Genesys Web Services and Applications Private Edition Guide

Before you begin

4/25/2024

Contents

Find out what to do before deploying Genesys Web Services and Applications.

Related documentation:

-
-
-

RSS:

- For private edition

Download the Helm charts

Genesys Web Services and Applications (GWS) in Genesys Multicloud CX private edition is made up of multiple containers and Helm charts. The pages in this "Configure and deploy" chapter walk you through how to deploy the following Helm charts:

- GWS services (gws-services) - all the GWS components.
- GWS ingress (gws-ingress) - provides internal and external access to GWS services. Internal ingress is used for cross-component communication inside the GWS deployment. It also can be used by other clients located inside the same Kubernetes cluster. External ingress provides access to GWS services to clients located outside the Kubernetes cluster. If you are deploying Genesys Web Services and Applications in a single namespace with other private edition services, then you do not need to deploy GWS ingress.

GWS also includes a Helm chart for Nginx (wwe-nginx) for Workspace Web Edition - see the Workspace Web Edition Private Edition Guide for details about how to deploy this chart.

See Helm charts and containers for Genesys Web Services and Applications for the Helm chart versions you must download for your release.

For information about downloading Helm charts from JFrog Edge, see Downloading your Genesys Multicloud CX containers.

Third-party prerequisites

Install the prerequisite dependencies listed in the **Third-party services** table before you deploy Genesys Web Services and Applications. See Software requirements for a full list of prerequisites and third-party services required by all Genesys Multicloud CX private edition services.

Third-party services

Name	Version	Purpose	Notes

Elasticsearch	7.x	Used for text searching and indexing. Deployed per service that needs Elasticsearch during runtime.	**GWS requires Elasticsearch 7.17+**. You must configure additional options for Elasticsearch to support the Data Collector Service.
			`action.auto_create_index: false`
			`thread_pool.write.queue_size: -1`
			You can set up Elasticsearch as a shared or dedicated service.

Redis	6.x	Used for caching. Only distributions of Redis that support Redis cluster mode are supported, however, some services may not support cluster mode.	The Redis server must run in cluster mode. You can set up Redis as a shared or dedicated service.
PostgreSQL	11.x	Relational database.	**GWS supports PostgreSQL 12.x.** You can set up PostgreSQL as a shared or dedicated service.
Consul	1.13.x	Service discovery, service mesh, and key/value store.	**GWS supports Consul 1.8**. Consul can be installed either inside or outside the Kubernetes cluster. GWS pods require a Consul agent that is running at the Kubernetes node and GWS only communicates with this Consul agent. You must configure a connection to the Consul server in the local Consul agent.
Ingress controller		HTTPS ingress controller.	
HTTPS certificates - Let's Encrypt		Use with cert-manager to provide free rotating TLS certificates for NGINX Ingress Controller. **Note:** Let's Encrypt is a suite-wide	

Name	Version	Purpose	Notes
		requirement if you choose an Ingress Controller that needs it.	
HTTPS certificates - cert-manager		Use with Let's Encrypt to provide free rotating TLS certificates for NGINX Ingress Controller.	
Load balancer		VPC ingress. For NGINX Ingress Controller, a single regional Google external network LB with a static IP and wildcard DNS entry will pass HTTPS traffic to NGINX Ingress Controller which will terminate SSL traffic and will be setup as part of the platform setup.	
A container image registry and Helm chart repository		Used for downloading Genesys containers and Helm charts into the customer's repository to support a CI/CD pipeline. You can use any Docker OCI compliant registry.	
Command Line Interface		The command line interface tools to log in and work with the Kubernetes clusters.	

Storage requirements

GWS uses PostgreSQL to store tenant information, Redis to cache session data, and Elasticsearch to store monitored statistics for fast access. If you set up any of these services as dedicated services for GWS, they have the following minimal requirements:

PostgreSQL

- CPU: 2
- RAM: 8 GB
- HDD: 50 GB

Redis

- 2 nodes:
  - CPU: 2
  - RAM: 8 GB
  - HDD: 20 GB

Elasticsearch

- 3 "master" nodes:
  - CPU: 2
  - RAM: 8 GB
  - HDD: 20 GB
- 4 "data" nodes
  - CPU: 4
  - RAM: 16 GB
  - HDD: 20 GB

Network requirements

GWS ingress objects support Transport Layer Security (TLS) version 1.2 for a secure connection between Kubernetes cluster ingress and GWS ingress. TLS is disabled by default, but you can configure it for internal and external ingress by overriding the **entryPoints.internal.ingress.tls** and **entryPoints.external.ingress.tls** sections of the GWS ingress Helm chart.

For example:

```
entryPoints:
  external:
    ingress:
    tls:
      - secretName: gws-secret-ext
        hosts:
          - gws.genesys.com
```

In the example above:

- **secretName** is the name of the Kubernetes secret that contains the certificate. The secret is a prerequisite and must be created before you deploy GWS ingress.
- **hosts** is a list of the fully qualified domain names that should use the certificate. The list must be the same as the value configured for the **entryPoints.external.ingress.hosts** parameter.

Cookies

GWS components use cookies for following purposes:

- identify HTTP/HTTPS user sessions
- identify CometD user sessions
- support session stickiness

Genesys dependencies

Genesys Web Services and Applications must be deployed after Genesys Authentication.

For a look at the high-level deployment order, see Order of services deployment in the *Setting up Genesys Multicloud CX Private Edition* guide.

Next steps

- Configure GWS Services
- Deploy GWS Services
- Configure GWS Ingress
- Deploy GWS Ingress