ets connect UK

Contributor Connectivity Guide

30 March 2026
Version 1.0

Contents

CTP Contributor Connectivity Guide

1. Scope

This document provides external-facing technical guidance for Contributors connecting to the Consolidated Tape Provider (CTP). It focuses exclusively on network connectivity, supported connection models, routing, resiliency, and infrastructure responsibilities required to establish and maintain connectivity to CTP service endpoints.

This document does not define or specify any application-layer protocols or message schemas. Such details are intentionally out of scope and will be documented separately in a dedicated specification and Rules of Engagement.

1.1. Version History

Version	Date	Description
0.1	18/12/2025	Initial draft
0.2	24/03/2026	Added Mutal TLS (mTLS) section
1.0	30/03/2026	Approved Final version

1.2. Introduction

Contributors connect to the CTP to publish post-trade Bond data over secure network connections. Connectivity may be established using either public or private network paths. This guide describes the supported connectivity architectures, service locations, and recommended high-availability models for production operations.

2. Service Locations and Protocols

2.1. Service Locations

The CTP operates in two AWS Regions in an active-active configuration. Each region functions as a fully independent service location.

- Each region operates independently with no real-time dependency on the other.
- Contributors must connect to both regions to achieve resilience and fault isolation required by the FCA.

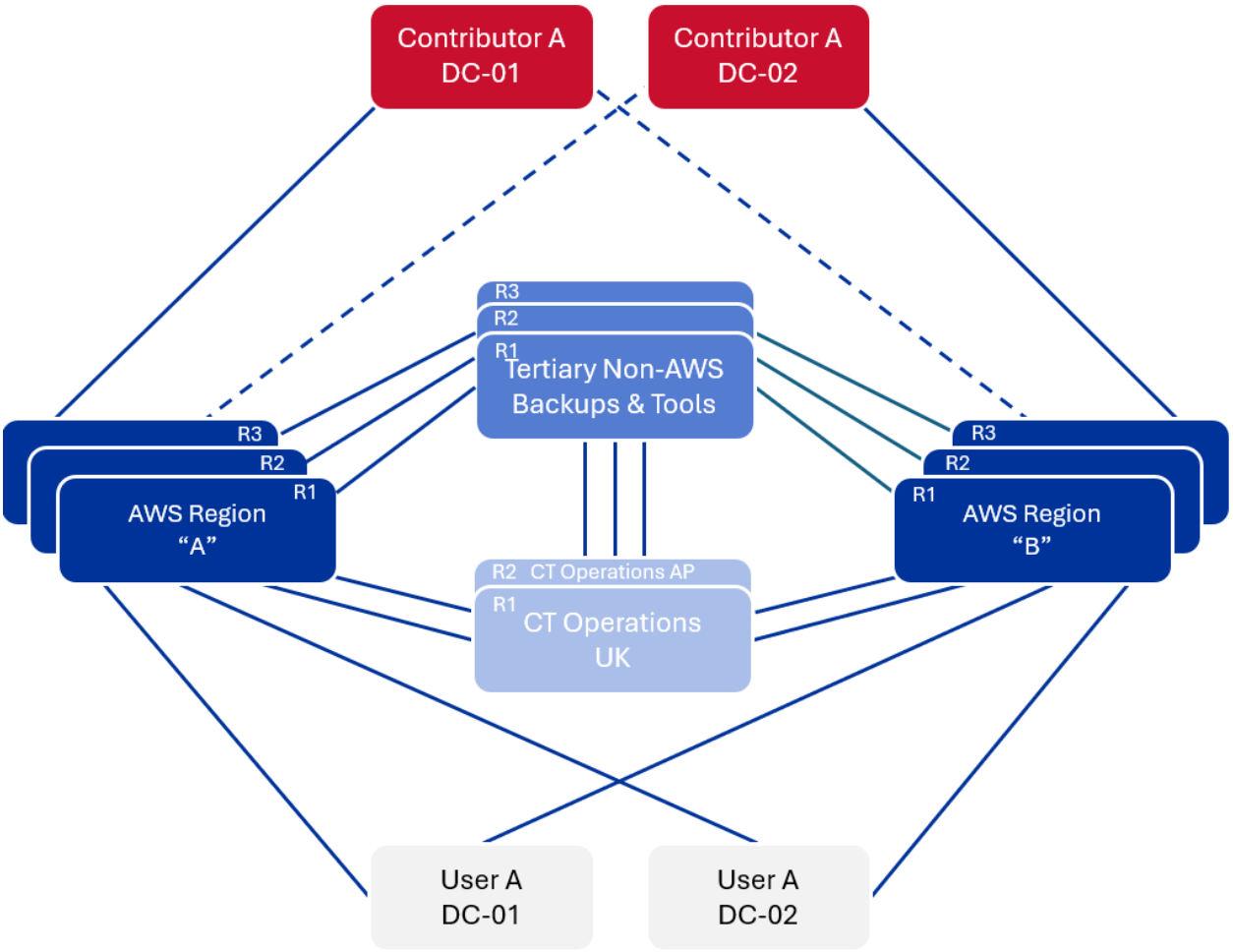
A third non-AWS location acts as a tertiary backup location, receiving replicated data from both primary regions. Contributors do not establish network connectivity to this region.

