Cora SeQuence Cloud Topologies

Last Modified on 02/18/2019 11:41 am EST

Overview

The Cora SeQuence platform can be deployed as a managed service on Microsoft Azure Cloud.

All of the cloud environments available are hosted in a dedicated Azure tenant, which are separate directories with no connection to other Genpact tenants. Cora SeQuence is deployed as a stand-alone Azure cloud service and does not depend on shared resources or any other Genpact product. All instances and managed services are provisioned within a private network.

Each cloud environment uses Microsoft Azure SQL Database provided as Platform-as-a-Service (PaaS).

The standard offering includes three environments:

- DEV (Development): Single Azure virtual machine for development purposes.
- TST (Testing): Single Azure virtual machine for testing purposes.
- PRD (Production): four Azure virtual machines to support high availability for a live production environment.

DEV and TST	PRD

• Web and Application tiers
  ◦ Single server
  ▪ Cora Sequence Administration site
  ▪ Cora Sequence Flowtime site
  ▪ Product services
• Database tier
  ◦ SQL Azure database (PaaS)
• Scalability
  ◦ None
	• Web tier
	  ◦ Two front-end servers
	  ▪ Cora Sequence Flowtime site
	• Application tier
	  ◦ Two back-end servers
	  ▪ Cora Sequence Administration site
	  ▪ Product services
	• Database tier
	  ◦ SQL Azure database (PaaS)
	• Scalability
	  ◦ Scale-out approach: Additional machines can be added depending on system load.
	  ◦ Database power is optimized for actual load.

NOTES

- The PRD environment requires an Identity Provider Service (IPS) on the customer side to authenticate users.
  For more information on authentication methods, see this article.
- All the environments require a Genpact administrator access for ongoing maintenance and support.
- A jump server can be used for system administration tasks, and other maintenance and support activities.

Cora SeQuence integration

There are two options to the connect between your organization network to the Cora SeQuence cloud:

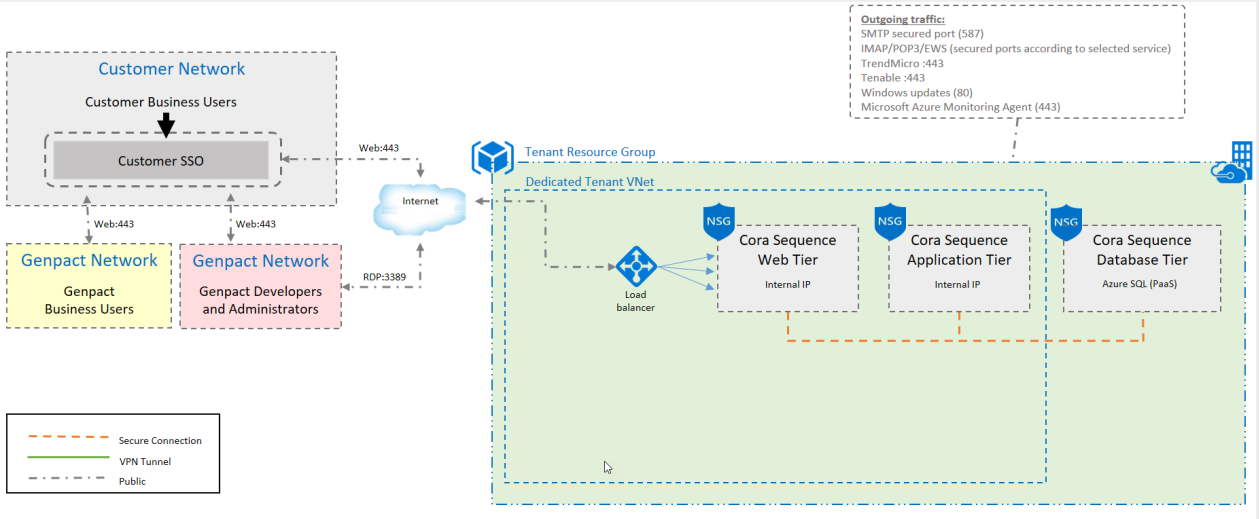
- Secured internet facing
- Private network (VPN site-to-site IP-Sec)

Each option can be adjusted to meet requirements according to the customer's license terms and agreement.

