Consolidated Audit Trail

AWS PrivateLink Connectivity

2/4/2020

Connectivity Methods – AWS PrivateLink

- Industry Members (IMs) and CAT Reporting Agents (CRAs) with existing operations and data processing presence in the AWS cloud (VPC) may establish a cloud-to-cloud connection to CAT using the AWS PrivateLink service for an associated AWS fee.
- An AWS PrivateLink connection enables communication from an Industry Member's AWS VPC to FINRA CAT services without traversing the public Internet.
- IMs and CRAs interested in AWS PrivateLink should contact the FINRA CAT Helpdesk.
- PrivateLink is available in the Industry Test Environment starting on January 27, 2020 and will be available in the Production Environment in mid-March.

Detailed AWS PrivateLink Implementation Guide can be found in the IM Connectivity Supplement at:
https://www.catnmsplan.com/wp-content/uploads/2020/01/FINRA_CAT_Connectivity_Supplement_for_Industry_Members_1.4.pdf

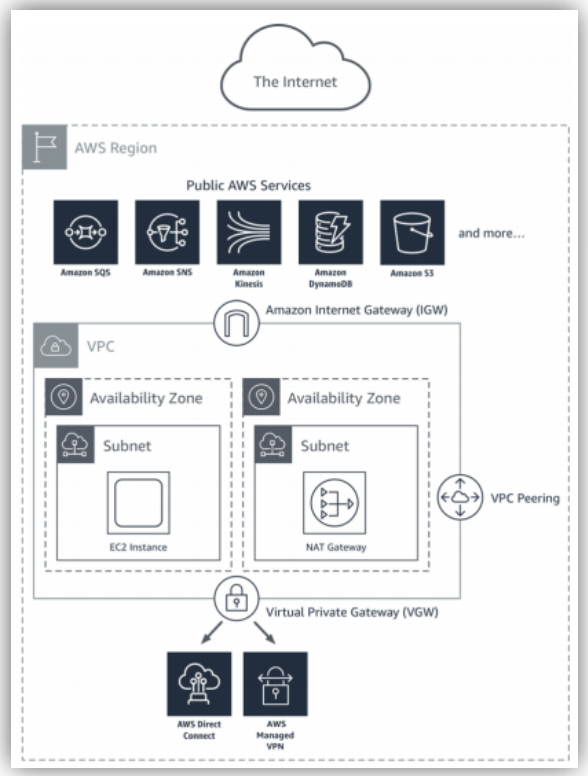
More information on AWS PrivateLink can be found at:
https://aws.amazon.com/privatelink/

More information on the AWS Cloud Formation service can be found at:
https://aws.amazon.com/cloudformation

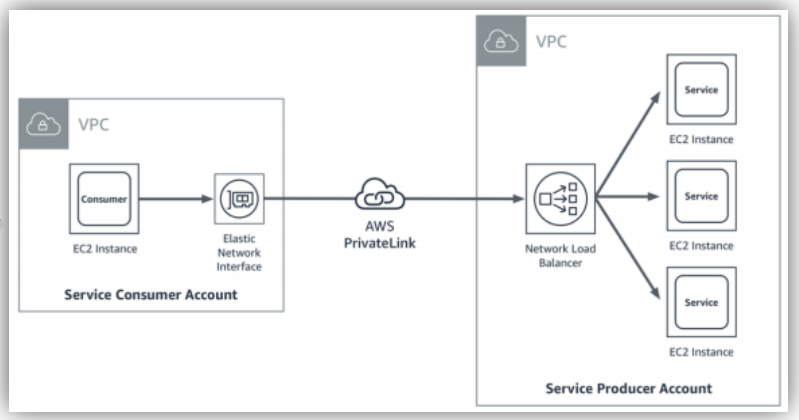
What Is AWS PrivateLink

- Amazon Virtual Private Cloud (Amazon VPC) gives AWS customers the ability to define a virtual private network within the AWS cloud to build services securely and keep data internal.
- AWS PrivateLink uses AWS internal network to allow AWS users to connect and transfer data across VPCs within their own organization or with other organizations that also use AWS VPCs.
- AWS PrivateLink uses AWS internal network connectivity over Transmission Control Protocol (TCP) versus the internet (public IP address) to ensure internal and secure connectivity.
- AWS PrivateLink is NOT intended to be a network traffic router across different data centers.

Use of VPCs



Use of VPCs with PrivateLink



Source:
1) https://d1.awsstatic.com/whitepapers/aws-privatelink.pdf
2) https://aws.amazon.com/privatelink/

Why Use AWS PrivateLink

Use of Private IP Addresses for Traffic

- AWS PrivateLink uses Private IP addresses and security groups to connect to services.
- All services appear as if they are internal to your own VPC even if AWS users connect to other AWS users VPCs.