2.2. High-Level Architecture

CTP operates an active-active, dual-region architecture where each AWS Region functions as a fully independent post-trade processing site, supplemented by a tertiary region that serves exclusively as a data backup and disaster-recovery repository for both primary regions.

ETS Operations – Asia Pacific and UK, is responsible for managing the active and tertiary regions, ensuring that data processing runs smoothly and that disaster recovery protocols are in place.

The following diagram shows the high-level connectivity model of CTP:



Key characteristics:

1. Contributors must establish connectivity to both CTP locations for resiliency.
2. Each location independently processes, validates, and disseminates post-trade bond data.
3. There is no automatic cross-region trade replication for real-time submission flows.
4. The architecture is designed to support high availability, fault isolation, and operational resilience.

Contributor Publishing Model:

- Contributors must connect to both locations and publish the same post-trade data.
- Dual publishing ensures regional resilience, regulatory continuity, and uninterrupted dissemination in the event of a regional outage.

High-Level Processing Flow (Per Region):

1. Contributor establishes connection to both CTP locations
2. Trades are submitted to both CTP locations
3. CTP validates and enriches trade data on each location independently
4. Valid messages are routed into the regional CTP processing and dissemination platform

3. Network Connectivity

This section describes the supported connectivity methods for CTP Contributors.

3.1. Connectivity Options

CTP supports the following two (2) connectivity options:

- Public endpoints
- Private connectivity

3.1.1 Public Endpoints

CTP exposes public ingress endpoints that provides globally optimized routing over the public internet. Contributors can connect securely to both CTP regions using TLS-encrypted TCP.

CTP supports the following public connectivity models:

Public Connectivity Model 1: Active–Passive

In this model, the Contributor implements a region-preferred publishing strategy with built-in redundancy across both CTP regions and Contributor data centers.

