FINRA CAT Connectivity Supplement for Industry Members

Version 1.8

FINRA CAT™

Table of Contents

Change Log

Version	Date Published	Description of Changes
1.0	August 16,2019	• Initial Version
1.1	September 25, 2019	• Updated with additional information on AWS PrivateLink • Updated to include BT Radianz as Private Line MNSP
1.2	October 31, 2019	• Added Private Line 3rd Party Extranet Provider in section 3.2 Updated AWS PrivateLink details in section 3.3 • Updated CAT File Transfer (SFTP) test instructions in section 4.1 • Added Firewall Policy Requirements in section 4.3, including DUO Multi-factor Authentication (MFA)
1.3	December 17, 2019	• Added Section 4.3.4: Additional Access Requirements • Added Section 5: AWS PrivateLink Client Implementation Guide
1.4	January 22, 2020	• Added two Production FIP URLs to Section 4.3.4: Additional access requirements. • Removed a duplicative and misplaced URL for reporter portal in CT.
1.5	February 27, 2020	• Added a clarification related to Third Party Extranet connectivity in sections 2 and 3. • Added a statement on the permitted use of shared connectivity access by affiliated entities in section 3. • Provided additional detail related to manual implementation of DNS for AWS PrivateLink in section 5.
1.6	May 26, 2020	• Added “Deny Access from Anonymous Networks” for DUO MFA in 4.3.3 • Added Prod and CT (2) URL’s to the 4.3.4: Additional access requirements section that are required to support SAML authentication through the Secure Reporting Gateway over the Internet. • Removed the requirement for three URLs related to the access of style sheets and fonts over the Internet from section, 4.3.4: Additional access requirements.

1,7	Jul 30, 2020	• Added troubleshooting guidance for SFTP connections
1.8	Aug 24, 2020	• Added CAIS connectivity information and updated the associated diagrams.

1. Introduction

Industry Members and CAT Reporting Agents ("CRA") must establish and maintain redundant connectivity to CAT to support daily data submissions. This document describes the methods available for Industry Members and CRAs to connect to the CAT and CAIS system.

Industry Members and CRAs interface with the CAT System using the CAT File Transfer and/or the CAT/CAIS Reporter Portal as described in Section 2. Access to CAT/CAIS requires at least one of the connectivity methods described in Section 3. The combinations of Connectivity and Interface Methods along with the dates when Connectivity Testing may begin are shown below in Table 1.

Table 1: Network Testing Availability Dates

Connectivity Methods	Interface Methods		
	CAT File Transfer	CAT Reporter Portal	CAIS Reporter Portal
Private Line provided by an MNSP	October 15, 2019 (Century Link) October 21, 2019 (BT Radianz)	October 15, 2019 (Century Link) October 21, 2019 (BT Radianz)	October 15, 2019 (Century Link) October 21, 2019 (BT Radianz)
AWS PrivateLink	January 27, 2020	January 27, 2020	August 24, 2020
CAT Secure Reporting Gateway	Not Applicable	November 18, 2019	August 24, 2020

1.1. Support

Industry Members and CRAs should contact the FINRA CAT Help Desk for support, to initiate a request, and for any changes to connectivity methods.

Questions related to this document may be directed to the FINRA CAT Helpdesk at 888-696-3348 or at help@finracat.com.

2. CAT Interface Methods

The interface methods available to Industry Members and CRAs to submit data and retrieve reporting feedback include CAT File Transfer and the CAT/CAIS Reporter Portals.

2.1. CAT File Transfer

The CAT File Transfer method is an automated, machine-to-machine interface utilizing the Secure File Transfer Protocol ("SFTP") for file submissions, acknowledgements, rejections and corrections. CAT File Transfer may be accessed via Private Line, 3rd Party Extranet, or AWS PrivateLink.

SFTP enables Industry Members and CRAs to create machine-to-machine connections to securely transmit data and retrieve data from FINRA CAT. To use SFTP, FINRA CAT requires each Industry Member and CRA to utilize the appropriate connectivity methods (Private Line, 3rd Party Extranet, or AWS PrivateLink). SFTP requirements include:

- SSH Key Exchange Algorithms
  - diffie-hellman-group-exchange-sha256
- SSH Ciphers
- aes128-ctr, aes192-ctr, aes256-ctrSSH MAC Algorithms
  - hmac-sha256, hmac-sha256@ssh.com
- A connection with bandwidth appropriate for the file sizes submitted

2.2. CAT Reporter Portal

The CAT Reporter Portal is a web interface utilizing secure encryption protocols (HTTPS/TLS) and multi-factor authentication (MFA) for submissions (by either direct entry or manually uploaded file), rejections, corrections, and compliance reports. The CAT Reporter Portal may be accessed via the Private Line, a 3rd Party Extranet connection through MNSP (BT Radianz), AWS PrivateLink, or the CAT Secure Reporting Gateway. Use of Reporter Portal does not require SFTP access and is granted via entitlements.

The Reporter Portal supports a browser-based, manual upload of files. Reporter Portal requirements include:

- TLS 1.2 requiring at a minimum NIST compliant 128-bit ciphers
- HTML5 Compatible browsers, including: Chrome, Firefox, and Safari
- Multi-factor authentication setup[1]

[1] More details on the Multi-factor authentication setup and required software will be published in a future version of the FINRA CAT Industry Member Onboarding Guide.

Additionally, for manual file uploads the reporter portal has the following requirements:

- All files must meet technical specification requirements (naming, syntax, compression requirements, etc.)
- Files must be <=1GB in size AND total record count may not exceed 100,000
- Meta files and Data files are BOTH required – Data files must be submitted prior or at the same time as Meta Files
- No limit to the number of files submitted using File Upload; however, a limit max limit of 10 files for a single submit with max limit of 5GB.

Note: A user guide and demo will able available in alignment with user testing of the upload functionality on the CATNMSPlan.com website.

The following identifies the types of CAT Data and Feedback with the respective interface methods available for each:

Table 2: CAT Reporter Portal Data Submission and Feedback Interface Methods

CAT Data Submission and Feedback	CAT File Transfer	CAT Reporter Portal
Submission of CAT Events and Resubmission of Rejected Files/Records, Corrections and Deletions	✓	✓ *Files submitted through the CAT Reporter Portal are limited to 100,000 records*
File Status Retrieval	✓	✓
Reporting Statistics		✓
Interactive CAT Reportable Event Entry		✓
Error Feedback	✓	✓
Corrections Feedback		✓
Account Maintenance		✓
Establishment of Reporting Relationships and ATS Order Types		✓

2.3. CAIS File Transfer

The CAIS File Transfer method is an automated, machine-to-machine interface utilizing the Secure File Transfer Protocol (“SFTP”) for file submissions, acknowledgements, rejections and corrections. CAIS File Transfer may be accessed via Private Line, Third party Extranet, or AWS PrivateLink.

SFTP enables Industry Members and CRAs to create machine-to-machine connections to securely transmit data and retrieve data from FINRA CAT. To use SFTP, FINRA CAT requires each Industry Member and CRA to utilize the appropriate connectivity methods (Private Line, 3rd Party Extranet, or AWS PrivateLink). SFTP requirements include:

- SSH Key Exchange Algorithms
    - diffie-hellman-group-exchange-sha256
- SSH Ciphers
- aes128-ctr, aes192-ctr, aes256-ctrSSH MAC Algorithms
    - hmac-sha256, hmac-sha256@ssh.com
- A connection with bandwidth appropriate for the file sizes submitted

2.4. CAIS Reporter Portal

The CAIS Reporter Portal is a web interface utilizing secure encryption protocols (HTTPS/TLS) and multi- factor authentication (MFA) for submissions (by either direct entry or manually uploaded file), rejections, corrections, and compliance reports. The CAIS Reporter Portal may be accessed via the Private Line, a 3rd Party Extranet connection through MNSP (BT Radianz), AWS PrivateLink, or the CAT Secure Reporting Gateway. Use of CAIS Reporter Portal does not require SFTP access and is granted via entitlements.

The CAIS Reporter Portal supports a browser-based, manual upload of files. CAIS Reporter Portal requirements include:

- TLS 1.2 requiring at a minimum NIST compliant 128-bit ciphers
- HTML5 Compatible browsers, including: Chrome, Firefox, and Safari
- Multi-factor authentication setup

Additionally, for manual file uploads the reporter portal has the following requirements:

- All files must meet technical specification requirements (naming, syntax, compression requirements, etc.)
- Files must be <1GB in size AND total record count may not exceed 100,000
- No limit to the number of files submitted using File Upload; however, a max limit of 5 files for a single submit with max limit of 5GB.

The following identifies the types of CAT CAIS Data and Feedback with the respective interface methods available for each:

Table 3: CAT CAIS Data Submission and Feedback Interface Methods

CAT Data Submission and Feedback	CAIS File Transfer	CAT CAIS Reporter Portal
Submission of CAT Account records and Resubmission of Rejected Files/Records, Corrections and Deletions	✓	✓ *Files submitted through the CAT CAIS Reporter Portal are limited to 100,000 records*
File Status Retrieval	✓	✓
Reporting Statistics		✓
Interactive CAT Reportable Account Entry		✓
Error Feedback	✓	✓
FDID Reconciliation Report		✓

3. Connectivity Methods

Industry Members and CRAs may connect to the FINRA CAT/CAIS systems by either Private Line, a 3rd Party Extranet connection through MNSP (BT Radianz), AWS PrivateLink, or the CAT Secure Reporting Gateway.

3.1. Shared Connectivity

Affiliated entities such as Industry Members, CRA's, and Plan Participants may leverage/share a common connection or connectivity method in situations where their corporate affiliation and enterprise networks support the consolidated access of a shared network resource.

When choosing to leverage shared connectivity, it is required for the Industry Member or CRA to source each affiliates network traffic from a dedicated IP address(es) from their assigned pool. The associated affiliate specific IP address(es) must be submitted to FINRA CAT for identification and permissions on FINRA CAT firewalls. The affiliate entity managing the connection with the MNSP is responsible for;

a) the configuration management and support of the NAT'd IP address(es) and;

b) submitting a FINRA CAT Help Desk request for the necessary permissions and whitelisting for application access.

The IP address(es) used for the affiliate entity can be part of an existing network range but must be dedicated for the affiliates traffic. Organizations interested in leveraging a connection method across multiple affiliates may contact the FINRA CAT Help Desk to obtain additional guidance. Each entity leveraging connectivity in this manner is responsible for their own CAT reporting agreement and account management request made through the FINRA CAT Help Desk.

