Google Cloud

Operational environments

Projects and Conversational Agents (1 of 2)

Ensure that you understand the difference between projects and Conversational Agents, and that you can implement both.

Projects

A logical collection of Cloud resources that delegate the same IAM access controls to each resource.

For CES, we recommend:

- One project containing all non-production CES resources (with dev and test environments).
- One project containing all production CES resources (with staging and prod environments).

Projects and Conversational Agents (1 of 2)

Ensure that you understand the difference between projects and Conversational Agents, and that you can implement both.

Projects

A logical collection of Cloud resources that delegate the same IAM access controls to each resource.

For CES, we recommend:

- One project containing all non-production CES resources (with dev and test environments).
- One project containing all production CES resources (with staging and prod environments).

Projects and Conversational Agents (1 of 2)

Ensure that you understand the difference between projects and Conversational Agents, and that you can implement both.

Projects

A logical collection of Cloud resources that delegate the same IAM access controls to each resource.

For CES, we recommend:

- One project containing all non-production CES resources (with dev and test environments).
- One project containing all production CES resources (with staging and prod environments).

Projects and Conversational Agents (2 of 2)

Ensure that you understand the difference between projects and Conversational Agents, and that you can implement both.

Projects

A logical collection of Cloud resources that delegate the same IAM access controls to each resource.

For CES, we recommend:

- One project containing all non-production CES resources (with dev and test environments).
- One project containing all production CES resources (with staging and prod environments).

Conversational Agents

A logical collection of interactions targeting fulfillments for a particular type of end-user.

A Conversational Agent has built-in environments, so you usually only need one Conversational Agent in each of your projects.

If Conversational Agents have different user groups or development teams, use separate projects for access control.

Projects and Conversational Agents (2 of 2)

Ensure that you understand the difference between projects and Conversational Agents, and that you can implement both.

Projects

A logical collection of Cloud resources that delegate the same IAM access controls to each resource.

For CES, we recommend:

- One project containing all non-production CES resources (with dev and test environments).
- One project containing all production CES resources (with staging and prod environments).

Conversational Agents

A logical collection of interactions targeting fulfillments for a particular type of end-user.

A Conversational Agent has built-in environments, so you usually only need one Conversational Agent in each of your projects.

If Conversational Agents have different user groups or development teams, use separate projects for access control.

Client communications with the Conversational Agents API (1 of 2)

Manage client communication with the Conversational Agents API using public or private methods.

Public

No additional infrastructure is required.

Your Conversational Agents clients will connect to Google Cloud's public Conversational Agents API endpoints.

The endpoints are encrypted with TLS and use a service account to authenticate and authorize with OAuth credentials.

Client communications with the Conversational Agents API (1 of 2)

Manage client communication with the Conversational Agents API using public or private methods.

Public

No additional infrastructure is required.

Your Conversational Agents clients will connect to Google Cloud's public Conversational Agents API endpoints.

The endpoints are encrypted with TLS and use a service account to authenticate and authorize with OAuth credentials.

Client communications with the Conversational Agents API (2 of 2)

Manage client communication with the Conversational Agents API using public or private methods.

Public

No additional infrastructure is required.

Your Conversational Agents clients will connect to Google Cloud's public Conversational Agents API endpoints.

The endpoints are encrypted with TLS and use a service account to authenticate and authorize with OAuth credentials.

Private

Requires adding a private interconnect to a Google Cloud VPC.

Add a Private Service Connect for Google Cloud APIs to this VPC.

Make sure the PSC's IP address is routable from your private network.

Add Conversational Agents hostnames to internal DNS that resolve to the PSC's IP address.

Client communications with the Conversational Agents API (2 of 2)

Manage client communication with the Conversational Agents API using public or private methods.

Public

No additional infrastructure is required.

Your Conversational Agents clients will connect to Google Cloud's public Conversational Agents API endpoints.

The endpoints are encrypted with TLS and use a service account to authenticate and authorize with OAuth credentials.

Private

Requires adding a private interconnect to a Google Cloud VPC.

Add a Private Service Connect for Google Cloud APIs to this VPC.

Make sure the PSC's IP address is routable from your private network.

Add Conversational Agents hostnames to internal DNS that resolve to the PSC's IP address.

Client communications with the Conversational Agents API (2 of 2)

Manage client communication with the Conversational Agents API using public or private methods.

Public

No additional infrastructure is required.

Your Conversational Agents clients will connect to Google Cloud's public Conversational Agents API endpoints.

The endpoints are encrypted with TLS and use a service account to authenticate and authorize with OAuth credentials.

Private

Requires adding a private interconnect to a Google Cloud VPC.

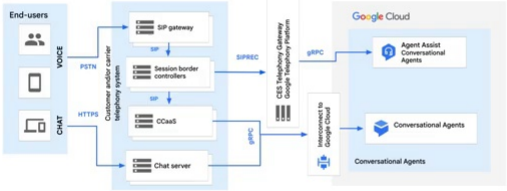
Add a Private Service Connect for Google Cloud APIs to this VPC.

Make sure the PSC's IP address is routable from your private network.

