Common Components Blueprint

Reference Architecture

Authors: Don Huovinen, Abdul Samin

Version: 2.0

Status: Released

Published: 11/12/2018

GENESYS

Table of Contents

Table of Figures

Table of Tables

Revision History

Rev	Date Published	Author	Reason for Revision
0.1	5/2/16	Don Huovinen	Initial release
0.2	5/17/16	Don Huovinen	Added interaction views and appendix
0.3	6/17/16	Don Huovinen	Updated based upon reviews and feedback
0.4	6/23/16	Don Huovinen	Additional updates. Draft released for additional review.
0.5	7/12/16	Don Huovinen	Incorporated Engineering and SC feedback
1.0	7/14/16	Don Huovinen	Finalized formatting and released.
1.1	9/1/16	Don Huovinen	Updated disclosure language.
2.0	11/12/18	Abdul Samin	Updated content to reflect current view of architecture

1 Introduction

The purpose of the Common Components Blueprint is to establish a foundational architecture which consists of elements utilized across all Blueprint architectures. The Common Components architecture is not intended as a standalone solution. The solution Blueprint architectures (SIP, Digital, WFO, EWM) layer on top of the Common Components detailed within this document.

This document provides a prescriptive list of components (both Genesys and 3rd party) that should be considered when deploying the Common Components.

This document provides guidance for implementing and deploying the solution including sizing and configuration as well as addressing several system concerns such as security, high availability, disaster recovery and serviceability.

1.1 Document Overview

The document contains the following sections:

- Chapter 2: Definitions and Acronyms
- Chapter 3: Overall Architecture
- Chapter 4: Deployment View
- Chapter 5: Interaction View
- Chapter 6: Implementation View

1.2 Intended Audience

The Blueprint Architectures are intended to provide Genesys pre-sales, professional services and partners with information on the general architecture design and considerations for the solution. The information provided in this document should meet the needs of pre-sales and provide appropriate general guidance and practices for professional services. This document is not intended to provide configuration level information for professional services.

Describing system and solution architectures can be difficult as there are multiple audiences each with different expectations. This document is intended for multiple audiences with various chapters being more interesting to some readers than others. It is expected that readers will already have knowledge and training on Genesys products. Some high level information is still provided in this document for completeness.

The Overall Architecture and Deployment View are likely meaningful to most audiences. However the Interaction View and the Implementation View may be of more interest to those configuring the network and components. Some high level information is still provided throughout this document for completeness.

2 Definitions, Acronyms, and Document Standards

2.1 Definitions

This document uses various abbreviations and acronyms that are commonly used in Genesys product documentation and the telecommunications and contact center industries. The following table defines terms that will be referenced subsequently in this document.

2.2 Glossary

CMS	Content Management System
CS	Config Server
CSP	Config Server Proxy
CSV	Comma Separated Values
DB	Database
DBMS	Database Management System
DN	Directory number
DNS	Domain Name System
FTP	File Transfer Protocol
GA	Genesys Administrator
GAX	Genesys Administrator Extension
GCXI	Genesys Customer Experience Insights
GIM	Genesys Info Mart
GIR	Genesys Interaction Recording
GES	Genesys Engagement Services
GRAT	Genesys Rules Authoring Tool
GRE	Genesys Rules Engine
GRS	Genesys Rules System
GWS	Genesys Web Services
HA	High Availability
HTCC	Host Telephony Contact Center – now GWS
HTTP	Hypertext Transfer Protocol
ICON	Interaction Concentrator
IDB	ICON Database

IP	Internet Protocol
IVR	Interactive Voice Response
JVM	Java Virtual Machine
LAN	Local Area Network
LCA	Local Control Agent
MCP	Media Control Platform
MS	Message Server
NMS	Network Management System
OCS	Outbound Contact Server
ORS	Orchestration Server
OS	Operating System
RDBMS	Relational Database Management System
SCS	Solution Control Server
SCXML	State Chart XML: State Machine Notation for Control Abstraction
SDK	Software Development Kit
SIP	Session Initiation Protocol
SMS	
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
UCS	
UI	User Interface
URS	Universal Routing Server
VM	Virtual Machine
VoIP	Voice over IP, digitized voice segments transported in fixed packets across the IP network and re-assembled in sequence at the destination

2.3 Document Conventions

The following documentation and naming conventions are used throughout the document:

- Code and configuration property names & values will appear in console font.
- References to other documents are bracketed ([]).

3 Architecture - Overview

The Genesys Common Components architecture covers standard elements which are shared by multiple blueprint architectures with the common components establishing the foundation that should be present in any architecture.

Genesys provides the following separate Blueprint Architectures

- SIP Voice Blueprint
- Digital Engagement Center Solution Blueprint
- WFO Solution Blueprint Recording Analytics
- WFO Solution Blueprint for Workforce Management
- Enterprise Workload Management Solution Blueprint

The appropriate Blueprint Architecture should be consulted in addition to the Common Components to provide a complete understanding of the architecture.

Much of the guidance provided in this document is based on customer deployments and the lessons learned through implementing Genesys within those real-world scenarios.

This Common Components architecture is focused on 3 areas – Orchestration, Reporting and Configuration/Management.

Genesys Orchestration– Routing engine, business rules and contextual information which is used to intelligently distribute interactions to the right contact center resources based upon the business objectives and the current state of contact center resources.

Genesys Reporting – Real-time and Historical reporting provided by Pulse (Real-time) and ICON/Info Mart/CX Insights (Historical)

Genesys Configuration and Management – OAM&P layer enabling centralized configuration, management and alarming of the entire Genesys environment.

Third party components which are utilized in the architecture such as the databases are non-Genesys components. While they are required in the overall architecture Genesys does not go into detail on specific 3rd party components as these are a customer responsibility.

3.1 Logical Architecture Model

The following is a logical model of the Genesys Common Components architecture.

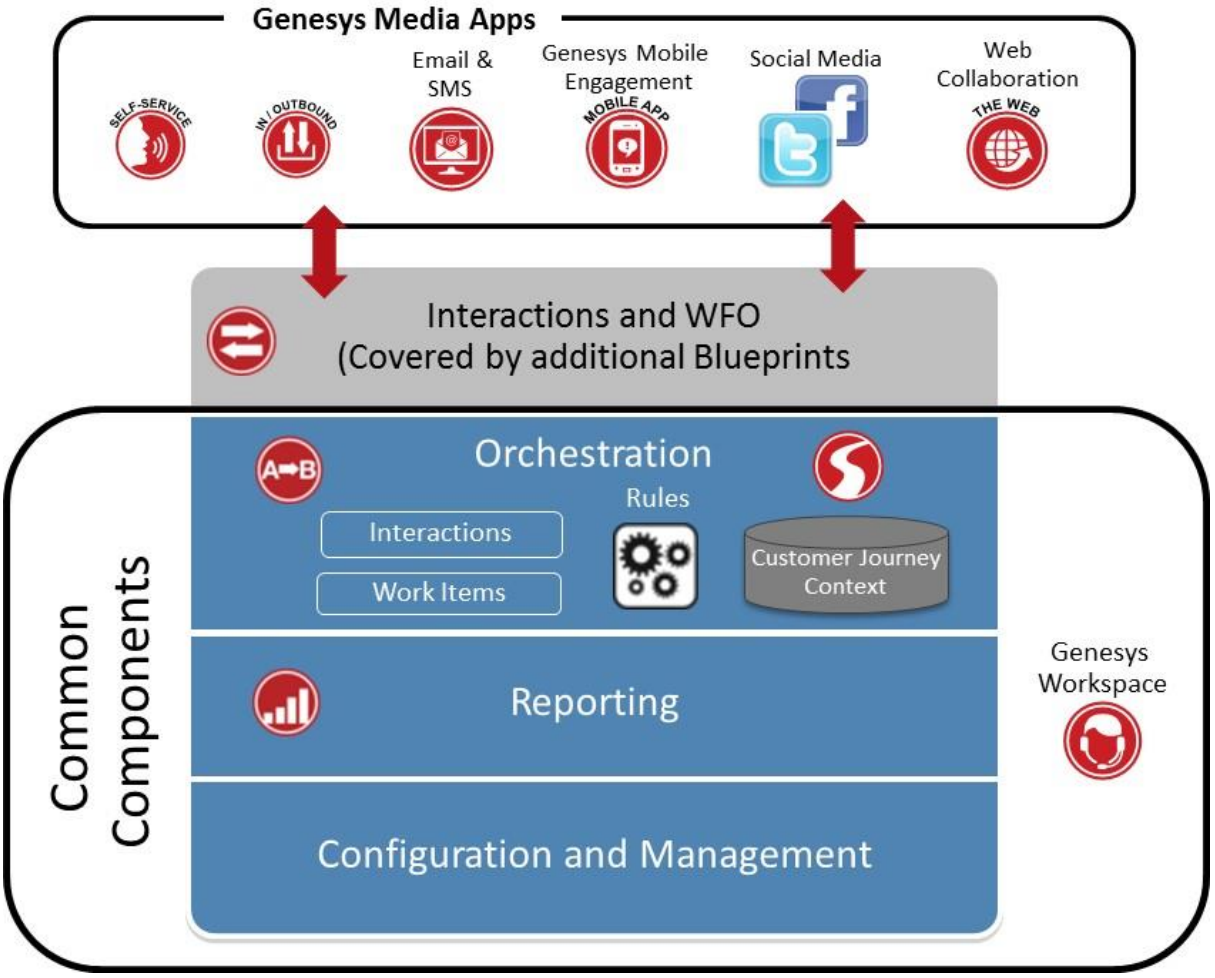

Figure 1 - Common Components High Level

3.2 Functional View

The Common Components architecture delivers a consistent architecture that is intended to be leveraged across all solutions. Many customer deployments may start out with a single solution. The establishment of a common architecture for shared components allows the architecture to consider future customer needs both managing interaction types and the application of more advanced business strategies. Establishing a comprehensive common component architecture as the allows customers to easily integrate new Genesys components or evolve their customer experience management strategy, such as the sophistication of the routing that is used, without changes to the core foundation.

The functionality delivered can be broken down in to the following areas:

- Orchestration and Routing
- Reporting
- Configuration and Management

3.2.1 Orchestration

The Orchestration provided by the common components delivers the following functionality:

- SCXML-based workflows to manage the routing of interactions across all media types and manage the customer journey across time
- Access to contextual information about the current interaction, prior interactions and customer details to optimize the routing decisions
- Real-time visibility to contact center resources (agents and queues)
- Business rules control to change routing and IVR behavior in real time
- Integration with external systems through web services (RESTful is recommended however both REST and SOAP are supported)

3.2.2 Reporting

The Reporting provided by the common components enables:

- Web based access to both real-time and historical reporting across all interactions
- Real-time visibility to contact center resources and measurement through standard and custom KPIs
- Intra-day metrics on contact center performance
- Visual alerting based upon user configured thresholds
- Integration with external sources through both RESTful web services and iFrames to provide a consolidated Dashboard which contains both Genesys and external information
- Standard historical reports and the ability to create custom historical reports through a web based interface
- A data universe, simplifying the process of creating historical reports that incorporate various facts and dimensions
- Report distribution capabilities to enable deliver of reports automatically via a variety of mediums (email, FTP, web) and in various formats (PDF, Excel, CSV)
- A well-defined, documented data model enabling the historical data to be directly accessed and used by 3rd party analytics packages

3.2.3 Configuration and Management

The Configuration and Management components provide:

- Centralized configuration of all applications and resources in the Genesys environment ranging from software configuration settings to resources such as agents
- Management and distribution of configuration changes to all applications

- Web based user interfaces to allow user access to configuration and management function
- Role based user access which controls both the functions a user can perform and objects they can access
- Business rules management of routing strategies with roles based access for authoring and deployment
- Manage and monitor the health of Genesys software components - controls the startup and status of solutions, logging, generation and processing of alarms, and management of application failures.

3.3 Standard Use Cases

The Common Components Blueprint architecture provides a common sets of capabilities which are used by all other Blueprint Architectures and required for the standard use cases. Details on the Standard Use Cases are available on Genie under Use Cases.

There may be some solutions or use cases which only rely on a portion of the Common Components. For example Genesys WFM requires only the Configuration and Stat Server reporting provided within the Common Components Blueprint.

Each individual blueprint architecture contains details on which mandatory Common Components are required to support the overall architecture.

3.4 Component View

The Component View describes the higher-level modules that make up the solution. The following diagram depicts the components required as part of the solution.

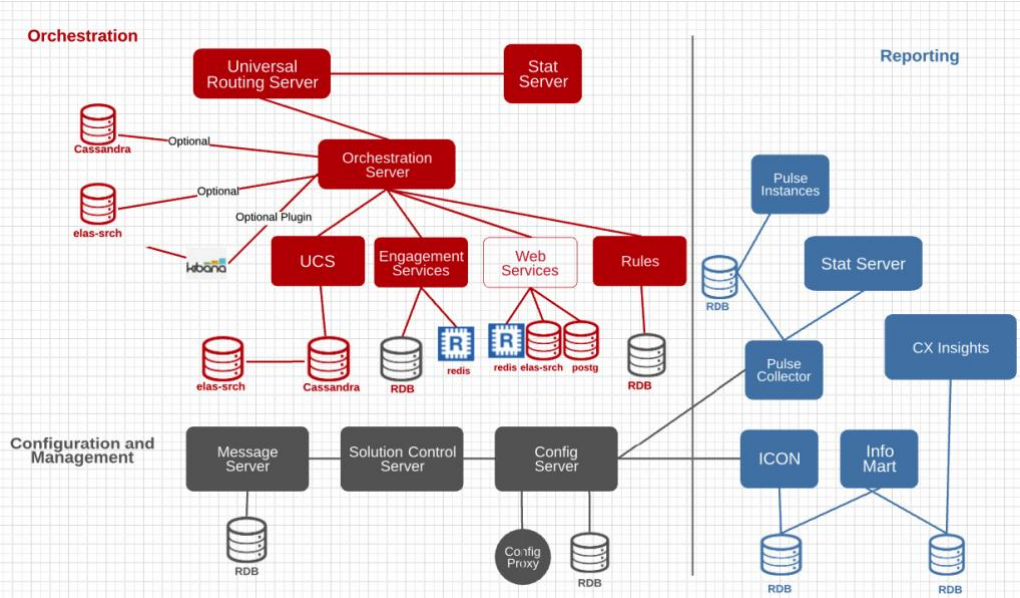

Figure 2 - Common Component Detail

Note: The diagram is intended to provide a clear understanding of the different areas which are addressed by the Blueprint and not all components or connections are shown, e.g. all components have connections to Config Server or Config Proxy but we have intentionally not shown specific components or connections where it would distract from the objective of the diagram. The diagram does show some detail such as separate Stat Servers for routing and reporting. Deployment of different Stat Servers based upon role is a common practice however a common Stat Server may be used for both routing and reporting for smaller deployments.

3.4.1 Orchestration

The following components are included within the logical Orchestration layer:

- Universal Routing Server
- Orchestration Server
- Stat Server
- Universal Contact Server
- Genesys Engagement Services (For Context Services)
- Genesys Rules
- Genesys Web Services

Both Genesys Rules and Genesys Web Services are considered Advanced Orchestration components therefore they may be optional in the architecture based upon the specific use case. All other components should be utilized.

Universal Routing Server
Genesys Universal Routing Server executes a set of routing rules called a routing strategy designed by the enterprise to meet the needs of the business. These rules can evaluate telephony data, customer IVR menu selections, time of day/week/year, real-time virtual contact center statistics, agent skills and customer profile data held in corporate databases or other enterprise systems. Universal Routing Server then determines the best resource to receive an interaction based upon the business rules or may queue and treat the interaction waiting for the correct resource to become available.

Orchestration Server
Genesys Orchestration Server (which works with URS) was designed to support the evolving customer interaction needs required enterprises to manage interactions in a coordinated journey towards specific end goals. Enterprises still develop rules or routing strategies which define how interactions are handled but now have greater flexibility in how they link and associate disparate interactions in a coordinated delivery process thereby delivering a continuous and seamless service experience for their customers. Orchestration is designed to support both synchronous and asynchronous interactions and easily integrate with external customers systems utilizing standard web based methodologies.

Stat Server
Statistical Server is the central informational component of the Genesys Suite that keeps track of the current states of contact center resources and collects various statistics about them. Through managing the real-time state of resources such as agents and queues Genesys is able deliver interactions meeting the specific business logic which was established. Stat Server transforms events, available from Genesys applications, into an integrated real-time view of contact center operations, and is the key element of the recognized intelligence of the Genesys interaction management platform.

