Quintrix
A MINDLANCE COMPANY

Amazon Connect Integration

MODULE 3.6 – NETWORK CONFIGURATION

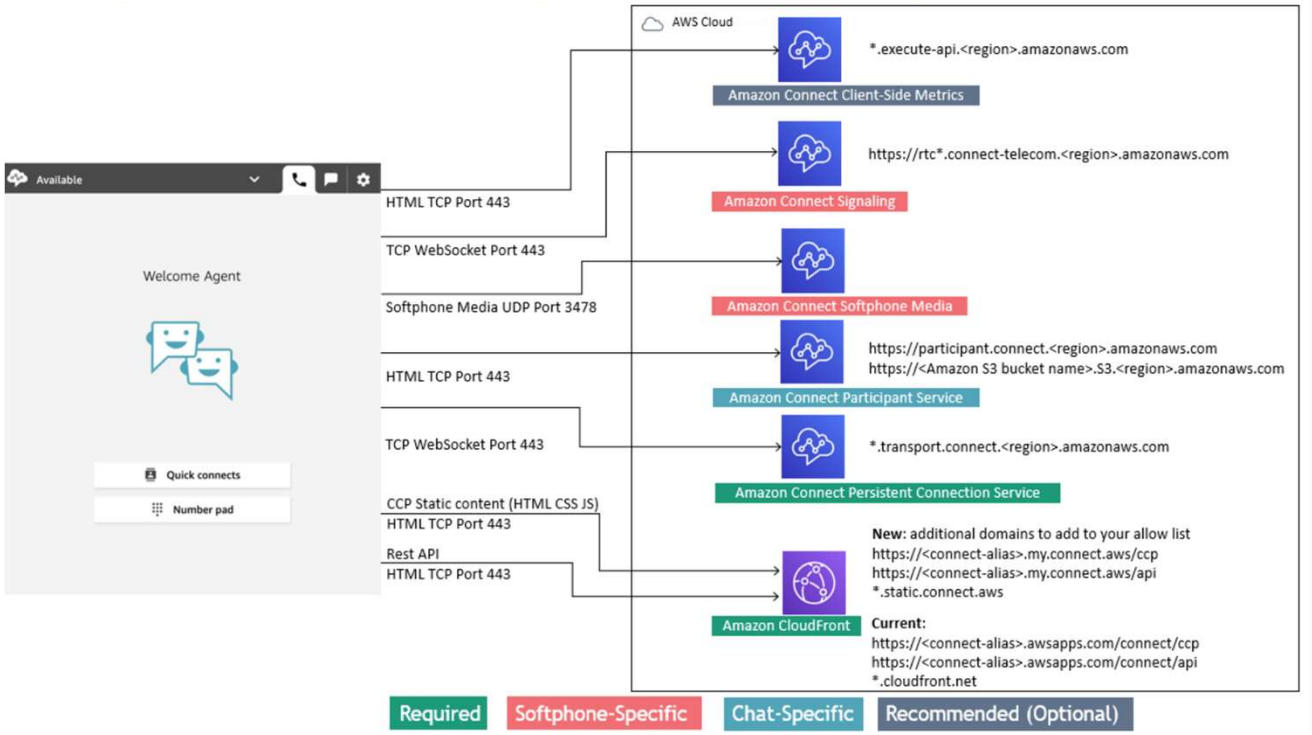
1095 Morris Ave, SUITE 101, Union NJ 07083
646-762-0305 | INFO@QUINTRIXSOLUTIONS.COM

Amazon Connect Networking

Setting up the network

Traditional VoIP solutions require you to allow both inbound and outbound for specific UDP port ranges and IPs, such as 80 and 443.

These solutions also apply to TCP. In comparison, the network requirements for using the Contact Control Panel (CCP) with a softphone are less intrusive. You can establish persistent outbound send/receive connections through your web browser. As a result, you don't need to open a client-side port to listen for inbound traffic.



Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

The following sections describe the two primary connectivity options for using the CCP.