3.2. Private Line

Industry Members and CRAs opting to use Private Line connectivity for CAT and CAIS File Transfer (SFTP) requires those Industry Members and CRAs to engage a managed network service provider (MNSP) to establish redundant private lines into the FINRA CAT/CAIS systems. Alternatively, Industry Members and CRAs may choose to use AWS PrivateLink, see Section 3.2, as the primary and/or backup connection for their CAT/CAIS File Transfer.

The MNSP serves as a connectivity service provider that facilitates carrier-based network connectivity to subscribers while providing traffic aggregation and routing services into the FINRA CAT/CAIS Systems within an

Amazon Web Services (AWS) cloud infrastructure. The MNSP offers the connectivity service for a monthly fee. Connectivity options include the use of private lines that may be established using either wide-area network circuits or data center cross-connects where available. In addition, the MNSP provides help desk support, trouble resolution, and escalations to subscribers, as well as, program management and status reporting through deployment.

CenturyLink and BT Radianz are the MNSPs that offer private line connectivity into CAT. Industry Members and CRAs must establish a contractual relationship with the MNSP[2]. Both MNSPs offer bandwidths ranging between 10 Mbps and 1 Gbps of throughput with redundant connectivity options that are necessary to meet technical specifications requirements.

Please note the following:

- Circuit delivery times can range widely and depend on the provider's network status at any location.
- Industry Members wishing to order connections should directly engage an MNSP to begin the ordering process.
- Industry Members and CRAs may begin to engage CenturyLink to begin the process of establishing private line connectivity through Industry Member's and CRA's existing sales contacts or by contacting CenturyLink by emailing FINRA_CAT-Services@centurylink.com or by phone call to **888-870-8402**.

[2] An additional MNSP may be considered depending on demand from Industry Members and CRAs.

- Industry Members and CRAs may begin to engage BT Radianz to begin the process of establishing private line connectivity through Industry Member's and CRA's existing sales contacts or by contacting BT Radianz by emailing finracat@bt.com or by phone call to:
    - **Timothy Chapman – (630) 923-2163**
    - **Sergio Angeloni – (646) 236-6183**
- Connectivity will be available in October 2019 for network testing.

******NOTE******

Industry Members and CRAs should engage an MNSP in order to begin the process of evaluating the status and estimated delivery time for connections to their location(s).

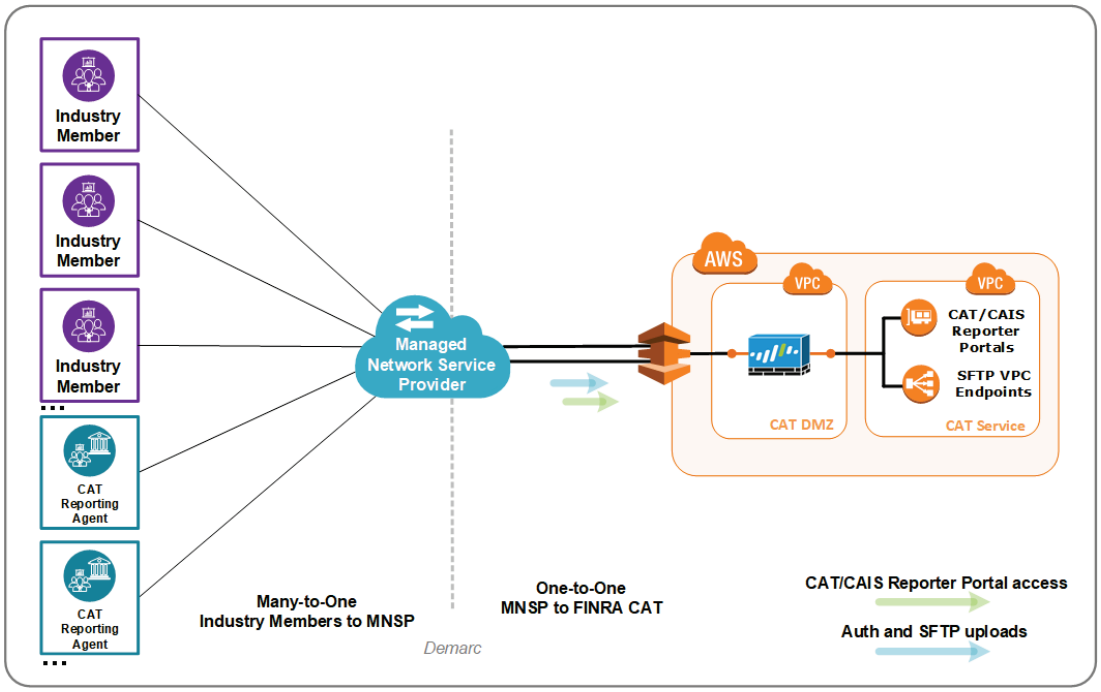


Figure 2: High Level Managed Network Service Provider Network Diagram

3.3. Third Party Extranet Network Service Providers

Industry Members and CRAs that prefer to use a 3rd Party Extranet network service provider may continue to do so with the requirement that their 3rd Party Extranet provider of choice, will enter into a contractual agreement and commercial terms with BT Radianz. Century Link does not offer a contract that governs a 3rd Party Extranet relationship into FINRA CAT over an MNSP connection. Industry Members and CRAs opting to use a 3rd party Extranet network service provider for connectivity are not

required to execute an agreement with the MNSP (BT Radianz). The contractual agreement between the MNSP (BT Radianz) and the 3rd Party Extranet provider governs the terms of the connectivity. The provider retains the contractual responsibility both with the MNSP (BT Radianz) and the Industry Member, independently, as an integration service provider between the two networks.

The use of a 3rd Party Extranet provider is not recommended; however, it is supported under the understanding that the MNSP's contractual and operational support obligations extend up to the point at which the connection demarcs between the MNSP and the 3rd Party Extranet provider's network. Consideration related to IM and CRA financial implications when using a 3rd Party Extranet provider should be discussed with the Industry Member's provider of choice.

- 3rd Party Extranet providers interested in establishing private line connectivity with BT Radianz as the authorized MNSP, may contact existing sales contacts or BT Radianz representatives directly through email at finracat@bt.com or by phone to:
    - **Timothy Chapman – (630) 923-2163**
    - **Sergio Angeloni – (646) 236-6183**

3.4. AWS PrivateLink

Industry Members and CRAs with existing operations and data processing presence in the AWS cloud (VPC) may establish a cloud-to-cloud connection using the AWS PrivateLink service established by FINRA CAT. An AWS PrivateLink connection enables communication from an Industry Member's AWS VPC to the FINRA CAT VPC without traversing the public Internet. CAT/CAIS File Transfer (SFTP) and the CAT/CAIS Reporter Portals can be accessed via AWS PrivateLink "Endpoints". A detailed AWS PrivateLink Client Implementation Guide is in **Section 5** of this document.

AWS PrivateLink is a managed service enabled for existing AWS customers to expose or connect to other AWS services (internal or external):

- 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 allows AWS users to connect and transfer data across these VPCs within their own organization or with other organizations that also use AWS VPCs.
- AWS PrivateLink uses connectivity over Transmission Control Protocol (TCP) vice 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.

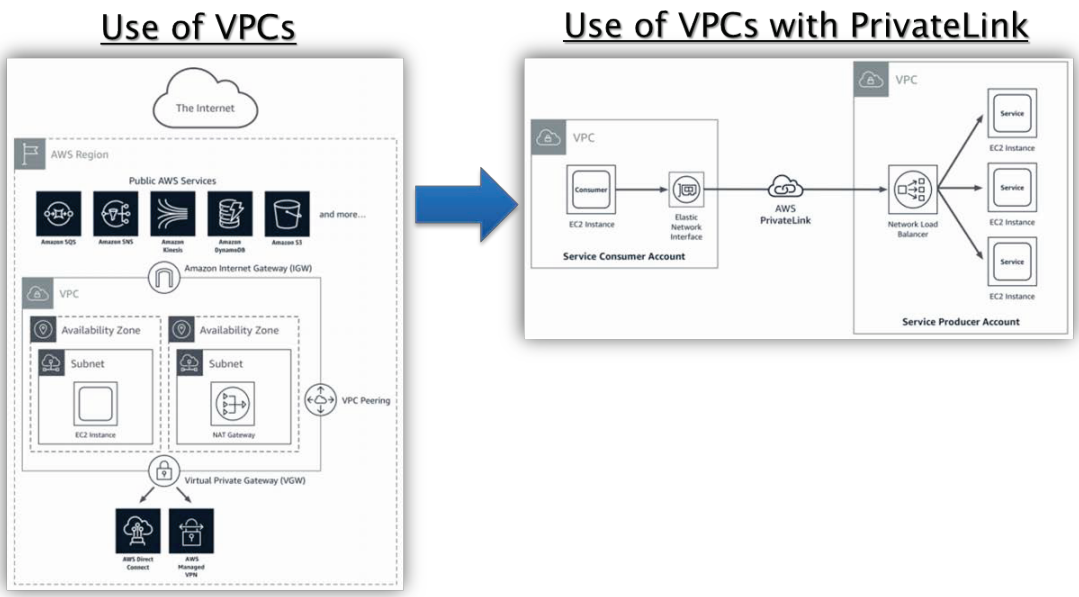


Figure 3: Traditional VPC vs PrivateLink VPC connectivity

AWS PrivateLink provides the following benefits:

1. **Private connectivity:** Via the use of private IP address all connectivity remains internal to AWS without the need for data transfer over public internet. External services appear as if they are internal to your own VPC
2. **Scalable Managed Service:** AWS PrivateLink is an AWS managed service that scales based on usage needs.
3. **Simple Network Management:** Simplifies network topology by maintaining all traffic internal to your own VPC
4. **Targeted /Specific Connectivity**: Via the use of "Endpoints", AWS users can expose or connect to specific services.