Universal Contact Server
The Universal Contact Server collect and stores information on every contact, the interaction history of all media channels, and associates related interactions to form a thread that provides a comprehensive contact history. The data contained in UCS can be leveraged by Genesys for a limited set of contextual routing use cases. These data is also made available to agents/supervisors at the desktop level so that, for example, agents can view all past interactions (across all media channels) for the current customer with whom they are communicating.
The Universal Contact Server (UCS) database may collect:

- Contact information, such as names, addresses, and phone numbers
- Contact history, such as previous interactions with a given contact

Genesys Engagement Services
Genesys Engagement Services is deployed as part of the Common Components architecture as it exposes a broad set of APIs used by numerous systems. The APIs may be used by Genesys within routing strategies, IVR applications, as part of call back, and from desktops. These APIs may also be invoked by systems external to Genesys such as web sites, mobile applications, etc.

Context Services

Context Services refers to a set of capabilities which are delivered by Genesys UCS and Genesys Engagement Services. Context Services can collect information about all the various conversation channels – phone, web, email, SMS - and captures information about customers and the things they are doing in a flexible, easy-to-integrate data model. Context Services is designed to help enterprises connect communication channels intelligently. It can store information captured both by Genesys and non-Genesys channels to provide a richer picture of customer interactions. In addition to capturing information about an interaction it provides a service/state/tasks hierarchy that can facilitate and coordinate customer journeys with an organization. From a technical standpoint Context Services is accessed through a RESTful web service and utilizes both Genesys Engagement Services (GEM) to store/access unstructured data and the Universal Contact Server database for access to common structured data. While Context Services relies on components previously described there are configuration options and databases specifically established which deliver the 'Context Services' capability.

Genesys Rules

Genesys Rules System (GRS) provides the ability to develop, author, and evaluate business rules. A business rule is a piece of logic defined by a business analyst. These rules are evaluated in a Rules Engine based upon requests received from client applications such as intelligent Workload Distribution, Genesys Proactive Engagement, Genesys Conversation Manager and general routing strategies.

The Genesys Rules System includes three components:

- The **Genesys Rules Development Tool** is an Eclipse plug-in that allows advanced users (business rules developers) to create templates that define the discrete rule conditions and actions that will comprise the rules. Each rule condition and action includes the plain-language label that the business rules author will see, as well as the rule language mapping that defines how the underlying data will be retrieved or updated.
- The **Genesys Rules Authoring Tool** is a browser-based application that is used by business analysts to create and edit business rules based on the templates created in the Genesys Rules Development Tool.
- The **Genesys Rules Engine** evaluates the rule packages (groups of rules). Rule packages are deployed to the Rules Engine by the Rules Authoring Tool. Once a rule package is deployed, Genesys applications can request the Rules Engine to evaluate the logic defined in this rule package.

Note: The Genesys Rules Engine is considered part of the logical Orchestration layer while the Development Tool and Rules Authoring Tool are Administration tools. All elements are described together for completeness.

Genesys Web Services

Genesys Web Services provides a high-level RESTful API that is used build web based desktop applications, and integration between different Genesys solutions. It is an application server which exposes a simple web services interface to clients and mediates communication between these clients and internal Genesys components through proprietary protocols such as T-Lib. Genesys Web Services provides high-level asynchronous notifications (events) for informing about changes in resources in real time. Genesys Web Services also provides additional layer of switch-independence, so that different telephony switches

can be handled uniformly. For example, it provides information about the operations available for a given telephony resource depending on the switch type. Products which rely of Genesys Web Services include:

- Workspace Web Edition

Note: Genesys Interaction Recording previously used GWS but has migrated to a new web services deployment specific to GIR, called Recording Web Services.

3.4.2 Reporting Components

The following components are included within common Reporting layer:

- Stat Server
- Pulse (Consists of Collector, Storage and Rabbit MQ)
- Interaction Concentrator
- Info Mart
- CX Insights

Note: Some Genesys solutions provide unique reporting capabilities which is either complementary or separate from the common reporting. Examples of production with additional reporting capabilities include Workforce Management, intelligent Workload Distribution, Genesys Web Engagement and Genesys Voice Platform. Details on these reporting requirements are covered in the appropriate individual solution architectures.

The following legacy components should not need to be deployed therefore they are not covered in the Common Components blueprint:

- CC Pulse+
- CC Analyzer

Stat Server

Genesys Stat Server provides a real-time statistical engine that tracks information about customer interaction networks (contact center, enterprise-wide, or multi-enterprise telephony and computer networks). Stat Server also converts the data accumulated for directory numbers (DNs), agents, agent groups, and non-telephony-specific object types, such as e-mail and chat sessions, into statistically useful information, and passes these calculations to other software applications that request data.

Some of the components that utilize Stat Server include:

- **Routing** – Genesys ORS and URS utilize Stat Server to provide agent state information, contact center statistics (such as estimated wait time, etc), and other statistics that are used for routing purposes.
- **Pulse** – Genesys Pulse utilizes Stat Server for real-time reporting data.
- **Wallboards** – Wallboard using the Genesys Statistics APIs can access real-time information from Stat Server.

- **Workforce Management** – Genesys WFM uses Stat Server to provide it with real-time adherence and other data.

Further information on Genesys Stat Server may be found at:

http://docs.genesys.com/Documentation/RTME

Pulse

Genesys Pulse is a widget-driven, graphical user application, which is accessible from a web browser as a Genesys Administrator Extension (GAX) plug-in application. Using a direct communication link to a real-time metrics engine, Stat Server, Pulse enables at-a-glance views of real-time contact center statistics within the GAX user interface.

The following provides a diagram of the underlying components which are used in Pulse

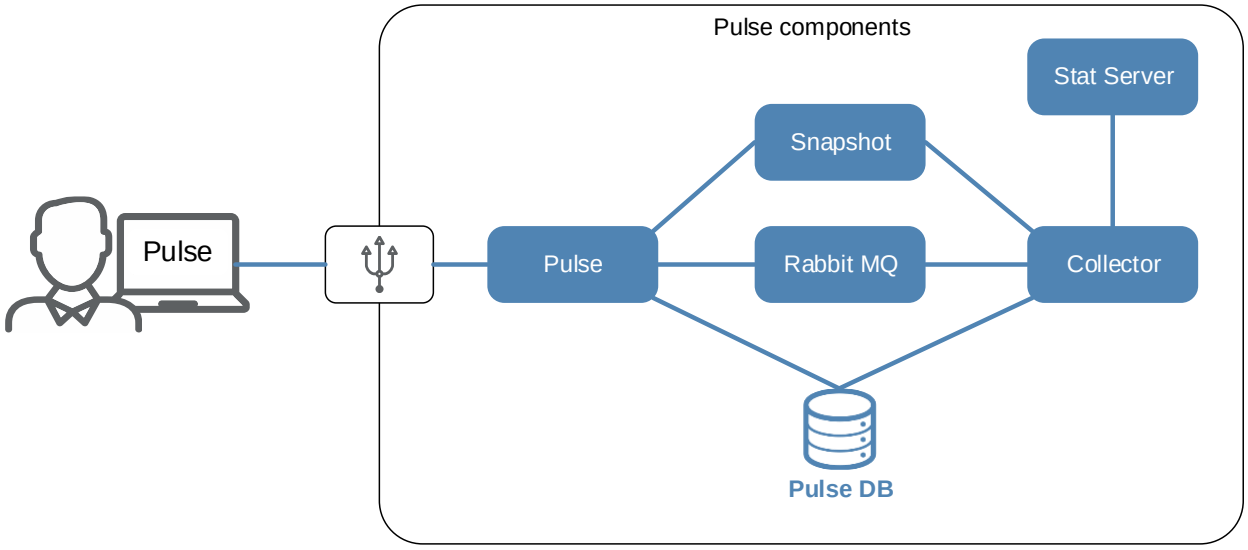

Figure 3 - Pulse Architecture

The following provides an example of the Pulse Dashboard showing a few of the widgets available to visualize operational performance.

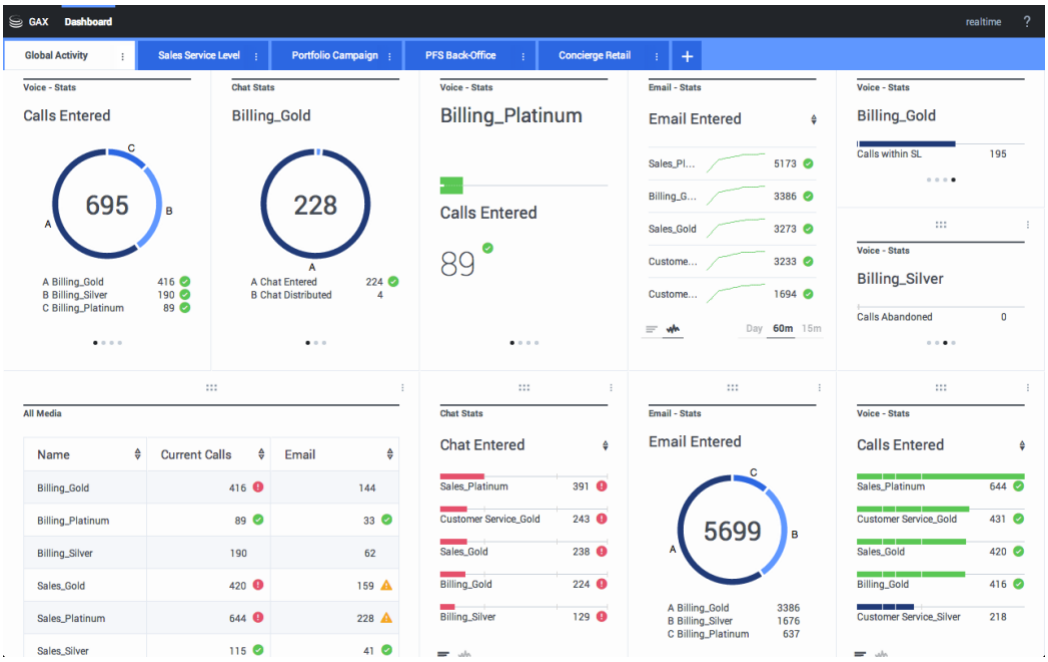

Figure 4 - Genesys Pulse

Further information on Genesys Pulse (including additional screen shots) may be found at:

http://docs.genesys.com/Documentation/EZP
http://docs.genesys.com/Documentation/EZP/8.5.0/Deploy/Pulse

Historical Reporting

Genesys Historical reporting consists of the Interaction Concentrator process and databases, Info Mart ELT process and Info Mart database and CX Insights. A high level diagram of these components is shown below:

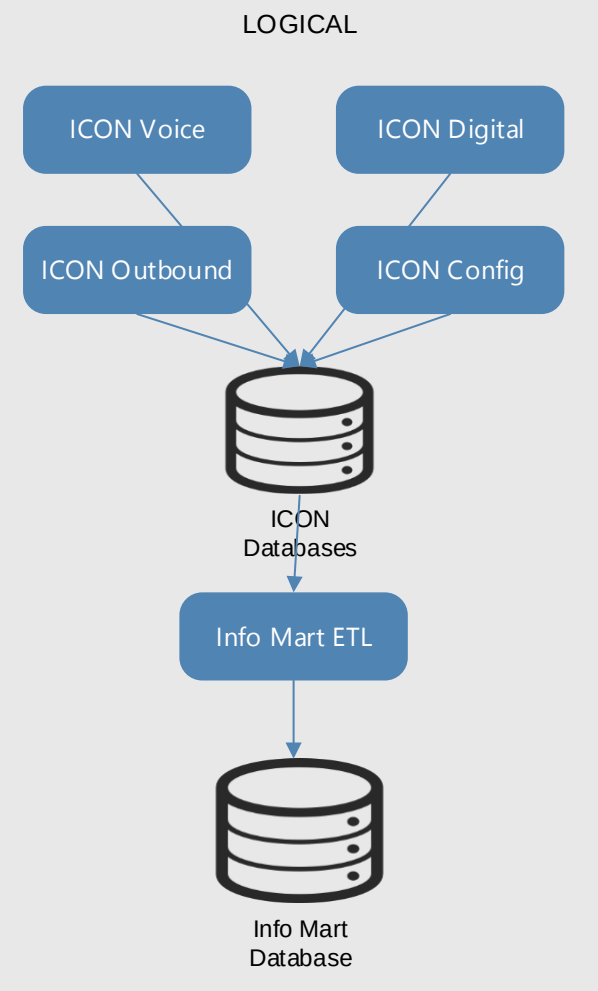

Figure 5 - Interaction Concentrator Architecture

Interaction Concentrator (ICON)

Interaction Concentrator collects and stores detailed data from various sources (such as SIP Server, T-Server, Interaction Server, Outbound Contact Server and Configuration Server) in a contact center that is powered with Genesys software. ICON provides detailed data generated by the individual component which is then correlated and combined by downstream processes such as Info Mart.

Further information on Genesys ICON may be found at:

http://docs.genesys.com/Documentation/ICON

Info Mart

Genesys Info Mart is used to create and maintain a datamart for contact center historical reporting. Info Mart provides a single, consolidated data source for business analytics and data-mining. Info Mart collects cradle to grave interaction details from Genesys ICON and other Genesys components, and transforms this data into a ready to report format for end users and applications, and supports data from all Genesys supported media types. The Info Mart database is utilized by Genesys CX Insights.

Further information on Genesys Info Mart can be found at:

http://docs.genesys.com/Documentation/GIM

Genesys Customer Experience (CX) Insights

Genesys CX Insights provides reports and dashboards that summarize contact center activity. Reports display contact center activity using easy-to-read grids, as shown in the figure Example Report, while dashboards summarize a wider range of information using a variety of visual devices, such as those shown in the figure Example Dashboard. Genesys CX Insights 9.0 is powered by MicroStrategy 10 software.
Beginning with release 9.0, Genesys CX Insights replaces Genesys Interactive Insights (GI2), the historical reporting tool used in previous Genesys releases. For information about historical reporting in older deployments that use GI2, see the GI2 documentation.

3.4.3 Configuration and Management

The Genesys Management Framework is the foundation which provides Configuration and Management of the Genesys CX Platform. The Genesys Management Framework provides the following administration functions: Configuration, Access Control, Solution Control, Alarm Processing, Troubleshooting, and Fault Management.

Further information on the Genesys Management Framework, which provides the Configuration and Management functions, may be found at:

http://docs.genesys.com/Documentation/FR

The following components are included within the Configuration and Management layer:

- Genesys Administrator / Genesys Administrator Extensions
- Configuration Server
- Solution Control Server
- SNMP Master Agent
- Message Server
- Local Control Agent
- DB Server (Used in prior Genesys version or for other Genesys components)

The following legacy components should not need to be deployed therefore they are not covered in the Common Components blueprint:

- Solution Control Interface

- Configuration Manager
- Load Distribution Server - LDS is not part of the Common Components Blueprint as it is not recommended for URS. It may be appropriate for some scenarios and is discussed in the other Blueprints where applicable.

Genesys Administrator / Genesys Administrator Extension (GAX)

Genesys Administrator is a Web-based product that simplifies operation management with the ability to provision, deploy, and monitor all Genesys applications. For monitoring GAX displays the status and configuration of all installed Genesys solutions and information about detected alarms and maintenance logs. You can start and stop solutions or single-server applications, including third-party applications, through this interface. GAX also allows advanced handling of maintenance logs and advanced viewing of host processes. Genesys Administrator was the first version of Genesys web best management interface. While Genesys Administrator may still be required in limited instances in general it has been superseded by Genesys Administrator Extension (GAX).

GAX is the next generation of Genesys Administrator and adds more flexibility and support for additional platforms, along with an improved user interface.

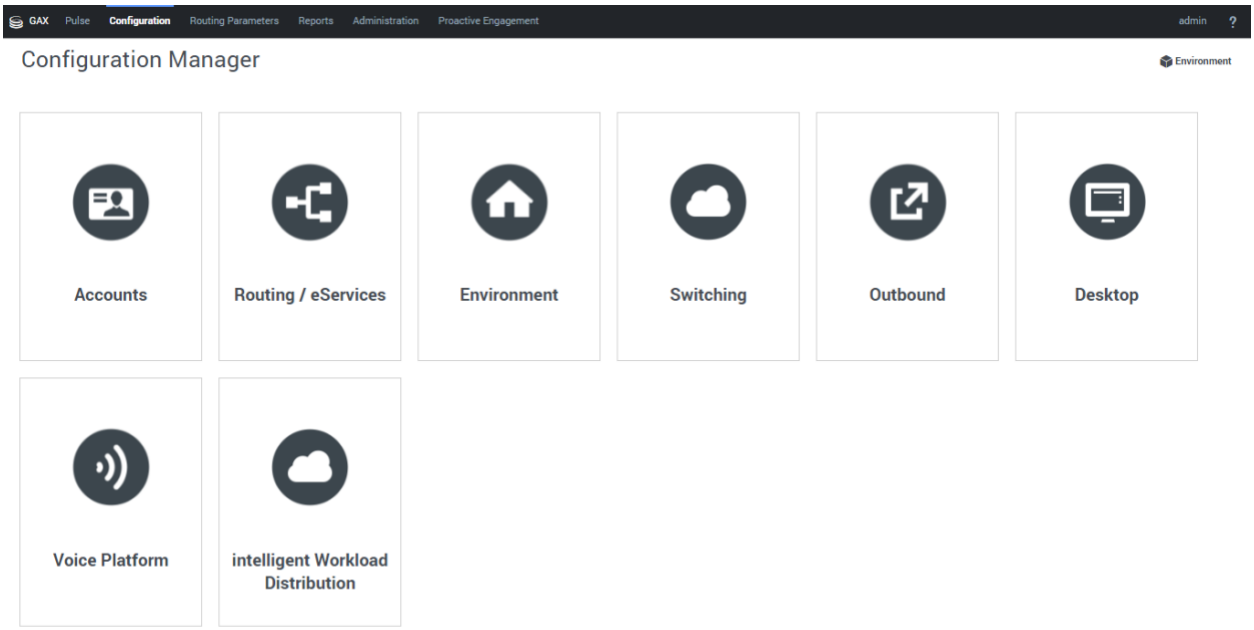

Figure 6 - Genesys Administrator Extension

Local Control Agent

The Local Control Agent (LCA) is a daemon component that monitors, starts, and stops Genesys server applications as well as third-party server applications that you have configured in the Genesys configuration environment. In addition, LCA detects failures of Genesys servers and communicates their roles in redundancy context.

