SIP Cluster Premise Solution Blueprint

Reference Architecture

Authors Gordon Bell

Version: 1.01

Status: PUBLISH

Published: 7/3/2018

GENESYS

Table of Contents

Table of Figures

Table of Tables

Revision History

Rev	Date Published	Author	Reason for Revision
0.1	03/12/2018	Gordon Bell	Initial draft
0.2	05/10/2018	Gordon Bell	Applied first set of review comments. Added Appendix A: Migration Strategy
0.3	06/12/2018	Gordon Bell	Applied second review comments.
0.4	6/18/2018	Gordon Bell	Applied Draft 3 review comments.
1.0	6/21/2018	Gordon Bell	Published first version
1.01	7/3/2018	Gordon Bell	Updated links to SIP Cluster documentation

1 Introduction

The purpose of the SIP Cluster Premise Solution Blueprint document is to provide a set of design practices and guidance to ensure consistent architecture approaches are used for all deployments of Genesys SIP Cluster on premise. It provides a prescriptive list of components (both Genesys and 3rd party) that should be included in the solution. It also provides deployment guidance, including sizing considerations, and addresses several system concerns such as security, high availability, disaster recovery and serviceability.

The SIP Voice Solution Blueprint focused on the traditional SIP Server deployment. SIP Cluster is based on the SIP Server components but the deployment model is constrained in several ways. These limitations result in vastly increased scalability.

The Genesys SIP Cluster Premise Solution consists of the following core Genesys components:

- SIP Server
- Resource Manager
- Media Server (Media Control Platform)
- SIP Feature Server
- Outbound Contact Server
- Genesys Interaction Recording
- Workspace Web Edition

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 Solution Consultants, 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 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. This document provides high-level information 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.

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

AMD	Answering Machine Detection
ASR	Advanced Speech Recognition
CAPS	Call Arrival Per Second
CPA	Call Progress Analysis
CPD	Call Progress Detection
CTI	Computer-telephony integration, the adding of computer intelligence to monitoring and control of telephone calls
DB	Database
DBMS	Database Management System
DN	Directory number
DNS	Domain Name System
DTMF	Dual Tone Multi-Frequency
eSBC / E-SBC	Enterprise Session Border Controller
FTP	File Transfer Protocol
GA	Genesys Administrator
GAX	Genesys Administrator Extension
GIM	Genesys Info Mart
GIR	Genesys Interaction Recording
GI2	Genesys Interactive Insights
GUI	Graphical User Interface
GVP	Genesys Voice Platform
HA	High Availability

HTTP	Hypertext Transfer Protocol
ICON	Interaction Concentrator
IM	Instant Messaging
IP	Internet Protocol
ISCC	Inter-Server Call Control
IVR	Interactive Voice Response
JDBC	Java Database Connectivity
LAN	Local Area Network
MCP	Media Control Platform
MGW	Media Gateway
NMS	Network Management System
OCS	Outbound Contact Server
ODBC	Open Database Connectivity
ORS	Orchestration Server
PBX	Private branch exchange
PSTN	Public Switched Telephone Network
QM	Quality Monitoring
Q&P	Qualification and Parking
RDBMS	Relational Database Management System
REST	Representational State Transfer
RM	Resource Manager
RTP	Real-time Transport Protocol, the media-stream transport used with SIP
SBC	Session Border Controller
SDK	Software Development Kit
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SQL	Structured Query Language

SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLib	TServer Library
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
WAN	Wide Area Network
WDE	Workspace Desktop Edition

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 Overall Architecture

With the SIP Cluster Premise Solution, you can create a highly scalable contact center architecture in which the system's capacity can be scaled up or down with minimal configuration changes. You can add new instances of SIP Server to the cluster at any time to increase its capacity. You can also reduce the cluster size when you need to, by gracefully removing any unnecessary nodes.

SIP Server in cluster mode is designed to support high call volumes over a large number of SIP phones and logged in agents.

3.1 Solution Overview

The SIP Cluster provides linear scalability of call handling capacity by treating multiple SIP Servers as a single system across multiple locations. New servers integrate seamlessly. The cluster simplifies system management by centralizing the configuration of agent DNs and Places within the single SIP Switch object (compared to a SIP BC deployment) and eliminating the need to configure agent logins.

The cluster is geographically aware and can maintain the geographical integrity of calls. Once a call is assigned to a SIP Server node, it is maintained exclusively by that node. Other nodes have no knowledge of calls not assigned to them.

SIP Cluster integrates with most other Genesys systems and solutions including:

- Genesys Voice Platform for IVR and media treatments
- Interaction Recording
- Outbound Campaign Server
- Digital Solutions (Chat, Email, SMS, etc.)

In addition to this blueprint, its recommended to consult the following related solution blueprints:

- [Common Components Solution Blueprint]
- [SIP Voice Solution Blueprint]
- [Digital Channels Blueprint]
- [Interaction Recording Blueprint]

3.2 Logical Architecture Model

SIP Cluster is a multi-site, geo-redundant, scalable and reliable VoIP solution for the contact center. The following diagram depicts the logical, high-level view of the overall solution.

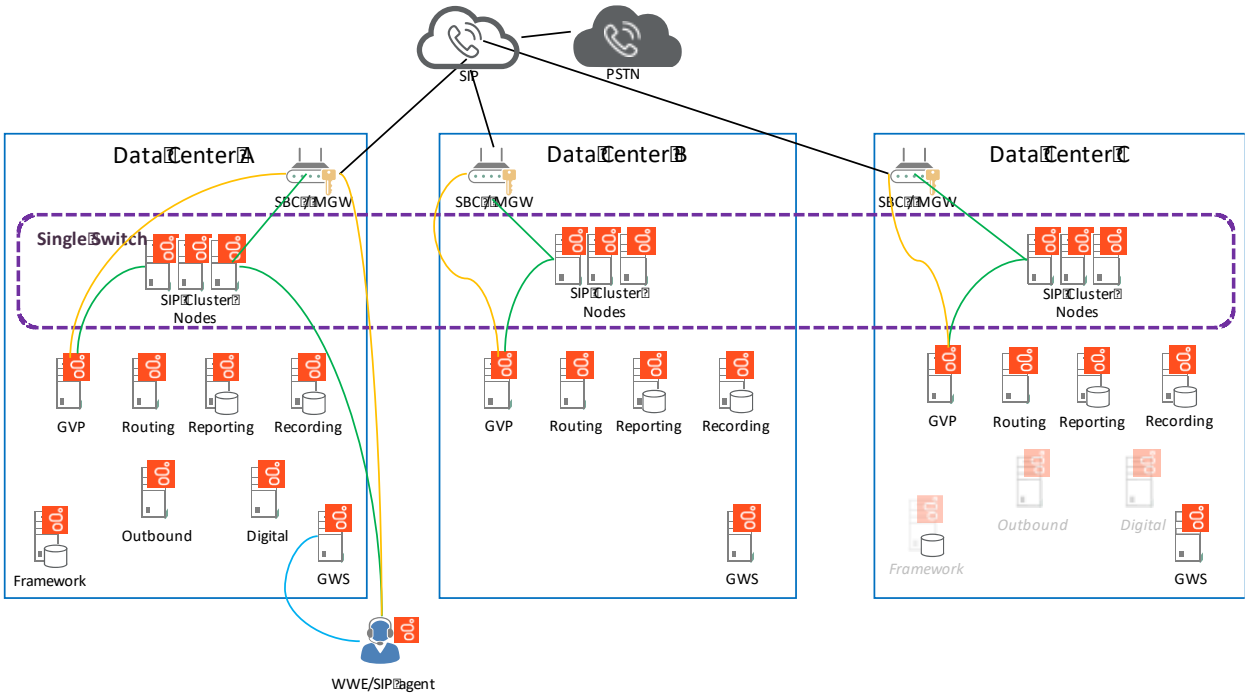

Figure 1: Logical Architecture Model

SIP Cluster nodes are deployed in each data center. These nodes are configured as a single switch within the Genesys environment, greatly reducing the number of elements that need to be configured and maintained for that switch. The SIP Cluster node components are deployed in primary/backup pairs to provide high availability. Additional cluster nodes can be easily added to the environment for horizontal scaling of the system.

SIP Cluster interoperates with GVP for IVR functionally and SQP using Genesys standard media servers for qualification and parking, Music On Hold and other media capabilities.

GIR recording inter works with SIP Cluster and GVP to record all voice interactions. It also works with the WWE components to capture screen-recording.

3.2.1 SIP Server Cluster Node

SIP Cluster nodes are essentially the same executable as a standard SIP Server with deployment flags and options set. These options will be discussed in subsequent sections. It is worth discussing the anatomy of the SIP Server when used in cluster mode.

When working in cluster mode, SIP Server uses the following three internal modules to provide cluster functionality:

- Session Controller—call processing engine; this module focuses on handling local calls.
- T-Controller—T-Library interface for agent desktops and Genesys servers, which monitor

agent- and DN-related T-Events; it essentially maintains the agent state model.