Option 1: The recommended process is to replace Amazon EC2 and CloudFront IP range requirements with a domain allow list

Recommend trying Option 1 and testing it with more than 200 calls. Test for softphone errors, dropped calls, and conference/transfer functionality. If your error rate is greater than 2 percent, there might be an issue with proxy resolution. If that's the case, consider using Option 2.

Tip
If you don't see an entry for your region, use GLOBAL. For example, there isn't an entry for apsoutheast-1, so you would use GLOBAL.

Amazon Connect Networking

To allow traffic for Amazon EC2 endpoints, allow access for the URL and port, as shown in the first row of the following table. Do this instead of allowing all of the IP address ranges listed in the ipranges.json file. You get the same benefit using a domain for CloudFront, as shown in the second row of the following table.

Domain/URL allow list	AWS Region	Ports	Direction	Traffic
rtc*.connecttelecom. {*region*}.amazonaws.com Please see the note following this table.	Replace {region} with the Region where your Amazon Connect instance is located	443 (TCP)	Outbound	Send/Receive
New: additional domains to add to your allow list, please see the note following this table {*myInstanceName*}.my.connect.aws/ ccp-v2 {*myInstanceName*}.my.connect.aws/ api *.static.connect.aws **Current:** {*myInstanceName*}.awsapps.com/ connect/ccp-v2 {*myInstanceName*}.awsapps.com/ connect/api *.cloudfront.net	Replace {*myInstanceName*} with the alias of your Amazon Connect instance	443 (TCP)	Outbound	Send/Receive

Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

Domain/URL allow list	AWS Region	Ports	Direction	Traffic
*.execute-api. {*region*}.amazonaws.com	Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	Outbound	Send/Receive
participant.connect. {*region*}.amazonaws.com	Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	Outbound	Send/Receive
*.transport.connect. {*region*}.amazonaws.com	Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	Outbound	Send/Receive
{*Amazon S3 bucket name*}.s3. {*region*}.amazonaws.com	Replace *Amazon S3 bucket name* with the name of the location where you store attachments. Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	Outbound	Send/Receive

Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

Domain/URL allow list	AWS Region	Ports	Direction	Traffic
TurnNlb-*.elb.{*region*}.amazonaws.com To instead add specific endpoints to your allow list based on Region, see NLB endpoints (p. 365).	Replace {*region*} with the location of your Amazon Connect instance	3478 (UDP)	Outbound	Send/Receive

Note

IT administrators: In the future, the access URL is going to change. For the release schedule and technical details.

Amazon Connect Networking

Note

The new region telecom endpoints follow a different format. Here's a complete list of telecom endpoints:

Region	Domain/URL
us-west-2	rtc*.connect-telecom.uswest-2.amazonaws.com
us-east-1	rtc*.connect-telecom.useast-1.amazonaws.com
eu-central-1	rtc*.connect-telecom.eucentral-1.amazonaws.com
ap-southeast-2	rtc*.connect-telecom.apsoutheast-2.amazonaws.com
ap-northeast-1	rtc*.connect-telecom.apnortheast-1.amazonaws.com
eu-west-2	rtc.cell-1.prod.euwest-2.prod.connect.aws.a2z.com
ap-southeast-1	rtc.cell-1.prod.apsoutheast-1.prod.connect.aws.a2z.com

Tip

When using rtc*.connect-telecom.{*region*}.amazonaws.com and https://myInstanceName.awsapps.com, in certain proxy applications, web socket handling may impact functionality. Be sure to test and validate before deploying to a production environment.

Amazon Connect Networking

NLB endpoints

The following table lists the specific endpoints for the Region the Amazon Connect instance is in. If you don't want to use the TurnNlb-*.elb.{*region*}.amazonaws.com wildcard, you can use add these endpoints to your allow list instead.

