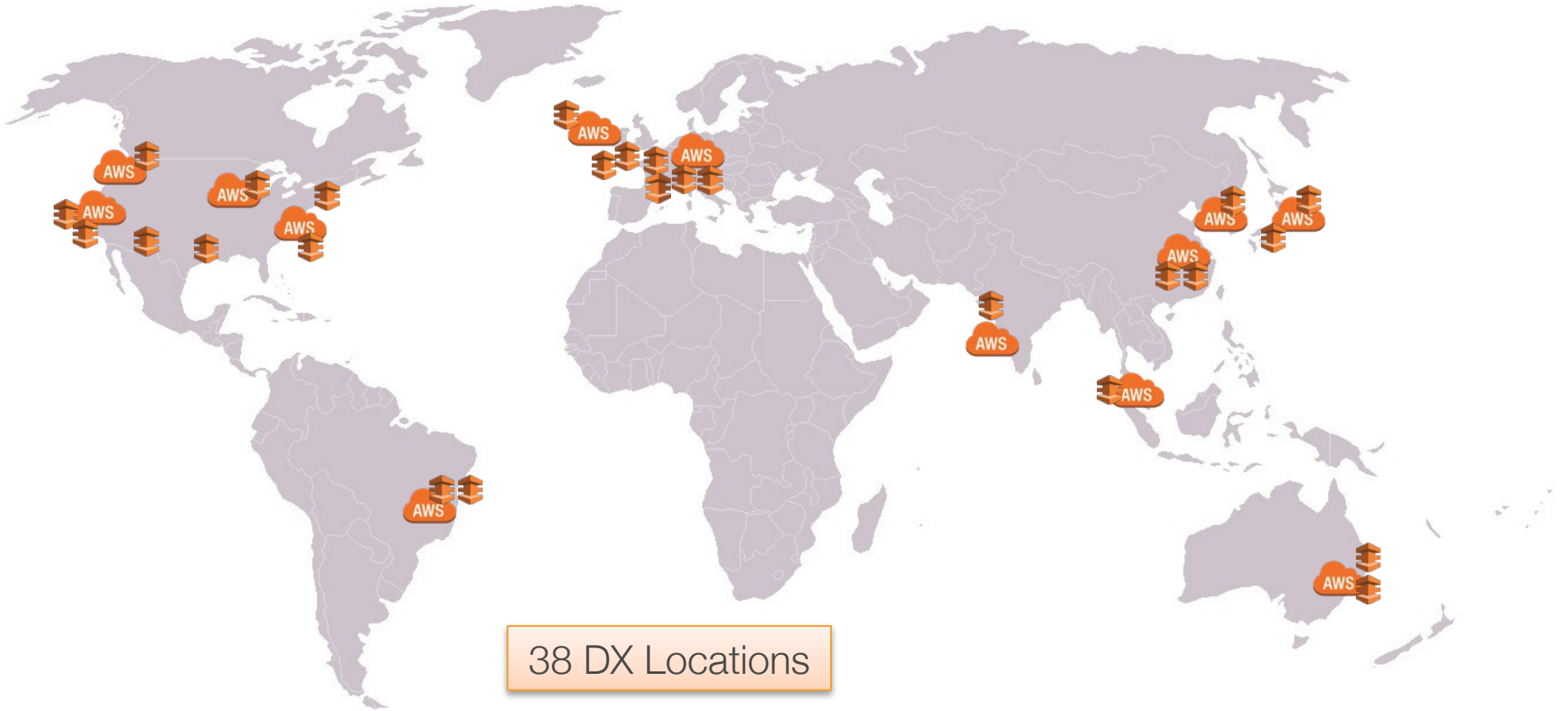
Case study: Goodman Group

https://aws.amazon.com/solutions/case-studies/goodman-group/



"We've achieved near 100 percent availability for the knowledge management application on AWS and now have the ability to scale up the infrastructure to support business growth."