- Interaction Proxy—T-Library interface that distributes interactions across the clients in a pool; it ensures that all events are sent in the proper order for accurate reporting.

Important: All three modules operate within one executable file.

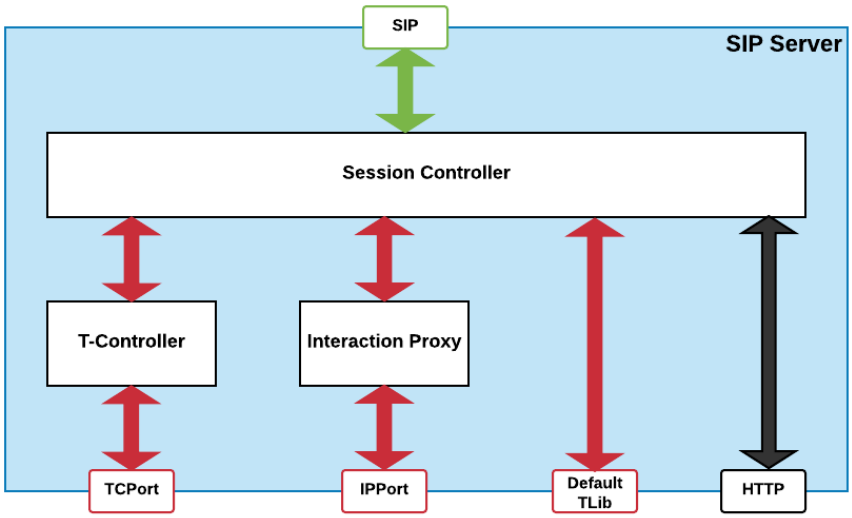

Figure 2: Anatomy of SIP Cluster Node

Each internal module has a separate T-Lib port. For the proper functioning of the cluster, various Genesys and 3rd party components must be connected to the appropriate ports as indicated in the following diagram.

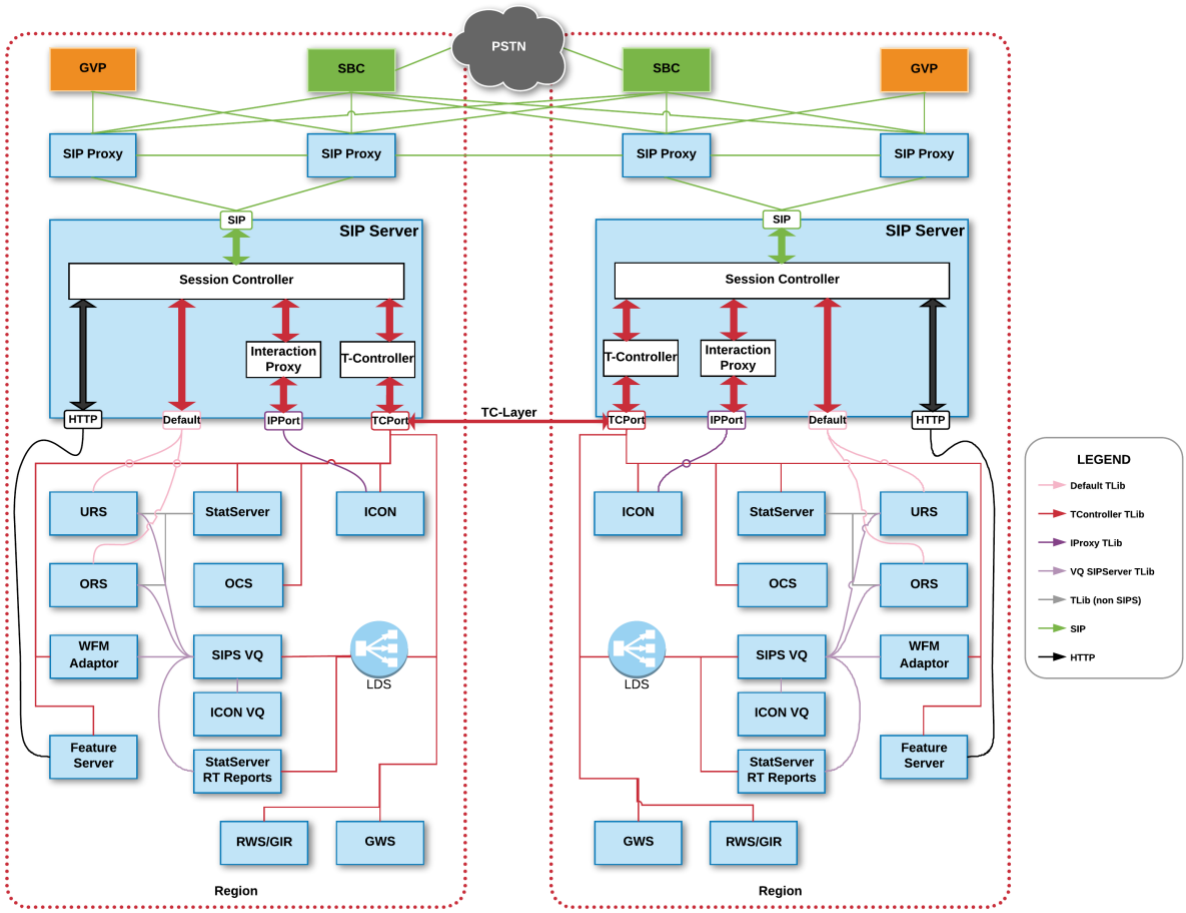

Figure 3: SIP Cluster Node Connections

The connections are discussed later in the deployment and configuration sections. Of special note is that all SIP Servers functioning in cluster mode are connected together using the T-Controller port (TCPort), creating a T-Controller layer. It is important to minimize the number of clients connected to the TCPort as data is propagated across the entire cluster. The main component connections are detailed later in the layered architecture sections.

For SIP communications, each SIP Server is connected to a group of SIP Proxies (a minimum of two are required per Data Center). Not shown in the diagram is the HA backup SIP Server instance that the proxies monitor and failover to in the case of a SIP Server failure.

All SIP Proxies within the entire SIP Cluster are connected together, enabling the proxies to manage registrations of all SIP endpoints. SIP Proxies also provide high availability to SIP Server HA pairs without requiring a virtual IP address (this is the only supported HA mode for SIP Servers within the cluster).

Session Border Controllers can be configured in several ways, but its recommended that each SBC within the environment is aware and connected to each of the SIP Proxy instances within the cluster.

GVP/Media Server should be setup within each data center using geo-location configuration flags so that media can be localized to the data center where a call first enters the cluster.

3.3 Functional View

SIP Cluster is an intrinsic component of most voiced-based interactions within the Genesys PureEngage platform. This solution also focuses on the integration with many of the other suite components including GVP, Digital Channels and Reporting.

The two typical areas that SIP Cluster functions are:

- Customer Engagement
- Employee Engagement

3.3.1 Customer Engagement

Typical customer engagement use cases where the SIP Cluster may be used include but are not limited to:

- UC - CE01 - Inbound - Connect Voice Interaction to Right Resource
- UC - CE02 - Inbound - Personalized And Value Based Routing For Voice
- UC - CE03 - Inbound - Dynamic Voice CallBack
- UC - CE10 - Genesys Multi-modal IVR
- UC - CE11 - Outbound - Improve Telemarketing Success By Moving Beyond Cold Calling
- UC - CE14 - Outbound - Proactive Contact Based on Customer Context and Journey

3.3.2 Employee Engagement

SIP Cluster is an underlying element in most employee engagement/recording solutions within PureEngage. SIP Cluster may be used in many of the Employee Engagement use cases, including:

- UC - EE07 - WFO - Record Voice Interactions
- UC - EE08 - WFO - Record Voice And Screen Interactions
- UC - EE21 - Genesys IVR Recording
- UC - EE22 - Genesys Speech Analytics

3.4 Component View

3.4.1 Genesys Components

Common Components such as Framework, Reporting and Routing are key components within the solution. More details on them can be found in the [Common Components Solution Blueprint]. Variants to how these components are normally deployed and configured will be noted where applicable.

Workspace Web Edition (WWE) is the required desktop for this solution. The Genesys softphone or a Genesys supported SIP hardphone can be used for voice interactions with the Agent. Note that the agent can log into any data center as she is effectively logging into a single switch.