Requirement	Internet facing topology	Private network topology
SSO authentication	✔	✔
Cora SeQuence outbound traffic	From Azure Virtual Network	From customer network
Access to Cora SeQuence sites	Secured HTTP	Secured HTTP
Customer can create and remove user accounts for Cora SeQuence sites	✔	✔
Business users access to Flowtime	• From anywhere • Option to limit to IP whitelist	From customer network
Genpact business users access to Flowtime site	• From anywhere • Option to limit to IP whitelist	• Via customer VPN • Via customer Citrix
Genpact developers access to Cora SeQuence sites (Administration or Flowtime)	• From anywhere • Option to limit to IP whitelist	• Via customer VPN • Via customer Citrix
Genpact administrators access to Cora SeQuence sites (Administration / Flowtime)	• From anywhere • Option to limit to IP whitelist	• Via customer VPN • Via customer Citrix • Via Genpact jump server
Genpact administrators access to: • Cora SeQuence virtual machines • Cora SeQuence Database	• Remote desktop connection to the application and web tiers • SSH to database from Genpact offices only	• Remote desktop connection to application and web tiers and SSH to database from Genpact office only. • Via Genpact Jump server on public internet or Azure Gateway VPN.

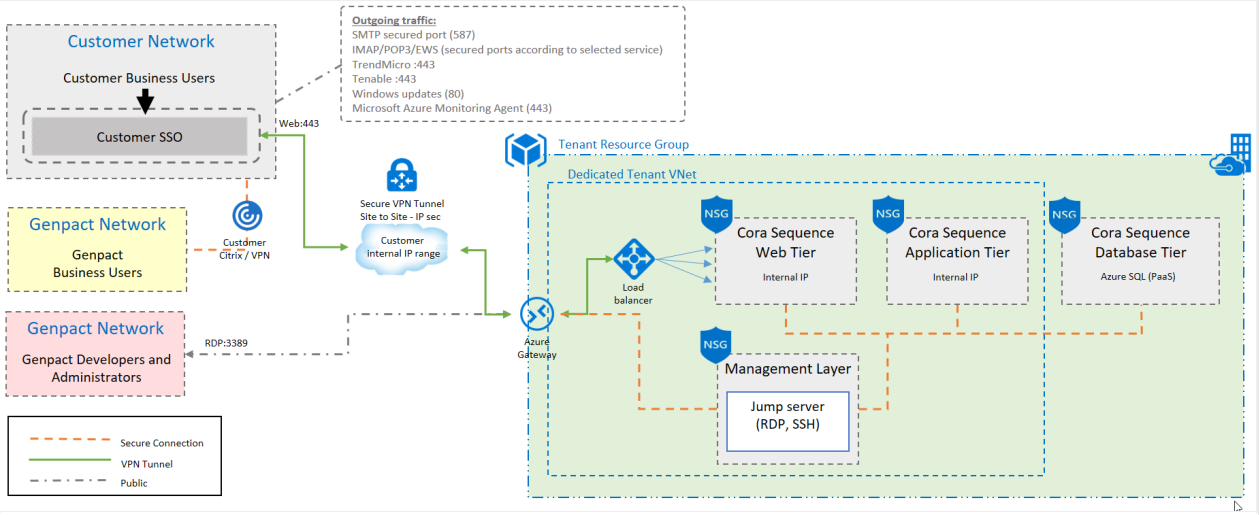
Secured internet-facing integration

This integration offers secured traffic over a public IP.



Private network integration

This integration requires a VPN connection between the cloud tenant and the customer data center.



User types

The cloud environments typically include the following types of users.

User type	Purpose	Roles	Relevant environments
Business users	• Use Flowtime for business operations	• Customer operation teams and leaders • Genpact operation teams and leaders	• PRD
Genpact developers	• Develop, test, and deploy workflows	• Genpact BPM developers (Professional Services)	• DEV • TST • PRD

User type	Purpose	Roles	Relevant environments

Genpact administrators	• Product maintenance
	• Product updates
	• Troubleshooting and support activities
		• On-going support and maintenance by
		  ◦ Cloud System Administrator
		  ◦ Cora SeQuence Support
			• DEV
			• TST
			• PRD

User access

The access level of user types varies depending on business needs. For example, business users have access only to Flowtime, whereas developers have access to additional components.