DX locations

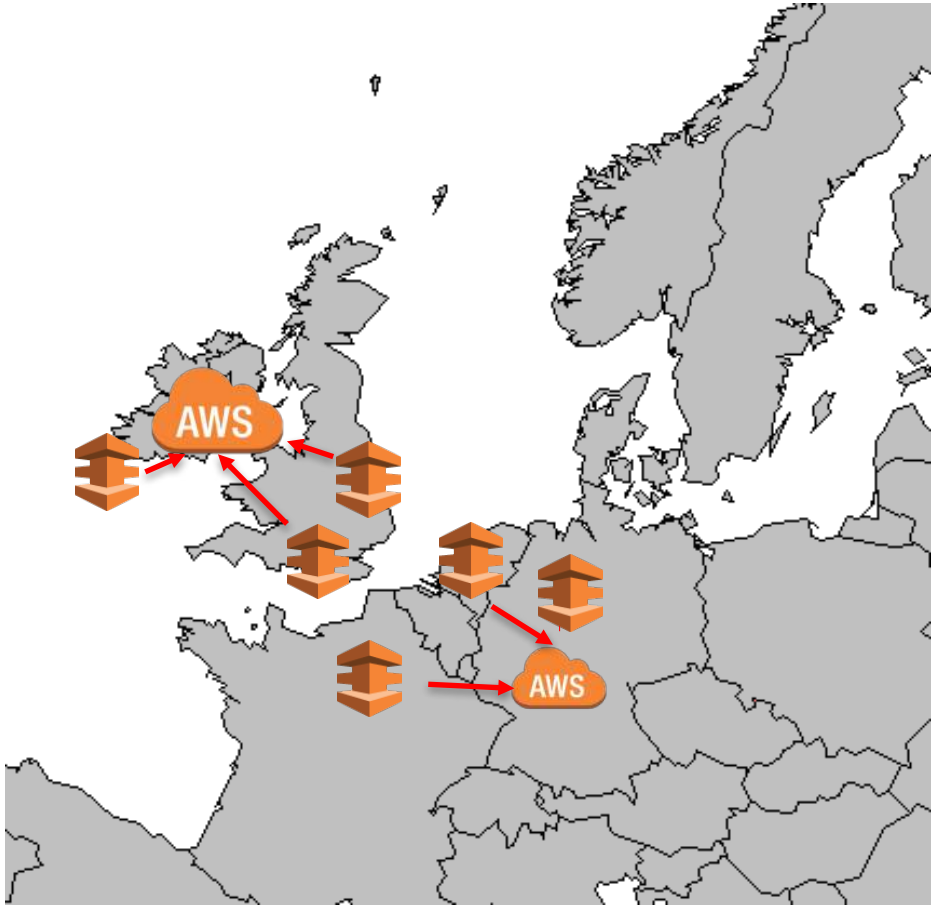


https://aws.amazon.com/fr/directconnect/details/

DX in Europe

EU West (Ireland)
Interxion, Dublin, Ireland
Eircom Clonshaugh, Dublin, Ireland
Digital Realty (UK), London Docks, UK
Equinix LD4 – LD6, London, UK

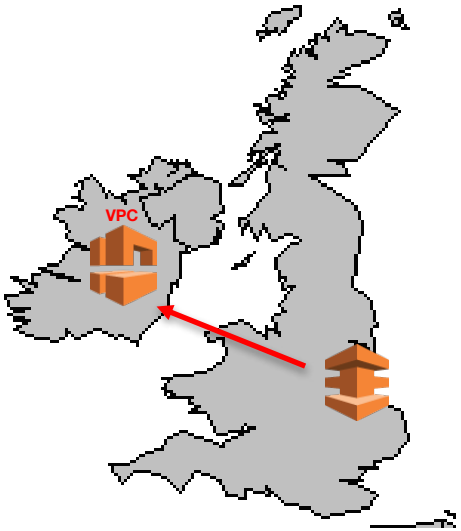
EU Central (Frankfurt)
Equinix AM3, Amsterdam, Netherlands
Interxion, Frankfurt, Germany
Telehouse Voltaire, Paris, France