Configuration Server

Configuration Server provides centralized access to the Configuration Database, based on permissions that super administrators can set for any user to any configuration object. Configuration Server also maintains the common logical integrity of configuration data and notifies applications of changes made to the data. Optionally, you can run Configuration Server in Proxy mode to support a geographically distributed environment or reduce the client load on the Configuration Server.

Solution Control Server

Solution Control Server (SCS) is the processing center of the Management Layer. It uses Local Control Agents to start solution components in the proper order, monitor their status, and provide a restart or switchover in case of application failure. SCS also processes user-specified alarms. In a multi-site environment multiple Solution Control Servers can be deployed in Distributed mode (referred to as Distributed Solution Control Servers) to distribute management-related tasks locally to each site.

SNMP Master Agent

SNMP Master Agent is an interface between the Management Layer and an SNMP-compliant network management system (NMS). It distributes:

- SNMP traps, which are converted from alarms, from Solution Control Server to NMS.
- SNMP commands, which a user enters from an NMS interface, back to SCS for further processing

Note: Genesys recommends that Net-SNMP is deployed instead of the Genesys SNMP Master Agent.

Message Server

Message Server provides centralized processing and storage of all maintenance events that Genesys server applications generate. Events are stored as log records in the Centralized Log Database (also referred to as Log Database) where they are available for further centralized processing. Message Server also checks for log events configured to trigger alarms. If it detects a match, it sends the alarm to Solution Control Server (SCS) for immediate processing. If Distributed Solution Control Servers are deployed then a dedicated Message Server is deployed through which the SCS will communicate with each other.

DB Server

Provides the interface between some Genesys applications and the RDBMS holding the operational databases for solutions. The latest instances of many Genesys applications access the RDBMS directly. Customers utilize several industry standard RDBMS to store the actual data.

Databases

The Genesys Management layer stores information in several databases:

- Configuration Database – Stores configuration details on all applications and resources
- Log Database - stores all log records, including interaction-related records, alarm history records, and audit records.
- Cassandra – NoSQL database

Customers are responsible for providing the appropriate DBMS.

3.5 Component View

3.5.1 Genesys Components

The following table lists the Genesys components that make up the Genesys Common Components.

Category	Component	Version	Notes
Routing	Orchestration Server (ORS)	8.1.4+	
	Universal Routing Server (URS)	8.1.4+	
	Stat Server	8.5.1+	
	Universal Contact Server (UCS)	8.5.0+	
	Genesys Engagement Services (GES)	8.5.1+	
	Genesys Rules	8.1.3+	Required for additional HA support
	Genesys Web Services (GWS)	8.1.2+	

Category	Component	Version	Notes
Administration			
	Genesys Administrator	8.1.3+	UI
	Genesys Administrator Extension (GAX)	8.5.2+	
	Genesys Rules Authoring Tool	8.1.3+	
Configuration	Configuration Server	8.1.3+	
	Local Control Agent (LCA)	8.1.3+	
	Message Server	8.1.3+	
	SNMP Master Agent	8.1.3+	
	Solution Control Server (SCS)	8.1.3+	
Database			
	DBServer	8.1.3+	

Category	Component	Version	Notes

Reporting			
	Stat Server	8.5.1+	
	Pulse	8.5.1+	
	Interaction Concentrator	8.1.5+	
	Info Mart	8.5.0+	
	CX Insights	8.5.0+	

The following desktop applications or deployment services may also be deployed. These applications typically execute at the local desktop rather than server applications.

Category	Component	Version	Notes
Agent Application	Workspace Desktop Edition	8.5.1+	
Agent Endpoint	Interaction Workspace SIP Endpoint	8.5.1+	
Script Development	Composer	8.1.3+	Used for IVR & routing strategy development
	Genesys Rules Development Tool		Eclipse plug-in used for Rules development

Table 1 - Genesys Component List

3.5.2 3rd Party Components

The following provides an overview of 3rd party components which are utilized within this solution and provides specific recommended 3rd party components. Some alternatives may be utilized however the recommended components are encouraged due to the level of field knowledge and experience with these technologies.

Cassandra
Cassandra is an open source, fault-tolerant, and highly scalable NoSQL database for mission-critical data. It provides built-in support for replication of data across multiple data centers. Cassandra has been used in many high profile, high volume systems including Facebook. Cassandra is part of the Apache Software Foundation.

Genesys utilizes Cassandra for a number of components including Genesys Feature Server (for voicemail and provisioning storage), Genesys Orchestration Routing Server (ORS), Genesys Interaction Recording (GIR), and Genesys Engagement Services (GES) which is used to provide callbacks. Genesys recommends that customers deploy an externalized Cassandra instance which used by Genesys solutions. A single exception to this recommendation is Genesys Feature Server which currently its' own embedded Cassandra instance.

Further information on Cassandra may be found at the following web links:

http://en.wikipedia.org/wiki/Apache_Cassandra
http://cassandra.apache.org/

Elasticsearch

Elasticsearch is a search engine based upon Lucene. It provides a distributed, full-text search engine with an HTTP web interface and schema-free JSON documents. Genesys uses Elasticsearch to store used within ORS, Genesys Web Services including Workspace Web Edition, Web Engagement and Knowledge Center. Elasticsearch is also a component which is being considered for additional products. The data in Elasticsearch may be used to drive quick interactivity and searching or it may be used for operational/performance monitoring and analytics via Kibana (Elasticsearch visualization tool) or custom tools.

Cassandra and Elasticsearch are required based upon the specific Genesys products which will be deployed. The table below provides a matrix to indicate when these components are required within the Genesys deployment.

	Cassandra	Elasticsearch / Kibana
Common Components		
ORS	Optional	Optional
UCS	Required	Required
GWS	N/A	Optional
Voice		
SIP Voice with ORS	No	N/A
SIP Voice Mail	Mandatory/Embedded in Feature Server	N/A
GIR	Mandatory	Mandatory
Digital		
Email	N/A	N/A
Chat	Optional for HA. Required for GMS	N/A
Co-Browse	Mandatory	N/A
Genesys Engagement Engagement (GES)	Mandatory	N/A
Knowledge Center	Optional for CMS	Mandatory
Other		
Web Services	Mandatory	Mandatory

UCS	Not required in 8.5. Required in 9.0	Not required in 8.5. Required in 9.0
Context Services	Required due to use of UCS	N/A

Table 2 – Cassandra/ES Required Matrix

Redis

Genesys components such as Engagement Services, Web Services and CX Contact use Redis for caching. These components are delivered using Microservices patterns utilizing Docker and Redis images are provided as part of the deployment pipeline.

Web Servers

Web/application servers are used to serve up the application logic for the Genesys solutions such as the SCXML which defines the routing strategy and VoiceXML which defines the IVR logic. Typically a J2EE application server is used. The actual web/application server chosen will vary based upon the customer's preferences for deployment and operations.

HTTP Load Balancer

An HTTP Load Balancer is commonly required to distribute inbound requests across multiple servers. The load balancer may manage request distribution across a server farm at a physical location or distribution and failover across multiple physical locations. The load balancer may establish affinity between the client and server if "sticky sessions" are required. A load balancer may also perform some security management tasks such as client authentication via tokens or certificates thereby reducing the demand on the application tier.

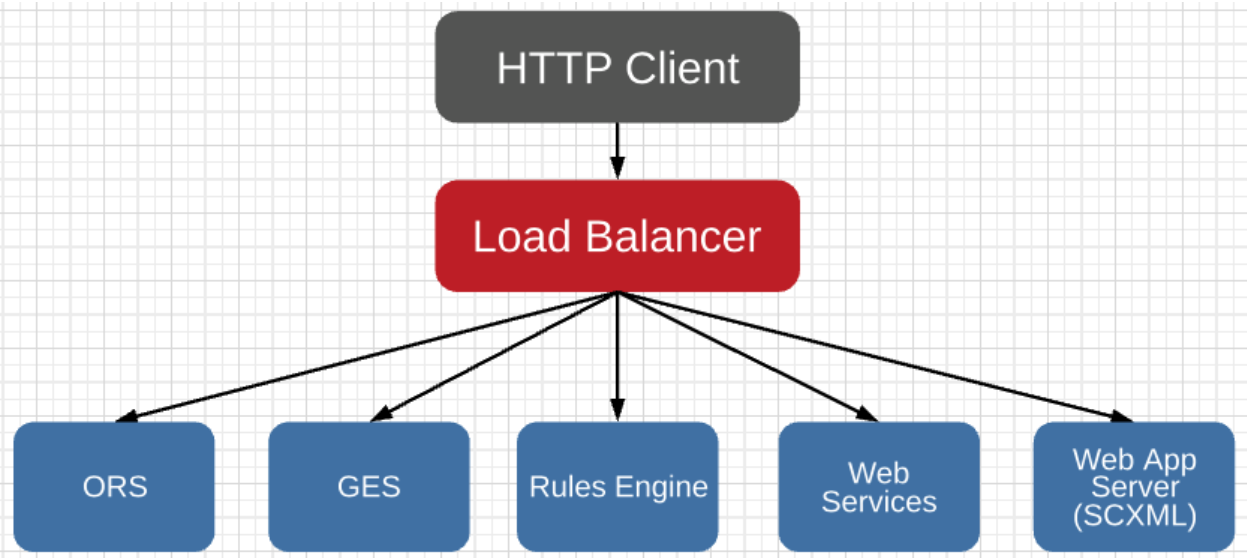

Figure 7 - HTTP Load Balancer Scope

Network Management System (NMS)
A network management system (NMS) is a set of operations and management tools deployed which allow an enterprise to monitor the health of the various components (hardware and software) connected to a network. A NMS can perform a myriad of tasks. Genesys can send alarms via SNMP to the NMS using Net-SNMP, or the SNMP Master Agent if applicable, to provide the enterprise visibility to specific performance metrics or events. Genesys also supports polling allowing an NMS to proactively check on the status of Genesys applications.

Component	Recommended	Version	Note
Network Management System	Zabbix		Alternatives - HP OpenView, Nagios, Tivoli, OpenNMS
HTTP Load Balancer	Customer preference		Genesys has provided sample documentation on NGINX for several components. F5 and other load balancers may also be used.
Database	Microsoft SQL Server Oracle	2012 12c	
Storage	Cassandra	3.x+	
Operating System	Windows Server Red Hat Linux	2012 6	
Virtualization	VMWare ESXi	5.1+	
Storage for Visualization	Elasticsearch	2.x	
Catching	Redis		

Table 3 - 3rd Party Component List

Note:

- RDBMS is often a customer preference. Genesys recommends either Microsoft SQL 2012 or Oracle. For Business Continuity solutions there are specific requirements on the features utilized.

3.6 Limits and Constraints

There are components which have specific limitations on the operating system, database or deployment model. Key limitations are:

- Cassandra may be deployed on either Linux or Windows. Genesys recommends Cassandra is deployed on Linux
- Pulse supports a clustered configuration where multiple pairs of Stat Servers as well as Collectors can be used to spread the load. When the clustered configuration is used all Stat Servers must be configured to with identical connections to receive same events feeds – e.g. connected to the same T-Servers/Interaction Servers. You cannot use an Interaction Stat Server and Voice Stat Server.
- Pulse Quick Updates should be used for change based Agent statistics. While Quick Updates can be configured to deliver change based notifications for numerous statistics such as virtual queues this is not recommended due to the additional Stat Server load, hardware required and minimal benefit. Rather than using Quick Updates a shorter time based update such as 10 seconds should be configured within the Pulse Widget.
- While Genesys routing strategies can integrate with external systems using either RESTful or SOAP based web services Genesys strongly recommends that REST is used.

4 Deployment View

4.1 Solution Deployment

4.1.1 Centralized Deployment

The centralized deployment assumes that the customer has a data center that is reachable by all agents and that the network has the capacity to support the traffic between solution components in the data center and between the agents' desktop/endpoints and the data center.

The common components work with components from other solutions, such as the SIP Voice Blueprint, therefore the Common Components are shown below within the context of an overall architecture. This architecture has been greatly simplified to show communication between the processes. The subsequent text provides details on the inter-process communication.

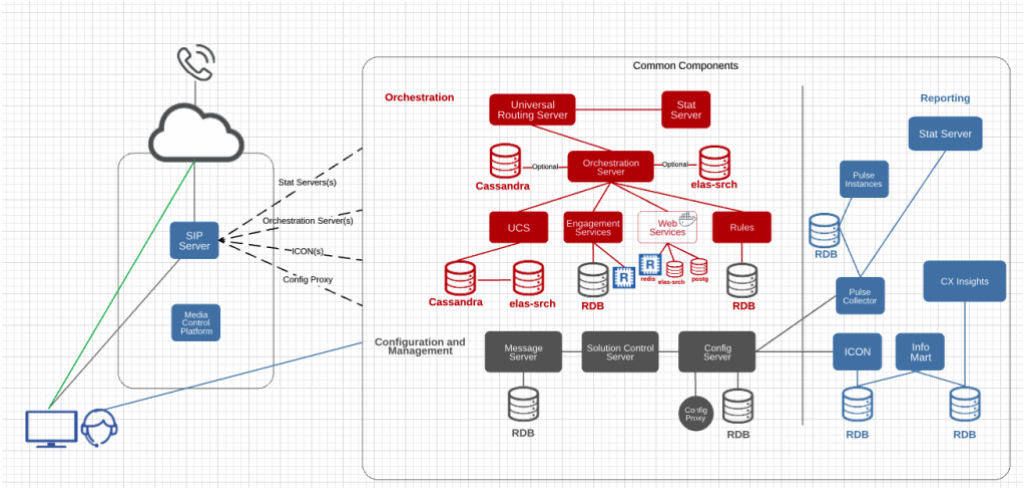

Figure 8 - Centralized Deployment

The Common Components diagram represents a top down or bottom up grouping on the solution components. This can be thought of as similar to a Northbound/Southbound approach. The lowest layer is Management and Configuration. Nothing can start without the management and configuration operating. Within the Management and Configuration layer the Solution Control Server manages all processes and components therefore it is designed to start and run autonomously. Once the Solution Control Server starts up it then will start all other components/solutions within the environment starting with the Configuration Server. The Configuration Server allows all other components to receive details on their software configuration and resources within the environment. As the SCS starts other components each component will inquire with the Configuration Server (or Config Server Proxy…) to receive details on it's configuration as well as the configuration of other applications and resources in the environment. The SCS will start the Orchestration layer and required solution, Interaction processing

components (SIP Server, Interaction Server, Media Control Platform), Workforce Optimization and Reporting.

The Orchestration layer executes the interaction handling strategy that has been established by the enterprise. If any interaction is received by Genesys (voice, email, chat, SMS, etc.) it is passed over to the Orchestration layer which invokes a strategy to run. The strategy is simply a set of logical events that are performed to process the interaction. For example with voice call the strategy may look at the ANI/CLID and query Context Services to determine if a caller can be found with that caller id. If it is found the strategy may look at recent interactions the customer has had, utilizing further information from Context Services, and then query Genesys Rules to business rules which may define parameters and conditions on how the interaction should be handled. For example if the customer has contacted the enterprise previously within the prior 24 hour period this call may be directed the last agent if available. The routing strategy would contact Stat Server to determine is this agent is available. If the last agent is not available then the call may be routed to agents that are most proficient in resolution for repeat callers. As multiple agents may meet this criteria the routing strategy would then contact Stat Server to determine the most appropriate agent to receive this interaction, for example the agent that has been idle the longest and then route the interaction to the selected agent.

The other layer contained in the common components is the reporting layer which is predominantly passive. The components within the Reporting layer receive events on the processing of interactions and the current status of contact center resources, or changes in status, and processing of interactions. Real-time reports are provided through Pulse Dashboards and while historical data is captured and transformed into historical reports which are accessed through CX Insights. The majority of the reporting information is received from interactions and agents and not directly generated via the Orchestration layer. Reporting data may also be generated without any interactions present. For example if an agent logs into the system and places and outbound call then the Reporting layer would receive information both about the agent activity (login) as well as the actual interaction (voice call).