Scalable Managed Service

- AWS PrivateLink is an AWS managed service that scales based on usage needs.
- AWS users pay for usage and can terminate connectivity at any time with no long term contracts.

Simplify Network Management

- Removes the need to setup complex networking.
- Simplifies network topology by removing the need to create route tables.

Allow Service Specific Connectivity

- Use of “Endpoints” allows AWS users to expose specific service connectivity via PrivateLink.
- Endpoints are individually scalable and AWS users can create multiple endpoints.

How AWS PrivateLink Works At FINRA CAT

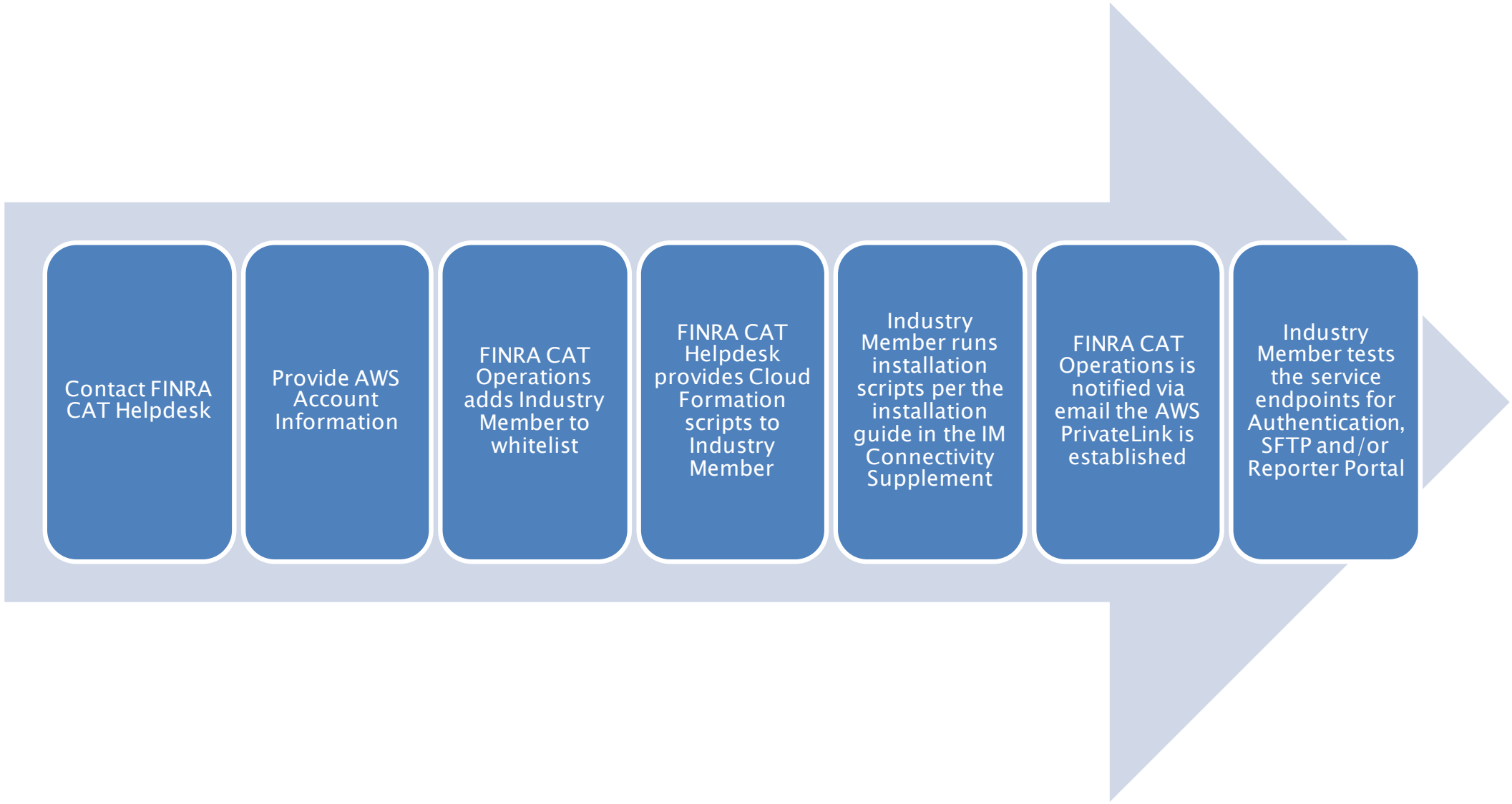
For FINRA CAT Industry Members that already have presence in AWS and are comfortable using AWS managed services:

- FINRA CAT will enable multiple connectivity "Endpoints" for the following services:
  - The Authorization interface for all FINRA CAT services
  - The CAT Reporter Portal
  - The CAT SFTP File Transfer interface
- IMs can connect their existing VPCs to FINRA CAT services in AWS in a secure and scalable manner.
- FINRA CAT will provide automation package to create an interface VPC endpoint for a FINRA CAT service in your own VPC. This creates an Elastic Network Interface (ENI) in your subnet with a private IP address that serves as an entry point for traffic destined to the FINRA CAT service.
- FINRA CAT AWS PrivateLink package is designed to work with all FINRA CAT's availability zones in the US-East-1 Region.

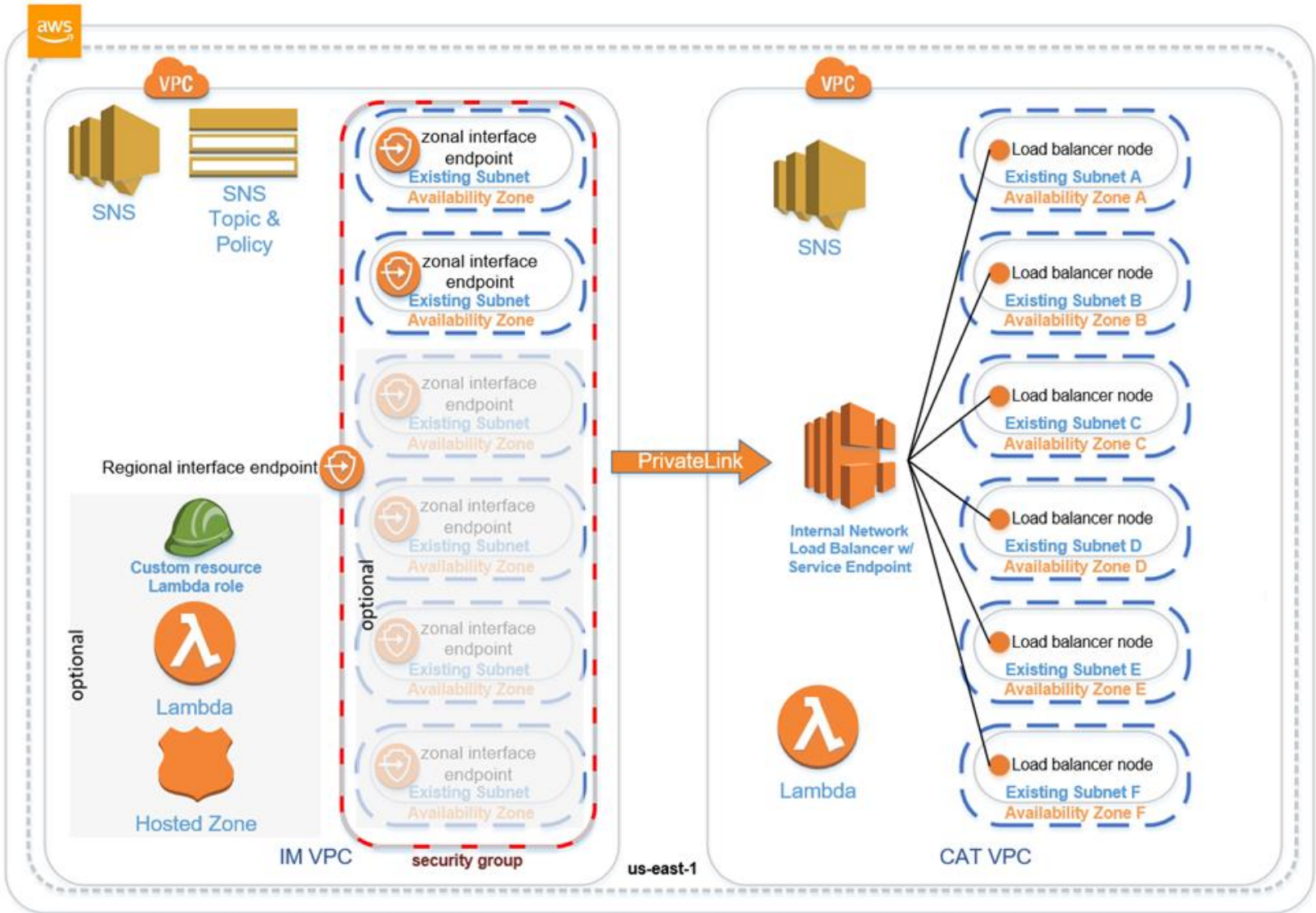
Using FINRA CAT AWS PrivateLink

- IMs and CRAs who use AWS PrivateLink to connect to FINRA CAT Endpoints are responsible for:
  - Setup of their own AWS VPCs and internal data connectivity, and internal data transfer into and out of their VPCs including their own On-Prem environments.
  - Execution of FINRA CAT "CloudFormation" scripts to connect their own VPC to FINRA CAT Endpoints.
    - Must select between option of small, medium, or large based on individual bandwidth and AWS availability zone connectivity needs.
  - Setup of DNS using Route 53 or the client's self supported DNS service to translate URLs to the Industry Member's private IP addresses.
  - The management of web traffic in and out of their own VPCs.
  - Responsible for their own AWS billing for AWS Services.