Virtual Interfaces

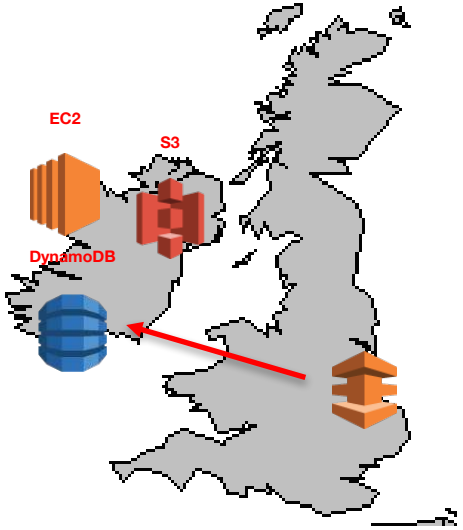
Two types of connections are available in each region

Private



- Connects to a VPC: one private virtual interface for each VPC
- Each DX connection can have multiple private virtual interfaces
- Supports multiple accounts

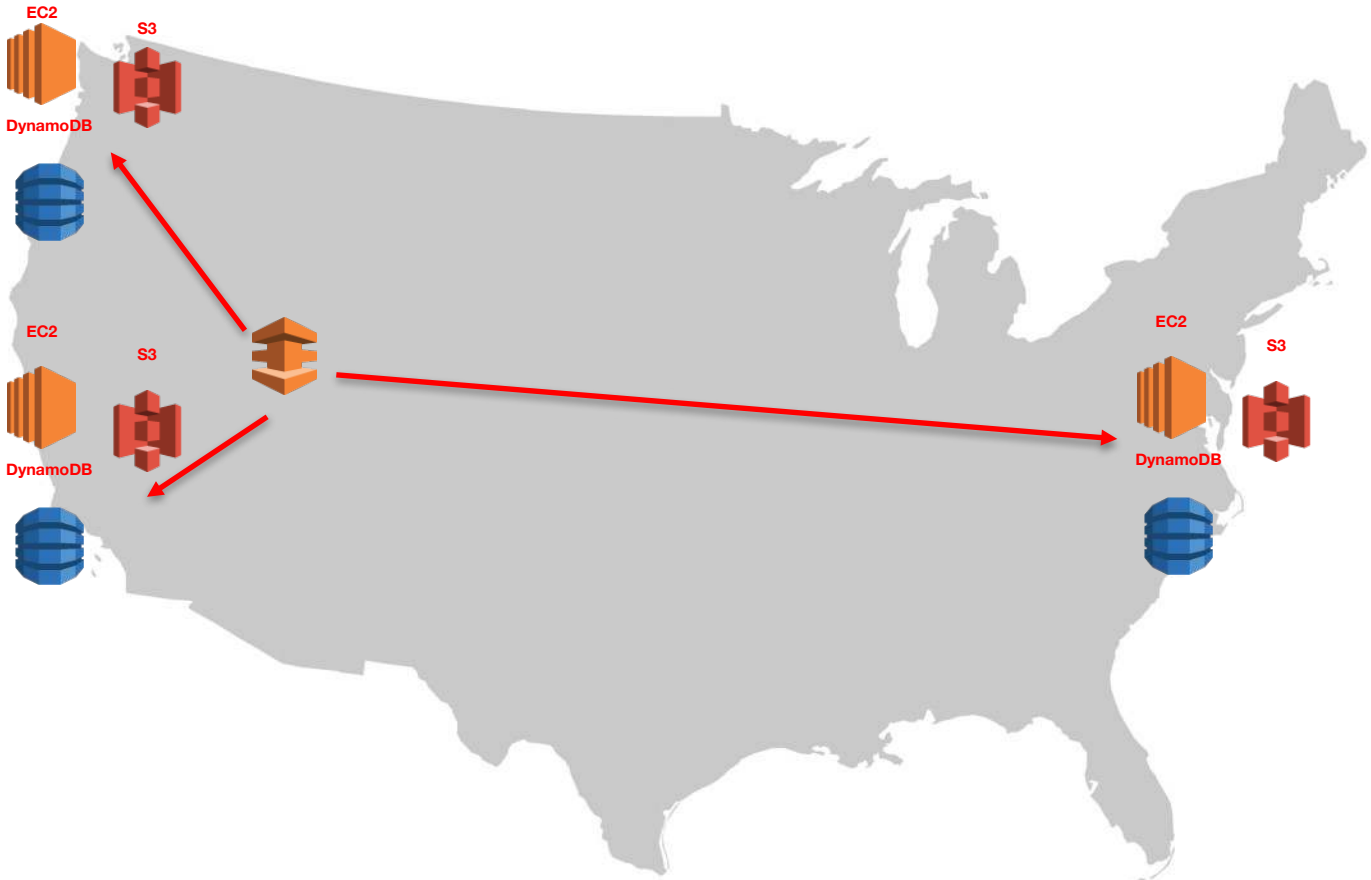
Public



- Connects to the public AWS IP address space in a region
- Public S3, EC2, DynamoDB, etc.

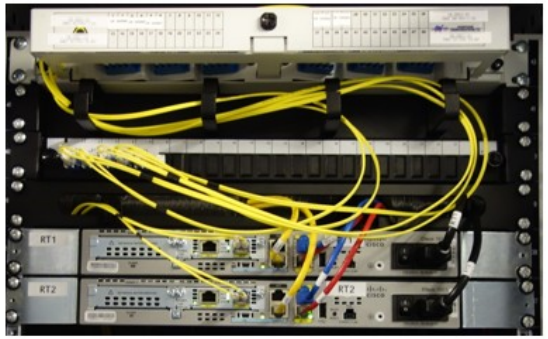
Virtual Interfaces: North America

You can use a single DX connection to build multi-region services



- Public interfaces in North America provide connectivity to all the AWS public IP space in all of NA.
- Published speeds are only guaranteed to the AWS region which the DX location connects to
- Private interfaces only connect to the one region their DX location is connected to (*)