There are user interfaces provided for administration, reporting and agent/supervisors. Both Administration and Reporting are accessed exclusively through web based interfaces. For agents/supervisors you have both thick client and thin client options (WDE and WWE).

Note that the DBMS node is another component typically provided by the customer

The following table lists the components that make up each of the nodes. Note: Each node may represent one or more servers.

Node	Component	Comments
Orchestration	Orchestration Server (ORS)	
	Universal Routing Server (URS) Stat Server Routing	
	Stat Server Routing	
	Universal Contact Server	
	Genesys Engagement Services	

	Genesys Rules Engine	
	Genesys Web Services	
Framework	Configuration Server	
	Configuration Server Proxy	
	Solution Control Server	
	Distributed Message Server	
	Config DB Server	
	Log DB Server	
	SNMP Master Agent	Net-SNMP is recommended instead of SNMP Master Agent
	Genesys Administrator	
	Genesys Administrator Extensions	
	Genesys Rules Development Tool and Authoring Tool	
Reporting	Stat Server (Multiple instances as required)	
	Pulse (and components)	
	Interaction Concentrator	
	Info Mart	
	CX Insights	
Agent Support	Workspace Desktop Edition or Workspace Web Edition	Workspace Desktop or Web Edition may be used Workspace Web only requires a browser as the logic is delivered by Genesys Web Services
	Composer	

Table 4 – Logical Data Center Nodes

Please see section 6.1 Solution Sizing Guidelines for details on the sizing of the architecture.

4.2 High Availability Deployment

Genesys has architected our software to deliver the robustness and availability expected of the world's leading customer experience platform. To provide resiliency Genesys recommends deploying the solution with High Availability (HA) options for all components.

4.2.1 High Availability Overview

There are several high availability models used by Genesys. The following provides an overview of the models and their definitions.

Hot Standby Redundancy Type
Genesys uses the term hot standby to describe the redundancy type with which a backup server application remains initialized, clients connect to both the primary and the backup servers at startup, and the backup server data is synchronized from the primary server. Data synchronization and existing client connections to the backup guarantee higher availability of a component. Configuration Layer and Management Layer components do not support hot standby between pairs of redundant components. They do support switchover between client applications configured with this type.

Hot standby redundancy type with client connection support is implemented in T-Servers for most types of switches and also implemented in URS. It is not implemented in applications of other types.

Active / Active Redundancy Type
Some Genesys components operate in an Active / Active configuration. In an Active/Active model the single common characteristic is that each component is actively processing client requests.

- Most Active/Active components are stateless while others share state via active synchronization.
- For many Active/Active components Genesys follows a web/application server paradigm, clustering multiple instances together for availability and scalability using a standard N+1 deployment. Other components may only be deployed as an Active/Active pair.

There are some Genesys processes such as Interaction Concentrator which provide Active Redundancy but follow a parallel processing model.

Warm Standby Redundancy Type
Genesys uses the term warm standby to describe the redundancy type with which a backup server application remains initialized and ready to take over the operations of the primary server. Inability to process interactions that may have originated during the time it took to detect the failure is reduced to a minimum. Warm standby redundancy type also eliminates the need to bring a standby server online, thereby increasing solution availability.

The standby server recognizes its role as a backup and does not process client requests until its role is changed to primary by the Management Layer. When a connection is broken between the primary server and the LCA running on the same host, a failure of the primary process is reported. The Management Layer will communicate with the LCA where the standby process resides, instructs the process to change its role from standby to primary, and the former standby starts processing all new requests for service.

While normal operations are restored as soon as the standby process takes over, the fault management effort continues. It consists of repeated attempts to restart the process that failed. Once successfully restarted, the process is assigned the standby role.

There are some components such as Outbound Contact Server which vary from this model. For example OCS uses Enhanced Warm Standby. It still follows the Warm Standby definition but there is some campaign synchronization that occurs so that on a failover the active campaigns will continue to operate.

Cold Standby Redundancy Type

Some Genesys components may be deployed in cold standby. With cold standby a component is deployed but not running and must be explicitly started based upon a failure condition. Cold standby components may be started through scripting or manual intervention. Cold standby is most often used to provide continued operations if there is a site or data center failure. Specifically if one site is lost altogether, which includes both the primary and backup instances, then alternative cold standby components which reside at a secondary site may be started.

Platform Independent versus Platform Specific Redundancy

Genesys high availability design operates at a Genesys component level and is not dependent upon a specific Operating System or hardware platform. Genesys high availability represents a proven, hardened approach to help maximize service availability.

Customers may also want to leverage high availability options provided at lower layers within by their current technology stack. The high availability options and flexibility that customers use has increased significantly with virtualization as the virtual (logical) servers operate on top of a hypervisor and the hypervisor may provide flexibility in how it manages the virtual servers. Current hardware based high-availability may provide duplicate hardware systems with fully replicated sets of components, and more advanced cluster architectures, in which a group of independent loosely coupled computers act as a single system from an external viewpoint. In case of a hardware failure, the high availability configuration will typically attempt to switch over to the standby system in traditional configurations, or disperse the work to the other systems in the cluster.

While customers may want to leverage their hardware redundancy in addition to Genesys provided high availability it is important to understand the capabilities and scope that each solution can address. With virtualization there are a number of solutions now available to customers. For example with VMWare two common technologies that may be used are vMotion and DRS. While these technologies have clear benefits one limitation is that these technologies do not typically protect from failures which are covered by Genesys High Availability such as potential software isolation scenarios or software faults. If a virtual or physical server failure occurs and the server needs to be moved this may be equivalent to rebooting the machine. Once the server comes up the Genesys software will initialize and begin operating normally however during the window if Genesys high availability was not implemented then the contact center would lose functionality. With Genesys high availability a server failure would result in Genesys switching over/redirecting communication as appropriate and Genesys would manage the contact center services delivered to ensure continued operation.

A more widely accepted use of VMWare HA/DR capabilities with Genesys is to support geographic diversity and business continuity. In this instance if there is a complete site failure the business must understand and tolerate the potential service impact as acceptable. Acceptable is typically quantified based upon the probability of such an occurrence, measurable business impact, and the investment required to support a higher level of availability. Enterprises may also distribute components across

locations to mitigate the business impact of a failure. A common approach is to move from two primary data center to three data centers. Additionally the business may require and architect different levels of availability based upon the channel. For example voice processing components may be active across multiple sites to ensure continued operations while other channels such as email which are considered less critical may tolerate an interruption in availability, provided that customer interactions are never lost.

4.2.2 High Availability Summary

High availability for Genesys components generally follows one of two models:

1) Genesys components use a primary and backup process

2) Genesys components use HTTP and rely on a load balancer for HA

In both models a minimum of two instances must be deployed for high availability.

With Genesys High Availability Primary/Backup if a backup application is configured and started and the Management Layer detects a failure of the primary application then Genesys will automatically switch operations over to the backup instance. The one exception to this is the Solution Control Server which manages the primary/backup failure of other components. It must be able to operate independently therefore has an autonomous, self-aware primary/backup negotiation that occurs on start up.

For Genesys components which use HTTP a load balancer is generally required to distribute the requests as well as determine the active instances and manage failover. Genesys components may be deployed in an active/active configuration while other components operate in warm standby. There are also be requirements for sticky sessions (session persistence) with some components while other components are stateless. The load balancer must be capable of supporting both types of configuration.

The following diagram depicts high availability mechanisms for each component considered in the Common Components blueprint.

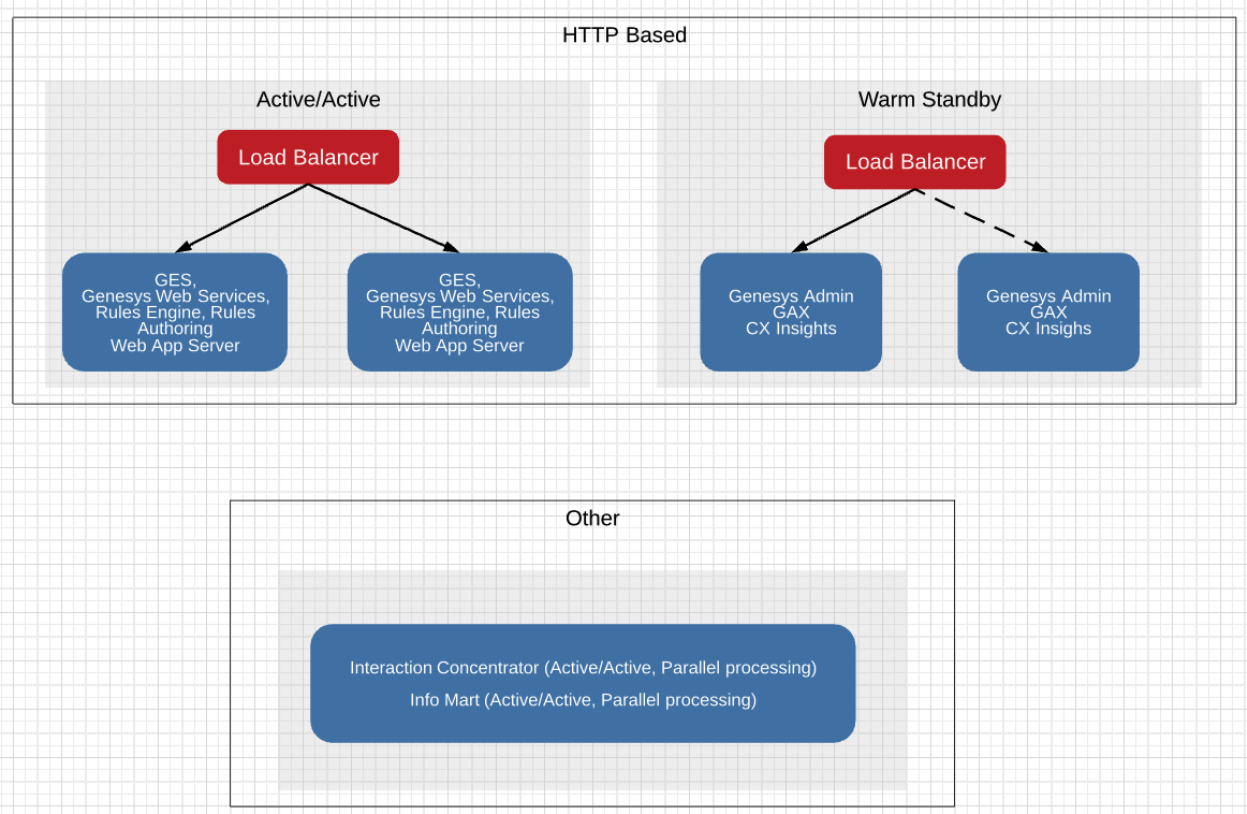

Figure 9 - High Availability Approaches

The following list the high availability levels supported by the respective components:

Genesys Component	HA Level
Universal Routing Server (URS)	Hot Standby
Orchestration Server (ORS)	Warm Standby / Cluster
Stat Server	Warm Standby
Universal Contact Server (UCS)	Warm Standby
Genesys Engagement Services (for Context Services)	Load Balanced / Active
Genesys Rules Engine (GRE)	Load Balanced / Active
Genesys Web Services	Load Balanced / Active

Genesys Component	HA Level
Configuration Server	Warm Standby
Config Server Proxy (CSP)	Warm Standby
Solution Control Server (SCS)	Warm Standby
Message Servers	Warm Standby
SNMP Master Agent	Warm Standby
Genesys Administrator / Administrator Extensions	Load Balanced / Warm-Standby
GRAT	Load Balanced / Active

Genesys Component	HA Level
Stat Server	Warm Standby
Pulse	Warm Standby
Interaction Concentrator	Active/Active (Paired data collectors)
Info Mart	Active/Active (Redundant ETL and Databases)
CX Insights	Load Balanced / Warm-Standby (with data replication)

Table 5 - High Availability Summary

Note: All components of the Common Components blueprint should be deployed. The specific components which will be active will depend upon your purchased solutions and the specific use case.

4.2.3 High Availability – Orchestration

The following section provides details on the high availability mechanism and considerations for each of the Orchestration components.

Universal Routing Server

High Availability options for Universal Routing are provided through both Redundancy and High Availability.

Redundancy and service recovery occurs through automatic Management Layer failover processes. With high availability both primary and backup URS are active and have data synchronization. If URS fails, the service may be on hold briefly, which could result in non-routable interactions that are recoverable. Virtually no loss of data or interactions will occur for affected interactions processed by the failed URS. Only a routing delay occurs for these interactions. Genesys URS also uses strategy replay which can replay Routing Strategies from the point of failure to ensure continuous real-time routing.

Orchestration Server
Orchestration server can be deployed in either a primary/backup or clustered mode to provide redundancy and scalability.

Standard high availability (HA) is provided by deployment a primary/backup ORS pair in a warm standby redundancy configuration. A pair consisting of primary/backup ORS instances is referred to as a Node. Multiple ORS Nodes can work together in a clustered environment. Within the cluster an ORS Node (primary/backup pair) called the assigned node is responsible for processing given interactions. An alternative Node (primary/backup pair) called the reserved node provides Node level redundancy. The reserved node can be another node in the same data center or another node in another data center. Each ORS Node in the cluster has it's own connection to URS.

The ORS cluster deployment introduces the possibility to distribute the load of incoming Interactions (voice calls, multimedia and http requests) across all ORS Nodes. Load Balancing for Multimedia Interactions means that the nature of the "pulling" mechanism provided by Interaction Server guarantees that new sessions created from this trigger are automatically distributed across the cluster.

Starting with 8.1.400.45, ORS can be configured for voice call processing recovery upon an ORS primary/backup switchover without the Cassandra persistence/recovery feature. Requires Universal Routing Server 8.1.400.27+.

The following diagram illustrates an ORS Cluster showing both ORS HA and logical cluster nodes.

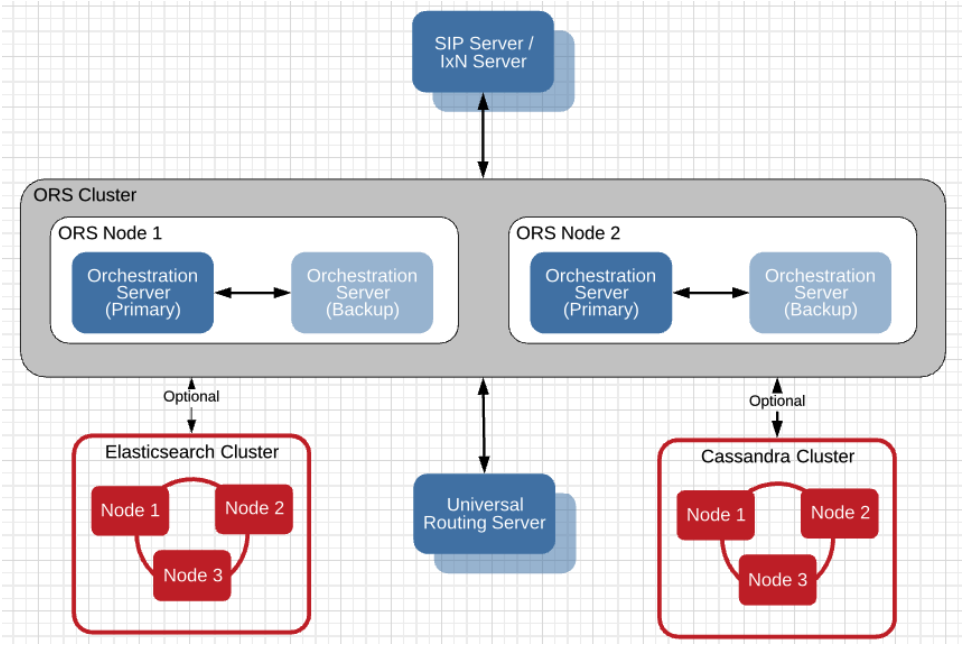

Figure 10 - Orchestration Cluster

Stat Server

Genesys Stat Server is deployed in primary/backup warm stand-by configuration. It begins tracking metrics for resources/objects as soon as it receives a request. There statistics requests are not shared between primary and backup instances therefore there is not synchronization. Upon failure the Stat Server client applications would simply connect to the alternative Stat Server instance – the backup which is now primary – and it will provide metrics updates and distribution.

Universal Contact Server

Universal Contact Server is deployed in a primary/backup configuration. UCS does not scale beyond a single instance therefore a primary/backup pair is the maximum UCS footprint in any architecture. It is recommended to have the UCS primary/backup instances should be in the same location as the UCS database.

Genesys Web Services

Genesys Web Services (aka HTCC) is a RESTful web services layer which is deployed within an application server. High availability of GWS is accomplished by deployment multiple instances in an Active/Active configuration with the traffic distributed across instances using a standard HTTP load balancer. GWS also uses Cassandra.