AWS PrivateLink Onboarding Process



AWS PrivateLink High Level Architecture



Data Flow Through AWS PrivateLink

- A client application, either a browser or SFTP client, initiates a connection to a CAT service URL (sftp-pl.ct.catnms.com or reporterportal-pl.ct.catnms.com, for example). The client application requests the operating system to resolve the service URL to an IP address.

- The resolution may be performed by either the AWS Route 53 DNS service or the client's self-supported service. The resolution directs the client to a PrivateLink endpoint in the client VPC that securely connects to the CAT service over the AWS internal network.

Installation and Instantiations

- The client solution is installed multiple times, once for each desired service type (SFTP, Reporter Portal, and Authentication, etc.) in each environment (Industry Test and Production) they are required.
- A set of independent AWS resources are created for each installation instantiation in the client-selected AWS account and VPC.
- If AWS Route 53 DNS service is utilized (according to a client-selected installation parameter), all solution installations in the same VPC share a private hosted zone that contains records to resolve CAT service URLs for the purpose of network connectivity.

Installation Requirements

- The solution requires an existing AWS account, VPC, and between two and six existing subnets in different Availability Zones in the US-East-1 Region.
- All desired services may be installed into the same VPC, separate VPCs or separate accounts and separate VPCs. Only one instance of a service type should be installed into a single VPC.
- AWS Accounts must be **pre-approved by FINRA CAT** before connectivity can be established. Connectivity is not possible without the pre-approval. Pre-approval can be obtained by contacting the FINRA CAT Helpdesk.
- Industry Members and CRAs will need to provide their AWS account numbers to FINRA CAT in order to facilitate PrivateLink access.
- FINRA CAT Operations is notified of an Industry Member's client connectivity changes via a SNS topic and policy that is created and configured during the installation process.

Installation Options

- Bandwidth/Subnet combinations:

Bandwidth and Resiliency Options Summary			
Option	**Subnets Required**	**Resilient**	**Bandwidth**
Small	2	Yes	20Gbps
Medium	4	Yes	40Gbps
Large	6	Yes	60Gbps

- Optionally, CAT service URLs are configured in an AWS Route 53 private hosted zone. The configuration of the hosted zone may be performed automatically. Automatic configuration requires either the selection to automatically establish the required permissions for this activity or manually establish permissions in advance.

Support and Troubleshooting

- If an Industry Member is experiencing connectivity issues with their AWS PrivateLink they should contact the FINRA CAT Helpdesk.
- After consultation with FINRA CAT Operations, the IM may be directed to recreate one or more solution types in your VPC. This method may be the fastest path to reestablish connectivity.
- If the installation has failed, you must wait for it to roll back completely, when all resources have been deleted. Once it has rolled back, you may delete the stack by selecting it on the left side of the CloudFormation pane and then selecting delete.
  - Deleting the stack will destroy the stack and all resources created by that stack. This operation cannot be undone.
- FINRA CAT Helpdesk and Operations do not have visibility into an Industry Members' AWS account to help troubleshoot. IMs need to consider their AWS expertise and support from within their organization and their AWS support level for networking and operations before pursuing AWS PrivateLink connectivity to the CAT.

Engaging with Amazon Web Services (AWS)

Industry Members *that are AWS customers:*

- IMs that use AWS can setup the networking and application infrastructure to submit CAT data
- Submit data to FINRA CAT via a cloud-to-cloud connection, by leveraging the SFTP services FINRA is exposing through PrivateLink
- Contact the FINRA CAT Helpdesk, or cathelp@amazon.com for assistance

Industry Members *that are not AWS customers:*

- For IMs that are not AWS customers, AWS will work with each IM to design the appropriate solution
- AWS will share a standard on-boarding package, including reference architecture, on-boarding instructions, and technical support
- Please contact cathelp@amazon.com for assistance

AWS Support Plans:

While Basic Support is included for all AWS customers, we recommend enabling Business or Enterprise support based on your business requirements. Additional details of the AWS Support Plans are available here.