Category	Component	Version	Notes
SIP Server	SIP Server	8.1.1+	Standards-based contact center software solution
	SIP Proxy	8.1.1+	SIP Proxy provides SIP registrar functionality for SIP Cluster and supports SIP Server HA. .
	Feature Server	8.1.2+	Provides supplementary services for SIP Server including voicemail, dial plan services and phone provisioning/management.
GVP	Resource Manager	8.5.2+	RM controls the access and routing of all resources within the GVP deployment.
	Media Control Platform	8.5.2+	Delivers media services to for interactive voice response, menus, on hold treatments and call recording.
SIP Softphone	SIP Softphone	8.5.2+	A Genesys provided software based SIP endpoint used by agents to provide voice communication directly through the agent's desktop. Used as part of the Hybrid Option discussed later.
Recording	Genesys Interaction Recording	8.5.2+	A call recording solution, screen capture, and Quality Monitoring (QM) tool utilized to store,

			manage, and playback recorded voice conversations and screen captures, as well as provide quality assurance.
Desktop	Workspace Web Edition	8.5.2+	Web-based Agent desktop application supporting all media types.
	Web Services API (GWS)	8.5.2+	Web Services are the REST APIs that can be used by developers to create custom agent applications that integrate with Genesys. These applications can include features such as state management, call control, supervisor monitoring, and call recording
Outbound	OCS	8.1.508+	An automated system that is used to create, modify, and run outbound dialing campaigns/dialing sessions in which agents interact with customers
Mobile	GMS	8.5.2+	GMS contains multiple APIs that allow developers to create mobile applications using Genesys capabilities.
Callback	Callback	8.5.2	The Callback solution is based on GMS and enables applications to make scheduled, immediate or delayed callback requests to the user.
Common Components	Genesys Routing Mgt Framework DB Server	8.1+ 8.5.1+ 8.1.3+	See the Common Component Blueprint for information on Management Framework, Orchestration/Routing and Reporting components used by this solution.
Common Components	Historical Reporting (ICON/GIM/GI2)	8.5+	

	Pulse - Real Time Reporting	8.5.1+	

Table 1 - Genesys Component List

Other supported solutions and components include:

- Digital (see the [Digital Solution Blueprint])
- Outbound (see the [SIP Voice Solution Blueprint])

3.4.2 3rd Party Components

The following table lists the recommended 3rd party components for this solution. Alternatives are also noted though the recommended components are encouraged.

Component	Recommended	Version	Note
SBC/Media Gateways	AudioCodes		
Administration Tools	Zabbix		
Web Application Server	Microsoft IIS		
	Apache Tomcat 6.x	6.x	
Web Server	Apache HTTPD		WebDAV support required for GIR
File Server	NAS/SAN		
Virtualization	VMWare	5.1+	
Database	MS-SQL	2014	MS-SQL Always On is highly recommended
	Cassandra	2+	
	Elasticsearch		
Load Balancer	F5, NGINX		

Table 2 - 3rd Party Components

3.5 Limits and Constraints

Although SIP Cluster is based on Genesys SIP Server technology, it uses advanced principals and patterns to provide highly scalable and geo-distributed capabilities. Due to this approach, there are several limitations and changes compared to traditional SIP Server. For a complete list of the latest issues and limitations, please see the section, [SIP Cluster:Unsupported Features], in the Genesys documentation site.

This following is a high level view of some of the key limitations:

- ISCC protocol between SIP Cluster and other Genesys T-Server environments not supported.
- Migration strategies impacted by lack of ISCC – use of GMS as a Federation mechanism is discussed in Appendix A.
- Agent Logins objects are not required and not recommended due to overall cluster performance.
- Recording on SIP Cluster must use GIR.
- WWE desktop or GWS based custom desktops are only supported. WDE is specifically not supported by SIP Cluster as WDE's architecture adversely impacts cluster scalability and performance.
- Nailed up agents are not supported

4 Deployment View

The SIP Cluster Premise deployments typically involve 2 or more data centers in geographically distinct locations. The solution involves multiple components as mentioned in the previous sections. Some such as the SIP Cluster are designed to operate in a geo-dispersed manner while others need to be deployed in more traditional local or disaster recover modes. This section describes how the various components need to be deployed.

4.1 Genesys Deployment

The Cluster deployment involves several different areas or layers of functionality. The following diagram depicts those deployment layers.

The following sections will discuss the deployment of these component layers within a 2 data center network topology. This will be used to explain the concepts and approaches required to deploy this solution across multiple data centers. Where needed, additional information will be provided if there are any special accommodations for deploying across 3 or more data centers.

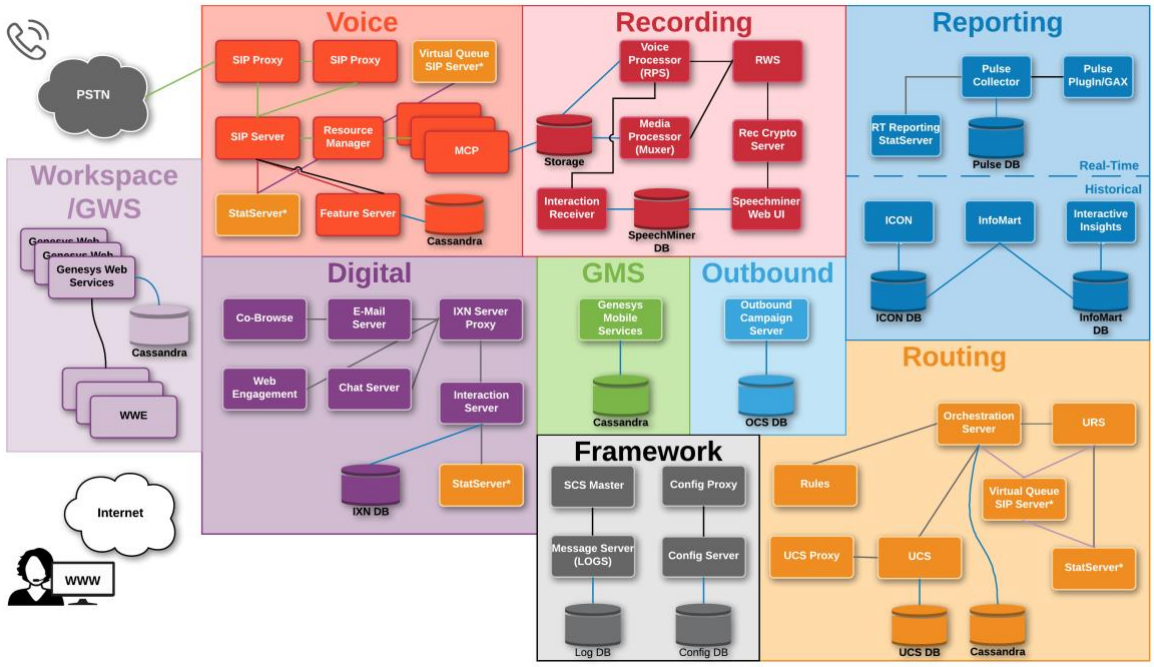

Figure 4: Cluster Deployment Layers

4.1.1 SIP Voice Layer

The SIP Voice layer includes the various SIP elements that control voice traffic through the solution, GVP elements for IVR and other media treatments; and Voicemail elements.

- The solution includes multiple instances of SIP Server. SIP Server cluster nodes manage the

bulk of the voice traffic. They are deployed in HA pairs with one or more pairs deployed per data center based on traffic. The SIP Server cluster nodes are configured as one single Switch in the Genesys configuration environment.

- Virtual Queue SIP Servers are used primarily to manage virtual queues. They are configured as HA pair of SIP Servers running in stand-alone mode deployed in each DC (one HA pair per DC). This eliminates the need to synchronize virtual queue states across SIP Server cluster nodes.
- SIP Proxy is a required element of the voice layer. It is used to register endpoints, manage the availability of SIP Server HA pairs, and coordinate traffic through the cluster. At least two SIP Proxies need to be deployed for each Data Center. SIP endpoints (agent softphones, etc.) can either register directly with the SIP Proxy or to an SBC which then forwards the registration to the SIP Proxies.

GVP elements include:

- Resource Managers are deployed as an active-active pair for each Data Center
- Media Control Platform (MCPs) are deployed as an N+1 cluster for handling audio/RTP processing. Each Data Center has its local independent MCP farm controlled by the local active-active pair of Resource Managers.
- Reporting Server
- GVP Application Server
- Nuance or any compatible MRCP client
- GAX

Voicemail elements consist of Genesys Feature Servers supported by a Cassandra cluster ring.

ORS, URS and StatServer are described in the Routing Layer. Note that a separate pair of URS and StatServers should each be deployed for each SIP Server Cluster pair.