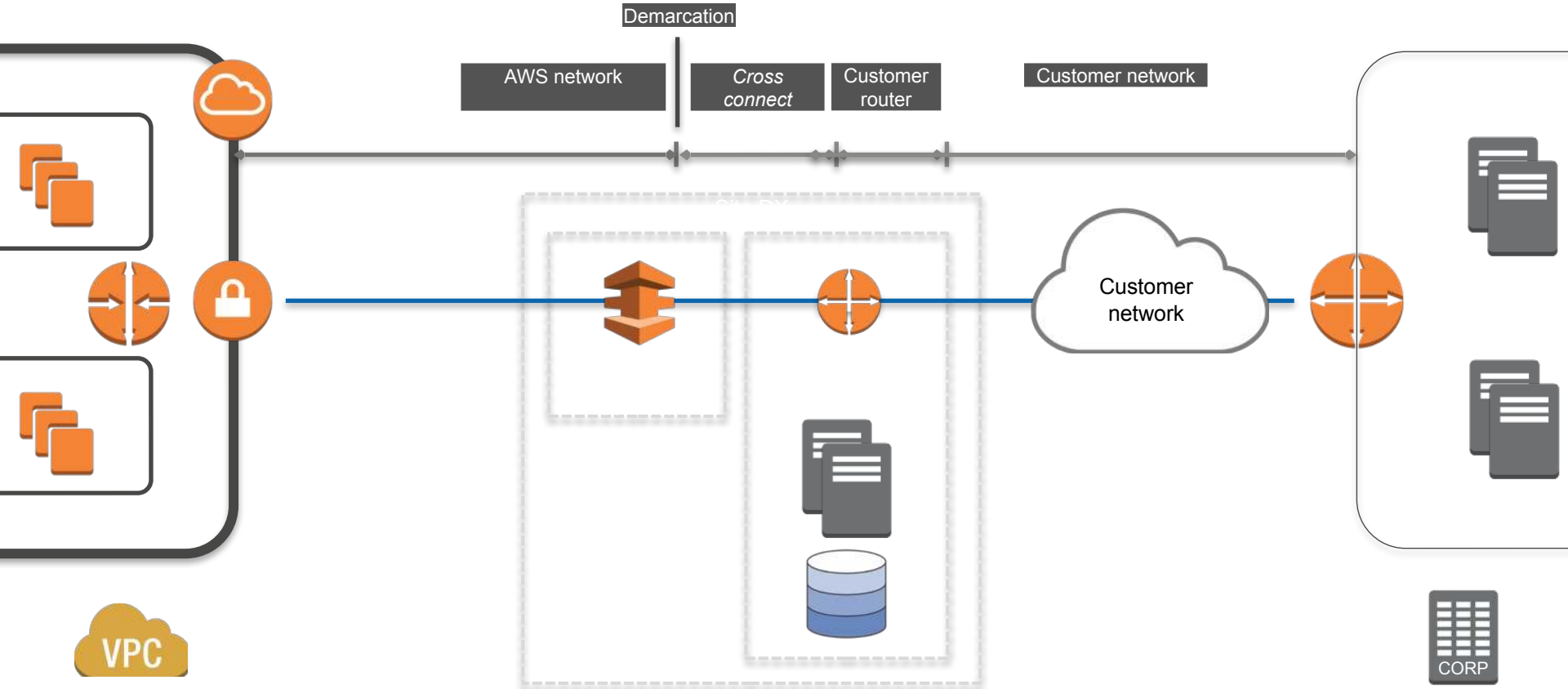
Connecting to DX: 2 options



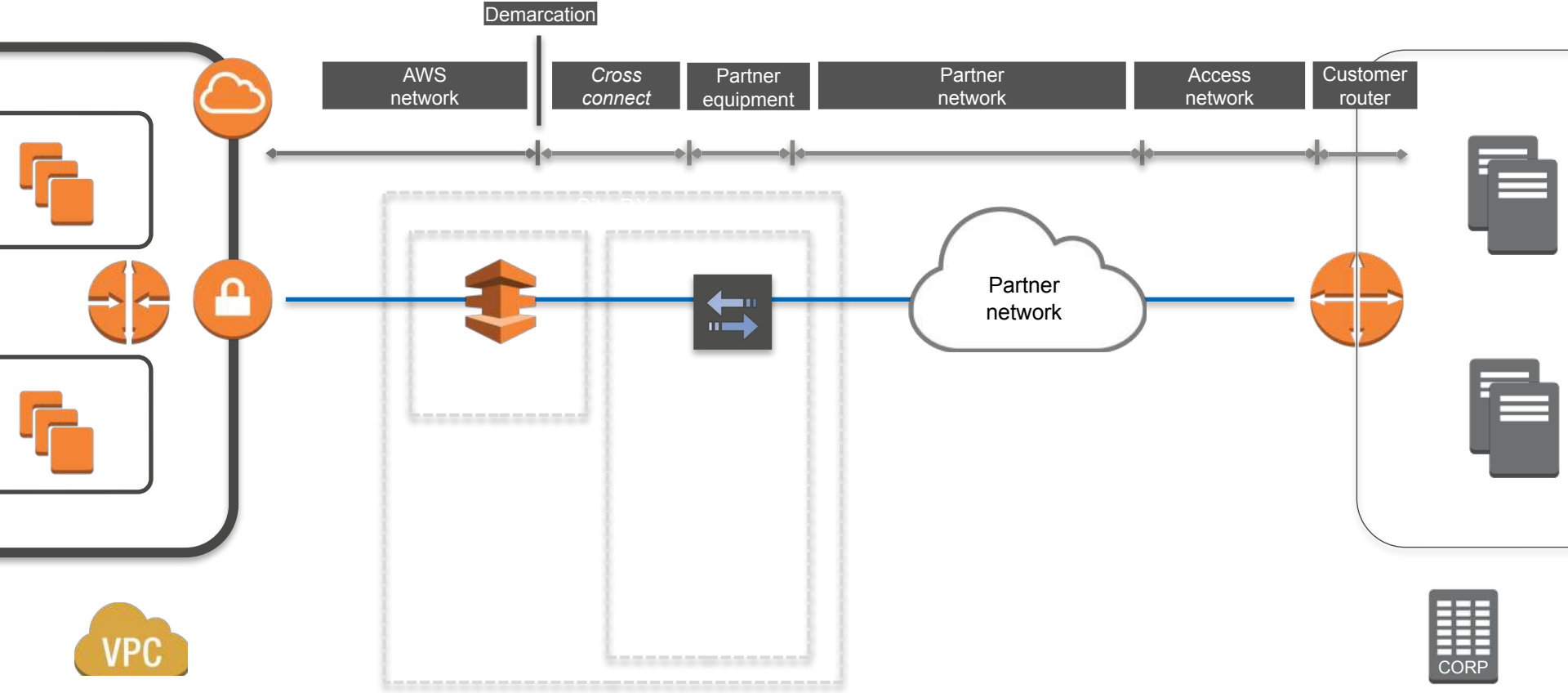
- Customer router present at DX location
  - *Cross-connect :* 1G or 10G
  - Single-mode fiber: 1000BASE-LX or 10GBASE-LR