Genesys Engagement Services

Genesys Engagement Services is deployed in an Active/Active configuration and provides high availability by supporting the ability to run multiple instances of Genesys Engagement Services server in a single,

logical entity called a cluster. In this context, a cluster refers to running instances of Genesys Engagement Services Server (GMS) or nodes, where each additional GMS instance is able to share in the handling of the workload as well as resume the tasks of a failed or removed node. Each GMS node has similar configurations: connection to Orchestration Server and Configuration Server. GMS and its components do not maintain any of its state data in memory so any GMS node can process a given API request. The API state data is maintained in Cassandra (distributed data store) so that any node can access the data.

For example, if there are two nodes within a GMS cluster and Node 2 fails then Node 1 can continue processing Node 2 sessions.

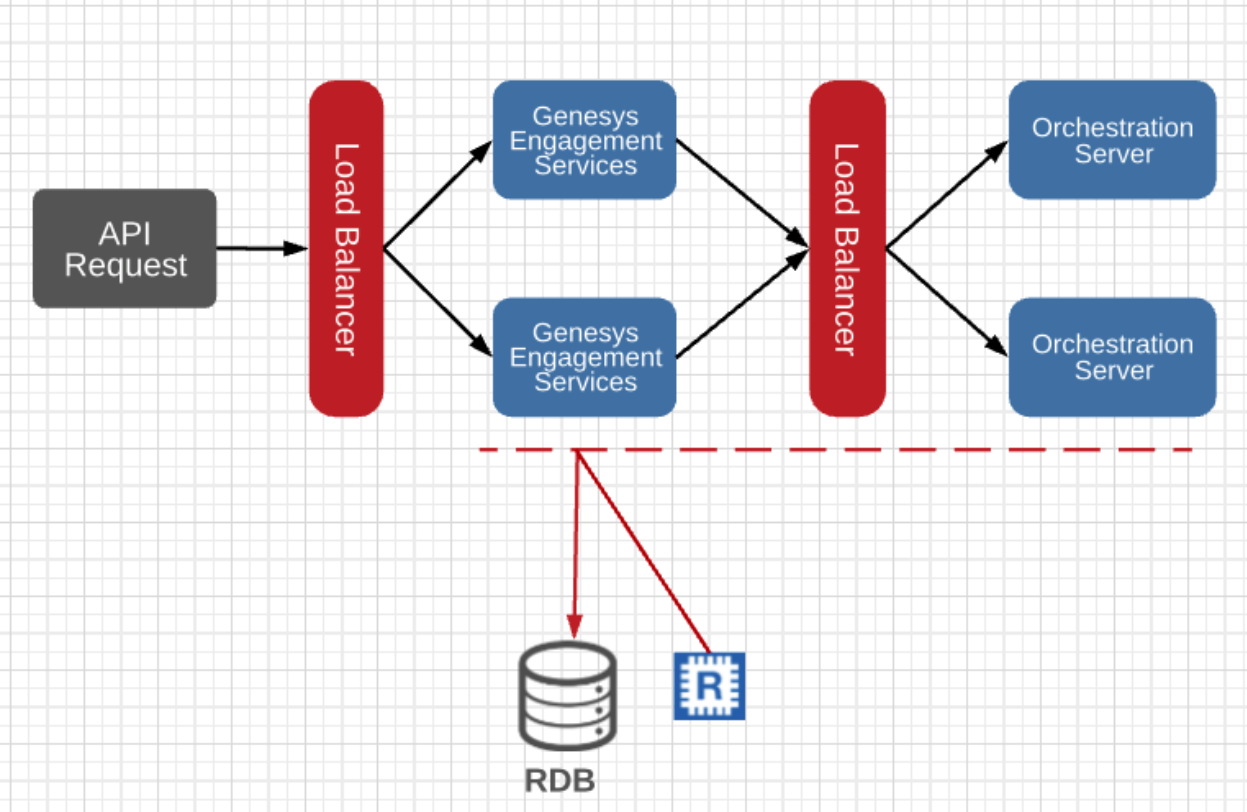

Figure 11 - Genesys Engagement Services High Availability

Genesys Rules High-availability

GRAT

GRAT servers can be configured as active/active (or used in warm standby) for resiliency and availability, enabling almost instant switchovers between GRAT nodes that are members of the cluster. All cluster members connect to the same database repository. No single GRAT node is considered primary - they are all equal partners in the n-node cluster. The load balancer must be configured for session persistence so that once the initial communication has been established all subsequent communication is sent to the same GRAT node. Note: Active/Active support was added to GRAT in version 8.5.3

GRE

The Genesys Rules Engine (GRE) can be set up as a HTTP cluster in order to provide a highly available configuration. GRE is considered a critical path application because the execution of rules depends upon at least one node in the system being available. Since GRE is stateless, each rule execution request can be dispatched to any node in the cluster, and should a node fail, another node could execute the request.

The load balancer can be set up to dispatch requests to each GRE node at random, or in a round-robin fashion. There is no need to configure "session stickiness" as there are no sessions to maintain between rule execution requests.

Cassandra

The Orchestration layer uses a Cassandra NoSQL DB. Cassandra is used by multiple components including such as Orchestration Server, Genesys Engagement Services and Genesys Web Services. In addition to the components covered in the Common Components blueprint Cassandra may also be required in a number of other Genesys blueprints (SIP Voice, Digital, GIR/GIA).

Cassandra supports multiple deployment options to provide availability and data consistency. Genesys recommends the use of a 3 node Cassandra cluster. Customers have several options on how Cassandra may be deployed. For example a Cassandra cluster may be shared by all required Genesys components or separate Cassandra clusters may be established to support specific Genesys components. Genesys recommends that customers work with your Cassandra technical experts for further guidance.

Elasticsearch

Orchestration Server uses Elasticsearch to store data, such as ORS session, performance, and node data. That data may then be used for operational/performance monitoring and analytics via Kibana (Elasticsearch visualization tool) or custom tools.

Web Servers

Web/application servers are typically clustered in a standard N+1 deployment to provide high availability and redundancy. An HTTP load balancer is used to receive all the traffic and distribute it to the web servers. The load balancers managing the availability and load. The Workflows and IVR applications which are developed through Genesys Composer are intended to be stateless therefore the load balancer may not require sticky sessions (session persistence) however the specific load balancing requirements will depend upon the application design. The capacity of an individual application server will vary based upon the application complexity and load therefore HTTP load balancers are also used to allow the web server tier to scale horizontally to support the overall need.

4.2.4 High Availability – Reporting

The following diagram depicts high availability of the Reporting layer. Further details on the high availability mechanism and considerations for each component is provided further below.

Pulse (Real-Time)
The following depicts the components which are utilized within Genesys Pulse.

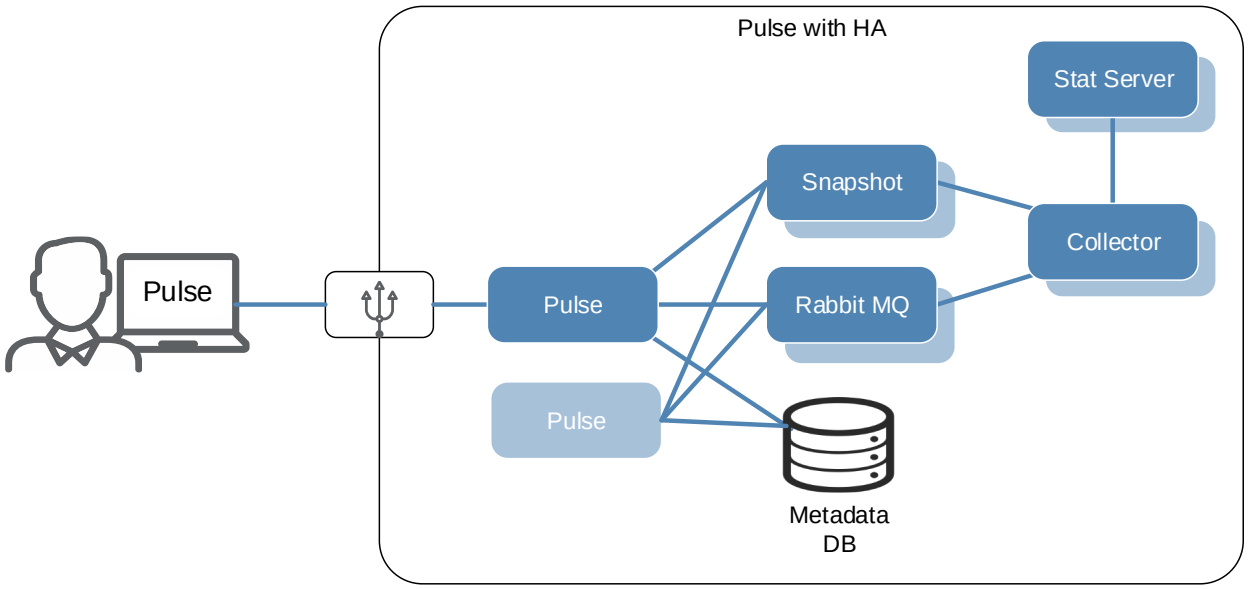

Figure 12 - Pulse High Availability

All real-time metrics originate via Stat Server. Intermediary processes manage the collection, assembly and distribution of this information as defined by the configuration of the Pulse widgets.

High availability is provided at multiple levels and components with Pulse. A Primary/Backup pair of Collectors are deployed. Each Collector is active and connects to both the primary and backup Stat Servers to obtain metrics. Both Stat Servers are actively calculating the same statistics and generating the same real-time data.

Each Collector obtains an identical set of metrics and writes to it's own snapshot file. Pulse directly reads updates from the active (available) snapshot. If Quick Updates are enabled then Pulse will also subscribe to updates provided via Rabbit MQ. RabbitMQ can be deployed in an HA cluster mode to provide high availability however as the impact of a failure of RabbitMQ is limited this component is not typically deployed in high availability. Quick updates are only provided for a set of change based updates therefore if there is a RabbitMQ failure the only impact to a Pulse user is that they would receive updates from the snapshot on the configured time based interval, e.g. 10-15 seconds, rather than the 2-3 second update provided with Quick Updates.

High availability of the GAX/Pulse web server is provided through GAX.

Historical

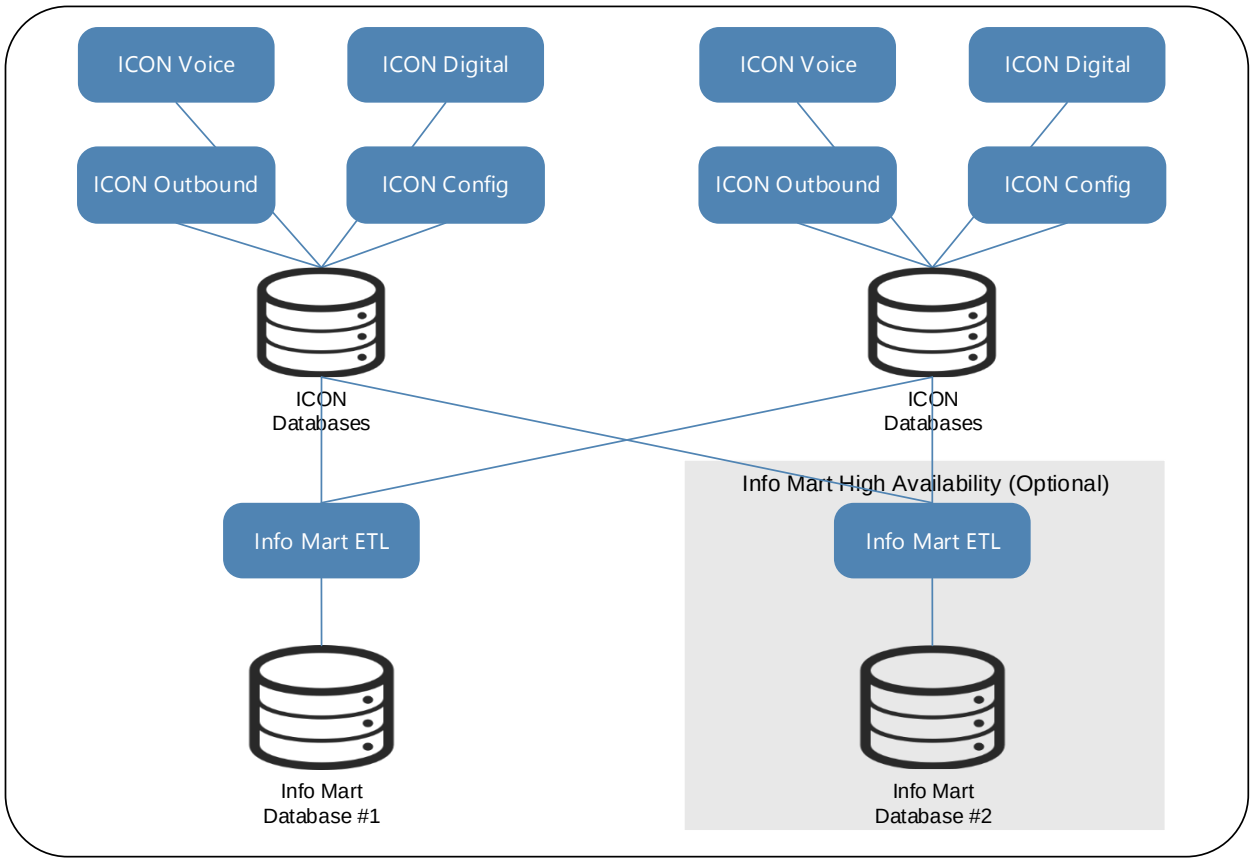

Figure 13 - ICON and Info Mart High Availability

Interaction Concentrator

To provide high availability (HA) of Interaction Concentrator a redundant pair of Interaction Concentrators are deployed to receive events from the each data source (SIP Server, Interaction Server, Config Server etc.). Both ICONs in an HA pair operate in parallel as stand-alone servers; they process incoming data independently and store data in two independent IDBs.

If ICON is located away from its data source, the connection between the two servers is more likely to break. A loss of connection can result in missing notifications about the interaction or agent activity; this data cannot be restored. To prevent data loss due to a loss of connection it is recommended to collocate (install on same host) the HA pair of Icons with the HA pair of their data source (SIP Server, Interaction Server, Config Server, etc.).

A loss of connection between ICON and its ICON database does not necessarily result in a loss of data because ICON continues to write data to the persistent storage until the database connection is restored. However, to minimize network latencies between ICON and the ICON databases it is also recommended to locate the ICON database on same site as corresponding ICON server.

To maximize the availability of the data, Genesys strongly recommends that you:

- Use a separate ICON application instance to store the contact center configuration history.
- Install HA pair of ICON applications on the same hosts as HA pair of their data source (Genesys Configuration Server / SIP Server / Interaction Server / Outbound) that that provides the source event stream
- Genesys also recommends HA architecture for configuration data.

Info Mart

Genesys Info Mart is a process that runs on a regularly scheduled basis to extract, transform (including de-duplication) and load the final historical reporting events into the Info Mart database. Info Mart does not include a native HA product capability. If there is a failure in Info Mart or failure of the host that Info Mart is running on there can be a delay in the historical event processing but there is no data loss to historical reporting. Because Info Mart is not critical to interaction processing and there is no potential data loss with an Info Mart failure many enterprises do not deploy high availability for Info Mart.

While Genesys does not have product level High Availability for Info Mart it can be deployed as cold standby or in an active redundant fashion. For a single data center deployment a cold-standby approach is most common. The cold-standby Info Mart instance would be manually activated if the primary instance is no longer available. The keys which control at which point Info Mart should extract and process records are stored in the Configuration database which is external to Info Mart. High Availability of the database is critical element to historical reporting and should be implemented by the customer based upon the options and standards appropriate for their selected database.

CX Insights

CX Insights is primarily a web based application and delivered through Docker. High availability can be provided by running multiple instances in an active/active manner with traffic distributed through an HTTP load balancer. In order to have high availability all CX Insights instances need to utilize a common data repository.

As CX Insights is not a real-time component and does not impact interaction processing an alternative deployment approach can eliminate the need for a share file system. The BIAR file is simply synchronized from the primary to backup instance. The CX Insights will operate in a primary/backup manner with traffic distributed through an HTTP load balancer. The load balancer should be configured to ensure traffic is directed to the primary instance. If the primary CX Insights instances is unavailable then the HTTP load balancer should be redirected to the backup CX Insights instance.

Genesys recommends that you always deploy MicroStrategy and Genesys CX Insights using Docker, as described in Preparing to install Genesys CX Insights and Installing Genesys CX Insights. Genesys does not support installing Genesys CX Insights without Docker; however, it is technically possible to do so. Genesys does not document the procedures necessary for such a deployment, which requires you to manually install MicroStrategy software, perform a database dump, and then deploy Genesys CX Insights. If you encounter difficulties in deploying MicroStrategy in such a non-Docker deployment, contact MicroStrategy for support.