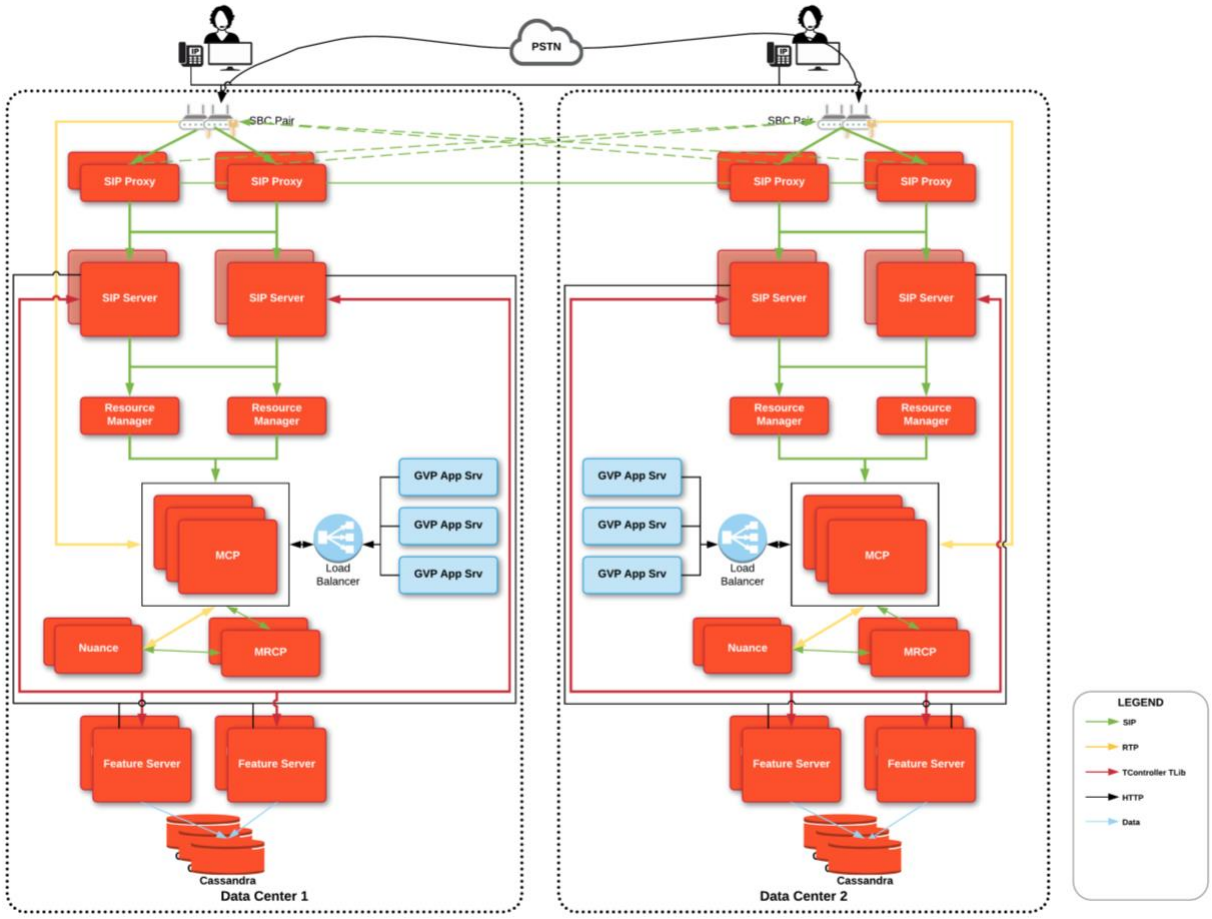

Figure 5: Voice Layer

4.1.1.1 High Availability

SIP Server uses a hot standby pair for each cluster "node". This ensure that calls on that SIP Server will survive a single failure.

SIP Proxies are deployed as an active cluster. Each proxy synchronizes SIP registration information within the cluster so that if one Proxy goes down, the other Proxies will have the relevant registration information.

Resource Managers function as an active-active pair in front of a large cluster of MCPs.

MRCP Proxy is used to talk with Nuance and other MRCP clients. For HA, the MRCP Proxy can be deployed with a warm-standby.

Nuance or any other MRCP compatible client should also be deployed in an HA fashion – see the vendor's deployment documentation.

GVP application servers can be deployed using standard clustered web application servers such as Tomcat and Jetty.

Feature Server can be deployed as a cluster. For SIP Cluster deployments, 2 Feature Servers need to be deployed for each SIP Server cluster node HA pair.

4.1.1.2 Disaster Recovery

In the case of a disaster at one of the data center, PSTN traffic can be routed to the other data center either via the service provider or SBCs.

Agent SIP Phones/endpoints are connected to the SIP Proxy using a DNS SRV record. The record should be configured with the SIP Proxies in the agent's main geolocation first followed by the proxies in the other data center(s) as backup. The A-rec FQDN for the SIP Proxies in the agent's main geolocation should be given a higher priority than the A-rec for the other data center. During normal operations, DNS will resolve to the addresses in the agent's local data center as it has higher priority. During a disaster, DNS will resolve to the address to the available SIP Proxies in the operational data. The Genesys SIP Softphone will automatically switch over to the new data center. The Workspace Web Edition will require the agent to log into the other data center (this is typically done using a separate URL and re-entering credentials to reactivate the session).

4.1.2 Management Framework Layer

The Management Framework Layer includes the Configuration Server, Solution Control Servers (SCS), Message Servers and the rest of the Genesys management framework. The deployment model must match the Business Continuity model for the Management Framework as described in the [Common Components Blueprint] and [Management Framework - Disaster Recovery/Business Continuity].

Only one Config Server can be used within a SIP Cluster environment. The Config Server must be configured as a Genesys legacy single tenant deployment. This does not limit the total number of lines of business that may be served by SIP Cluster. It should be setup in one main data center. The Config Server, SCS Master server and Message Server for Config Server should be setup in the same VM. A standby VM with the HA standby servers should also be setup within that data center. Note that the Message Server (CFG) is used for gather logs of all components within the same VM as the Config Server.

For disaster recovery, a second dormant cold-standby HA pair of VMs should also be setup. These cold-standby hosts must contain the same set of applications as those installed as the current, running, hosts in the primary data center.

In a SIP Cluster deployment, it is important to properly setup a Distributed SCS environment. This is depicted in the diagram below. A Distributed HA pair needs to be deployed in each data center which is connected to the Genesys applications within each data center. All Distributed SCS's need to send messages to the same Message Server. This should be in the same data center as the Framework VM. This is depicted as Message Server (DSCS) in the diagram. A dormant cold-standby instance may also be setup in the second data center for failover scenarios.

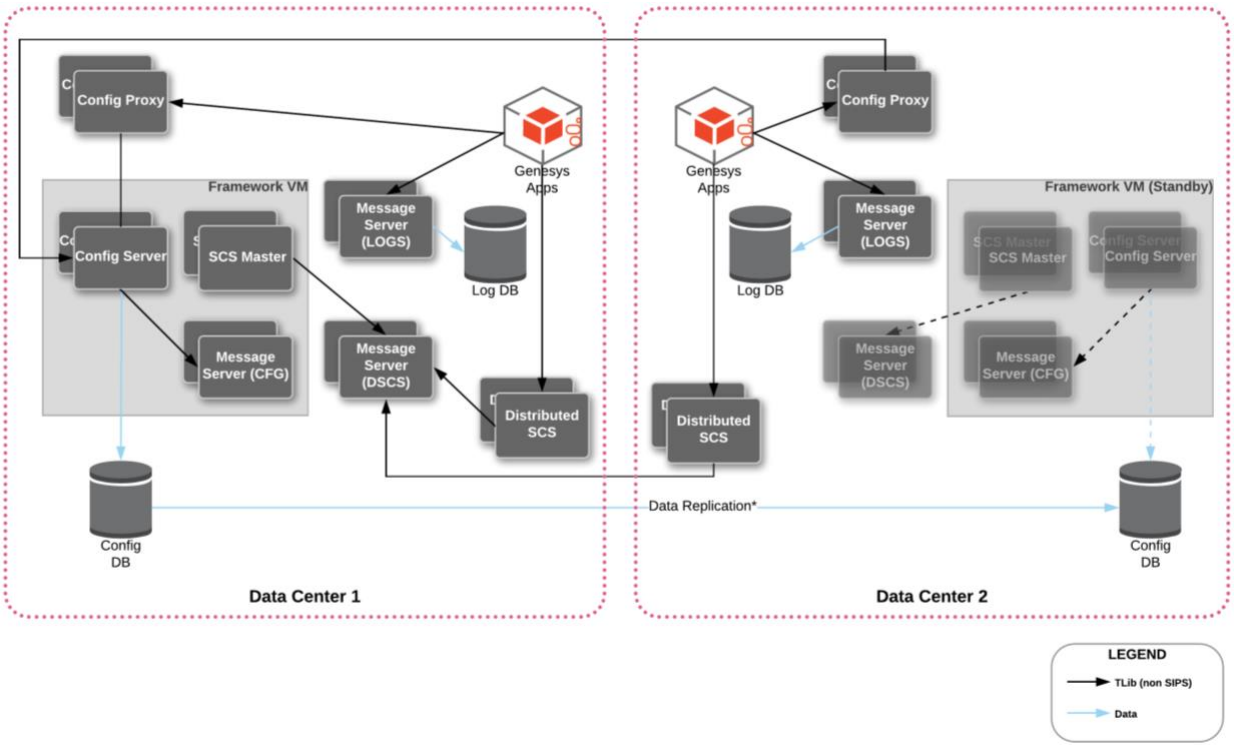

Figure 6: Framework Layer

Other key components to note are the HA pair of Config Proxies in each data center, used to isolate Configuration requests from the Config Server, and a third set of Message Servers dedicated to logging for all applications. An HA pair of Message Server (LOGS) should be deployed in each data center.

For more details on the Framework layer, see the [Common Components Blueprint] and docs.genesys.com

4.1.2.1 High Availability

High Availability for Framework components is setup with standard primary backup HA pairs. As mentioned earlier, Config Server, SCS Master server and Message Server for Config Server should be setup in the same VM for easy switchover in both HA and disaster recovery scenarios.

