Setting up Genesys Multicloud CX Private Edition

Security overview

12/12/2025

Contents

Learn about general security considerations involved in deploying Genesys Multicloud CX private edition.

Related documentation:

-
-

RSS:

- For private edition

Because security is a growing priority for today's enterprises, Genesys works hard to provide a full range of security-related features, such as authentication, role-based access control (RBAC), and many more.

Note, however, that you are responsible for maintaining the security of your private edition infrastructure, such as network security, firewalls, and so on.

Built-in security features

Genesys Multicloud CX private edition has been developed using industry-standard tools and best practices to identify and eliminate security vulnerabilities.

The services that ship with private edition are built with the following features, which provide a strong basis for you to create a secure, enterprise-grade solution:

- Containers are immutable and follow hardening best practices.
- Services run in least-privileged accounts based on the feature functionality needed by a given service.
- You can deploy your Kubernetes clusters into different network segments to partition software into security zones. To do this, you must create new Kubernetes Service Objects with load balancers, which expose the necessary connections between Kubernetes clusters.
- You can put security tool agents on your Kubernetes nodes to carry out the appropriate security tasks, such as host-based intrusion detection system (HIDS), file integrity management (FIM), user and entity behavior analytics (UEBA), and so on.
- If you need encryption in transit within the cluster, you can use a service mesh or various cloud-native solutions. You can also enable encryption in transit outside the cluster by using an ingress controller.
- Private edition services support encryption of their data at rest as well secure connections to datastores using Transport Layer Security (TLS) protocol.
- Appropriate Center for Internet Security (CIS) benchmarks are generally built into services' container images and are applied to how Kubernetes node resources are accessed. Please see specific service documentation for limited exceptions and specific requirements.

Overrides

Genesys recognizes that your own stringent security requirements can differ from those that are enabled by default in Genesys Multicloud CX services. You can customize many of these security requirements by overriding Helm chart values, in accordance with the information in the appropriate service guide.

In that context, here are additional security requirements for you to consider as you set up your environment.

Pod security policies

Private edition does not support pod security policies.

Secrets

Secrets are namespace objects that contain a small amount of sensitive data, such as a password, a token, or a key. Most of the Genesys Multicloud CX services require secrets at deployment time, for dependencies, such as Postgres, Redis, email server, Genesys Cloud CX, and so on.

The scope of a secret is the namespace in which the secret is created. Unless you are using a single namespace for all private edition services, in each namespace you must create secrets for the third-party dependencies that are required by the service(s) in that namespace. If a secret is shared by different services in different namespaces, you must duplicate the secret in all the respective namespaces. Depending on how complex you want to make management of credentials for shared datastores and other shared dependencies, you can either replicate the same secret across multiple namespaces, so that different services use the same credentials for a given datastore, or create different secrets in each namespace, so that individual services use their own credentials for a given datastore.

You must use only Kubernetes secrets at runtime, and they must support user-supplied values and secrets via Helm-value overrides.

Data encryption through TLS/SSL

Genesys Multicloud CX services support TLS protocol for connections into the cluster up to the ingress controller. Data is not encrypted beyond the ingress controller.

Genesys Multicloud CX services support TLS protocol for connections to third-party dependencies based on the details and capabilities of those dependencies. The credentials associated with each connection are managed through secrets associated with the relevant services.