Add Conversational Agents hostnames to internal DNS that resolve to the PSC's IP address.

Customer to Agent ingress routing (1 of 5)

Communications flow between an end user and a Conversational Agent.

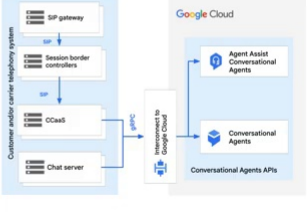


Customer to Agent ingress routing (2 of 5)

How does this work in an environment?

No access to public API endpoints

- Setup a private connection between your data center and Google Cloud.
- Communicate via a Private Service Connect in the VPC.
- Conversational Agnets uses internal DNS to resolve hostnames.

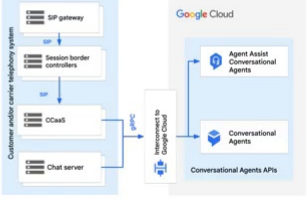


Customer to Agent ingress routing (2 of 5)

How does this work in an environment?

No access to public API endpoints

- Setup a private connection between your data center and Google Cloud.
- Communicate via a Private Service Connect in the VPC.
- Conversational Agnets uses internal DNS to resolve hostnames.

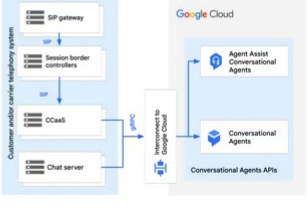


Customer to Agent ingress routing (2 of 5)

How does this work in an environment?

No access to public API endpoints

- Setup a private connection between your data center and Google Cloud.
- Communicate via a Private Service Connect in the VPC.
- Conversational Agnets uses internal DNS to resolve hostnames.



Customer to Agent ingress routing (3 of 5)

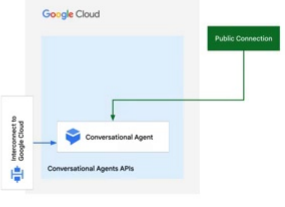
How does this work in an environment?

If Conversational Agents are in scope:

Conversational Agents secures its **public** API endpoints using mechanisms such as:

- TLS
- OAuth
- VPC service controls

A Cloud **Interconnect** can also be used if private connectivity is a requirement from customer.



Customer to Agent ingress routing (3 of 5)

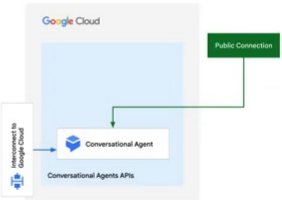
How does this work in an environment?

If Conversational Agents are in scope:

Conversational Agents secures its **public** API endpoints using mechanisms such as:

- TLS
- OAuth
- VPC service controls

A Cloud **Interconnect** can also be used if private connectivity is a requirement from customer.



Customer to Agent ingress routing (4 of 5)

Communications flow between an end user and a Conversational Agent.

If Agent Assist is in scope

- Determine if you're implementing
  - A Google Cloud CCaaS
  - Hybrid on-premise Contact Center + CES on Google Cloud solution
- Check for Cloud-native integration with Google CES and Conversational Agents API's Agent Assist functionality.
- This lets the system share conversations based on its configuration.

Customer to Agent ingress routing (4 of 5)

Communications flow between an end user and a Conversational Agent.

If Agent Assist is in scope

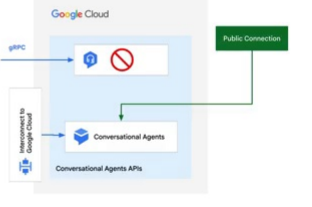
- Determine if you're implementing
  - A Google Cloud CCaaS
  - Hybrid on-premise Contact Center + CES on Google Cloud solution
- Check for Cloud-native integration with Google CES and Conversational Agents API's Agent Assist functionality.
- This lets the system share conversations based on its configuration.

Customer to Agent ingress routing (5 of 5)

Communications flow between an end user and a Conversational Agent.

If Agent Assist is not in scope

- Determine how audio is to be sent to Conversational Agents.
- You can use an API via gRPC requests.
- Or use a service that can transcode to gRPC.
- Note that SIPREC endpoint is public only, but is secured via mutual TLS.

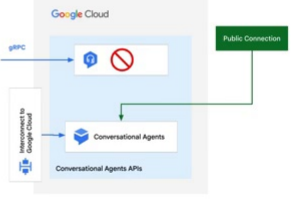


Customer to Agent ingress routing (5 of 5)

Communications flow between an end user and a Conversational Agent.

If Agent Assist is not in scope

- Determine how audio is to be sent to Conversational Agents.
- You can use an API via gRPC requests.
- Or use a service that can transcode to gRPC.
- Note that SIPREC endpoint is public only, but is secured via mutual TLS.



Customer to Agent ingress routing (5 of 5)

Communications flow between an end user and a Conversational Agent.

If Agent Assist is not in scope

- Determine how audio is to be sent to Conversational Agents.
- You can use an API via gRPC requests.
- Or use a service that can transcode to gRPC.
- Note that SIPREC endpoint is public only, but is secured via mutual TLS.