- Connectivity provided by DX partner (who is present on DX location)
  - https://aws.amazon.com/fr/directconnect/partners/
  - Multiple connection methods: Point to point, Full Mesh. YMMV!
  - Lower speeds available : 50M, 100M, 200M, 300M, 400M, 500M but you only get one virtual interface (*) http://docs.aws.amazon.com/directconnect/latest/UserGuide/getstarted_sub1g_provider.html

Option 1 : customer router at DX location



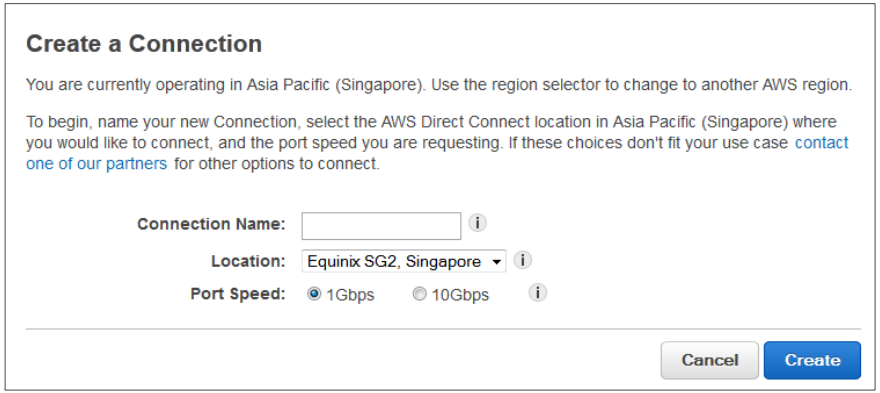
Option 2 : DX partner



The actual process

For 1G and 10G AWS provided connections

- Log into the console
- Choose desired region
- Select ‘Direct Connect’
- Select ‘Create a Connection’
- Name your connection,
  pick the desired location and port speed
- Wait for the Letter of Authorization