Region	Turn Domain/URL
us-west-2	TurnNlb-8d79b4466d82ad0e.elb.us-west-2.amazonaws.com TurnNlb-dbc4ebb71307fda2.elb.us-west-2.amazonaws.com
us-east-1	TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com
eu-central-1	TurnNlb-ea5316ebe2759cbc.elb.eu-central-1.amazonaws.com

Amazon Connect Networking

NLB endpoints (cont)

Region	Turn Domain/URL
ap-southeast-2	TurnNlb-93f2de0c97c4316b.elb.ap-southeast-2.amazonaws.com
ap-northeast-1	TurnNlb-3c6ddabcbeb821d8.elb.ap-northeast-1.amazonaws.com
eu-west-2	TurnNlb-1dc64a459ead57ea.elb.eu-west-2.amazonaws.com
ap-southeast-1	TurnNlb-261982506d86d300.elb.ap-southeast-1.amazonaws.com

Amazon Connect Networking

Option 2: Allow IP address ranges

The second option (not recommended) relies on using an allow list, also known as whitelisting, the IP addresses used by

Amazon Connect. You create this allow list using the IP addresses in the AWS ip-ranges.json file.

IP-Ranges entry	AWS Region	Ports/Protocols	Direction	Traffic
AMAZON_CONNECT	GLOBAL and Region where your Amazon Connect instance is located (add GLOBAL AND any region-specific entry to your allow list)	3478 (UDP)	OUTBOUND	SEND/RECEIVE
EC2	GLOBAL and Region where your Amazon Connect instance is located (GLOBAL only if a region-specific entry doesn't exist)	443 (TCP)	OUTBOUND	SEND/RECEIVE
CLOUDFRONT	Global*	443 (TCP)	OUTBOUND	SEND/RECEIVE

Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

Amazon Connect IP address ranges

In the AWS ip-ranges.json file, the whole /19 IP address range is owned by Amazon Connect. All traffic to and from the /19 range comes to and from Amazon Connect.

The /19 IP address range isn't shared with other services. It's for the exclusive use to Amazon Connect globally.

In the AWS ip-ranges.json file, you can see the same range listed twice. For example:

```
{ "ip_prefix": "15.193.0.0/19",
"region": "GLOBAL",
"service": "AMAZON"
},
{
"ip_prefix": "15.193.0.0/19",
"region": "GLOBAL",
"service": "AMAZON_CONNECT"
},
```

Amazon Connect Networking

AWS always publishes any IP range twice: one for the specific service, and one for “AMAZON” service. There could even be a third listing for a more specific use case within a service.

When there are new IP address ranges supported for Amazon Connect, they are added to the publicly available ip-ranges.json file. They are kept for a minimum of 30 days before they are used by the service. After 30 days, softphone traffic through the new IP address ranges increases over the subsequent two weeks. After two weeks, traffic is routed through the new ranges equivalent to all available ranges.

Amazon Connect Networking

Stateless firewalls
If you're using a stateless firewall for both options, use the requirements described in the previous sections. Then you must add to your allow list the ephemeral port range used by your browser.

IP-Range entry
AMAZON_CONNECT

Port
49152-65535 (UDP)

Direction
INBOUND

Traffic
SEND/RECEIVE

Amazon Connect Networking

Allow DNS resolution for softphones

If you already added Amazon Connect IP ranges to your allow list, and you don't have any restriction on DNS name resolution, then you don't need to add **TurnNlb-*.elb.{*region*}.amazonaws.com** to your allow list.

• To check whether there are restrictions on DNS name resolution, while on your network, use the nslookup command. For example:

nslookup TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com

If you can't resolve the DNS, you must add the TurnNLB endpoints listed above (p. 365) or **TurnNlb-*.elb.{*region*}.amazonaws.com** to your allow list.

If you don't allow this domain, your agents will get the following error in their Contact Control Panel (CCP) when they try to answer a call:

Failed to establish softphone connection. Try again or contact your administrator with the following: Browser unable to establish media channel with turn:TurnNlb-xxxxxxxxxxxxx.elb.{*region*}.amazonaws.com:3478?transport=udp

Amazon Connect Networking

Port and protocol considerations

Consider the following when implementing your network configuration changes for Amazon Connect:

• You need to allow traffic for all addresses and ranges for the Region in which you created your Amazon Connect instance.