4.1.2.2 Disaster Recovery

A dormant, cold standby VM needs to be setup in one of the other Data Centers for disaster recovery purposes. It must include the Config Server, SCS, and Message Server for Config Server.

A replica database needs to be created in the DR data center as well. Database replication needs to be setup between the main data center and the DR data center databases using the appropriate replication technology for the selected database (e.g. Oracle Golden Gate, SQL Server SQL Anywhere, etc.).

During a disaster, this VM (and the backup VM) need to be activated. A new SCS Master must be created and connections between the DB Server and the backup database need to be created (either manually or using a script).

During a disaster scenario, DNS/FQDN resolution should be changed to point to the cold standby instance of the Management Framework VM and CS proxies should be restarted to reconnect to the proper Config Server.

For more details, see [Management Framework - Disaster Recovery/Business Continuity].

4.1.3 Routing Layer

The routing layer consists of URS, ORS and StatServer elements required for each of the media types (SIP and Digital). It may also involve the Rules engine and UCS for providing Conversation Manager functionality. The routing elements are fully described in the [Common Components Blueprint].

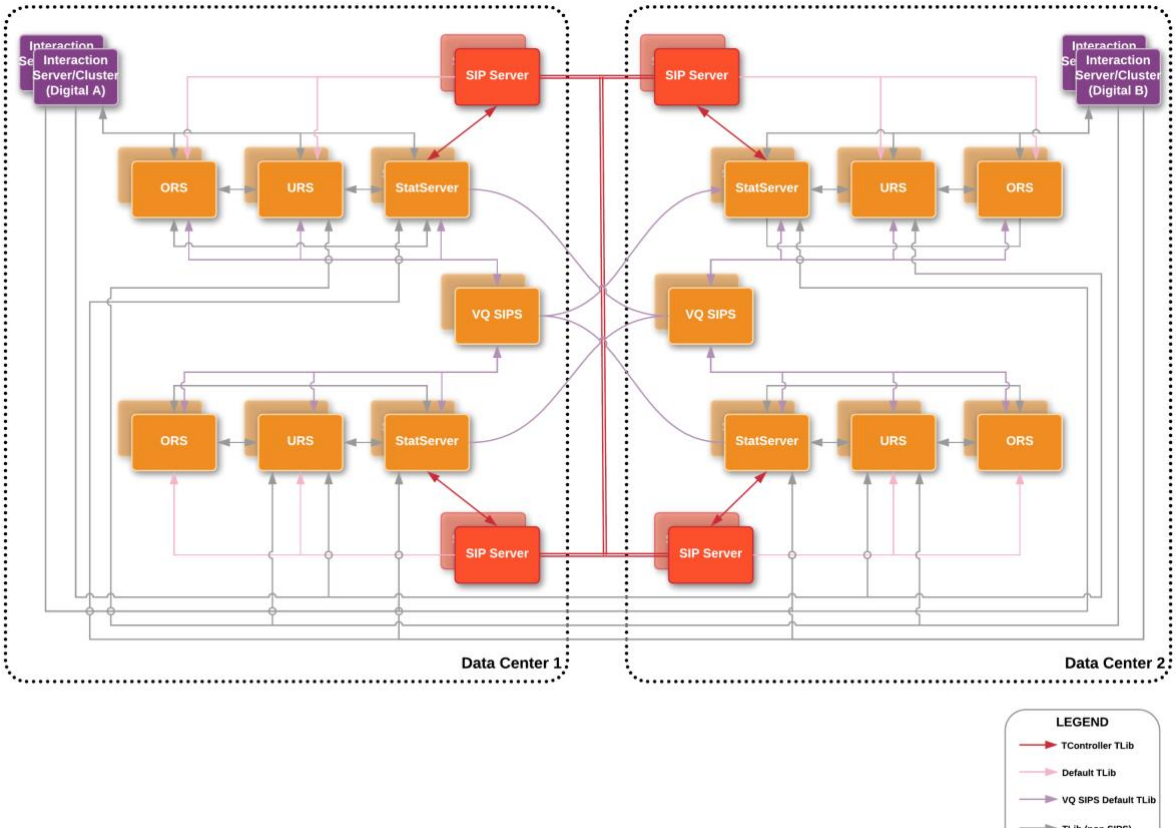

Figure 7: Routing Layer

Virtual Queue SIP Servers are used for reporting and routing purposes. There needs to be one HA pair of VQ SIP Servers in each data center. VQ Sip Servers in all data centers use the same Virtual Queue switch (VQ Switch). Virtual Queue DNs are configured on the VQ Switch. This removes Virtual Queue events from the SIP Cluster nodes to increase the clusters overall performance.

The Virtual Queue SIP Servers are also used for agent reservation. This is why all URS instances must be connected to all VQ SIP Servers. URS sends all Virtual Queue DN T-Requests to the local instance of the VQ SIP Server but URS needs access to all other VQ SIP Server instances for agent reservation.

To support blended agents, Interaction Servers must also be connected to all StatServers so they can see the agent states for SIP Cluster voice agents and all other Interaction Server/Cluster agents.

URS and ORS support location-based routing. The `sitex()` function is used in strategies to dictate the geo-location for the desired resources.

4.1.3.1 High Availability

URS and StatServer should be deployed as HA pairs in hot standby mode.

ORS can be deployed as an N+1 cluster. ORS also supports a primary/backup HA model.

4.1.3.2 Disaster Recovery

The routing layer operates independently on each data center albeit with the same routing strategies.

4.1.4 Workspace Layer

The following diagram depicts the Workspace Web Edition (WWE) layer along with the supporting Genesys Web Services (GWS). Note that this is based on the current WWE v8.5.

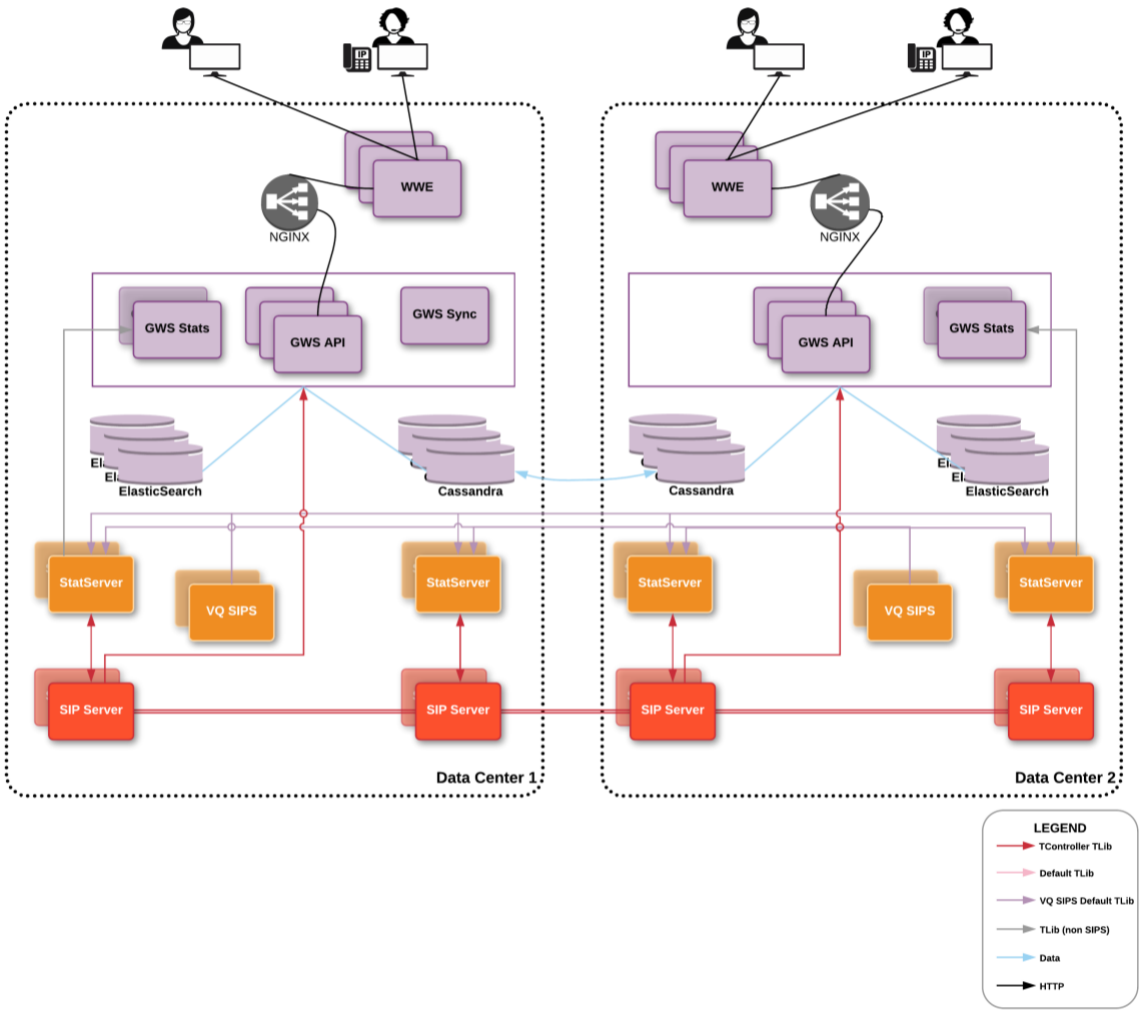

Figure 8: Workspace Layer

Workspace Web Edition is a web application that supports the agent and supervisor user experience into the SIP Cluster. WWE uses the Genesys Web Services (GWS) REST API to access the Genesys infrastructure and capabilities.