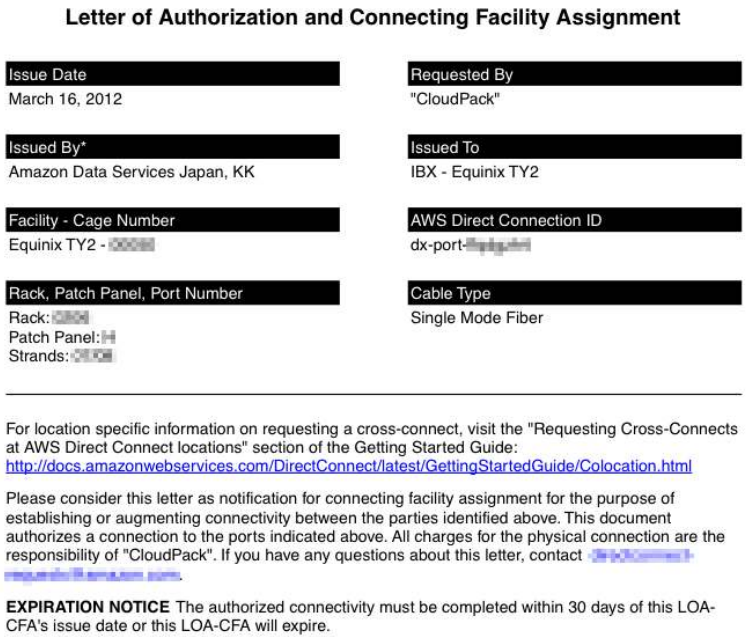


For partner provided connections

- Work directly with the partner to get the connection set up

Letter of Authorization and Connecting Facility Assignment

- LOA-CFA grants access to the AWS cage in the data center for the cross connect to be completed
- You can download it directly from the AWS console
- We may ask the customer for more information before issuing the LOA-CFA



Letter of Authorization and Connecting Facility Assignment

Issue Date	Requested By
March 16, 2012	"CloudPack"
Issued By*	**Issued To**
Amazon Data Services Japan, KK	IBX - Equinix TY2
Facility - Cage Number	**AWS Direct Connection ID**
Equinix TY2 - [redacted]	dx-port-[redacted]
Rack, Patch Panel, Port Number	**Cable Type**
Rack: [redacted] Patch Panel: [redacted] Strands: [redacted]	Single Mode Fiber

For location specific information on requesting a cross-connect, visit the "Requesting Cross-Connects at AWS Direct Connect locations" section of the Getting Started Guide:
http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Colocation.html

Please consider this letter as notification for connecting facility assignment for the purpose of establishing or augmenting connectivity between the parties identified above. This document authorizes a connection to the ports indicated above. All charges for the physical connection are the responsibility of "CloudPack". If you have any questions about this letter, contact [redacted].

EXPIRATION NOTICE The authorized connectivity must be completed within 30 days of this LOA-CFA's issue date or this LOA-CFA will expire.

Closing the loop

- Contact the colocation provider to request a cross connect
- Provide the LOA-CFA to allow them to access the AWS router and complete the connection

- Work with partner to complete the circuit to the customers location
- Customer or partner must request a cross connect to connect the circuit to the DX router

Creating a Virtual Interface

- Choose your DX connection
- Select if you'd like a Public or Private interface
- You can have both interfaces on one DX connection
- Download configuration (Cisco, Juniper)
- Configure router
- Test connectivity
- Have a drink (you'll need it whatever happens…)

Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

- **Private** - A private virtual interface should be used to access an Amazon VPC using private IP addresses.
- **Public** - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Public Virtual Interface

Enter the name of your virtual interface. If you're creating a virtual interface for another account, you'll need to provide the other AWS account ID. For more information about virtual interface ownership, see "Hosted Virtual Interfaces" in the AWS Direct Connect Getting Started Guide.

Connection: dxcon-ffs3dp1s (Far East Offices)

Interface Name: e.g. My Virtual Interface

Interface Owner: My AWS Account Another AWS Account

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: e.g. 100

Your router peer IP: e.g. 8.18.144.1/31

Amazon router peer IP: e.g. 8.18.144.2/31

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. and any prefixes you would like to announce to AWS. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: e.g. 65000

Auto-generate BGP key: ☑

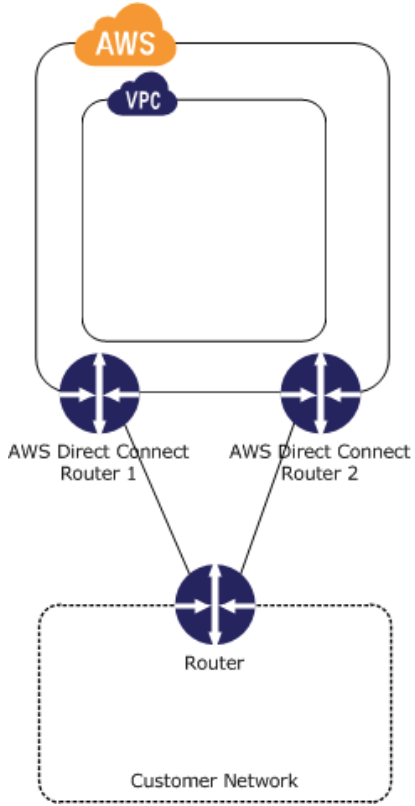
Prefixes you want to advertise: e.g. 8.18.144.0/24, 8.18.