Establishing AWS PrivateLink connectivity from an Industry Member's and CRA's VPC to the FINRA CAT VPC can be accomplished by executing an AWS CloudFormation template. Industry Members and CRAs will need to provide their AWS account numbers to FINRA CAT in order to facilitate PrivateLink access. Upon providing this information to FINRA CAT and completing the enrollment process, the execution of the FINRA CAT CloudFormation template creates the necessary resources in the Industry Member's and CRA's VPC and automatically establishes VPC-to-VPC connectivity to FINRA CAT. The CloudFormation script will allow IM's/CRAs to select between small, medium, or large setup based on bandwidth

requirements or the need to span across multiple AWS availability zones[3]. The template optionally creates AWS-hosted DNS records for CAT services that will be used by Industry Member and CRA client software. Industry Members and CRAs may also select to configure DNS records manually, for example, to use a different DNS service. A sample notional architecture for an Industry Member or CRA connecting to FINRA CAT is shown below:

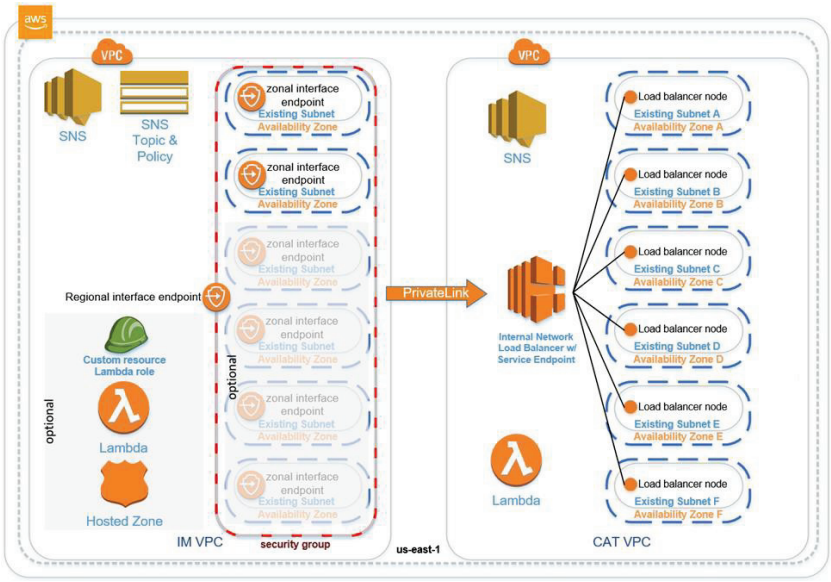


Figure 4: Sample architecture constructed by FINRA CAT provided scripts

Industry Members and CRAs interested in AWS PrivateLink should contact the FINRA CAT Help Desk at 888-696-3348 or at help@finracat.com.

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

3.5. CAT Secure Reporting Gateway

Industry Members and CRAs using public lines will only be able to access the CAT/CAIS Reporter Portal[4] by establishing an authenticated, encrypted connection through the CAT Secure Reporting Gateway (SRG). The CAT Secure Reporting Gateway requires multi-factor authentication (MFA) to establish a secure, encrypted session before accessing the CAT/CAIS Reporter Portals. The CAT Secure Reporting Gateway meets all Plan requirements for data connectivity and encryption, specifically: 1) Network isolation limiting

[3] FINRA CAT AWS PrivateLink endpoints are setup in all three of its availability zones for maximum flexibility.
[4] CAT File Transfer (SFTP) is not available through the SRG.

access to only authorized endpoints, 2) Strong authentication using MFA, and 3) Encryption of the data in transit. The CAT SRG does not limit Industry Members with respect to their choice of Internet Service Providers.

The CAT Secure Reporting Gateway enables end users with secure access to the CAT/CAIS Reporter Portal via a web browser. The SRG does not require any specialized client software to be installed on the Industry Members' or CRAs' computers other than a modern web browser as specified in Section 2.2. The SRG provides refined control over the web applications through the use of policy manager controls and content inspection of the application data. Through the use of the SRG the client computer never communicates directly with the CAT web application.

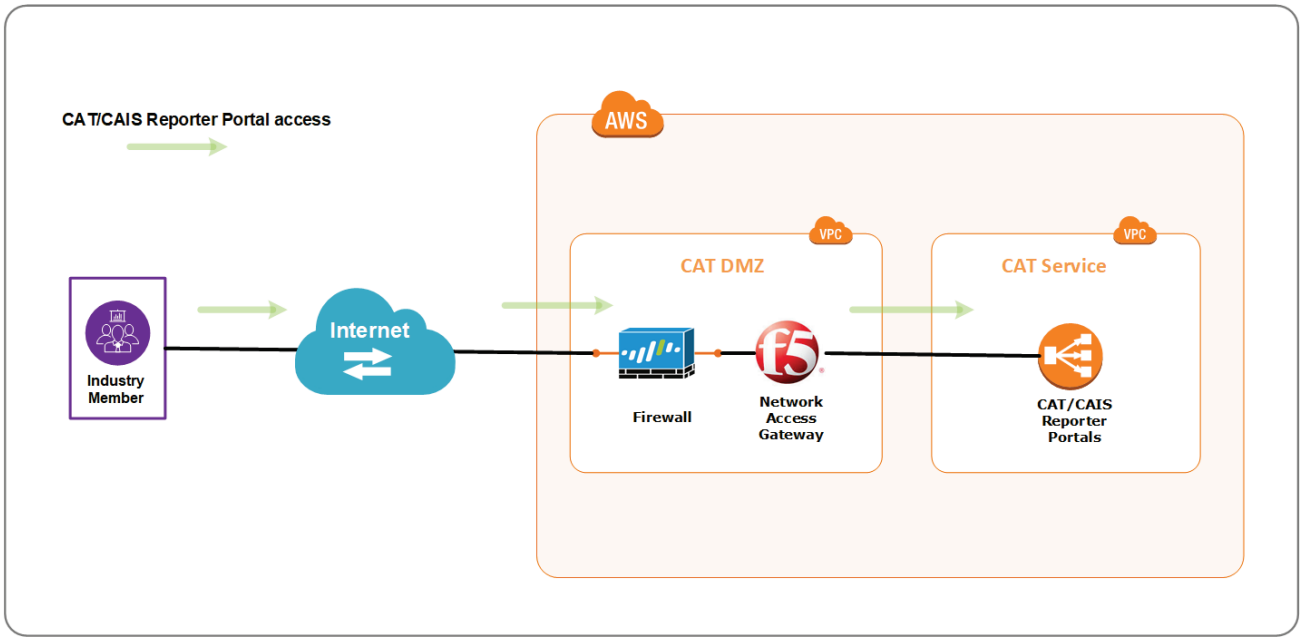


Figure 5: High Level CAT Secure Reporting Gateway Diagram

4. Connecting to the CAT System

Testing the ability to connect to the CAT system is a required step documented in the FINRA CAT Industry Member Onboarding Guides located at https://www.catnmsplan.com/registration/. Once the requirements for establishing Access and Connectivity have been completed as per this document, Industry Members and CRAs must test connecting to the CAT System for each interface method that will be used to report to CAT and/or retrieve associated feedback.

4.1. CAT File Transfer

The following URLs are required to access the CAT system using SFTP:

Table 4: SFTP URLs

Method	Production	Industry Test
Private Line (Transaction Data)	sftp.catnms.com	sftp.ct.catnms.com
AWS Private Link (Transaction Data)	sftp-pl.catnms.com	sftp-pl.ct.catnms.com
Private Line (CAIS Data)	sftp.cais.catnms.com	sftp.ct.cais.catnms.com
AWS Private Link (CAIS Data)	sftp-pl.cais.catnms.com	sftp-pl.ct.cais.catnms.com

The steps to test network connectivity to the CAT File Transfer interface method via SFTP:

1. Connect to SFTP service (sftp {user}@sftp.ct.catnms.com). Note: Refer to the table above for the URL associated with the selected Connectivity Method
2. Perform an “ls” operation and see the first directory, which would be named for the CRD # of the CAT SFTP User

Note: CATFT SFTP service limits the number of authentication attempts per SFTP connection. Please refer to section **5.4** for troubleshooting SFTP connections.

4.2. CAT / CAIS Reporter Portals

The following URLs are required to interface the CAT / CAIS Reporter Portals:

Table 5: CAT / CAIS Reporter Portal URLs

Method	Production	Industry Test
Private Line (Transaction Data)	reporterportal.catnms.com	reporterportal.ct.catnms.com
AWS Private Link (Transaction Data)	reporterportal-pl.catnms.com	reporterportal-pl.ct.catnms.com

Private Line (CAIS Data)	reporterportal.cais.catnms.com	reporterportal.ct.cais.catnms.com
AWS Private Link (CAIS Data)	reporterportal-pl.cais.catnms.com	reporterportal-pl.ct.cais.catnms.com
CAT Secure Reporting Gateway	srg.catnms.com	srg.ct.catnms.com

Steps to test network connectivity to the CAT/CAIS Reporter Portals:

1. In a browser, go to https://srg.ct.catnms.com. Note: see table in URLs section above for correct the URL for your Connectivity Method.

2. Upon login using the CAT User Account established during the CAT Entitlement Onboarding step, an Under-Construction page will be displayed, which demonstrates a successful login while the CAT Reporter Portal is being built.

4.3 Firewall Policy Requirements

4.3.1. Private Line access

Industry Members using private line connectivity should configure network firewall policies to permit outbound requests on tcp ports 443 and 22 to the 150.123.250.0/24 network. A network-based firewall permissions approach enables the dynamic scaling of capacity and application failover of FINRA CAT systems when necessary without an interruption of service to Industry Members. Additionally, a network-based firewall permissions approach allows for the access of new FINRA CAT/CAIS applications and services when launched without delay associated with the need to submit new or expanding firewall requirements. FINRA CAT recommends the use of a network-based firewall permissions to ensure that Industry Members systems and staff maintain access to FINRA CAT/CAIS systems in the AWS environment. Firewall policy should be configured to enable the same access over their primary and backup connections.

Environment	Destination Network	Application	TCP Ports
Production and CT	150.123.250.0/24	Secure Web	443
Production and CT	150.123.250.0/24	SFTP	22

FINRA CAT application domain names are resolvable through public DNS services over the Internet.

When supported by Industry Members firewall infrastructure, a DNS based firewall policy may be leveraged to maintain a more specific approach to firewall permissions. The dynamic nature of capacity scaling and application failover can be addressed through the use of a DNS based firewall policy.

4.3.2. Secure Reporting Gateway access

Industry Members using the Internet to access the Secure Reporting Gateway should configure network firewall policies to permit outbound requests on tcp port 443 to the IP addresses listed in the table below. Firewall policies should be configured to enable the same access over their primary and backup Internet connections.

Environment	Destination Addresses	Application	TCP Ports
Production	54.197.166.31/32 54.81.25.168/32 3.231.65.161/32 52.70.199.220/32	https://srg.catnms.com	443
CT	18.214.18.121/32 52.201.80.164/32	https://srg.ct.catnms.com	443

4.3.3. DUO Multi-Factor Authentication access

To support multi-factor authentication (MFA) requirements into FINRA CAT applications over both private lines and through the Secure Reporting Gateway, Industry Members should configure their network firewall policies to permit outbound requests on tcp port 443 to the IP networks listed in the table below. This access is required to support client browser authentication requirements during the MFA login process. Starting June 1, 2020 FINRA CAT will enable the "Deny Access from Anonymous Networks" feature. More information on this feature can be found at: https://duo.com/blog/blocking-authentication-attempts-from-anonymous-networks.