Note that WWE is the only supported desktop for SIP Cluster (custom desktops using GWS may also be considered).

GWS cluster is deployed across data centers. Within each data center, a GWS Statistics node is required. It is attached to one of the Routing StatServers within its data center to gather and display necessary statistics.

The GWS cluster also attaches to one of the SIP Cluster nodes within its data center, using the SIP Cluster's T-Controller port. This enables GWS to view the status of all DNs within the cluster.

4.1.4.1 High Availability

WWE is deployed on a clustered web application server.

GWS also uses a clustered approach to HA. It does require a GWS Sync Node (in the current release) to coordinate the cluster. GWS also includes a GWS Statistics node in each data center – the GWS Stats node should be configured with a primary/backup HA pair.

GWS stores metadata within a Cassandra ring and indexes that data using a localized ElasticSearch cluster within each data center. The cluster and ring are within each data center. Cassandra also replicates data across to the Cassandra ring in the other data center for DR purposes.

4.1.4.2 Disaster Recovery

Other than the GWS Sync Node, all components are available in all data centers. Traffic can be readily shifted in case of data center failure. A cold standby GWS Sync node can also be deployed in the second data center.

As mentioned, the metadata within Cassandra is replicated across to the other data center and is available during DR. ElasticSearch will index the replicated data as part of its indexing source.

4.1.5 Reporting Layer

The Reporting Layer includes both Real-Time Reporting (Pulse) and Historical Reporting (InfoMart).

Historical reporting is based on data from ICON. ICON receives call data from the IProxy port on SIP Server and agent data from the TController port. For HA, there needs to be a primary and backup ICON on each SIP Server pair, each writing to its own ICON database. They operate in an active-active mode.

Genesys InfoMart reads from all ICON databases and combines the data accounting for any ICON failures. It also assimilates call, agent and user data for a given call, as that data may be coming from different ICON databases attached to different SIP Cluster nodes.

Real-time reporting utilizes a dedicated Real Time Reporting StatServer that reads from the TController feed of one of the SIP Servers. Note that since SIP Servers within the cluster share DN status information using the TController layer, a Stat Server attached to one of the cluster nodes can report on all DNs within the cluster.

An LDS may be placed in front of the Real Time Reporting StatServer and other components (GPlus Adaptors and VQ SIP Servers) using the TController port of that SIP Server to reduce the load on that SIP Server.

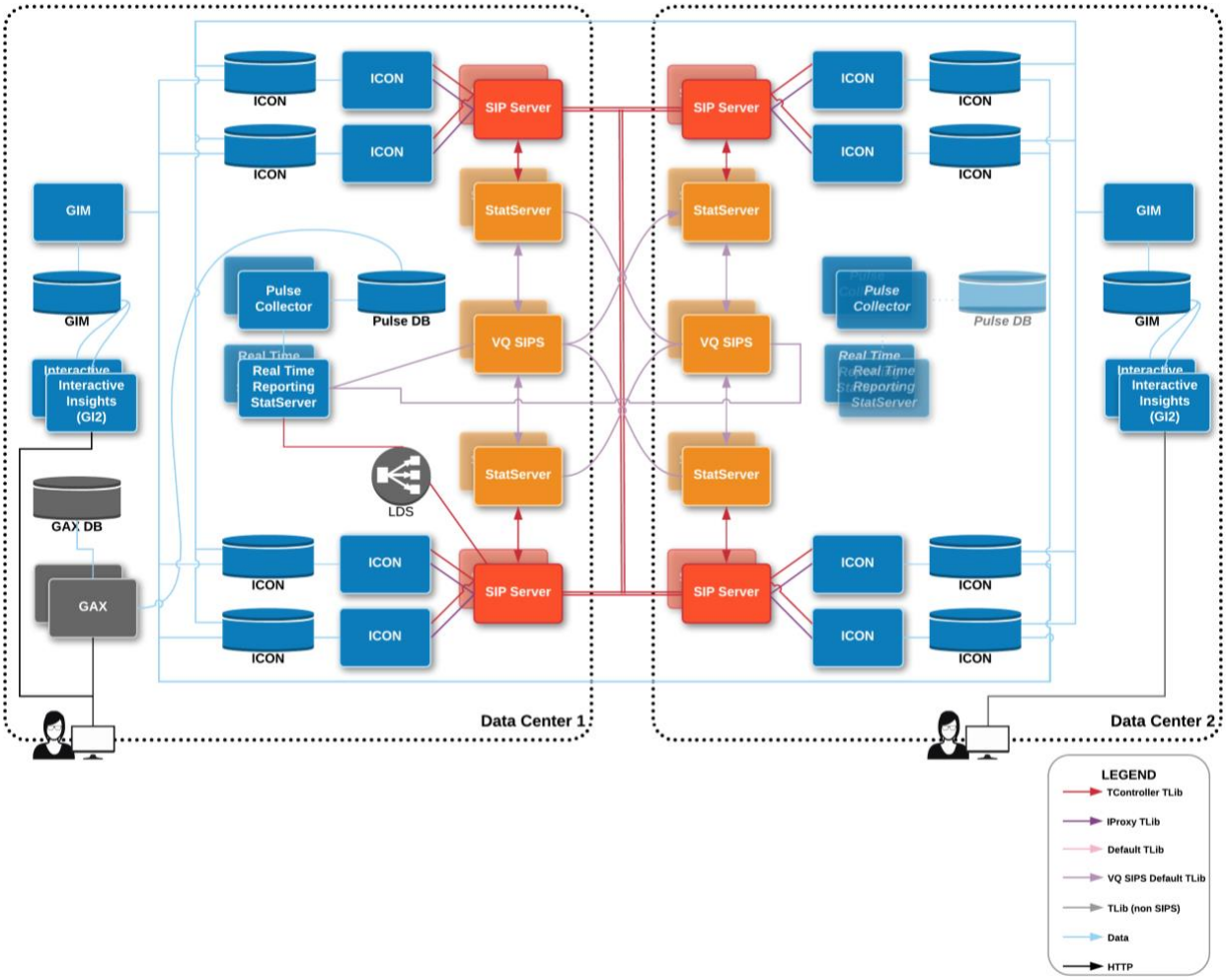

Figure 9: Reporting Layer

High Availability

For Historical Reporting, two ICONs are setup for each SIP Server cluster node. Each has a connection to the primary and backup SIP Servers so that they can continue to receive events when a switchover happens. Each ICON writes to its own database, providing data redundancy. If one ICON fails, the other will continue writing data. GIM will consolidate data when it extracts data from all ICON databases, accounting for any failures.

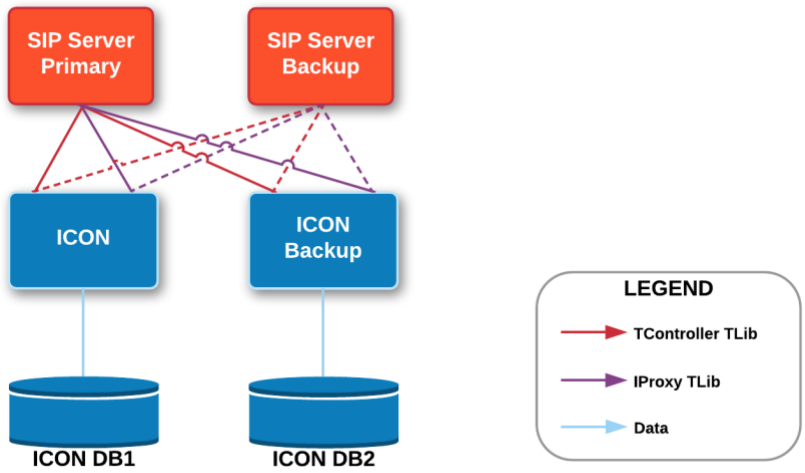

Figure 10: ICON HA

Note that the data redundancy also enables upgrades and maintenance on a single ICON at a time. ICON only records data on new calls; ensure that the ICON going out of service has complete recording all calls before switching over or call data may be lost.

For Real-time Reporting, each real-time StatServer is deployed as an HA pair against a SIP Server cluster HA pair.

Pulse collector nodes should be deployed as HA pairs. Note that multiple Collector Nodes may be required depending on the number of statistics being collected and displayed in real-time.

4.1.5.1 Disaster Recovery

ICON is mainly a data pulling tool and can pull data from remote sites if required. In a clustered environment, ICON should be setup locally with each SIP Server cluster node. In a DR scenario, calls will move to SIP Server cluster nodes within the active data centers and ICONs there will continue to pull data from them. ICON databases can be replicated for additional data redundancy if required.