• If you are using a proxy or firewall between the CCP and Amazon Connect, increase the SSL certificate cache timeout to cover the duration of an entire shift for your agents, Do this to avoid connectivity issues with certificate renewals during their scheduled working time. For example, if your agents are scheduled to work 8 hour shifts that include breaks, increase the interval to 8 hours plus time for breaks and lunch.

Amazon Connect Networking

Port and protocol considerations

Consider the following when implementing your network configuration changes for Amazon Connect:

• When opening ports, Amazon EC2 and Amazon Connect require only the ports for endpoints in the same Region as your instance. CloudFront, however, serves static content from an edge location that has the lowest latency in relation to where your agents are located. IP range allow lists for CloudFront are global and require all IP ranges associated with "service": "CLOUDFRONT" in ip-ranges.json.

• Once ip-ranges.json is updated, the associated AWS service will begin using the updated IP ranges after 30 days. To avoid intermittent connectivity issues when the service begins routing traffic to the new IP ranges, be sure to add the new IP ranges to your allow list, within 30 days from the time they were added to ip-ranges.json.

• If you are using a custom CCP with the Amazon Connect Streams API, you can create a media-less CCP that does not require opening ports for communication with Amazon Connect, but still requires ports opened for communication with Amazon EC2 and CloudFront.

Amazon Connect Networking

Region selection considerations

Amazon Connect Region selection is contingent upon data governance requirements, use case, services available in each Region, and latency in relation to your agents, contacts, and external transfer endpoint geography.

• **Agent location/network**—CCP connectivity traverses the public WAN, so it is important that the workstation has the lowest latency and fewest hops possible, specifically to the AWS Region where your resources and Amazon Connect instance are hosted. For example, hub and spoke networks that need to make several hops to reach an edge router can add latency and reduce the quality of experience.

When you set up your instance and agents, make sure to create your instance in the Region that is geographically closest to the Region where you create your instance. If you need to set up an instance in a specific Region to comply with company policies or other regulations, choose the configuration that results in the fewest network hops between your agent computers and your Amazon Connect instance.

Amazon Connect Networking

Region selection considerations

• **Location of your callers**—Because calls are anchored to your Amazon Connect Region endpoint, they are subject to PSTN latency. Ideally your callers and transfer endpoints are geographically located as closely as possible to the AWS Region where your Amazon Connect instance is hosted for lowest latency.

For optimal performance, and to limit the latency for your customers when they call in to your contact center, create your Amazon Connect instance in the Region that is geographically closest to where your customers call from. You might consider creating multiple Amazon Connect instances and providing contact information to customers for the number that is closest to where they call from.

• **External transfers**—from Amazon Connect remain anchored to your Amazon Connect Region endpoint for the duration of the call. Per-minute usage continues to accrue until the call is disconnected by the recipient of the transferred call. The call is not recorded after the agent drops or the transfer completes. The CTR data and associated call recording of a transferred call are generated after the call is terminated. Whenever possible, don't transfer calls that could be transferred back into Amazon Connect, known as circular transfers, to avoid compounding PSTN latency.

Amazon Connect Networking

Agents using Amazon Connect remotely

Remote agents, those that use Amazon Connect from a location other than those connected to your organization's main network, may experience issues relating to their local network if they have an unstable connection, packet loss, or high latency. This is compounded if a VPN is required to access resources. Ideally, the agents are located close to the AWS Region where your AWS resources and Amazon Connect instance are hosted and have a stable connection to the public WAN.

Amazon Connect Networking

Rerouting audio

When rerouting audio to an existing device, consider the location of the device in relation to your Amazon Connect Region. This is so you can account for potential additional latency. If you reroute your audio, whenever there is a call intended for the agent, an outbound call is placed to the configured device. When the agent answers the device, that agent is connected with the caller. If the agent does not answer their device, they are moved into a missed contact state until they or a supervisor changes their state back to available.