High availability and automated failover mechanisms can trigger a change in IP addressing. For this reason, FINRA CAT recommends the use of network-based firewall permissions to ensure that Industry Member staff maintain access to the DUO cloud authentication service. Firewall policies should be configured to enable the same access over of their primary and backup Internet connections.

Environment	Destination Network	Application	TCP Ports
DUO, Internet based MFA	54.241.191.128/26 54.236.251.192/26 52.19.127.192/26 52.32.63.128/26 52.59.243.192/26 35.182.14.128/26	HTTPS	443

More information related to DUO MFA connectivity can be found here.

4.3.4. Additional access requirements

Industry Members staff accessing FINRA CAT systems require access to the following sites in order to support full functionality. The list below has been updated to add two Internet based URL's that are required to support SAML authentication into the Secure Reporting Gateway in Customer Test and Production. Additionally, three URL's have been removed that were previously required to support style sheets and fonts.

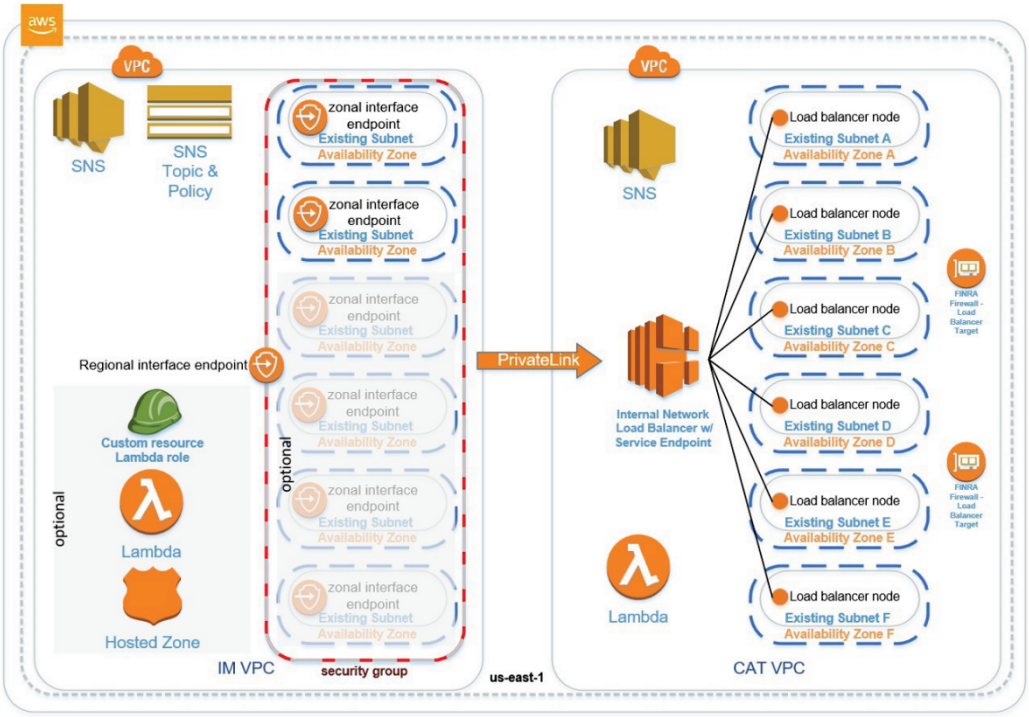
Environment	Destination URLs	Access Path	Access Requirement
Production and CT	ews-ct.fip.catnms.com	Private line	User Authentication - CT
	ewslogin-ct.fip.catnms.com	Private line	User Authentication - CT
	ews.fip.catnms.com	Private line	User Authentication – PD
	ewslogin.fip.catnms.com	Private line	User Authentication – PD
	api-f0075de7.duosecurity.com	Internet	Multi-Factor Auth - PD/CT
<Effective May 29th>	ews-public-ct.fip.catnms.com	Internet	SRG SAML Authentication - CT
<Effective June 29th>	ews-public.fip.catnms.com	Internet	SRG SAML Authentication - PD
<no longer required>	~~*maxcdn.bootstrapcdn.com*~~	~~*Internet*~~	~~*Application CSS access**~~ - PD/CT
<no longer required>	~~*fonts.googleapis.com*~~	~~*Internet*~~	~~*Application fonts access**~~ - PD/CT
<no longer required>	~~*fonts.gstatic.com*~~	~~*Internet*~~	~~*Application fonts access**~~ - PD/CT

5. AWS PrivateLink Client Implementation Guide

5.1. Overview

This section provides a guide to implement the FINRA CAT PrivateLink client solutions enabling IMs and CRAs to connect to CAT interfaces from their AWS VPCs. The focus of this guide is to implement the resources in the IM VPC depicted below.

5.1.1. General High-Level Design Diagram



This solution installs the client portion of the CAT PrivateLink network connectivity option. The client solution creates resources in an IM-selected AWS account or accounts and one or more IM-selected VPCs. These resources enable private connectivity to CAT permitting Industry Members (IMs) with network connectivity to authentication services, web-based services and secure file transport protocol (SFTP) services. The network connectivity is limited to the internal AWS boundary.

5.1.2. Data Flow

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 the AWS Route53 service or the client's self-supported service. Resolution directs the client to a PrivateLink endpoint in the client VPC that securely connects to the CAT service over the AWS internal network.

5.1.3. Installation Instantiations

This client solution is installed multiple times, once for each desired service type. A set of independent resources are created for each installation instantiation in the client-selected AWS account and VPC. If AWS Route53 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 a CAT service URLs for the purpose of network connectivity.

5.1.4. General Environmental Requirements

The solution requires an existing AWS account, VPC and between two and six existing subnets in different availability zones according to the bandwidth and resiliency option selected. An installation of the authentication service is required in each VPC that any other CAT services are installed into. 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. 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 Help Desk (see Section 1.1 Support for information on how to contact the Help Desk).

5.1.5. Connectivity Notification

FINRA CAT Operations is notified of client connectivity changes via a SNS topic and policy that is created and configured during installation.

5.1.6. Options

Optionally, CAT service URLs are configured in a Route53 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.

5.2. Implementation Steps

5.2.1. Establish Prerequisites

1. Determine your bandwidth and resiliency needs according to three options.
    a. The small option provides redundancy by creating two channels to the CAT PrivateLink service. Each channel is an endpoint existing in a different subnet with each subnet

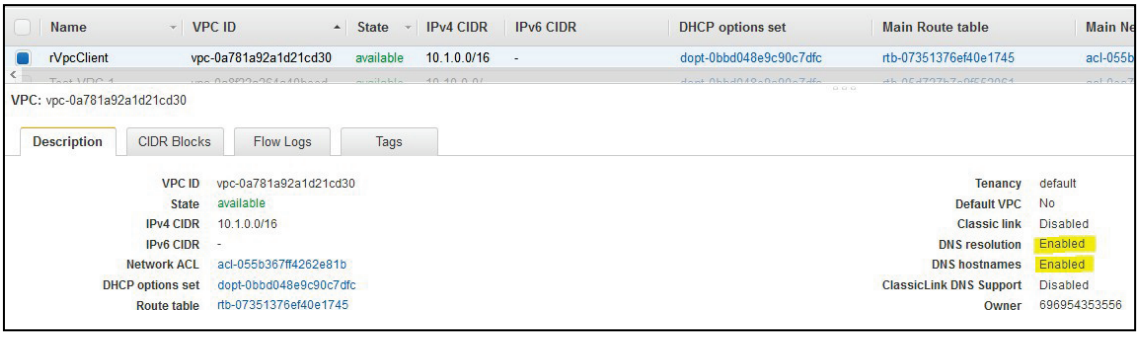
existing in a different AWS availability zone. Each endpoint provides 10Gbps of network bandwidth that may increase according to usage.

b. The medium option provides redundancy by creating four channels to the CAT PrivateLink service. Each channel is an endpoint existing in a different subnet with each subnet existing in a different AWS availability zone. Each endpoint provides 10Gbps of network bandwidth that may increase according to usage.

c. The large option provides redundancy by creating six channels to the CAT PrivateLink service. Each channel is an endpoint existing in a different subnet with each subnet existing in a different AWS availability zone. Each endpoint provides 10Gbps of network bandwidth that may increase according to usage.

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

2. Identify or create a VPC in the **AWS us-east-1 region** to install the solution into. The VPC must not be the default VPC. If domain name services (DNS) will be provided by an AWS Route53 private hosted zone (not your own DNS service), then the VPC must have the following two settings enabled:
   a. enableDnsHostnames
   b. EnableDnsSupport
   c. To verify these settings:
      i. On the AWS console, navigate to the VPC service and select “Your VPCs”.
      ii. Select the VPC that the client solution will be installed into by clicking the box on the left of the VPC name.
      iii. Check the two settings on the lower right of the screen:



      iv. These settings are not required if you will use a non-AWS DNS service.

3. In the VPC from the previous step, identify or create between two and six subnets in different availability zones. The number of subnets is determined by the selected bandwidth and resiliency option. See Appendix B for more information.
4. Determine if you would like DNS configured automatically. DNS will convert CAT service names (e.g. ccft.catnms.com) to addresses used by the network for communication. Skip this step if you will configure your own DNS.
    a. Automatically configuring DNS requires permissions, called a role. You may configure this role yourself or have the implementation create the role automatically. Determine if you would like the role automatically created.
    b. If you would like the role created automatically, skip to the next step.
    c. If you will configure the role yourself, create a role in the account the solution is being installed into that permits an AWS CloudFormation custom resource Lambda function to configure DNS and log to CloudWatch Logs. Note that the log group and log stream resource name must not be changed from "*rLambdaPrivateHostedZone*", else the function will not be able to log which may impact operational support. Once created, note the role's Amazon Resource Name, called an ARN.