Genesys InfoMart can be setup in two data centers to provide disaster recovery. Each GIM will pull data from all ICON databases and transform the data for historical reporting. Note that both GIM instances run independently against the same data sets. The reports generated should reflect the same output, but internal keys may be different. This mechanism is not intended to be used for High Availability.

Pulse Collector nodes, DB and RT StatServer can be setup in cold standby mode in the secondary data center to start collecting real time stats if there is a disaster. The nodes as well as the cold RT StatServer and Pulse DB would need to be manually restarted in a disaster scenario.

Pulse is not necessarily a mission critical component – the cold standby components are not necessarily required.

4.1.6 Outbound Layer

The Outbound layer mainly consists of the Outbound Campaign Server (OCS) and its underlying database. It connects with ORS, SIP Server and the StatServer associated with that SIP Server using TLib connections.

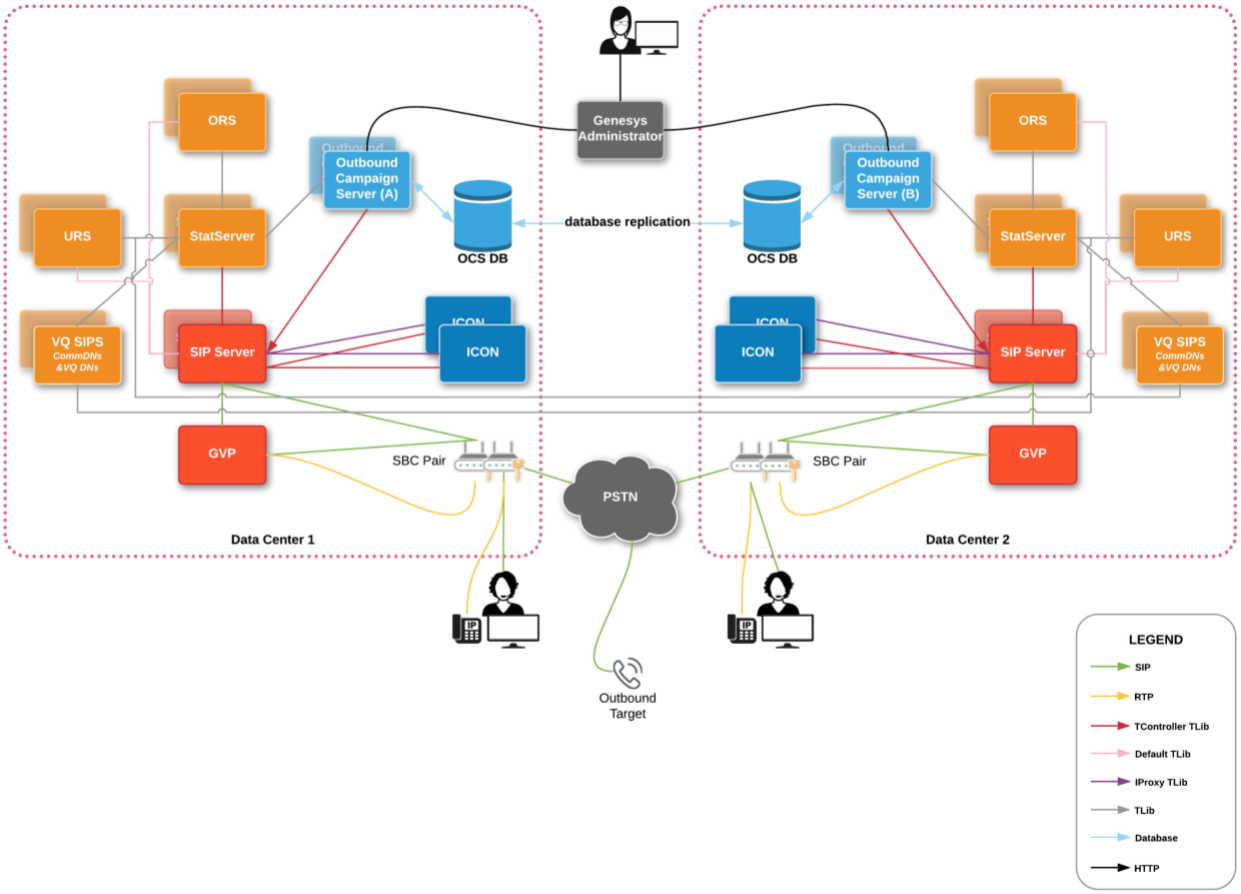

Figure 11: Outbound Layer

Multiple Outbound Campaign Servers can be deployed. They can be deployed as Active-Backup where the OCS in the secondary Data Center is only use in disaster scenarios. An Active-Active setup (as depicted in the diagram above) enables distribution of the campaign load across the Data Centers. Note that one OCS cannot see the campaign groups being run on the other server.

If one OCS cannot handle the load, multiple OCS servers can be configured within each Data Center. Campaign groups must be manually distributed across available OCS instances.

OCS does require Communication DNs to be configured on the VQ Switch associated with the VQ SIP Servers. This enables communication between OCS and StatServer as well as OCS third party software using the Communication DN API.

One or more Trunk Group DNs should be configured for each data center. Multiple OCS campaign groups can use the same Trunk Group DN within the OCS data center. A single Trunk Group DN for the enterprise is also supported but requires geo-aware SRV FQDNs for the GVP Resource Managers.

A pool of CPD (Call Progress Detection) ports should be configured within GVP in each Data Center. SIP Cluster nodes within that Data Center need to subscribe to that pool of CPD ports.

4.1.6.1 High Availability

OCS operates in a warm standby HA model. Campaign data in the database enables the backup OCS to recover the current outbound campaign from where it left off as campaign progress is persisted to the database.

4.1.6.2 Disaster Recovery

OCS supports either and Active-Backup or Active-Active disaster recovery mechanism. Database replication between the two Data Centers ensures that campaign progress persisted to the OCS database is available should one site fail.

In Active-Backup mode, only one OCS is used at a time. OCS in the other site is only used in the case of a disaster.

In Active-Active mode, different campaigns are run on each instance of OCS. During a disaster scenario, a campaign that was running on the failed site can be manually continued on the running site based on the replicated campaign data.

4.1.7 Callback Layer

The Callback layer utilizes GMS and callback strategies working on ORS and URS to reschedule chat or voice interactions. Callback calls are put into the queue for routing using logic to ensure the call is made at or near the scheduled time. When the callback call is processed, an outbound call is made versus the agent processing a real inbound call that is waiting in queue (on hold). Web callback are processed in a similar manner.

GMS nodes are configured in one active data center. GMS instances should be configured in a second data center as a cold standby for disaster recovery purposes. Each GMS utilizes its own Cassandra ring.

The ORS node that processes the original call will be used for the callback. This ensure a natural distribution of the callbacks based on the distribution of the original calls coming into the system.

Web callbacks end up on the same data center due to single site GMS. However, SIP Cluster distribution will balance out those calls.

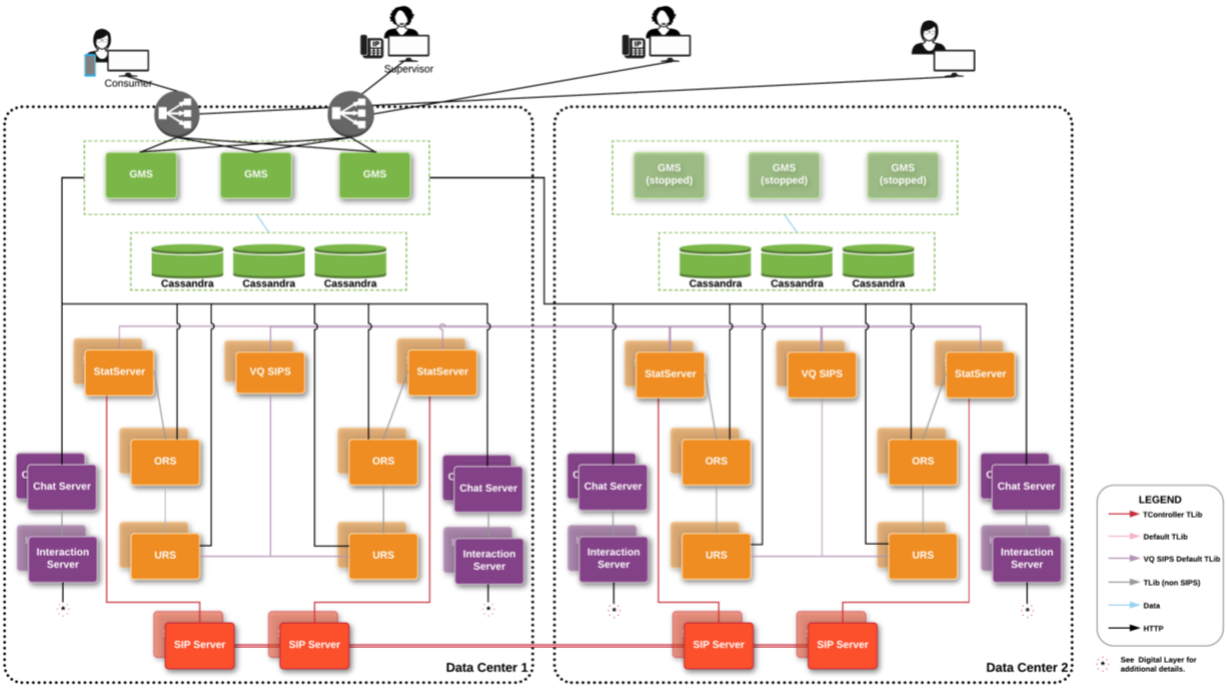

Figure 12: Callback Layer

GMS nodes connect to all URS and ORS nodes within the SIP Cluster. As mentioned in the Routing Layer section, each ORS and URS node connects to a routing StatServer that has a view of all DN states via the SIP Server cluster node's T-Controller port.

