Setting up Genesys Engage Cloud Private Edition

Software requirements

9/19/2021

Contents

Prerequisite software and third-party dependencies required for the Genesys Engage cloud private edition environment.

Early Adopter Program

Genesys Engage cloud private edition is being released to pre-approved customers as part of the Early Adopter Program. Please note that the documentation and the product are subject to change. For more details about the program, please contact your Genesys representative.

Prerequisites

This article describes the prerequisites and third-party infrastructure services (dependencies) you must deploy before deploying Genesys Engage services.

- Domain Name System (DNS)
- Helm 3.0+
- Ingress Controller
- JFrog Edge Artifactory account
- Kubernetes 1.18.x - 1.19.x **
- Session Border Controller (SBC)
- Web Application Firewall (WAF) - optional, but recommended.

***Currently, Genesys supports OpenShift Container Platform 4.6 as part of the cloud private edition offering. If you are looking for other Kubernetes offerings, contact your Genesys Account Representative.*

Third-party dependencies

Genesys Engage services require specific third-party back-end services as an infrastructure prerequisite. You can install these third-party infrastructure prerequisites in a different namespace or outside the cluster provided the namespace has direct network access to these services.

Important

Deploying and maintaining the third-party dependencies is your responsibility. For more information on your responsibilities and how Genesys supports the deployment process, see Understanding responsibilities.

See the table below for details about the prerequisite third-party dependencies.

Genesys has tested the OpenShift Operators listed in the table, but you can check with Genesys regarding replacing them with other cloud managed services (such as, Azure Postgres or AWS RDS Postgres). You could also run these services outside of OpenShift if you prefer.

Name	Version	OpenShift Operator Hub	OpenShift Operator URL	Purpose
A container image registry and Helm chart repository	N/A	N/A	N/A	You can use any Docker OCI compliant registry.
An SMTP relay	N/A	N/A	N/A	Facilitates email communications in an environment where GCXI reports or voicemails are sent as emails to contact center personnel. Genesys recommends PostFix, but you can use any SMTP relay that supports standard mail libraries.
Kafka	2.x	Banzai Cloud Kafka Operator	https://operatorhub.io/operator/banzaicloud-kafka-operator	Message bus.
Keda	2.0	KEDA Operator	https://operatorhub.io/operator/keda	(Optional) Custom metrics for scaling. Use of Keda or HPA is configurable through Helm charts.
Redis	6.x	Redis Enterprise Operator	https://operatorhub.io/operator/redis-enterprise	Used for caching.
Consul	1.9.5	N/A	N/A	Service discovery, service mesh, and key/value store.
Elasticsearch	7.x	Elasticsearch (ECK) Operator	https://operatorhub.io/operator/elastic-cloud-eck	Used for text searching and indexing.

Name	Version	OpenShift Operator Hub	OpenShift Operator URL	Purpose
MS SQL Server	2016	N/A	N/A	Relational database.
PostgreSQL	11.x	N/A	N/A	Relational database.

Permissions

Security context parameters in the Helm charts specify the users authorized to access the pods and containers for the respective services. By default, the Helm charts specify the user, group, and file-service group IDs as `500:500:500`.

OpenShift

OpenShift controls the pod permissions (including user access) through a security feature called *security context constraints* (SCCs). Private edition supports the use of arbitrary user IDs (UIDs), with pods and containers using the **restricted** SCC (the most restrictive SCC defined by default).

In an early implementation, private edition required the use of a custom SCC called **genesys-restricted** to control permissions associated with the **genesys** user (500) specified by the services. The **genesys-restricted** SCC has now been deprecated.

Arbitrary UIDs

To use arbitrary UIDs, override the Helm chart values so that no specific IDs are defined for users and groups. See OpenShift security settings for more information.