It may take up to 72 hours to verify that your IP prefixes are valid for use with Direct Connect.

Cancel Continue

Redundancy: at the router level

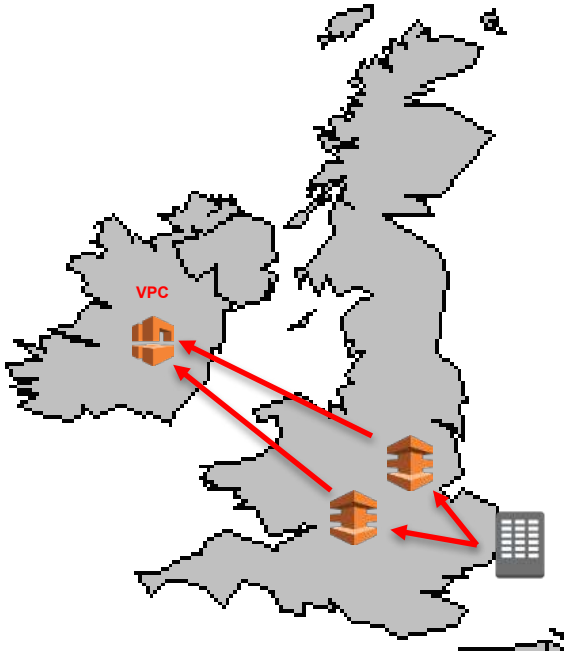
- We recommend that all customers request and configure two dedicated connections to AWS.
- Customers can terminate the connections on two different routers in their network
- We will configure connections to terminate on different routers in the AWS DX location
- Both connections can be active and in use by the customer
- VPN over the public Internet should also be used for even more redundancy



Redundancy: at facility level

- For additional resiliency, it's recommended that customer configure connections from multiple DX locations to their desired region

- It is possible for a single DX location to become unavailable and just like using multiple AZ's, using multiple locations will provide customers with increased HA



Redundancy configurations

- Active/Active (BGP multipath): this is the default DX behavior
  - Network traffic is load balanced across both connections
  - If one connection becomes unavailable, all traffic is routed through the other
- Active/Passive (failover).
  - One connection is handling traffic, and the other is on standby.
  - If the active connection becomes unavailable, all traffic is routed through the passive connection.

- Backup connections could be a low bandwidth connection

- VPN could also be used as the backup connection

Extra work

Direct Connect currently has no native encryption

- VPN encryption : Virtual Gateway with IPSec, EC2 Instances running IPSec
- Application Level encryption (HTTPS)

Direct Connect currently has no native monitoring (Amazon CloudWatch)

- Network stats available on customer's hardware
- Partner may provide monitoring in their customer portal
- Or you can build it yourself: https://github.com/awslabs/aws-dx-monitor

When things go wrong…

- Documentation is quite good, but it's not a BGP tutorial :)
- Setup issues can often result in lots of finger pointing, especially when partners are involved… wanna hear my horror story? ;)
- Gather as much data and debug info as you can
- Involve your Account Management team early
    - Account Manager, Solution Architect, Partner Solution Architect
    - Issues with your Partner? Let them know ASAP
- Business / Enterprise support is recommended

Resources

https://aws.amazon.com/fr/directconnect/

(NET201) VPC Fundamentals and Connectivity Options
https://www.youtube.com/watch?v=5_bQ6Dgk6k8

(NET406) Deep Dive: AWS Direct Connect and VPNs (Steve FTW!)
https://www.youtube.com/watch?v=SMvom9QjkPk

(ARC402) Double Redundancy with AWS Direct Connect https://www.youtube.com/watch?v=_JgNnmOfxLE

Thank you!

Julien Simon, Principal Technical Evangelist, AWS

julsimon@amazon.fr
@julsimon

amazon web services