Components	Business users	Genpact BPM Developers	Genpact Administrators
Cora SeQuence Administration	✗	• DEV/TST • PRD (limited to deployment only)	✓
Cora SeQuence Flowtime	✓ SSO account per user	✓ SSO account per user, or generic user.	✓ SSO account per user, or generic user.
Virtual machines (all environments)	✗	✗	✓ Ability to copy files to/from the servers
Database (all environments)	✗	Read-only	✓
Azure management	✗	✗	✓

User management

Cora SeQuence user accounts are created and disabled either manually or automatically. The automatic option requires integration with Active Directory.
For more information on authentication methods, see this article.

Task	Description	Additional details

Task	Description	Additional details
Create users	• Manual creation: Genpact administrators ("power-users") create or disable users via the Administration site. • Automatic creation: New users are automatically added to the system via the Active Directory Synchronization Service (ADSS). Disabled or deleted users are automatically marked as inactive.	Active Directory provisioning: • On-premises Active Directory • Azure Active Directory

Infrastructure security control

The available cloud environments provide several security tools to protect infrastructure components.

Item	Security controls
Traffic to the web application	• HTTPS, port 443, TLS 1.2 • When VPN IPSEC tunnel is used, traffic to the application uses the customer internal IP range only.
Network Security Group	• Communication between web, middleware, and database is restricted to using Network Security Group. • The Cora SeQuence application tier only accesses the Azure BLOB storage from within the Virtual network. • Azure virtual machines and SQL database are accessed within the tenant from a the jump server only and are not open to the internet.
Role-based access control (RBAC)	Azure identity and access management (IAM) roles are configured to limit exposure to Genpact admins only.
Azure Distributed Denial of Service (DDoS) protection	Backed up by Microsoft global network.
Security hardening	According to Microsoft Security Center best practices.

Database security control

Data is secured at-rest and in-transit.

Secured data at-rest	• Transparent Data Encryption (TDE) is used within the Microsoft Azure database.
	• Always encrypted
	  ◦ Additional encryption on the database level is available per implementation requirements.
	  ◦ Table columns with sensitive data (credit card details, social security number, etc.) can be encrypted with a unique key.
	  ◦ The key is stored in Azure Vault

Secured data transport	• Data transport is done over SSL. • XSRF protection is enabled to prevent attacks riding on client sessions.

Information security tools

Mitigation software	• Trend Micro: Deep security HIPS/HIDS systems are installed on each virtual machine. • Kenna security platform: Continuous vulnerability assessment scanning.
Monitoring software	• Azure Operation Management Suite (OMS): Security events are collected using Azure OMS. An event correlation rule is configured to trigger notifications in case of unauthorized or malicious activity. • Azure Security Center (ASM): Provides security management and advanced threat protection.

Standard inbound and outgoing traffic

The following ports are used for inbound and outbound traffic.

Basic inbound	Basic outbound	Extra outbound

• Port 443
  ◦ Cora Sequence sites
• Port 3389
  ◦ Remote desktop connection to the virtual machines
	• Port 80
	  ◦ Windows updates
	• Port 443
	  ◦ TrendMicro Deep Security
	  ◦ Tenable
	  ◦ Microsoft Azure Monitoring Agent
	• Port 587
	  ◦ SMTP service secured port
		• Email listener ports
		  ◦ IMAP/POP3/EWS
		  ◦ Secured ports according to selected service

NOTE
You may need to enable additional applications depending on the specific implementation

requirements.

Disaster recovery plan

Available for all environments: DEV, TST, and PRD. The Cora SeQuence Support team is responsible for performing system backup and recovery activities.

- Virtual machine servers:
  - Daily backup
  - Retention policy: 30 days
- Database
  - Backup: Azure SQL continuous backup.
  - Retention: 35 days
  - Geo replication: Available upon customer request.

Business continuity plan

Available for PRD environments only and managed by the Support team.

- Azure availability set
- Virtual machine redundancy and load balancer
- Product component distribution:
  - Front-end servers: Dedicated to Flowtime site only
  - Back-end servers include the following components:
    - Administration site
    - Cora SeQuence services
    - Automatic failover for Cora SeQuence services
- Monitors and alerts
  - Alerts are automatically sent to the Support team when a service or component is down.