4.2.5 High Availability – Configuration and Management

The standard approach to high availability supported by many of the Genesys components is to have redundant server processes deployed in a warm standby state. It is expected that most Genesys partners and professional services are familiar with implementing high availability deployments of the Management Framework. Warm standby is used for the following components:

- Configuration Server
- Message Server
- Solution Control Server
- SNMP Master Agent
- DB Servers

In addition, an HA port is configured between the primary and backup Solution Control Servers to allow synchronization of updates.

Specific components which deviate slightly or include additional considerations are:

Genesys Administrator / Genesys Administrator Extensions

Genesys Administrator / GAX is a web based application which is deployed on an application server. This would be deployed in a standard N+1 configuration with all traffic distributed using a a standard HTTP load balancer.

Configuration Server / Configuration Server Proxy

Configuration Server utilizes a standard warm standby deployment. The recommendation is that in addition Configuration Server Proxy should ALWAYS be deployed and deployed in an HA manner. Configuration Server Proxy provides abstraction and reduces the load on the Configuration Server and delivers an additional layer of availability (survivability).

Local Control Agent

Local Control Agent (LCA) is installed on a one-per-host basis and can connect to all Genesys applications located on the host. When a connection between LCA and the Solution Control Server (SCS) is broken then SCS will perform an appropriate recovery action according to the system configuration. SCS uses the Advanced Disconnect Detection Protocol (ADDP) to recognize a loss of connection with LCA. A loss of connection to LCA is interpreted as a failure of the host (that is, as failures of all Genesys components running on that host). LCA operates as a local service on the host and is configured to start automatically or restart upon failure. There is no high availability of LCA.

4.3 Dual Data Center Architecture

Many enterprises run contact-center operations at numerous locations and want to ensure that the architecture provides for geographic diversity and business continuity. These may be loaded or confusing terms but the business objective is simply, "How can I ensure that in a site catastrophe I can continue to deliver service?"

The current Genesys architecture has been designed to ensure that the voice layer can remain fully operational in the event of a disaster. The architecture for other channels may not currently provide the same level of overall availability and service in a worst case scenario. Genesys is continuing to enhance our product to provide more consistent availability support which aligns with current enterprise requirements.

There are a variety of architecture models and considerations based upon the level of survivability that the enterprise is seeking. The options also vary based upon what is supported by specific Genesys components. In general Genesys advocates:

- Local high availability of Genesys components at a site
- Distribution of components to another site to ensure continued operations, with high availability if there is a site failure.

If there is a LAN quality connection between sites it may be possible to split some high availability (primary/backup) components between sites. This is not presently a recommended best practice but it may be a required compromise if the customer does not accept the standard business continuity recommendation. If primary/backup components are going to be split between sites it is critical to review the failover and operational implications. While individual component failures can typically be accommodated, if there is a site failure the remaining location would be operating without any high availability and this may not meet the enterprise needs for business continuity.

More commonly those components which operate in a stateless cluster can be distributed evenly across sites while adhering to the principle of local high availability. Other components which use a single primary/backup pair would be active at one site and deployed in cold standby at the alternative site.

The following table lists each product's approach to High Availability and Dual Data Center deployment.

Genesys Component	HA Level	Failover Mode	Dual Data Center	Comments
Universal Routing Server (URS)	Hot Standby	Automatic	HA pair per DC	N+1 with LDS is not recommended
Orchestration Server (ORS)	Warm Standby	Automatic	Cluster of Nodes. HA pair (Node) per DC.	N+1 HA pairs. Load balancer for HTTP interfaces
Stat Server	Warm Standby	Automatic	HA pair per DC	

Genesys Component	HA Level	Failover Mode	Dual Data Center	Comments
Universal Contact Server (UCS)	Warm Standby	Automatic/ Manual	Cold-Standby at 2nd DC	
Genesys Engagement Services (for Context Services)	Active, Cluster	Automatic	Individual application per DC with load balancing	
Rules Engine (GRE)	Active, Cluster	Automatic	Individual application per DC with load balancing	
GRAT	Active, Cluster	Automaticl	Individual application per DC with load balancing	Requires persistent backend storage
Genesys Web Services	Active, Cluster	Automatic	Individual application per DC with load balancing	DNS can be used to redirect clients (browser) to alternate site

Genesys Component	HA Options	Failover Mode	Dual Data Center	Comments
Configuration Server	Warm Standby	Automatic	Cold-Standby	CS Proxy provides N+1 read cluster.
Config Server Proxy (CSP)	Warm Standby	Automatic	HA pair per DC	Need to reconfigure to reconnect to Cold Standby CS on DC failure
Solution Control Server (SCS)	Warm Standby	Automatic	HA pair per DC	
Message Servers	Warm Standby	Automatic	HA pair per DC	

Genesys Component	HA Options	Failover Mode	Multi-Site	Comments
ICON	Paired data collectors	N/A	HA pair per DC, processes local traffic	ICON pairs should be at the site where the

				"server" traffic is generated
Info Mart	Cold Standby	Manual/ Automatic	Active parallel processing	While Info Mart is commonly cold standby in a single DC deployment with dual DS a separate instance may be recommended
Stat Server	Warm Standby	Automatic	HA pair per DC	
CX Insights	Warm Standby	Manual / Manual	Warm Standby	Requires common backend DB and distributed file system

Genesys Component	HA Options	Failover Mode	Multi-Site	Comments
Workspace Desktop Edition	Client	Automatic	DR based on Business Continuity solution	
Composer	N/A	N/A	N/A	End User tool

Table 6 - Local HA and Dual Data Center Availability

4.3.1 Dual Data Center Considerations – Orchestration

To provide a single virtualized set of agents for all interactions a common Stat Server must be used and Agent-Reservation must be used.

An ORS Cluster can be established between the two data centers. Each site will have it's own ORS Nodes (ORS primary/backup pair) as well as a local URS primary/backup pair. The ORS Cluster will utilize a common Cassandra cluster.

Cassandra is typically deployed in a 3 node cluster. To support a multi-site deployment the deployment should be expanded to a 6 node cluster. The Cassandra cluster continues to operate as a single logical entity even when spanning data centers. Instead of a 3 node cluster it is simply a larger 6 node cluster. If there is a data center failure then Cassandra is simply reduced back to a local 3 node cluster in the remaining site.

4.3.2 Dual Data Center Considerations – Reporting

In a dual data center deployment separate Genesys Info Mart instances would be deployed at each site which operate independently and in parallel. Each Info Mart will connect to ALL Icon database instances.

Info Mart will select which Icon database to use based upon the data quality. If the data quality is the same Info Mart will give preference to the local Icon database. Each Info Mart instance will write the processed data into it's own Info Mart database. While this approach requires twice the data storage requirements of a single Info Mart database many customers would normally be performing data replication at a remote site which would have already doubled the storage requirements. Parallel Info Mart instances is recommended as it eliminates the need to perform additional data replication and ensures up to date data access in case of a failure.

CX Insights should be installed on multiple servers at each data center in N+1 configuration. At the primary data center all instances of CX Insights are active while at the other data center the CX Insights may be passive.

Since CX Insights is using Docker, it allows you to build, run, test, and deploy distributed applications that are based on Linux containers.

Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple CX Insights instances. It enables you to achieve fault tolerance in your applications, seamlessly providing the required amount of load balancing capacity needed to route application traffic.

Proper access to historical reports is predicated on the customer ensuring that data replication/redundancy has been addressed so that even in the event of a site failure the historical reporting data can continue to be accessed. Either database replication or redundant Info Mart architecture may be used to help ensure data availability.

4.3.3 Dual Data Center Considerations – Configuration and Management

For Genesys software to function as a single unit it is critical that all configuration objects comprising an enterprise be stored in a single Genesys Configuration Database. In a multi-data center deployment elements such as network delays, component failures, and similar factors might complicate or slow down the operations.

Genesys recommends the use of Configuration Server Proxies and Distributed SCS in a dual-data center environment. The following diagram depicts the components necessary to distribute solution configuration and state information between geographically distributed sites.

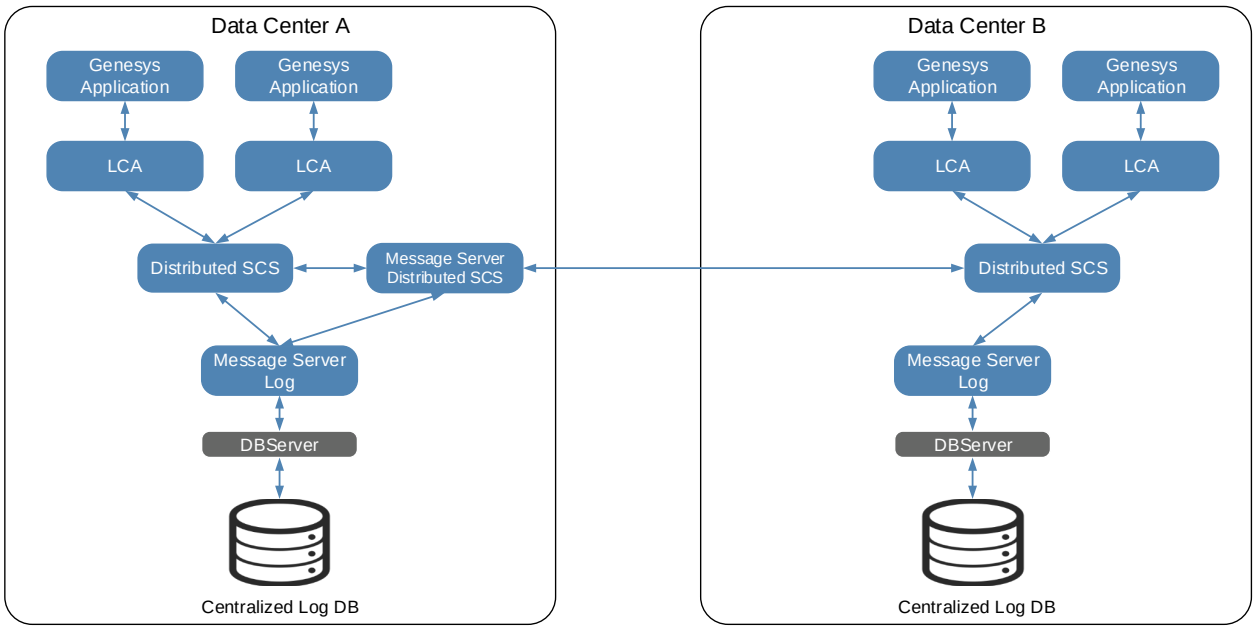

Figure 14 - Configuration Distribution

Configuration Server

In a geographically distributed configuration environment, the master Configuration Server is running at the site where the Configuration Database is located. A cold standby Configuration Server is typically deployed at a remote site where a replica of the database is located. Configuration Server Proxies are deployed at each site, including the site there the master Configuration Server is running.

Instead of sending all the requests to Configuration Server, Configuration Server clients can operate with one or more Configuration Server Proxies. Configuration Server Proxies help reduce the load on the Configuration Server. Configuration Server Proxy passes messages to and from Configuration Server. The Proxy keeps the configuration data in its memory and responds to client data requests directly. Any configuration data updates are passed immediately to Configuration Server Proxy, so that it is always up to date; no additional configuration is required to specify an update interval.

Using Configuration Server Proxy increases the robustness of the whole system, decreases the number of client connections to Configuration Server, and minimizes network traffic. When Configuration Server Proxy is configured, existing clients can continue, and new clients start, their operations when Configuration Server fails. Also, after Configuration Server recovers, the client reconnect takes far less time than if all clients were directly connected to Configuration Server.

You can configure a Configuration Server Proxy to operate as a writeable proxy to meet specific needs of Genesys Workspace Desktop Edition and other applications which need to update configuration data. When clients add, delete, or modify configuration objects and permissions through the proxy to which they are connected the requests for these changes are passed to the master Configuration Server by Configuration Server Proxy. The master Configuration Server then sends data updates to the Configuration

Server Proxy that sent the requests, which passes them to its clients. The writeable proxy mode supports a specific set of applications. General administration cannot be performed using the writeable proxy. The main benefit of this type of configuration is fewer connections as clients of Configuration Server Proxy do not have to connect directly to the master Configuration Server when requesting changes to configuration objects.

User authentication may be performed by the master Configuration Server or by the Configuration Server Proxy. If user authentication is managed by Genesys then all user authentication must pass through Configuration Server. If external authentication is performed then authentication can be offloaded to the Configuration Server Proxy. For larger deployments it is recommended that if Configuration Server Proxy is used it manages user authentication for the clients/users which connect to it.

In summary:

- A single Configuration Server HA pair should be deployed at one site which utilizes a single logical Configuration Database. A cold standby Configuration Server HA pair should be deployed at the secondary site.
- Separate Configuration Server instances operating in Proxy mode (referred to as Configuration Server Proxy) should be deployed at each site to support configuration-related tasks among the sites and provide an additional level of abstraction to reduce communication and simplify operations.

Distributed Solution Control Servers

In a geographically distributed configuration environment, a number of Solution Control Servers can communicate with each other and control a particular part of the Genesys environment while running at multiple remote sites (but within the same configuration environment).

Solution Control Servers can operate in Distributed mode (referred to as *Distributed Solution Control Server*) to distribute management-related tasks among the sites in a geographically distributed enterprise that uses a single Genesys Configuration Database.

You can install and use more than one Distributed Solution Control Server within a single configuration environment. In these installations, each such server controls its own subset of the hosts, applications, and solutions. Distributed Solution Control Servers communicate with each other through the dedicated Message Server.

When you are using Distributed SCSs, you must explicitly configure the servers' ownership of hosts, applications, and solutions: you must associate each host, application, and solution object with a particular SCS.

A Message Server needs to be setup in the master site to send application state between sites. This state information is used by the Solution Control System to ensure the applications are properly configured. Note: The Message Server delivering distributed SCS messages should be separately deployed from local Message Servers serving each site.

Genesys Administrator/GAX provide the user interface to the Configuration and Management layer. As web based applications they are deployed in an N+1 configuration and load balanced through a standard

HTTP load balancer. For operational simplicity it is easiest to have the application servers at a single site. In the instance of a site failure, which will also require a switch over to the cold-standby Configuration Server, then the customer's DNS can be used to determine the appropriate UI host name to use based upon it's availability (or that of the load balancer). If the primary application is down when the user attempts to connect to the UI they will be directed to the backup UI host name from the customer's DNS and connect to the backup UI application server.

4.4 Database Considerations

The RDBMS is a customer provided component of the solution and must be provided as part of the solution. Genesys-specific databases need to be setup within the database system and made accessible by the Genesys components. Follow the installation guides specific for each product and database vendor. Note that appropriate language/character sets need to be configured for some product databases.

Each database vendor has various strategies for providing high availability for their database system and customers may have their own setup which needs to be adhered to. Genesys should always be communicating with a single logical database.

To ensure site survivability the databases must be replicated to an alternative location such as the secondary data center. Business continuity is typically accomplished via some form of replication or clustering of databases. Genesys recommends either Microsoft SQL 2012 or Oracle. There may be specific requirements or features utilized such as Oracle Golden Gate or Microsoft SQL AlwaysOn Clustering to provide business continuity.

The specific configuration such as transaction replication, batch replication, etc. will also define what is possible for the Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

5 Interaction View

5.1 Component Interactions

The following diagrams provide high level sunny day scenarios which illustrate the interaction of the components in the Common Components blueprint. As the Common Components blueprint provides the foundation for interaction management and reporting other Genesys components are shown in the diagrams to better illustrate and the role these components provide.

Orchestration

In the following scenario a call is received by SIP Server and routed to a destination. The routing is performed using various components in the Orchestration layer.