Amazon Connect Networking

Using AWS Direct Connect

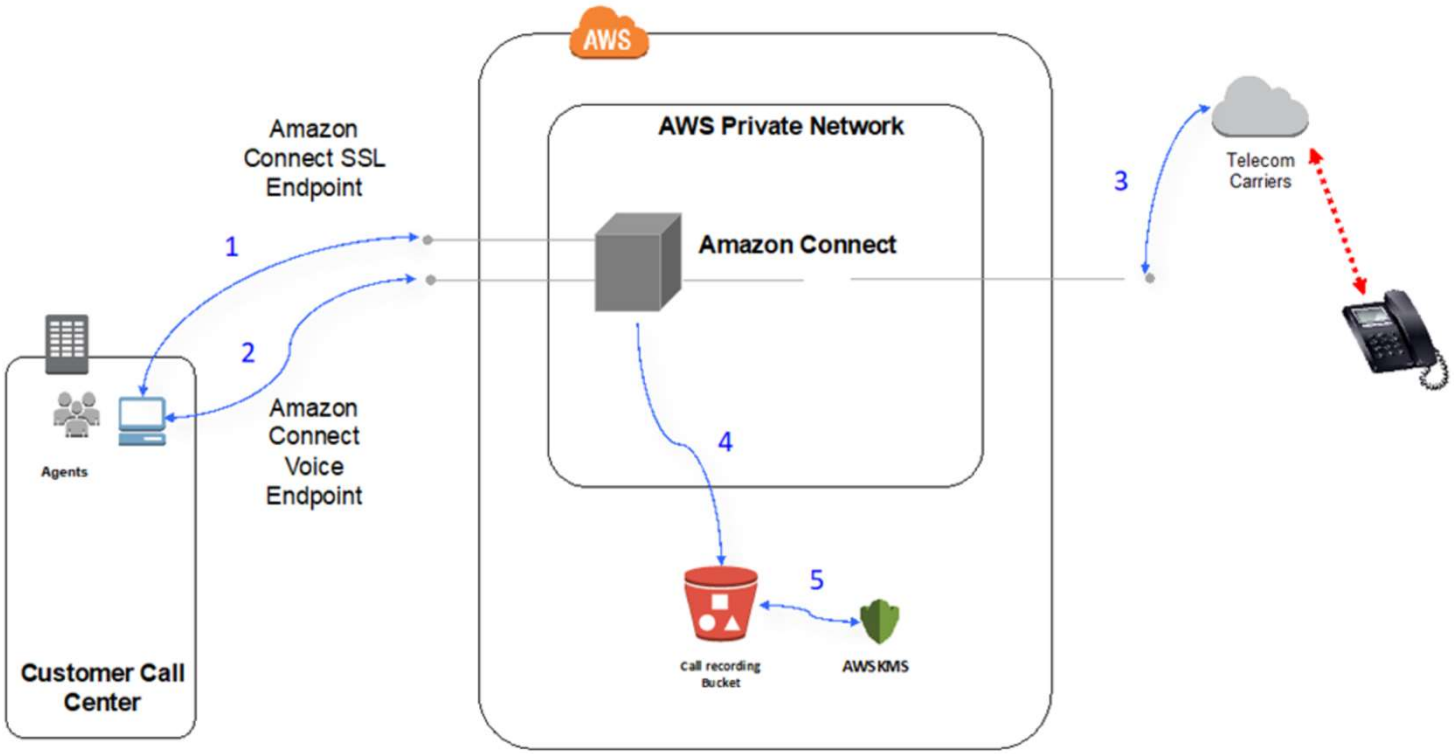
Contact Control Panel (CCP) network connectivity issues are most often rooted in your route to AWS via private WAN/LAN, ISP, or both. While AWS Direct Connect does not solve issues specific to private LAN/ WAN traversal to your edge router, it can help solve for latency and connectivity issues between your edge router and AWS resources. AWS Direct Connect provides a durable, consistent connection rather than relying on your ISP to dynamically route requests to AWS resources. It also allows you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN.