Role Trust Policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Role Policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DNS",
            "Effect": "Allow",
            "Action": [
                "route53:CreateHostedZone",
                "route53:ListHostedZonesByName",
                "route53:GetHostedZone",
                "route53:ChangeResourceRecordSets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions"
            ],
```

```
                "Resource": "*"
            },
            {
                "Sid": "Logstream",
                "Effect": "Allow",
                "Action": [
                    "logs:CreateLogStream",
                    "logs:DescribeLogStreams",
                    "logs:PutLogEvents"
                ],
                "Resource": "arn:aws:logs:*:*:log-
group:/aws/lambda/*rLambdaPrivateHostedZone*:log-stream:*"
            },
            {
                "Sid": "Loggroup",
                "Effect": "Allow",
                "Action": [
                    "logs:CreateLogGroup",
                    "logs:PutLogEvents"
                ],
                "Resource": "arn:aws:logs:*:*:log-
group:/aws/lambda/*rLambdaPrivateHostedZone*"
            }
        ]
    }
```

5. Determine the solution type that you will install. Available solution types are:
    - ccft for CAT Core File Transfer
    - ccrp for CAT Core Reporter Portal
    - caisft for CAIS File Transfer
    - caisrp for CAIS Reporter Portal
    - cauth for CAT authentication

    Note:

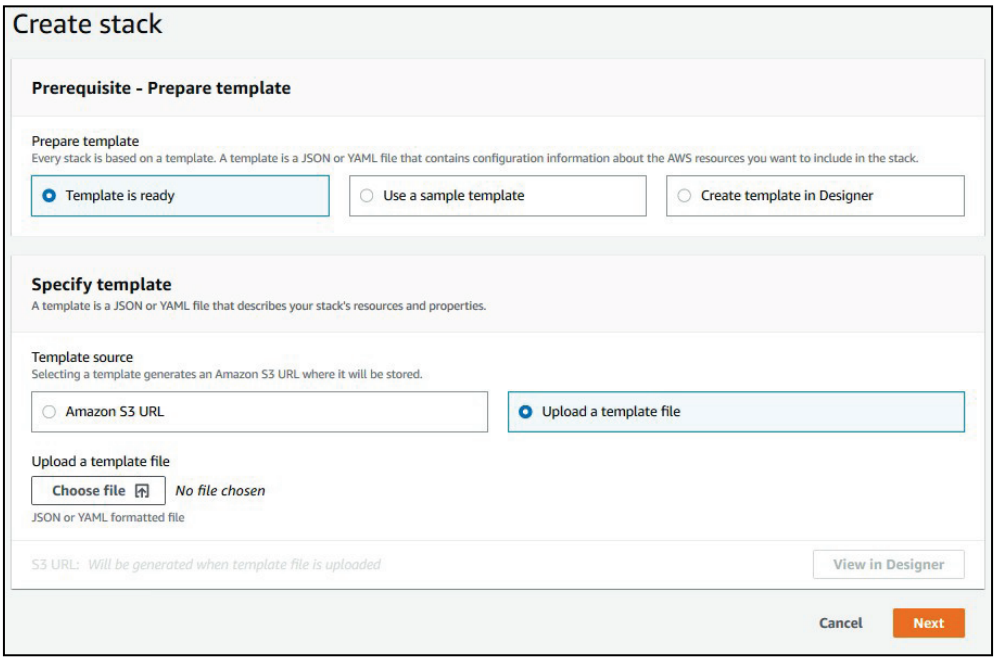
    - Duplicate instances of a solution type are not supported in a single VPC.
    - You may install all solution types in a single VPC.
    - Excluding cauth, you may install each solution type into different VPCs.
    - You must install cauth into each VPC that hosts a portal solution type.
6. Identify or create a role or identify that will be used by CloudFormation to implement the solution. The role or identity must have full permissions to create the resources types listed in Appendix A.

5.2.2. Install the Solution

1. Authenticate to the AWS Console and navigate to the CloudFormation service using the role or identity identified above and select the **us-east-1 AWS region** at the top right of the screen, which is titled **"N. Virginia"**. The selected region has an orange vertical bar to the left of its name. Selecting the wrong region will result in no resources being created during the installation.

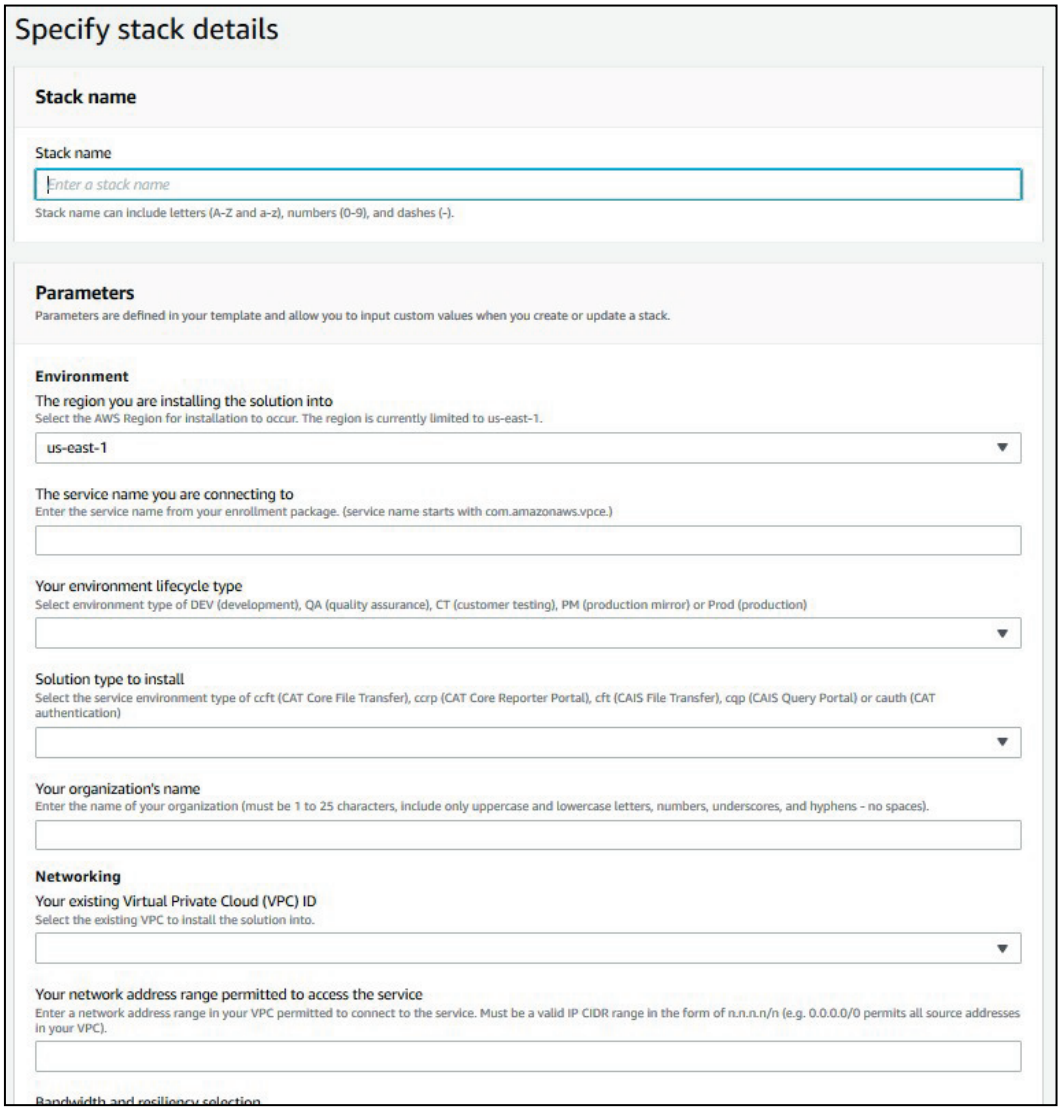
2. Select the “Create stack” button. (A stack is a collection of AWS resources that you can manage as a single unit[5].)

3. Select “Template is ready”, “Upload a template file” and select the “Choose file” button.



[5] https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacks.html

4. When the file open dialog appears, select “CAT PrivateLink Client Endpoint.yml” (or appropriate file name/version). This file is called the template and contains instructions to build AWS resources.
5. When the file open dialog closes, select the orange “Next” button in the CloudFormation Create stack dialog.
6. The “Specify stack details” dialog should now be displayed.



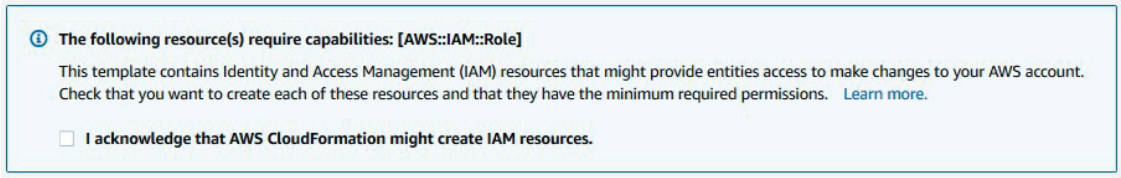
7. Enter a name for the stack. Enter a stack name that will differentiate it from other stacks such as “CAT-PrivateLink-Client-ccft” that would specify that the stack is for CAT, it is the PrivateLink client and it provides the ccft (CAT Core File Transfer, for example) solution.
8. Enter the parameter values for the stack’s “Environment” section:

a. Select the region to install the solution into from the dropdown list. The region is currently limited and defaulted to us-east-1. Attempting to install the solution into other regions will not provide connectivity.
b. Enter the CAT service name that you received from FINRA CAT. The service name is specific to the solution type being installed. The service name starts with com.amazonaws.vpce.
c. Select the environment lifecycle type from the dropdown list. This will tag stack resources with the lifecycle type, aiding in identification. Other tags will be applied to aid in resource association with the FINRA CAT PrivateLink solution and solution type (for resources that support tagging). The available lifecycle types are:
    i. DEV for development environments
    ii. QA for quality assurance environments
    iii. CT for customer testing environments
    iv. PM for production mirror environments
    v. Prod for production environments
d. Select the solution type to install from the dropdown list to connect with the associated CAT service:
    i. ccft for CAT Core File Transfer
    ii. ccrp for CAT Core Reporter Portal
    iii. caisft for CAIS File Transfer
    iv. caisrp for CAIS Reporter Portal
    v. cauth for CAT authentication (note that the small bandwidth and resiliency option will likely be sufficient for the cauth solution type)
e. Enter your organization's name, noting the stated constraints and acceptable characters that may be included in the name (e.g. no spaces).

9. Enter the parameter values for the stack's "Networking" section:
    a. Select the existing VPC ID from the dropdown list to install the solution into. The selected VPC must not be the default VPC.
    b. Enter the network IP address range within your VPC that may connect to the CAT service. The range is expressed in CIDR block notation. Contact your network administrator if assistance is needed to determine this range. For example, if you have only one instance with an IP address of 10.1.1.1 that you would like to permit access to the service, enter 10.1.1.1/32. Addresses outside of the entered range will not be able to connect to the service. Note: Connectivity establishment from CAT to your VPC is not possible.
    c. Select the Bandwidth and resiliency selection according to your previous decision.

d. Select the first subnet from the dropdown list to install the connection into. The subnet must be in a different availability zone than the other subnets selected. A dropdown list is provided for subnets one and two because two subnets are required for high availability.
e. Select the second subnet from the dropdown list to install the solution into. The subnet must be in a different availability zone than the other subnets selected.
f. Continue entering subnet IDs until the number of subnets previously determined, according to the bandwidth and resiliency option selection, has been reached. Each subnet must be an existing subnet in the selected VPC and be in a different availability zone than the other subnets selected. See appendix B for instructions on locating subnet IDs. Note that the remaining subnet parameters are manually entered and not provided via dropdown list, to accommodate clients selecting the small or medium bandwidth and resiliency option.

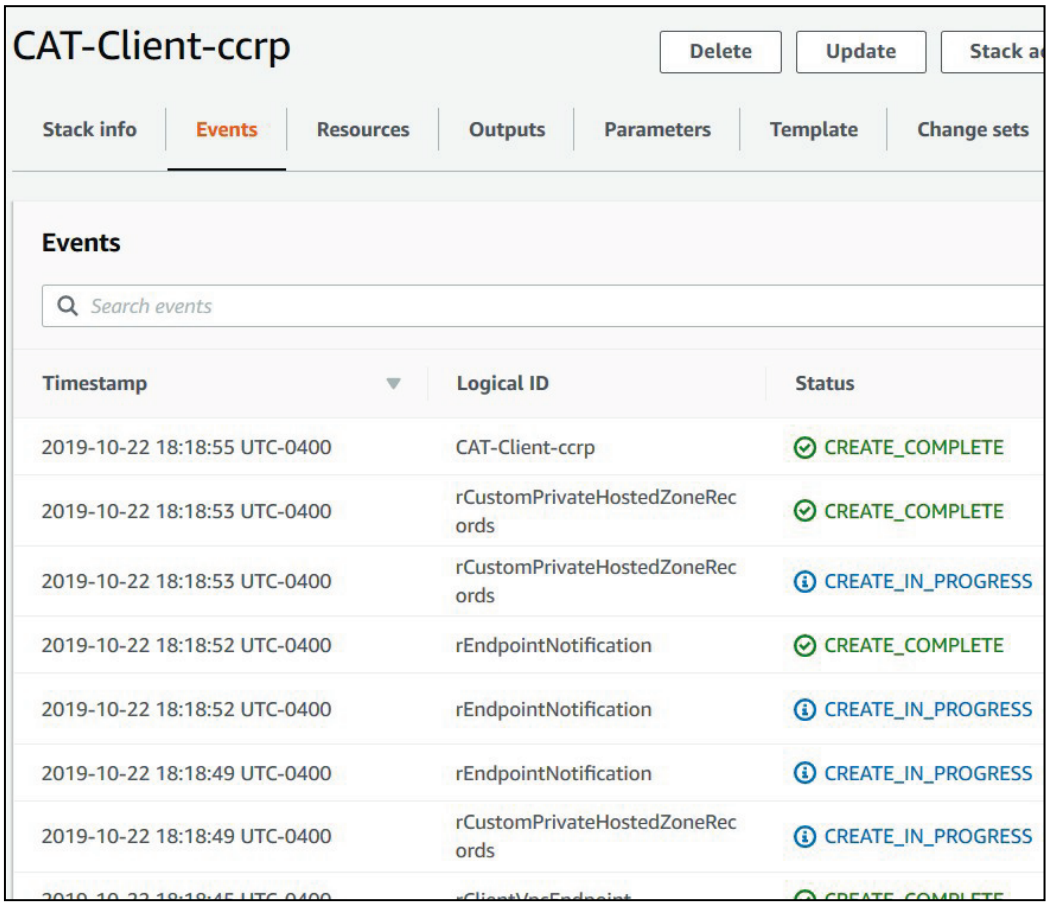
10. Enter the parameter value for the stack's "Domain Name Services (DNS)" section.
    a. If you would like DNS to be automatically configured for you, select "yes" from the dropdown list under the question: Should DNS be configured for you? Otherwise, select "no".
    b. If you selected "yes" to the previous question and would like a role creating permissions for automatic DNS configuration, select "yes" under the question: Should a role to configure DNS be created for you? Otherwise, select "no".
    c. Enter the role providing permissions to configure DNS. This value is required only if:
        i. You have selected DNS to be automatically configured **AND**
        ii. You have decided to configure the permissions role yourself.