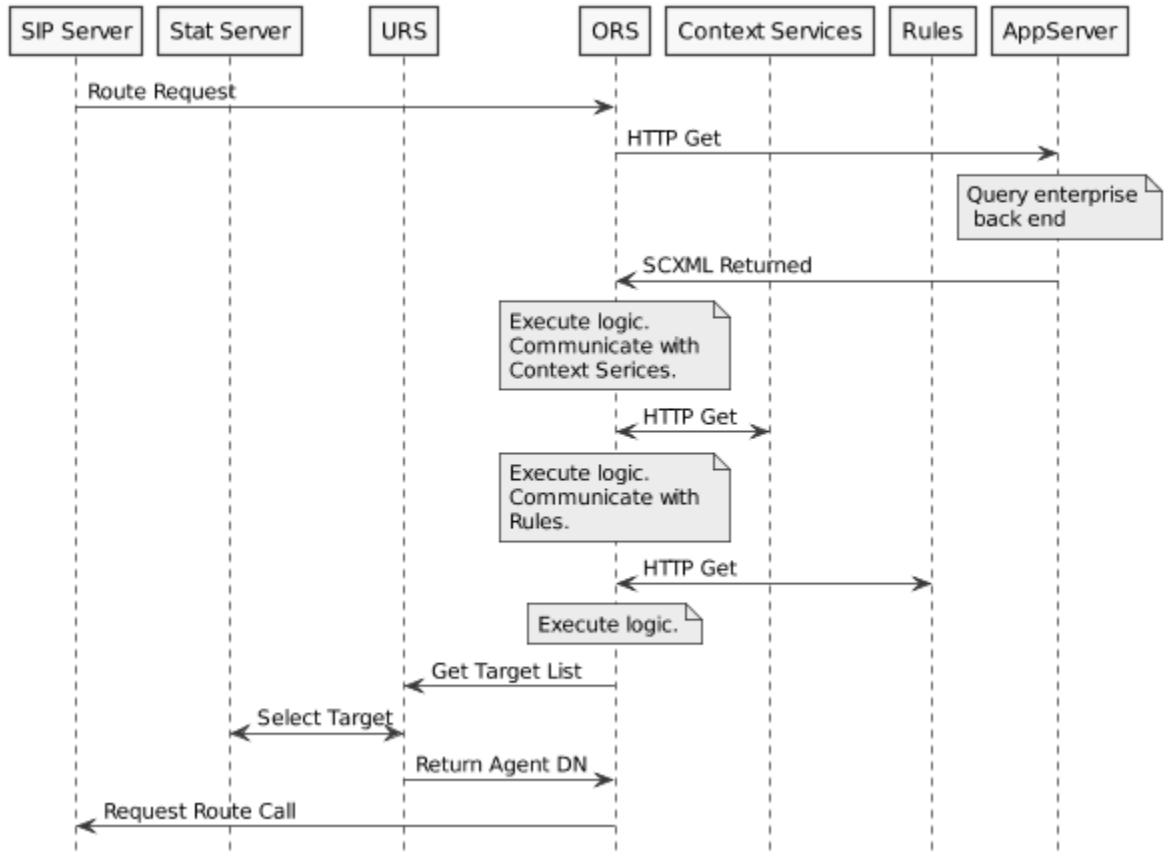

Figure 15 - Orchestration - Interaction Diagram

Configuration and Management

The following diagram shows the restart of components within a Genesys environment and the function of key configuration and management components in the initialization process. The diagram also shows an error being generated by SIP Server during start up.

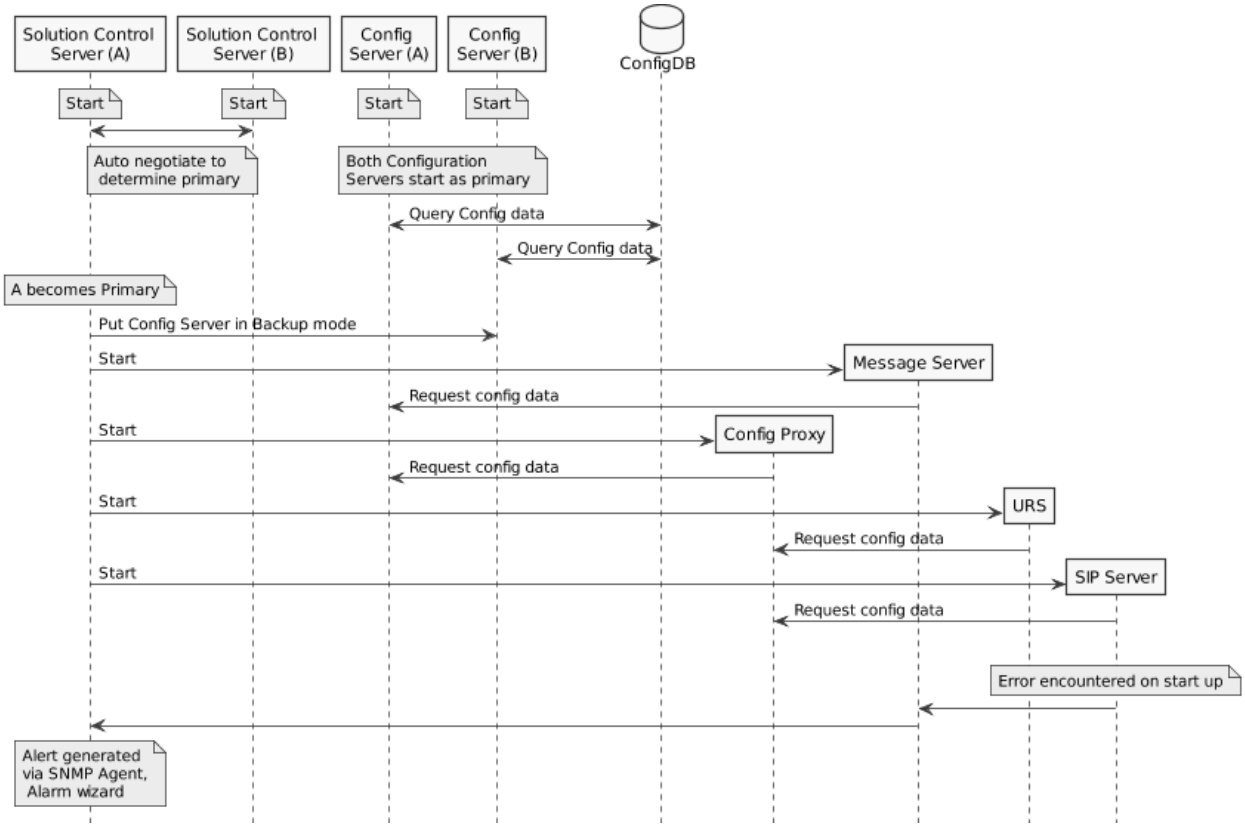

Figure 16 - Configuration and Management - Interaction Diagram

Reporting

The following diagram shows the data collection process for historical reporting, consolidation and user access to view historical reports.

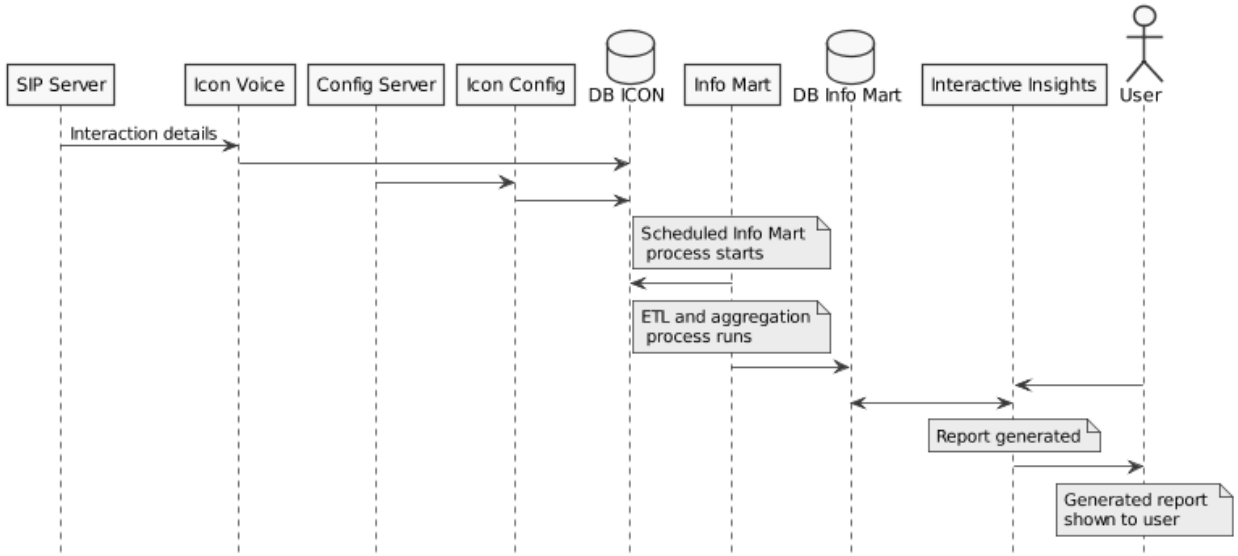

Figure 17 - Historical Reporting - Interaction Diagram

5.2 External Interfaces

The following table details each of the external interfaces, its protocols, the components within the solution that are impacted or connected to these external interfaces and lists the integration tasks required to setup the external interfaces.

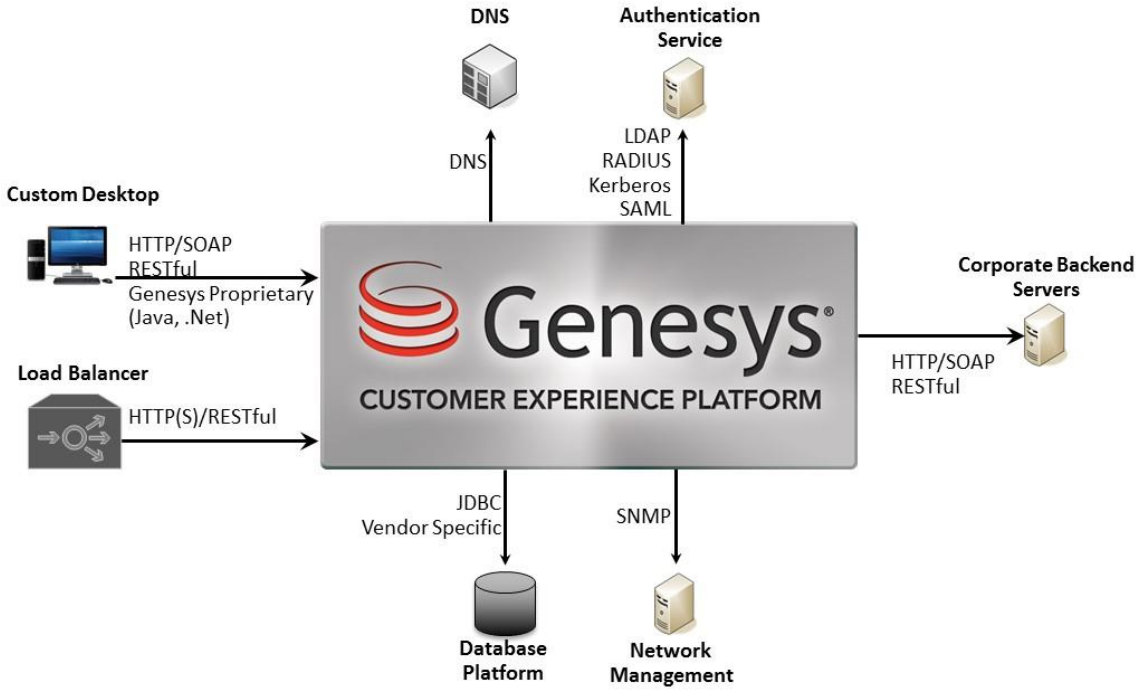

Figure 18 - External Interfaces

Interface	Protocol	Solution Components	Integration Tasks	Description
Domain Name Servers	DNS	Workspace Web, GA/GAX, CX Insights	Provision the DNS records along with appropriate weightings	This interface is used by the clients to perform the name/IP address translation. For specific cold standby components the DNS entries will be manually modified to redirect traffic in the event of a site failure.
Enterprise Authentication Service	LDAP, Radius, Kerberos, SAML	Configuration Server	Provision the network infrastructure (e.g. DNS) for the new traffic Create and provision the security information (certificates, etc.)	This interface is used to perform authentication of users using the solution. Note: Specific components such as GWS and iWD Manager currently support SAML. SAML support is on the roadmap to be added to Configuration Server.

Interface	Protocol	Solution Components	Integration Tasks	Description
Databases	TCP/SQL, TCP/THRIFT, CQL	Genesys Config, Log, ICON, Info Mart, CX Insights ORS, GMS	Provision the network infrastructure (e.g. DNS) for the new traffic Run the database scripts Provision appropriate user access to required database tables	This interface is used to store configuration data, reporting data and temporary session data. Data is stored in both SQL and NoSQL databases. Genesys may also access databases to get data from corporate systems to make decisions in solution.
Corporate Backend Servers	HTTPS (REST or SOAP)	ORS/URS, Workspace	Provision the network infrastructure (e.g. DNS) for the new traffic Create and provision the security information (certificates, etc.)	This interface is used to get data from the corporate systems to make decisions in solution (agent desktop, routing strategy, etc.). It also is used to perform certain business actions as well.
User of Solution Applications via Load Balancers	HTTP(S), TCP	GA, GAX, CX Insights, Workspace Web Edition, GWS, GMS	Provision the corporate load balancers and firewalls to handle the solution application traffic. Create and provision the security information (certificates, etc.)	This interface is used for user to access the solution's applications (GA, GAX, GI2, WWE) as well as web services based APIs (GWS and GMS)
Custom Enterprise Desktop	HTTP(S), TCP	Stat Server, Config Server and channel specific integrations	Provision firewalls to permit the application traffic. Create and provision the security information (certificates, etc.)	These interfaces are used by custom applications integrate with Genesys using the.NET and Java APIs/SDKs.

Interface	Protocol	Solution Components	Integration Tasks	Description
Corporate Network Management System	SNMP	Net-SNMP (preferred) or SNMP Master Agent	Provision the network infrastructure (e.g. DNS) for the new traffic Create and provision the security information (certificates, etc.)	This interface is used to integrate the solution with the Corporate network management system.

Table 7 - External Interfaces

5.3 Operational Management

Once a Genesys solution I s in place, managing the solution becomes a primary concern of the customer. There are two approaches to operational management that need to be considered for the solution.

1. If Genesys components are the main focus of the operation, then using Genesys Administrator and GAX becomes the primary mechanism for administering the solution.
2. If Genesys is part of a larger operation, then integration into the customer's operational management tool becomes advisable.

In both cases, Genesys Administration and GAX software need to be installed and configured to manage the solution.

5.3.1 Network Management Systems

If the customer does have a Network Management System (NMS), then Genesys components need to be integrated into their NMS. This is typically done by setting up the SNMP Master Agent to send SNMP events and info to their NMS.

Examples of supportable NMS include Zabbix, HP OpenView and OpenNMS (an open source NMS - http://www.opennms.org/).

5.3.2 Monitoring Details

In addition to Genesys monitoring the following additional recommendations should be considered:

- Monitor JVM status, especially memory usage. Note that a regular saw-tooth pattern should be observed due to Java garbage collection.
- Set alarms for specific disk and cpu thresholds
- Additional SNMP traps

Customers may also consider using ELK (ElasticSearch, LogStash & Kibana) or Splunk to harvest logs and build alarming for specific conditions within the logs.

Genesys recommends that customers also establish monitoring strategies for 3rd party components such both SQL and NoSQL. Detailed guidance in these areas should be provided by your DBA or others who are responsible for the management of these technologies in your environment.

5.3.3 Serviceability

Serviceability relates to the ability of technical support to identify issues and defects within the system. Many customers or partners will perform initial triage and analysis to determine whether Genesys Care should be engaged. If Genesys Care needs to be engaged it is critical to retrieve the required logs and configuration information and pass this information back to Genesys Care. The following recommendations provide guidance on improving serviceability which can accelerate issues analysis and resolution.

Logging

Setting up logical logging locations is a best practice that makes it easier to collect logs and reduce the time to send logs to support. Configuring 3rd party components to log into the same location is ideal as well. Genesys recommends to setup a "log" directory on a separate partition from the Operating System and applications:

```
D:\GCTI\log
/log
```

Many problems can occur when trying to retrieve the log files necessary for troubleshooting. Common problems include:

- The log files for the time when the problem occurred have been overwritten or otherwise lost.
- Log files delivered are not within the event time frame.
- Log files provided were created with log levels not detailed enough for the investigation.
- The set of log files provided is inaccurate or incomplete.

The Genesys Log File Management Tool (LFMT) is an intelligent, configurable log collection utility developed by Genesys Customer Care intended to minimize these issues, and thereby reduce the time required to resolve customer problems. It is recommended to include LFMT as a standard part of every deployment.

Log Analysis

To assist customers with performing log analysis of messaging Genesys recommends a network diagram should be maintained by customers and kept up to date to help with analysis. It is recommended to have this information readily available and, if possible, provide it to technical support together with the initial problem description and logs, to help reduce overall resolution time.

Additional Tools

Genesys Care Workbench is a suite of troubleshooting tools that can help you quickly and easily identify and resolve issues in your Genesys environment. Workbench collects data from multiple sources, analyzes it, and displays aggregate data and important data correlations in its Current and Historical dashboards as well as some specialized consoles. Types of information displayed on the Workbench Dashboard include:

- Configuration Server changes – Workbench monitors Configuration Server events for all Application objects, and displays recent configuration changes in the environment
- Alarms – Workbench configures a default set of alarms in Solution Control Server and displays alarms when thresholds are triggered. If you subscribe to Remote Alarm Monitoring, additional alarms may be displayed.
- Log events – If Log File Management Tool is deployed, Workbench can monitors log files from supported Genesys applications and display important events for troubleshooting.

Genesys Care Workbench is recommended to be included as a standard part of any deployment.

Proactive Monitoring

Genesys can provide proactive monitoring services which delivers the most complete servicing of a customer's environment. Genesys has the ability to perform proactive monitoring through our Premium Care offering. For details on Premium Care options consult the Genesys Account Team and Genesys Customer Care.