Amazon Connect Networking

Detailed network paths for Amazon Connect

Voice calls

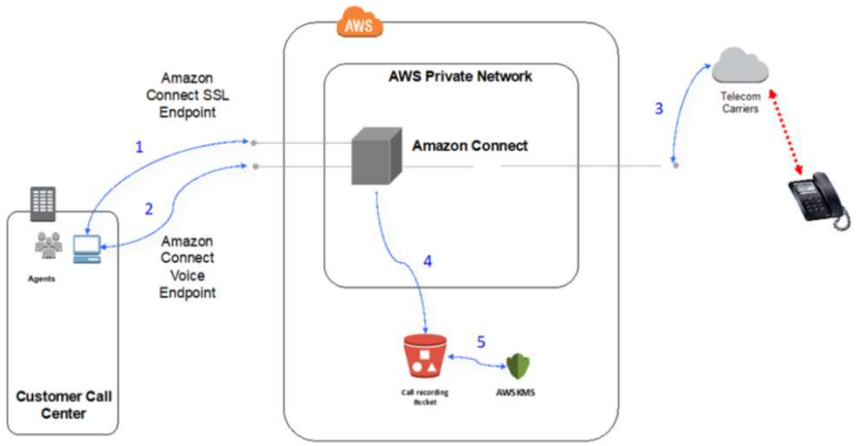
The following diagram shows how voice calls flow through Amazon Connect



Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

1. Users access the Amazon Connect application using a web browser. All communications are encrypted in transit using TLS.
2. Users establish voice connectivity to Amazon Connect from their browser using WebRTC. Signaling communication is encrypted in transit using TLS. Audio is encrypted in transit using SRTP.
3. Voice connectivity to traditional phones (PSTN) is established between Amazon Connect and AWS's telecommunications carrier partners using private network connectivity. In cases where shared network connectivity is used, signaling communication is encrypted in transit using TLS and audio is encrypted in transit using SRTP.
4. Call recordings are stored in your Amazon S3 bucket that Amazon Connect has been given permissions to access. This data is encrypted between Amazon Connect and Amazon S3 using TLS.
5. Amazon S3 server-side encryption is used to encrypt call recordings at rest using a customer-owned KMS key.

