Genesys Authentication Private Edition Guide

Architecture

10/2/2024

Contents

Learn about Genesys Authentication architecture

Related documentation:

-
-
-

RSS:

- For private edition

Introduction

The diagram below shows the architecture of the Genesys Authentication components:

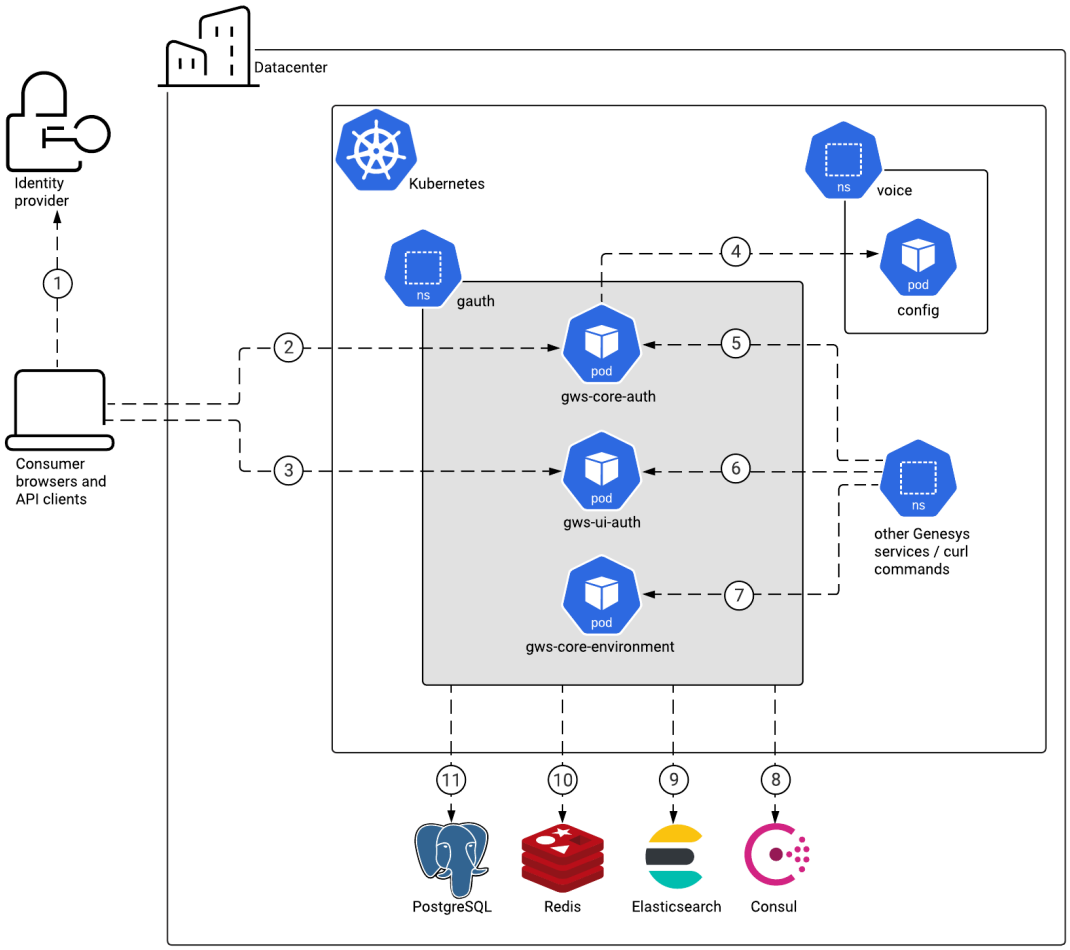
- Authentication API service
- Authentication UI service
- Environment API service

For information about the overall architecture of Genesys Multicloud CX private edition, see the high-level Architecture page.

See also High availability and disaster recovery for information about high availability/disaster recovery architecture.

Architecture diagram — Connections

The numbers on the connection lines refer to the connection numbers in the table that follows the diagram. The direction of the arrows indicates where the connection is initiated (the source) and where an initiated connection connects to (the destination), from the point of view of Genesys Authentication as a service in the network.



Connections table

The connection numbers refer to the numbers on the connection lines in the diagram. The **Source**, **Destination**, and **Connection Classification** columns in the table relate to the direction of the arrows in the Connections diagram above: The source is where the connection is initiated, and the destination is where an initiated connection connects to, from the point of view of Genesys Authentication as a service in the network. *Egress* means the Genesys Authentication service is the source, and *Ingress* means the Genesys Authentication service is the destination. *Intra-cluster* means the connection is between services in the cluster.

Connection	Source	Destination	Protocol	Port	Classification	Data that travels on this connection
1	Consumer browser	Identity provider	HTTPS	443	Ingress	For single sign-on support, the

Connection	Source	Destination	Protocol	Port	Classification	Data that travels on this connection
						consumer's browser communicates with the identity provider (IdP).
2	Consumer browser and API clients	Authentication Service	HTTPS	443	Ingress	Consumer browsers and API clients use one of the supported OAuth 2.0 grant types to authenticate. See the Authentication API for details.
3	Consumer browser	Authentication UI	HTTPS	443	Ingress	If an application uses the Genesys Authentication UI, users are redirected to the log in page. See for details.
4	Authentication Service	Voice Platform Configuration Server	TCP	8888	Ingress	Data from Configuration Server.
5	Other Genesys services	Authentication Service	HTTP/HTTPS	80/443	Ingress	Genesys services authenticate with Authentication API. Enable Transport Layer Security for this connection with in the **values.yaml** file.
6	Other	Authentication	HTTP/HTTPS	80/443	Ingress	Applications

Connection	Source	Destination	Protocol	Port	Classification	Data that travels on this connection
	Genesys services	UI				that use the Genesys Authentication UI. Enable Transport Layer Security for this connection with in the **values.yaml** file.
7	Other Genesys services / curl commands	Environment Service	HTTP/HTTPS	80/443	Ingress	Other Genesys services and the private edition installer (through curl commands) use the Environment API to manage their environments, contact centers, and settings. Enable Transport Layer Security for this connection with in the **values.yaml** file.
8	Genesys Authentication	Consul	HTTPS	443	Egress	Discovery of Configuration Server endpoints. This connection is optional and controlled by the options in the **values.yaml** file.

Connection	Source	Destination	Protocol	Port	Classification	Data that travels on this connection
9	Genesys Authentication	Elasticsearch	TCP	9200	Egress	Logging data.
10	Genesys Authentication	Redis	TCP	6379 (non SSL) or 6380 (SSL)	Egress	Session data. SSL is controlled by in the **values.yaml** file.
11	Genesys Authentication	PostgreSQL	TCP	5432	Egress	Configuration data for the Authentication Service and the Environment Service.