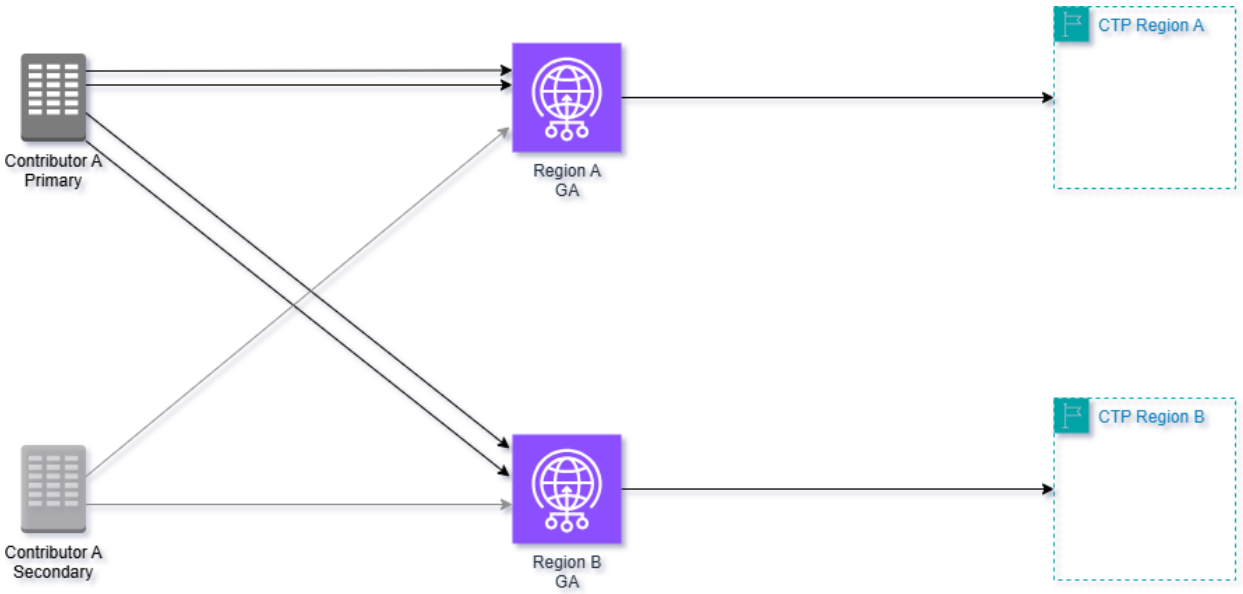
- **Contributor Primary DC**
    - Two (2) active connections to CTP Region A (primary publishing region).
    - Two (2) redundant connections to CTP Region B for resiliency.
- **Contributor Secondary DC**
    - At least one (1) connection to CTP Region A (active).

- One (1) connection to CTP Region B (passive), or
- May replicate the Primary DC connectivity model (i.e. multiple connections to both regions), subject to the Contributor's internal resilience requirements.

Characteristics:

- Ensures resilient connectivity from both Primary and Secondary Contributor data centers.
- Contributor Primary DC is the default only active DC
- Contributor Secondary DC provides standby and resilience in the event of regional or data center degradation.
- Failover and routing preference are managed entirely by the Contributor.

High-Level Diagram:



Public Connectivity Model 2: Active–Active

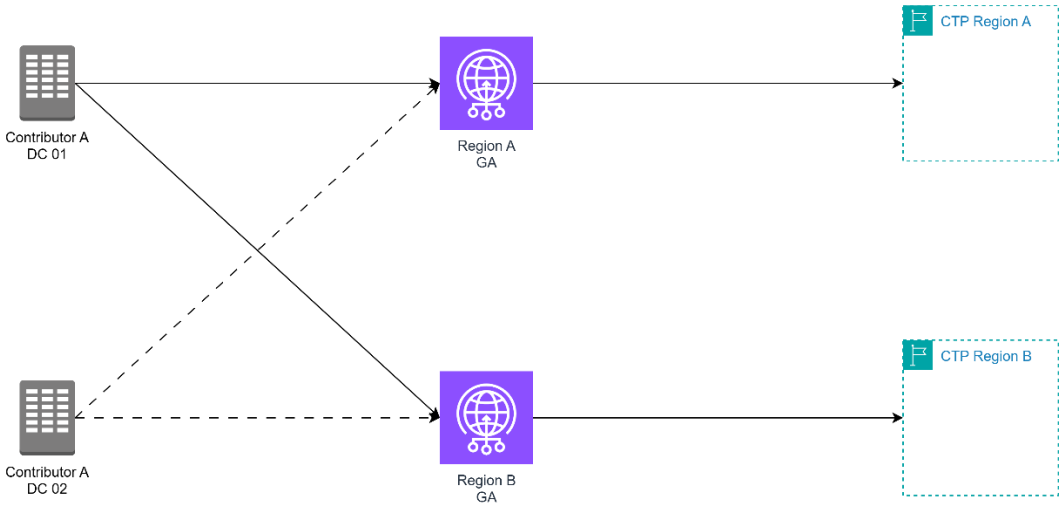
In this model, both Contributor data centers publish to both CTP regions.

- Primary DC → Region A and Region B (one path each)
- Secondary DC → Region A and Region B (one path each)

Characteristics:

- Maximizes resiliency through dual-region, dual-DC distribution.
- Load can be balanced across regions at the Contributor's discretion.
- Both regions receive data independently.