        iii. If this value is required according to the above conditions, enter the Amazon resource name (ARN) of the role you created in a previous step, else leave the value blank.
11. Select the orange "Next" button.
12. The "Configure stack options" dialog is displayed. Values here are optional and dependent on your organizational requirements.
13. Select the orange "Next" button.
14. The "Review [stack name]" dialog is displayed.
15. Verify that the parameters are correct.
16. Other values here are optional and dependent on your organizational requirements.
17. Since the CloudFormation template instructions contain optional instructions to create a role for optional DNS configuration, the following dialog is displayed even if you choose to not have a role created automatically. This does not necessarily mean that the role is being created. The message indicates that the template contains definitions for IAM (Identity and Access Management) resource creation. A role will only be created if directed by parameter selection.



18. Check the box next to “I acknowledge that AWS CloudFormation might create IAM resources”.
19. Select the orange “Create stack” button to create the solution.

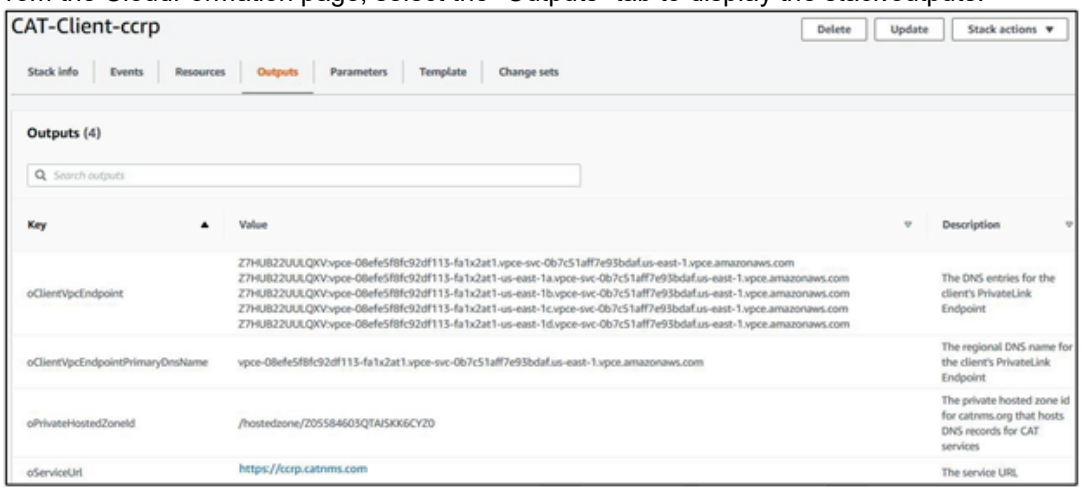
The solution will now be created by CloudFormation according to the template and parameters.

Stack creation is complete when the events tab displays the stack name followed by “CREATE_COMPLETE” as depicted below. Note that you will need to click the refresh button to display progress updates:

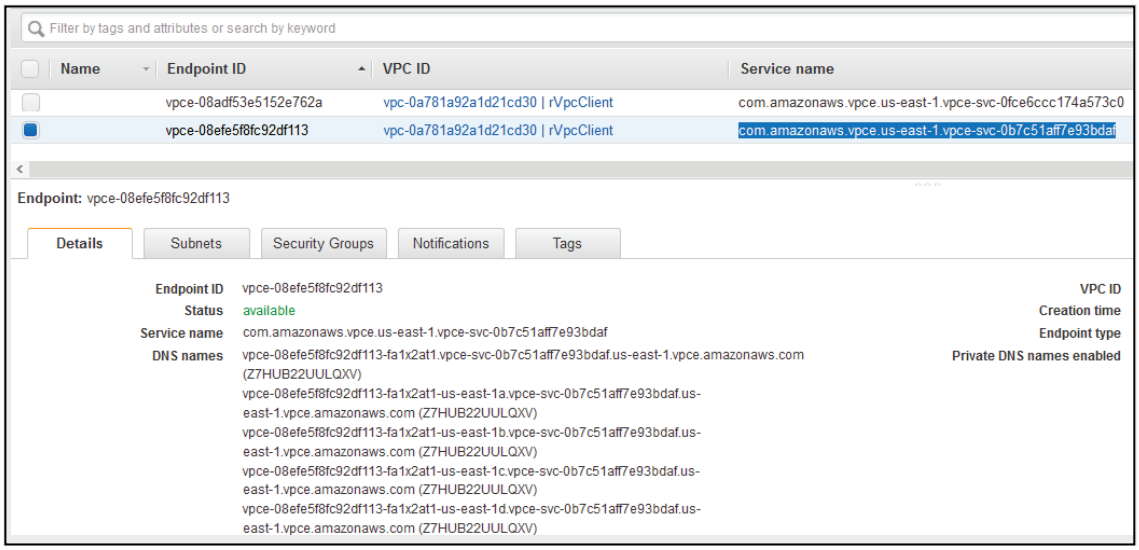


5.2.1. Obtain Stack Outputs

1. From the CloudFormation page, select the “Outputs” tab to display the stack outputs.



2. The first row contains DNS information for the client’s PrivateLink endpoints / channels created.
    a. This example has five entries. The first entry is the parent entry of the remaining four. There are four child entries because this example selected the medium bandwidth and resiliency option that creates four endpoints / channels.
3. The second row displays the regional DNS name of the client’s PrivateLink endpoint. This name is useful to locate your connection and determine connectivity status. To check connectivity status:
    a. On the AWS console, navigate to the VPC service and select “Endpoints”.
    b. Locate the endpoint with a service name that partially matches the CloudFormation output value (example highlighted below). This service name will be needed if you will configure DNS yourself.



c. The status of “available” indicates that you have network connectivity to the selected CAT service.

d. You will have one of these entries for each installation of a client solution to a CAT service.

4. The third output row displays the AWS Route53 hosted zone information that links to the DNS configuration. This value will only be displayed if DNS was automatically configured.
5. The fourth row displays the URL to the service. You will use this URL in your application to connect to the selected service.

Repeat these procedures to install connectivity to other CAT services such as:

- CAT Core File Transfer
- CAT Core Reporter Portal
- CAIS File Transfer
- CAIS Query Portal
- CAT authentication

Important:

Note that an installation of CAT authentication (cauth) is required to enable application authentication for all other solutions. If solutions are installed in different VPCs, an installation of CAT authentication is required in each VPC.

5.3. Manual DNS Configuration

This step is only required if you selected to configure DNS yourself. Follow the below steps to create a Route53 private hosted zone and enter a DNS record to resolve service’s fully qualified domain names.

This procedure must be performed for each VPC that a client solution is installed into. A hosted zone and record set(s) must be created for each DNS entry in the table below for the solution type in each VPC that a client solution is installed into[6]. If you are using a different DNS solution, adapt the below instructions according to the vendor's instructions.

1. On the AWS console, navigate to the Route53 service and select "Hosted zones".
2. Click the "Create Hosted Zone" button. A pane opens on the right side of the screen.
3. For Domain Name entries when using AWS Route53, enter the DNS entry below for installed client solution type:
    a. Replace clientsolutiontype with the type you are installing (e.g. ccft, ccrp, cft, cft, cqpor cauth, caisrp, or caisft) as shown in the table below.

Application	Service	Environment	DNS Entry	Access
ccft	SFTP	CT	sftp-pl.ct.catnms.com	CAT
ccrp	HTTPS	CT	reporterportal.ct.catnms.com	CAT
cauth (*required for ccrp*)	HTTPS	CT	ews-ct.fip.catnms.com	CAT
cauth (*required for ccrp*)	HTTPS	CT	ewslogin-ct.fip.catnms.com	CAT
ccft	SFTP	Prod	sftp-pl.catnms.com	CAT
ccrp	HTTPS	Prod	reporterportal.catnms.com	CAT
cauth (*required for ccrp*)	HTTPS	Prod	ews.fip.catnms.com	CAT
cauth (*required for ccrp*)	HTTPS	Prod	ewslogin.fip.catnms.com	CAT
caisrp	HTTPS	CT	reporterportal-pl.ct.cais.catnms.com	CAIS
caisrp	HTTPS	Prod	reporterportal-pl.cais.catnms.com	CAIS
caisft	HTTPS	CT	sftp-pl.ct.cais.catnms.com	CAIS
caisft	HTTPS	Prod	sftp-pl.cais.catnms.com	CAIS

4. For Domain Name entries when using an alternate DNS service, use a CNAME to point to AWS private endpoint names or an "A" record to point to AWS private VPC endpoint IP.
5. For Comment, enter: Private Hosted Zone For FINRA CAT - do not delete
6. For Type, select "Private Hosted Zone for Amazon VPC" from the dropdown list.
    a. If you are using a different DNS solution, adapt the below instructions according to the vendor's instructions.
    b. Create a DNS zone for each required DNS entry above based on client solution type installed.

    In each of the DNS zone:
    - if the DNS solution allows create CNAME for zone apex, create a CNAME to point zone apex to corresponding solution type privatelink service endpoint DNS name.

      For instance:
      reporterportal.ct.catnms.com. CNAME vpce-0aa6bf78ee91f0fc1-dbx9h3et.vpce-svc-0ff19f3e6597e137f.us-east-1.vpce.amazonaws.com.

    - if the DNS solution doesn't allow CNAME for zone apex, create round robin A records for zone apex, the ip addresses are the VPC endpoints IP for that PrivateLink service.

      For instance:
      reporterportal.ct.catnms.com. A 192.168.0.101
      reporterportal.ct.catnms.com. A 192.168.1.142

7. For VPC ID: select the VPC ID of the VPC that was selected during client solution installation.

8. Click the “Create” button.

The hosted zone is created and the hosted zone screen for the hosted zone just created is displayed.

9. Click “Create Record Set”.

   A pane opens on the right side of the screen.

10. Leave the Name field blank.

11. For Type, select “A – IPv4 address”.
12. Next to Alias, select the “Yes” radio button.
13. For Alias Target, enter the service name from step 28. In our previous example, this was “com.amazonaws.vpce.us-east-1.vpce-svc-0b7c51aff7e93bdaf”. This value is the endpoint service name on the console as previously depicted.
14. For Routing Policy, select “Simple”.
15. Next to Evaluate Target Health, select the “No” radio button.
16. Click the “Create” button.
17. Test DNS resolution:
    a. Login to an instance located in the same VPC that the solution was installed into.
    b. For Linux or Windows operating systems, execute the command nslookup aaaa.catnms.com where aaaa is the solution type of ccft, ccrp, cft, cqp or cauth.
    c. Command output will look similar to the below (your IP addresses will be different):

[6] Unless association is being used. See: https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-associate-vpcs.html