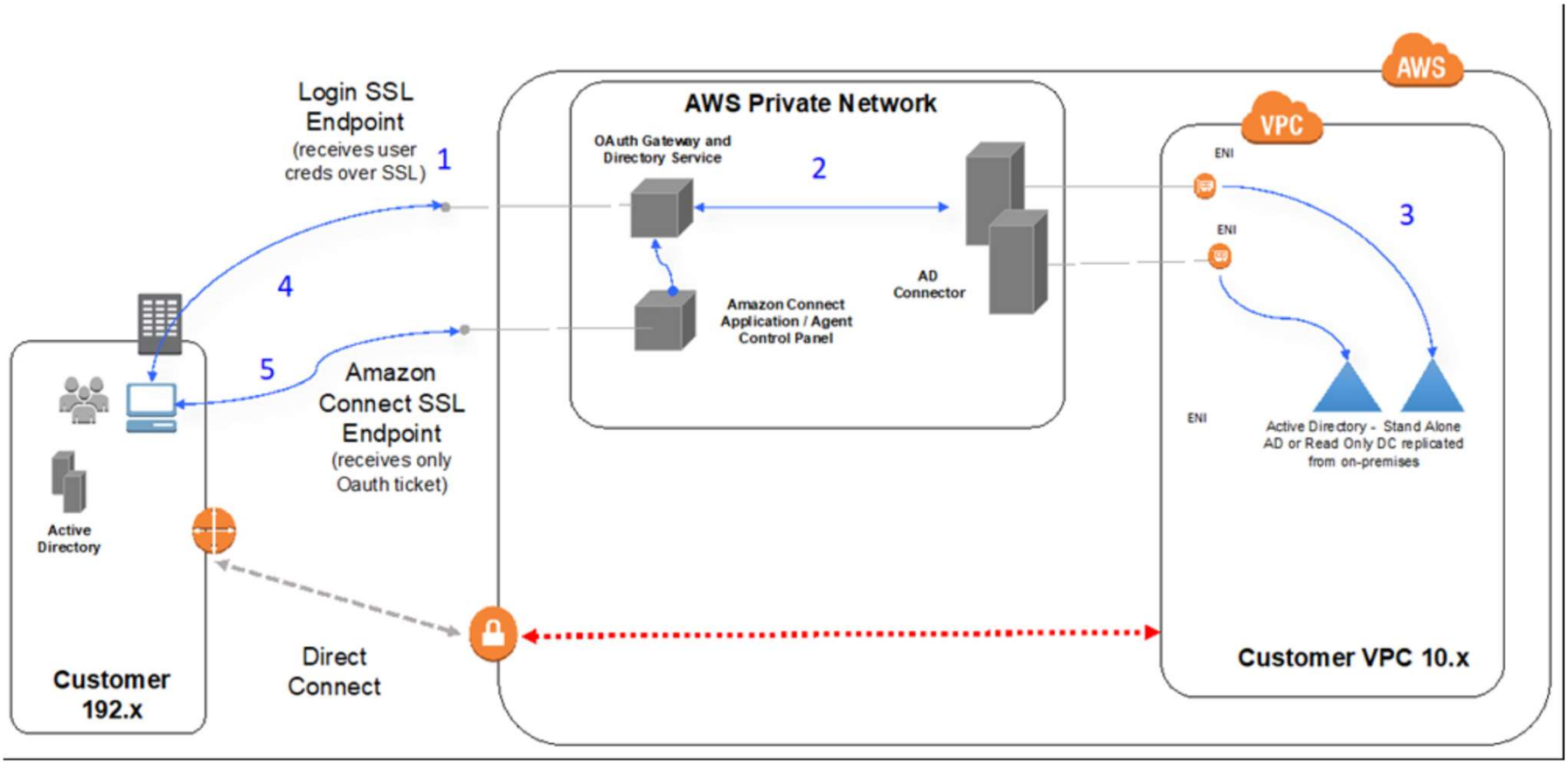


Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

Authentication

The following diagram shows using the AD Connector with AWS Directory Service to connect to an existing customer Active Directory installation. The flow is similar to using AWS Managed Microsoft AD.



Quintrix
A MINDLANCE COMPANY

Amazon Connect Networking

1. The user's web browser initiates authentication to an OAuth gateway over TLS via the public internet with user credentials (Amazon Connect login page).
2. OAuth gateway sends the authentication request over TLS to AD Connector.
3. AD Connector does LDAP authentication to Active Directory.
4. The user's web browser receives OAuth ticket back from gateway based on authentication request.
5. The client loads the Contact Control Panel (CCP). The request is over TLS and uses OAuth ticket to identify user/directory.

Amazon Connect Networking

Using Amazon Connect in a VDI environment

Virtual Desktop Infrastructure (VDI) environments add another layer of complexity to your solution that warrants separate POC efforts and performance testing to optimize. The Amazon Connect Contact Control Panel (CCP) can operate in thick, thin, and zero client VDI environments as any other WebRTC based browser application does, and the configuration/support/optimization is best handled by your VDI support team. That being said, the following is a collection of considerations and best practices that have been helpful for our VDI-based customers.

- **Location of your agents**—Ideally, there are as few hops as possible with the lowest round trip time between the location from which your agents use the CCP and the VDI host location.

- **Host location of your VDI solution**—Ideally, your VDI host location is on the same network segment as your agents, with as few hops as possible from both internal resources as well as an edge router. You also want the lowest round-trip time possible to both WebRTC and Amazon EC2 range endpoints

Amazon Connect Networking

Using Amazon Connect in a VDI environment

- **Network**—Each hop that traffic goes through between endpoints increases the possibility of failure and adds opportunity to introduce latency. VDI environments are particularly susceptible to call quality issues if the underlying route is not optimized or the pipe isn't either fast or wide enough. While AWS Direct Connect can improve call quality from the edge router to AWS, it will not address internal routing issues. You may need to upgrade or optimize your private LAN/WAN or redirect to an external device to circumvent call audio issues. In most scenarios, if this is required, the CCP is not the only application that is having issues.