High-Level Diagram:



3.1.2 Private Connectivity

- Contributors connect via cross-connect into Equinix Fabric.
- Provides private, non-internet-based connectivity into the CTP AWS environment.
- Recommended for Contributors who do not offer internet-based distribution services.
- Redundant (red and blue) fabric path for resilience.

When a Contributor establishes private network connectivity to CTP via cross-connect into Equinix Fabric, a Letter of Authorization (LOA) is required. The LOA formally authorizes the provisioning of private connectivity between the Contributor's Equinix presence and CTP's network termination points.

The LOA is typically required to:

- Approve Equinix cross-connects or virtual connections into CTP-owned infrastructure
- Enable third-party carriers or Equinix to complete connectivity on behalf of both parties
- Validate the legal entities, service identifiers, and connection parameters involved

CTP will issue the LOA upon request as part of the connectivity onboarding process. Contributors must ensure that a valid LOA is in place before submitting Equinix Fabric or carrier provisioning orders.

3.1.3 Private Connectivity Design for Dual CTP Regions

Because CTP operates two independent AWS Regions in an active-active model, Contributors must provision separate Equinix Fabric connections to each region.

Key Requirements:

- One Fabric path to CTP Region A
- One Fabric path to CTP Region B
- Independent routing tables and monitoring per region

Dual-Publishing Consideration:

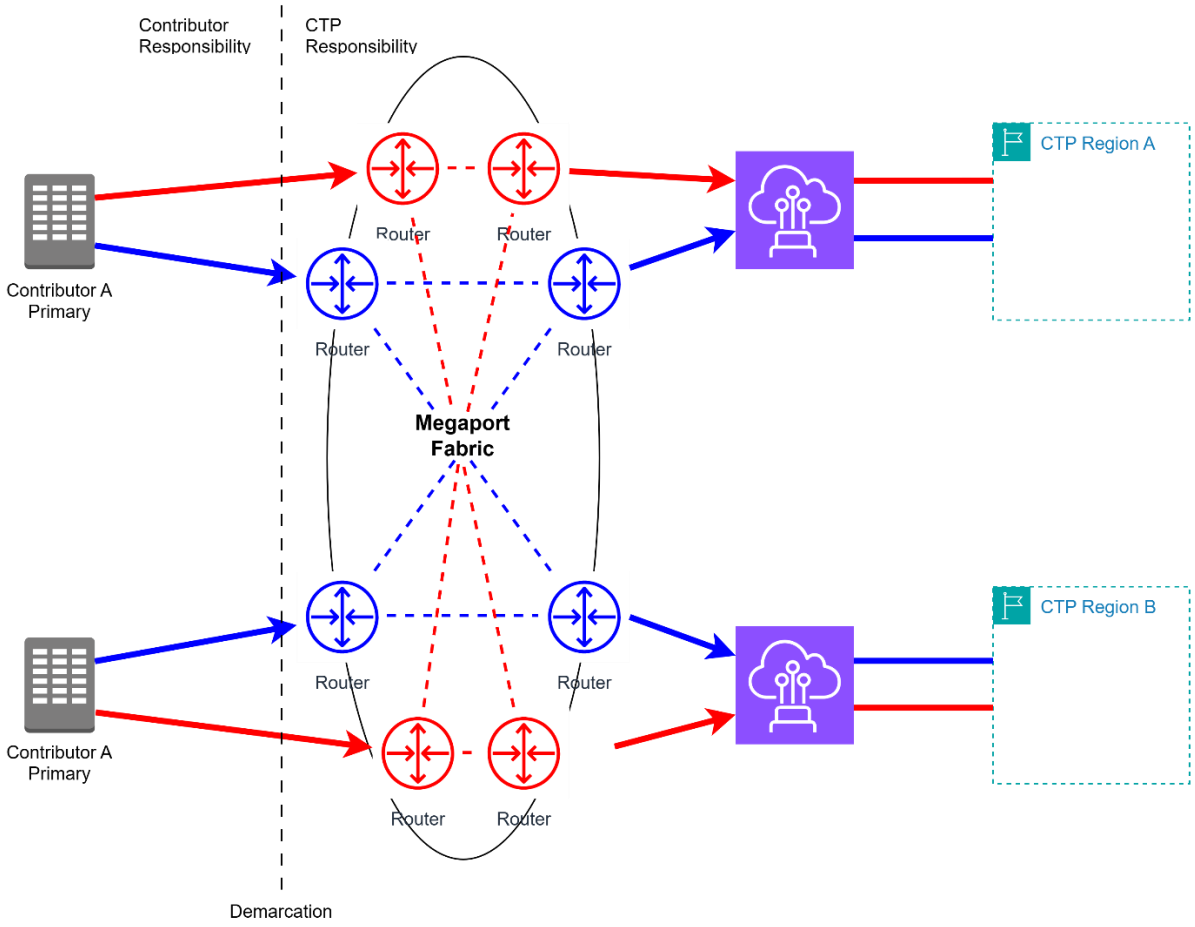
Contributors are encouraged to publish identical post-trade data to both regions, which requires:

- Dual routing paths (red and blue)
- Both regions advertising their static IP addresses
- Contributor FIX engines able to reach each region independently

Recommended Resiliency Model:

- Two redundant Fabric VCs per region (four total)
- Optional separate Cloud Routers or multi-VRF configuration
- No traffic flows between the two CTP regions; all publishing is region-specific

Connectivity Summary:



3.2. IP Addressing

Contributors will connect to the CTP using:

- Source IPs: Provided by Contributor
- Destination IPs & Ports: Provided by CTP during onboarding

IP whitelisting applies.

3.3. TCP Targets for Contributor FIX Gateway

Functional UAT TCP Prefixes (FIX Gateway)

Location	IP	Port
Region A	13.248.187.50 3.33.181.124	7101
Region B	*	7102

*To be updated

Production TCP Prefixes (FIX Gateway)

Location	*IP	Port
Region A		15001
Region B		15002

*IP addresses will be allocated per contributor

3.4. Network Requirements

- Latency-sensitive, persistent TCP connections
- Minimum MTU: 1500 bytes
- Redundant network paths recommended

3.5. Mutual TLS (mTLS)

3.5.1. Overview

All connectivity between Contributors and the CTP FIX Gateway shall be secured using Mutual Transport Layer Security (mTLS). This ensures bidirectional authentication, where both the Contributor and CTP authenticate each other during session establishment. mTLS is mandatory for all FIX sessions across both UAT and Production environments.

3.5.2. mTLS Requirements

Contributors must establish FIX sessions over TLS version 1.2 or higher with mutual authentication enabled, ensuring that a valid client certificate is presented during the TLS handshake. The CTP platform will present its own server certificate issued by a trusted Certificate Authority (CA). Any connection attempt will be rejected at the transport layer if the client certificate is invalid, expired, revoked, cannot be validated as part of a trusted certificate chain, or does not correspond to the registered Contributor identity.

Additionally, CTP maintains separate trust anchors (CA hierarchies) for UAT and Production environments, and certificates issued for one environment must not be used in another.

3.5.3. Certificate Signing Request (CSR) Requirements

Contributors must generate a Certificate Signing Request (CSR) that complies with CTP-defined cryptographic and identity standards prior to certificate issuance. The CSR must use a minimum key size of RSA 2048-bit (or an equivalent elliptic curve algorithm) and be signed using SHA-256 or a stronger hashing algorithm. The private key associated with the CSR must be securely generated and retained by the Contributor at all times and must not be shared with CTP.

The CSR must include a valid Distinguished Name (DN) containing the following attributes:

Field	Description
Common Name (CN) / Subject Alternative Names (SAN)	*SenderCompID* or the FQDN of the FIX gateway
Organization (O)	Contributor's legal company name
Organizational Unit (OU)	(Optional)
Country (C), State (ST), Locality (L)	Contributor's physical headquarters location.

4. Contacts

This section defines the primary points of contact for matters related to CTP network connectivity.

For general connectivity concerns please contact For general connectivity concerns please contact info@ets-connect.co.uk