```
[ec2-user@ip-10-1-1-39 ~]$ nslookup ccrp.catnms.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   ccrp.catnms.com
Address: 10.1.2.175
Name:   ccrp.catnms.com
Address: 10.1.3.225
Name:   ccrp.catnms.com
Address: 10.1.4.111
Name:   ccrp.catnms.com
Address: 10.1.1.59

[ec2-user@ip-10-1-1-39 ~]$
```

d. In this example, the medium bandwidth and resiliency option was selected, creating four endpoint channels which results in the nslookup command displaying four IP addresses for the same name, one IP address per endpoint.

e. Resolutions against the fully qualified domain name will return endpoint IP addresses in a round-robin selection method. Repeat the command several times to observe this behavior.

5.4. Troubleshooting

Connectivity challenges should be raised with the FINRA CAT Help Desk. Likely causes of connectivity issues are:

1. DNS resolution
    a. Use nslookup as described above to verify that name resolution is successful. The IP addresses returned by nslookup will be in the same network range as your VPC.
    b. Applications must connect to the CAT service using the correct URL, otherwise encryption certificate errors will be experienced.
    c. If domain name services (DNS) will be provided by a AWS Route53 private hostedzone, (not your own DNS service) then the VPC must have the following two settings enabled:
        i. enableDnsHostnames
        ii. EnableDnsSupport

    See instructions in this guide to determine these settings.
2. SFTP Connections
    a. The SFTP service limits the number of authentication attempts per SFTP connection. Even though CATFT SFTP does not accept ssh public keys for authentication, it is possible your sftp client is configured with keys for other SFTP servers and your client may attempt to connect CATFT SFTP using those keys first. If you have more than 10 such keys in your authorized_keys, this may cause you to fail at your SFTP connection attempts.

    b. A resolution for customers would be to add the following options to your SFTP

connection attempts so the connection is made via password instead of attempting with public keys:

- PreferredAuthentications=password
- PubkeyAuthentication=no

3. Account approval
    a. **Each AWS account that hosts a client solution must be pre-approved by FINRA CAT.** Connectivity is not possible without pre-approval.
4. PrivateLink Service Names
    a. FINRA CAT Operations will provide you with the PrivateLink service name for each service that you will connect to. The CAT service name, starting with "com.amazonaws.vpce", must be entered exactly into the CloudFormation parameter. Ensure that no leading or trailing spaces are being copied into the input field. Ensure that

the service name entered as a CloudFormation parameter is for the service that you are connected to.

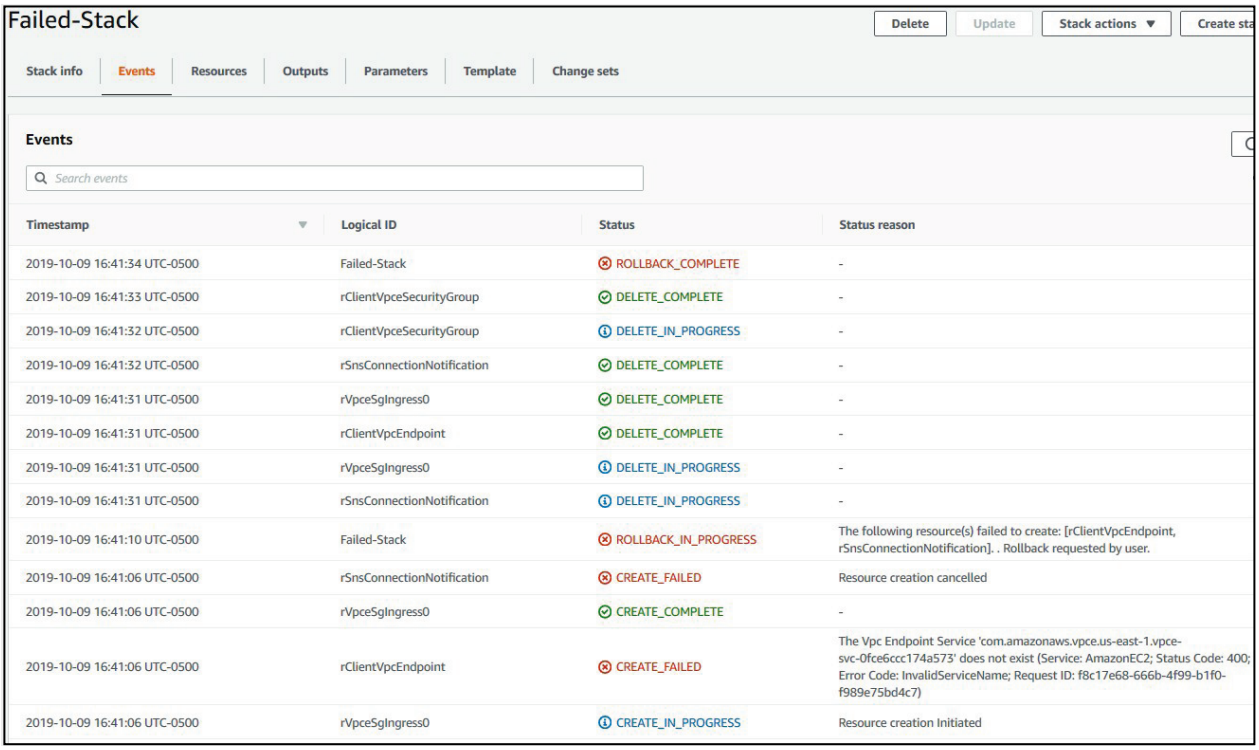
5. Authentication
    a. An installation of the cauth client type is required for every VPC where any other solution types are installed. Applications will not be able to reach the CAT authentication service if cauth is not installed into the same VPC as any other solution type.
6. Manual Resource Deletion
    a. If installed resources are deleted manually, various operational impacts may be experienced. See the Reinstallation and Repair section of this guide for instructions.
7. Installation
    a. Ensure that all instructions in this guide have been followed.
    b. Ensure that every selected subnet is in the same VPC as the installation and that each subnet is in a different availability zone. See Section 5.7 Appendix B for instructions.
    c. Ensure that the role or identity used to perform the installation has permission to create the resources in appendix A.
    d. If you have created your own role for DNS configuration, make sure it has rights as depicted in the example role and that the trust policy is correct.
    e. Ensure that the provided CloudFormation template has not been modified.
    f. If the installation completed immediately and no resources where created, then the installation was performed in an unsupported region. You must perform the installation in the **us-east-1 (N. Virginia) AWS region**. See instructions in this guide to select the correct region for the installation.

5.5. Reinstallation and Repair

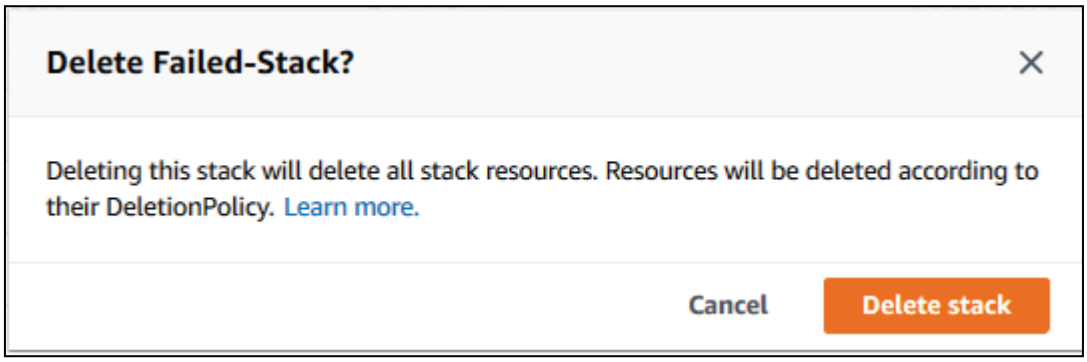
After consultation with FINRA CAT Operations, you may be directed to recreate one or more solution types in your VPC. This method may be the fastest path to reestablish connectivity.

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.

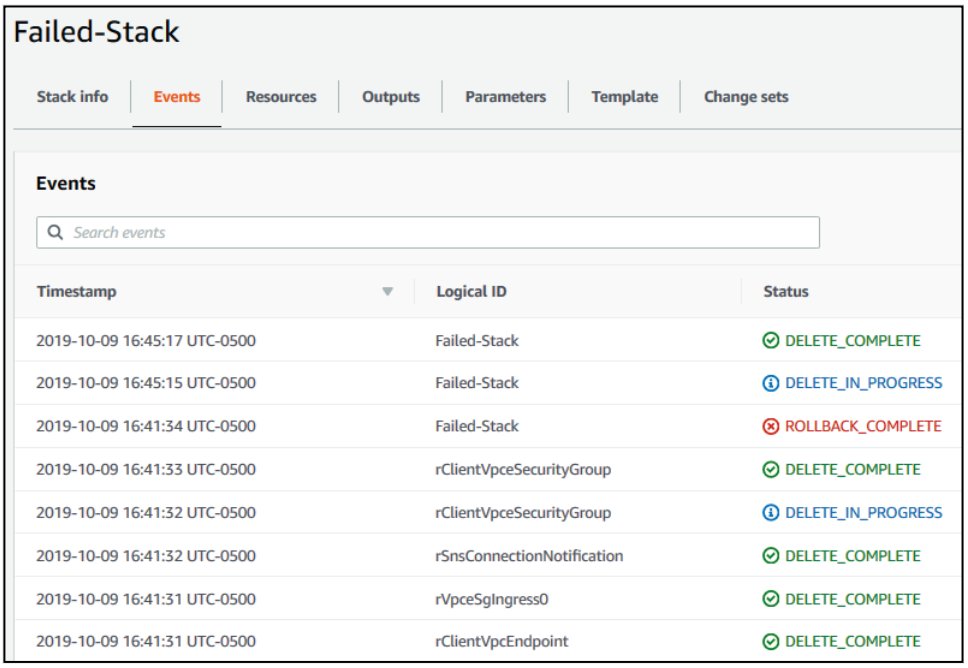
The following is an example of a stack where the PrivateLink service name was incorrect causing the stack installation to fail. The failure causes the stack to roll back, deleting all resources created.



Once the roll back is completed, the stack may be deleted by selecting the “Delete” button and confirming the operation.