- **Dedicated resources**—at the Network and desktop level are recommended to prevent an impact to available agent resources from activities, such as backups and large file transfers. One way to prevent resource contention is by restricting the desktop access to Amazon Connect users who will be using their environment similarly, instead of sharing resources with other business units who may use those resources differently.

Amazon Connect Networking

Using Amazon Connect in a VDI environment

- **Using a soft phone with remote connections**—in VDI environments can cause impact to audio quality. If your agents connect to a remote endpoint and operates in that environment, we recommend either rerouting audio to an external E.164 endpoint or connecting the media through the local device and then signaling through the remote connection. You can build a custom CCP with the Amazon Connect Streams API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media.

Amazon Connect Networking

CCP connectivity

When an agent logs in, the CCP attempts to connect to the Amazon EC2 signaling endpoints listed in the AWS ipranges.json file, Amazon Connect for media, and CloudFront for web artifacts such as images. When the agent logs out or the browser is closed, endpoints are reselected when the agent next logs in. If a connection to Amazon EC2 or Amazon Connect fails, errors display on the CCP. If a connection to CloudFront fails, web elements such as buttons and icons, or even the page itself fails to load correctly.

Outbound calls

- When an outbound call is placed, the event signal is sent to the Amazon EC2 endpoint, which then communicates with Amazon Connect to place the call. Upon a successful dial attempt, the agent is bridged in, which anchors the call to the agent's Amazon Connect endpoint. Any external transfers or conferences also uses the anchor until the call is disconnected. Anchoring can help reduce PSTN latency.

Amazon Connect Networking

CCP connectivity

Inbound calls

- When an inbound call is received, the call is anchored to an Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.
- When an agent is available, the call is pushed through via a new Amazon EC2 connection to their browser and offered to the agent.
- When the agent accepts the call and either the external device has been answered or the CCP determines it can receive a call, a connection to Amazon Connect is established for call media to the agent.

Amazon Connect Networking

CCP connectivity

Transferred calls

- When a call is transferred, the transfer event that signals to place an outbound call to the specified transfer destination is sent to Amazon EC2, which then communicates with Amazon Connect to place the call.
- When the call is connected, the agent is bridged in, anchoring the call to the agent's existing Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.
- If the agent hangs up after the call is bridged, the agent's connection to the call is terminated, but Amazon Connect hangs on to the call at the Amazon Connect anchor point until there is a far side disconnect. When the call is disconnected, CTRs and associated recordings are generated and made available for the call.

Amazon Connect Networking

CCP connectivity

Missed calls

- If the call is waiting on an agent, customer queue flow logic is used until an agent is available and the call has been successfully routed to that agent.
- If the agent does not accept the call, the agent moves into a Missed Call state and is unable to take calls until the agent, or a call center manager, changes their status to Available again. The caller does not hear ringing while the call is waiting for the agent, and continues to hold until connected with an agent as defined in the customer queue flow logic.

Panic logout

- If the browser window where the CCP is running is closed, the call remains connected, but opening the browser and logging back in will not allow you to re-establish the media connection. You are still able to transfer or end the call, but no audio path is established between the agent and caller.

Amazon Connect Networking

Use an allow list for integrated applications

All domains that embed the CCP for a particular instance must be explicitly allowed for cross-domain access to the instance. For example, to integrate with Salesforce, you must place your Salesforce Visualforce domain in an allow list.

To allow a domain URL

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from **Instance Alias**.
3. In the navigation pane, choose **Application integration**.
4. Choose **Add origin**.
5. Type the URL and choose **Add**.

Amazon Connect Networking

Exercise:

Use an allow list for integrated applications