5.3.4 Monitoring Details

The following provides details on additional monitoring considerations

ORS

- ORS version 8.1.400.24 or later should be used as it provides additional performance monitoring in logs.

URS

The following are URS log message IDs that should be alarmed on:

- **21005**: URS Unrecoverable Error
  /* Attention! interaction %s will be terminated, reason: %s */
- **21006**: URS Interaction Scalability Warning
  /* Attention! interaction %s is performing a lot of %s actions */
- **21007**: URS Interaction Configuration Warning
  /* Attention! interaction %s is removed without processing */
- **21008**: URS Interaction Performance Warning
  /* Attention! shortage of cpu resources, type:%d, severity:%d, reduce: %s */
- **21009**: URS Interaction Network Warning
  /* Attention! shortage of network resources, source:%s severity:%d */

UCS

- Alarming about UCS freeze - "**SYSTEM_FREEZE**"
  - By default the alarm is raised when the system detected a freeze up to 2 s.
  - As soon as this alarm is raised, it means the system has issue to handle request (Often it's a memory issue)
  - Change the value by setting the JavaArgs "**-Dsys-bhmon-limit=**" with the new value (in ms)
  - The default value is ok to monitor correctly the system
  - A UCS restart or switchover need to be study if it's raised frequently
- Alarming about UCS Memory - "**MEM_USAGE_REACHED**" / "**MEM_USAGE_NORMAL**"
  - The first alarm is raised when the memory usage is up to 80% (by default) during more than 5 min (by default)
  - Change the value by setting the JavaArgs "**-Dkpi.mem.limit=**" for percentage (ie: 0.8 for 80%) and "**-Dkpi.mem.limit.time=**" for time (in ms)
  - The second alarm is raised when the system come back to a normal situation
  - Default value are ok to monitor correctly the system
  - A UCS restart or switchover need to be study if the second alarm is not raised
- Add LogGC to the UCS startup file using the following settings:
  -Xloggc:gc.log -verbose:gc -XX:+PrintGCDetails -XX:+PrintGCDateStamps -XX:+PrintGCTimeStamps -XX:+UseGCLogFileRotation -XX:NumberOfGCLogFiles=50 -XX:GCLogFileSize=10M

6 Implementation View

The Implementation View describes details such as sizing, security and configuration of the solution based on the previous deployment considerations and interaction views.

6.1 Solution Sizing Guidelines

This section provides guidelines and an example of the content that a Solution Sizing should contain. The objective of this section is to help the reader understand how the prior components and architectural considerations are put into practice through a sample solution sizing. A similar Solution Sizing should be prepared when an architecture is proposed to a customer. The level of detail provided in a Solution Sizing will vary based upon the customer requirements.

Providing a simple and accurate sizing guideline is difficult as there are many variables, between the number of agents, the type of interactions, interaction rate, bandwidth, etc. that can occur within the customer's operations. **While the Common Components Blueprint does not address any of the components required to process interactions to help provide context the example Solution Sizing is created for an environment which requires voice, email and chat interactions. This approach was taken to help illustrate how the Common Components would be reflected in an overall architecture.**

When performing sizing the approach taken is to assume certain variables such as interaction volumes – busy hour calls, qualification, queue & talk times and a mix of call flows, email volume, chat needs, etc. Based on these assumptions, the CPU, memory and data requirements are calculated.

The sizing calculations is for a 2,000 agent target deployment. The sizing reflects a centralized, highly available deployment. Sizing for a dual-data center deployment is available as well.

The sizing provided assumes use of virtualization although details on the specific hardware (CPU profile) is provided.

Please treat this sizing estimates as a rule of thumb. Changes to any variable can impact the overall sizing.

6.1.1 Solution Sizing – Centralized Deployment

This section provides the sizing for a centralized deployment supporting 2,000 agents.

6.1.1.1 Sizing Assumptions

The following assumptions are made regarding the sizing of this solution.

Input Assumptions	2,000 Agents
Agents	2,000
Agent utilization	80%
Call qualification time	60s
Queue time	120s

Talk time	180s
Transfer Rate	10%
Conference Rate	10%
Percentage of Queued Calls	50%
Log retention	Debug 2 weeks
Reporting History	2 years
Non-aggregated Reporting History	3 months
Calculated worst case values	
Concurrent active calls (IVR + Queue + Agent)	1662
Peak CAPS	6
Busy hour calls	21600
Emails/Day	17,280
Chat – Peak interaction rate (in sec)	0.5
Chats/Day	8640
Pulse Users	200
Layouts	4
Objects	10
Icon DB Retention	35
GIM DB Retention	400
UCS DB Retention	300

Table 8 - Sizing Inputs

6.1.1.2 Hardware/Virtualization Assumption

The underlying hardware will impact the overall performance of any virtualization solution. To that end, the following hardware requirements are assumed:

- CPU Score per Core = 30
- Hyper-threading = Off
- Number of Chips (NUMA Nodes) = 2

- Oversubscription = None

In addition, it is assumed that each hardware server will be running ESXi v5.4 or greater directly on the hardware server.

6.1.1.3 Virtual Machine Sizing

The following table details the virtual machine sizing for CPU, RAM and disk. For further details please see the accompanying **Integrated Sizing Calculator**.

Note: Components which are not yet reflected in the Integrated Sizing Calculator include:

- ***Genesys Rules***
- ***Genesys Engagement Services (Context Services)***

The sizing calculator indicates that 25 VMs are required. The VM and component distribution is detailed below.

VM Assignment per DC

VM Name	Required	ESX1-1	ESX2-1	ESX3-1	ESX4-1	ESX5-1	ESX6-1	ESX7-1	Total Assigned	Cores	Memory (GB)	VM Priority	OS	Partition
cm-fw	1	0	0	0	0	0	1	0	1	8	16	2	Win	1
cm-fw-b	1	0	0	0	0	0	0	1	1	8	16	2	Win	1
cm-gi2	1	0	0	0	1	0	0	0	1	8	16	2	Win	1
vc-all.1	1	0	0	0	1	0	0	0	1	8	24	4	Linux	1
vc-all.1-b	1	0	0	0	0	1	0	0	1	8	24	4	Linux	1
dg-all.1	1	0	0	0	0	0	1	0	1	8	32	4	Win	1
dg-all.1-b	1	0	0	0	0	0	0	1	1	8	32	4	Win	1
cm-cas	5	1	1	1	1	1	0	0	5	8	16	2	Linux	1
cm-gws-api	2	1	0	0	0	1	0	0	2	4	4	2	Linux	1
cm-gws-stat	2	0	1	1	0	0	0	0	2	4	4	2	Linux	1
cm-gws-es	3	0	1	0	0	0	1	1	3	4	4	2	Linux	1
cm-cas-gws	3	0	0	1	0	0	1	1	3	4	4	2	Linux	1
vc-mcp	3	1	1	1	0	0	0	0	3	8	8	4	Linux	1
Totals	25	3	4	4	3	3	4	4	25	160	304			

Table 9 - Example Solution Sizing

6.1.2 Database Sizing

The following table summarizes the database sizing requirements for Genesys components stored within the RDBMS. These are estimates based on the sizing assumptions and should be treated as a starting point. Other customer factors can impact the overall data requirements.

Awaiting updated Sizing Calculator

System	2000 agents

Configuration Server	**1 GB**
Message Server	698 MB
Universal Contact Server	287 MB
Genesys Administrator Extension	_5000MB
Pulse	**100 MB**
Genesys Interaction Concentrator	250 MB
Genesys Info Mart	750 MB
Genesys CX Insights (GI2)	Insignificant
Total SQL database storage	**__10 GB**

Table 10 - Database Sizing

6.1.3 Network Sizing and Readiness

The success of any Genesys deployment hinges on ensuring that the network is ready and has the appropriate bandwidth. Customer networks are varied and a Network Assessment is truly the best course of action.

As guidance, the following network load has been calculated for the solution.

TBD

Network Traffic	2000 Agents
Within Data Center	
Between Data Centers (Business Continuity)	
Between Branches and Data Centers	N/A

Table 11- Network Traffic Guidance

6.2 Configuration Guidelines

The following guidelines provide typical settings that need to be configured within the Common Components or reviewed based upon the overall architecture and load. Variants in the customer's network environment may require alternate settings. See the notes section for the listed options.

6.2.1 Configuration Recommendations

The following configuration options relate to performance and reliability of the system in addition to other options that may require attention.

Workspace

- Review/reduce UCS timeout values
- Review data automatically downloaded to Workspace such as Team Communicator

Universal Routing Server

- Configure overload protection. With overload protection URS will enter a CPU savings mode on sudden changes in configurations, strategies or call rate. In this mode URS reduces the accuracy of its routing targets to free up CPU power. The following options are recommended:
  - set option **reduced** to 2048 (if it is not set at all).
  - set option **emergency_verbose** to 3

Universal Contact Server

- Ensure pruning is set to an appropriate value for the Archive
- Adding the option index/debug=true now activates Lucene debug logs in UCS logs. This can be used to troubleshoot index performance. The option takes effect upon restarting UCS.
- UCS now provides three log messages to monitor its performance:
  - UCS JVM was frozen for more than 2s
  - UCS heap memory usage exceeded the limit for more than NN seconds
  - UCS memory usage is now back to normal

Info Mart

- For high availability an Active/Active GIM architecture should be used. This eliminates the dependency on database replication. This can also rectify problems where an unusually large data set is being replicated between sites and interrupting the upgrade process. Note that table keys will be different between instances of GIM and must be addressed by data extraction.

Pulse

- For Pulse we recommend to collocate Pulse and collector on the same machine for best performance. If the deployment uses a shared network volume for storage or use WebDav server these components can be located on different machines

6.2.1.1 Other Considerations

The following are not configurations specifically but other considerations for performance and reliability:

- During strategy development it is beneficial to optimize handling of KVPs. Multiple KVPs should be updated together in a single transaction to help reduce traffic and load
- Review strategies to ensure that there is appropriate exception/event handlers to avoid sessions

being left open unnecessarily

- The 64-bit version of StatServer should be used as it supports larger virtual memory sizes and improved performance.
- Performance overall of UCS (and other Digital components) is strongly affected by the performance of the underlying database and connectivity to it. Databases should be kept co-resident with the primary processes and it is recommended that HA pairs for servers reside within the same data center with a cold standby environment at the DR site.
- Upgrade to the latest official release of Oracle's Java 7, in particular a minimum version that contains this fix http://bugs.java.com/view_bug.do?bug_id=8024838
- UCS Logs should be stored on a different drive from the indexes.
- Disable Jericho output from the logs by setting the following option in the UCS log section (note this is a dynamic setting):
log4j.logger.net.htmlparser.jericho=WARN
- UCS is critical for Workspace access to interaction history for all media types and operations of the Digital Solution. UCS needs to be managed for high performance and it is recommended that the Lucene index be maintained in HA mode (synchronous) between primary and secondary UCS instances.
- To reduce any kind of delays for Lucene operation we recommend for Lucene Index files to be located on local SSD -- please see here https://wiki.apache.org/lucene-java/ImproveSearchingSpeed
- There should not be any high CPU consuming processes running alongside Genesys on the same host, such as log archivers, anti-virus, 3rd-party monitoring software, etc at the time during peak production load.
- Special attention should be paid to the Genesys logging, aiming to minimize the number of log files kept in the logging folder. Generally it is recommended to use larger size segments (option log\'segment') with a smaller number of log segments kept in the logging folder (log\'expire').
- Genesys software should be provisioned with logging level adequate to quick issue analysis and resolution, which usually translates into log\verbose=all.
- Avoid using console and network devices for log output

Pre-production testing:

Prior to being deployed in production each Genesys system should undergo a rigorous set of tests aiming at determining its maximum sustainable interaction volume and fault tolerance (reliability).

Scalability:

For the maximum sustainable interaction volume determination the solution should be put under a gradually increasing interaction rate (calls, emails, chat, co-browse) closely emulating the required production lows.

Change Control Process:

In production implement change control processes.

Avoid making critical changes in the live environment. Make these changes only during maintenance windows.
Keep a backup copy of your configuration database current. Make a backup copy prior each configuration change.

6.3 Security

Protecting the customer's infrastructure should be imperative for any solution deployment. Genesys components can typically be deployed in a secure manner. Many customers have their own security procedures that our solution needs to conform to. The Genesys Security Deployment Guide provides details on security features offered by Genesys software and how these features are configured. This document can be accessed at: https://docs.genesys.com/Documentation/System/8.5.x/SDG/Welcome

The following are general guidelines for some of the common security requirements that may be encountered or should be recommended.

6.3.1 Secure Connections

Connections between components, especially those external to the solution (see **Error! Reference s ource not found. Error! Reference source not found.**) should be secured. Secure connections are typically performed using SSL or HTTPS. While secure connections can have a performance impact and addition operational considerations at a minimum Genesys recommends to secure any internal any communication which may contain sensitive data and any traffic external to the environment.

Typically customers will insist on firewalls to protect HTTP traffic from the wild internet. In a similar fashion Media Gateways or Session Border Controllers need to be configured to protect VoIP traffic.

6.3.2 VM and OS hardening

Operating Systems are often pre-configured for ease of use and development and not necessarily security. If the O/S is being installed or is part of a set of VMs being delivered, that O/S should be hardened to ensure that typical security holes are addressed.

The following document provides recommendations that can be used to harden the solution VMs and the OS.

Microsoft Word 97
- 2003 Document

6.4 Localization and Internationalization

Localization and Internationalization are topics for numerous Genesys components, especially user interfaces and reporting. Within the Genesys Common Components the main components to pay attention to are:

- Agent Desktop: Workspace Desktop Edition and Workspace Web Edition
- Administration: Genesys Administrator / Administrator Extensions
- Reporting: Pulse and CX Insights

Appendix A Application Threading

Understanding the threading of an application of an application is important when evaluating the application onto a server and appreciate how the application will behave under load.

> *One of the purposes for noting the single threaded applications is to ensure proper monitoring of those processes especially within multi-processor environment. For example if you are monitoring the CPU of a 4 vCPU virtual server and see that the load is 30% this does not provide insight into the whether a specific core is consuming the majority of the load the possibility that a single-threaded process is in fact overloaded on a lightly loaded system.*

The following table lists the various Genesys applications and their threaded nature:

Component	Number of Threads	Comment
SIP Server	1, 3	Configurable via Link Type. Recommended setting is 3.
ICON	1	
SIP Server Proxy	1	
ConfServer	1	An additional thread is used for each type of external auth. An additional thread is used for direct database communication (if DB Server is not used)
ConfServer Proxy	1	An additional thread is used for each type of external auth.
StatServer	1	
Message Server	1	An additional thread is also used for direct database communication to the Log DB (if DB Server is not used)
SCS	1	
DB Server	1	Separate dbclient threads are launched per connection.
GIM	many*	
MCP	many	
ORS	many	
Resource Manager	many	
Feature Server	many	
URS	1	
OCS	1	

Interaction Server	32	
UCS	many	
Chat Server	10	
Engagement Server	many	
Email Server	many	

Table 12 - Component Threading Behavior

*many – means that application uses all available cores on the computer or VM.

Multi-threading is one way to address parallel computing and efficient utilization of multi-core platforms. There are also other means such as deploying multiple process instances in N+1 load balancing cluster, which can be applied to several Genesys components. The latter can have benefits over multi-threading, because it eliminates need for inter-thread synchronization. Note: A quite modern technology such as node.js is intentionally single threaded for the above reason.

Appendix B Virtualization Guidelines

Genesys provides an open-software based solution that enables interoperability with other market-leading products, to enable you to deploy Genesys products in a virtualized environment. The virtualization products documented in the Genesys Supported Operational Environments guide are supported with Genesys products running in specified virtualized environments, according to the Genesys virtualization guidelines and support policy in this section.

Virtualization Needs

Products using virtualization must run on sufficiently equipped computing platforms, particularly with respect to CPU speed, available memory, and network interfaces. Virtualization may increase the processing load compared to native deployment on a given node. You should follow the recommendations and best practices discussed in the virtualization platform vendor's documentation.

In all scenarios, when planning a production deployment in a virtualized environment, it is strongly recommended that you test the proposed configuration under simulated production conditions, to ensure acceptable sizing and performance.

In order to ascertain the sizing of a virtualized environment, take an overhead factor of 15% of resource performance degradation over an individual host (maximum of 85% of 80%).

Physical Hardware/Virtualization Assumption

Even with virtualization the underlying hardware will impact the overall performance of a virtual server. The impact can vary based upon:

- CPU performance
- NIC cards
- RAID controllers and Storage subsystem

The performance will also be impacted by the ESX configuration. The resources available to the virtual server can be governed by the ESX settings such as

- Oversubscription
- Priorities

When deploying on a virtualized environment it is important to consider the configuration at each component (CPU, network, hard disk) as well as layer (physical versus hypervisor) to full understand whether the environment provided is adequate.