The stack will now reach the status of deleted complete.



The installation may now be performed again using the correct parameters.

In the same manner, at the direction of FINRA CAT Operations, you may delete a successfully created installation and recreate the solution. Recreation of a stack will require the DNS entries to be repointed to new aliases if you configured DNS manually because the PrivateLink service name will change with a new installation.

5.6. Appendix A - Resources Installed

AWS::EC2::SecurityGroup

AWS::EC2::SecurityGroupIngress

AWS::EC2::SecurityGroupEgress

AWS::EC2::VPCEndpoint

AWS::SNS::Topic

AWS::SNS::TopicPolicy

AWS::EC2::VPCEndpointConnectionNotification

Optional: AWS::IAM::Role

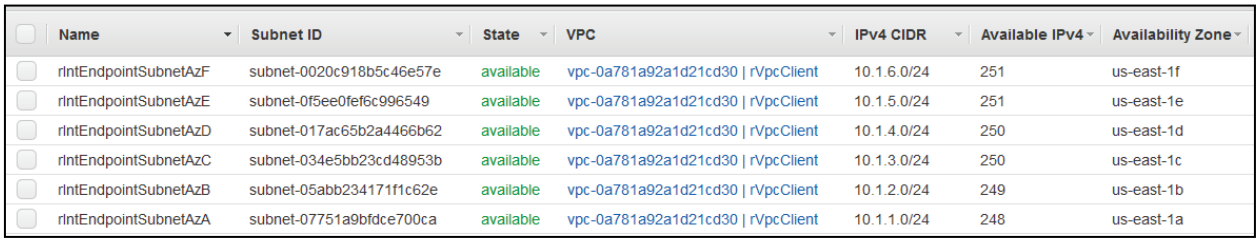
Optional: Custom::rCustomPrivateHostedZone

Optional: Custom::rCustomPrivateHostedZoneRecords

Optional: AWS::Lambda::Function

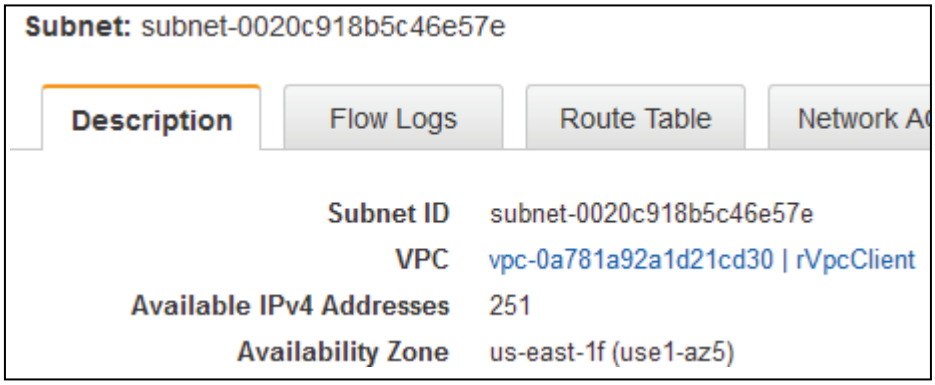
5.7. Appendix B – Identifying Subnet IDs

1. On the AWS console, navigate to the VPC service and select "Subnets".
2. Note that the subnets you select must be in the VPC you selected for the installation and be in a different availability zone than all other selected subnets.
3. Select a subnet by clicking on the box next left of the name.



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	Availability Zone
rIntEndpointSubnetAzF	subnet-0020c918b5c46e57e	available	vpc-0a781a92a1d21cd30 | rVpcClient	10.1.6.0/24	251	us-east-1f
rIntEndpointSubnetAzE	subnet-0f5ee0fef6c996549	available	vpc-0a781a92a1d21cd30 | rVpcClient	10.1.5.0/24	251	us-east-1e
rIntEndpointSubnetAzD	subnet-017ac65b2a4466b62	available	vpc-0a781a92a1d21cd30 | rVpcClient	10.1.4.0/24	250	us-east-1d
rIntEndpointSubnetAzC	subnet-034e5bb23cd48953b	available	vpc-0a781a92a1d21cd30 | rVpcClient	10.1.3.0/24	250	us-east-1c
rIntEndpointSubnetAzB	subnet-05abb234171f1c62e	available	vpc-0a781a92a1d21cd30 | rVpcClient	10.1.2.0/24	249	us-east-1b
rIntEndpointSubnetAzA	subnet-07751a9bfdce700ca	available	vpc-0a781a92a1d21cd30 | rVpcClient	10.1.1.0/24	248	us-east-1a

4. The subnet details for the selected subnet are display at the bottom of the screen.



5. Copy the value to the right of the "Subnet ID" label (which is subnet-0020c918b5c46e57e in this example) and paste the value into the CloudFormation parameter.

5.8. Appendix C – Performance

PrivateLink provides low-cost, high-speed connectivity between AWS accounts. This resilient connectivity solution provides 20Gbps, 40Gbps or 60Gbps for the small, medium and large bandwidth and resiliency option selections respectively.

PrivateLink creates one regional endpoint and multiple subordinate interface endpoints, one for each subnet selected during solution installation.

Application behavior is a factor in obtaining maximum transmission speed. Your application's behavior may vary from the following sequence description.

When an application connects through PrivateLink to a CAT service, the application will request its host operating system to resolve the service's FQDN to an IP address. This resolution will be against the FQDN's alias which is the PrivateLink regional endpoint. The IP addresses returned will vary in order (round-robin) amongst the available interface endpoints configured, either two, four or six according tothe selected bandwidth and resiliency option. Then, the application may connect to one of the returned IP addresses. The IP Address is associated with a single PrivateLink endpoint providing 10Gbps of bandwidth that may increase bandwidth according to usage. Other interface endpoints associated with the PrivateLink regional endpoint will not be engaged and therefore their available bandwidth will not be utilized.

To obtain maximum bandwidth for large file transmissions, transmit each individual file in a separate transmission request from the file transfer application. This will enable various simultaneous file transfers to use different endpoints and utilize available bandwidth from multiple interface endpoints, reducing overall transmission durations.

Additionally, the type of EC2 instance hosting the file transfer application influences performance. For maximum performance select an EC2 instance with high network bandwidth capacity and ensure that enhanced networking is enabled.

To check if enhanced networking is enabled, login to your EC2 instance and execute the following commands, noting that appropriate IAM permissions and AWS CLI installation and configuration are required:

```
INSTANCE_ID=$(curl -s http://169.254.169.254/latest/meta-data/instance-id)
aws ec2 describe-instances --instance-ids $INSTANCE_ID --query
"Reservations[].Instances[].EnaSupport"
```

Command output of `true` indicates that enhanced networking is enabled.

See the following link for more information:
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking-ena.html