All routing StatServers connect to a VQ SIP Server (HA pair) in each data center. The Virtual Queues defined on the VQ SIP Servers are used for the following:

- Reporting (RT & Historical)
- Agent Reservation for callback dialling (requires special URS option)
- Callback dialing schedule

Note that a global list of virtual queues requires a global stat server.

Callback reporting uses a special table to record user events (G_CUSTOME_S). The ORS nodes send these user events based on SCXML session events. GIM has specific ETL for handling CallBack data manipulation and reporting.

4.1.7.1 High Availability

GMS nodes function as an N+1 cluster for availability. Their connections to other Genesys components should use a load balancer.

GMS components need to be connect to primary and backup nodes of HA paired components like URS and StatServer to ensure operation if those HA paired components failover from primary to backup.

4.1.7.2 Disaster Recovery

GMS cluster does not support an active-active data center model. It requires cold standby instances of the GMS cluster that can be switched on during a disaster.

Cassandra should be configured to replicate data to the other data center in case of a disaster scenario.

4.1.8 Recording Layer

The following diagram depicts the components that make up the recording layer and how it integrates within the cluster environment. A two data center deployment with two SIP cluster nodes is shown.

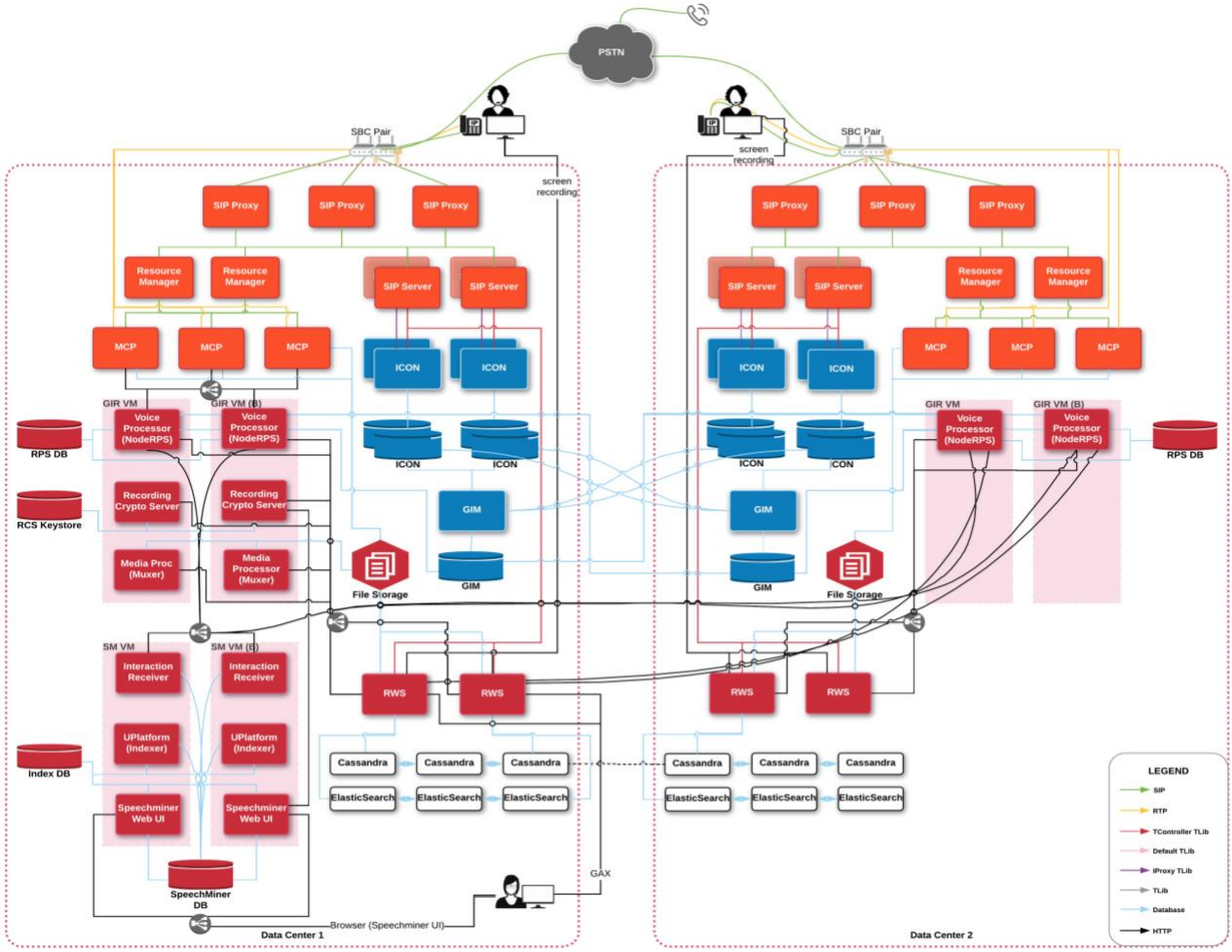

Figure 13: Recording Layer

The MCPs used within the Voice Layer can also be used for recording. Recordings are stored in the File Storage area. The File Storage should be a WebDAV enabled network storage. Please see the GIR Deployment Guide for more details. Note that all recordings are encrypted with the appropriate key based on the selected IVR Profile.

The GIR and Speechminer components are shown in their recommended VMs. This reflects the current deployment within Genesys' PureEngage Cloud at the time of this writing. Speechminer components are deployed in the main data center. If the main data center goes down, recordings can continue, and recordings will be stored within the local file storage. When the primary data center is restored, Speechminer can continue processing the cached recordings.

The Voice Processor (NodeRPS) retrieves metadata for the recordings from the GIM database. As shown in the Reporting Layer, GIM extracts and transforms data from all ICONs in the cluster. Voice Processor can retrieve data from GIM data sources in the other data center if the local GIM database is unavailable.

As metadata is processed by the Voice Processor, Speechminer's Interaction Receiver records the event in the Speechminer database for further processing within GIA/Speechminer. A message is also sent to the Recording Web Service (RWS) to store the metadata on the recordings. This will facilitate users retrieving the voice and screen recordings later. Note that RWS manages the storage and retention of recording files.

The UPlatform (Indexer) processes all audio and analyzes its content as part of the GIA/Speechminer product.

Screen recordings utilize a Screen Recording Service (a Windows Service) that communicates with Workspace Web Edition to determine which agent/Place/DN is logged into to the PC. The plug-in registers to RWS, RWS then registers the DN to SIP Cluster using the T-Controller port. RWS monitors the voice recording events (start/stop/pause/resume) and triggers screen recording based on the screen recording policy.

When the screen capture is complete, it is sent into GIR via RWS. The Media Processor (Muxer) retrieves the associated recording from the file storage, decrypts it, and mixes the recording with the video of the screen capture. The results are re-encrypted and stored in the File Storage area. RWS is also informed for caching the metadata on the screen recording. Note that the Muxer only operates within the primary data center.

To access recordings, privileged users utilize the Speechminer Web UI. Recordings are decrypted using the Recording Crypto Server. RWS is used to retrieve the files from File Storage. The UI is only available within the primary data center.

Note that the Recording Crypto Server has access to the appropriate keystores. There is an Administrator function to update the keystore via a web service within RWS.

4.1.8.1 High Availability

Speechminer components follow primary/backup HA pair model. The recommended VM layout follows this pairing model using a load balancer in front to control traffic to the current primary VM and components.

The GIR components, particularly the Voice Processor, use a cluster model for HA. Although two VMs/instances are shown, multiple instances can be deployed based on the load.

Recording Web Services also follows a cluster model and can expand based on the load. It also uses Cassandra rings for metadata storage and ElasticSearch clusters for indexing the metadata. The Cassandra data is replicated to the other data center (ElasticSearch on the other data center only indexes its local Cassandra data; remote data replicated into the same Cassandra storage should get indexed).

4.1.8.2 Disaster Recovery

All data centers will have MCPs, File Storage, RWS and Voice Processors. This ensures that recordings can continue even if the primary data center goes down. Certain activities like muxing the screen recordings and indexing the audio recordings will need to wait until the primary data center operations are restored.

4.1.9 Digital Layer

The digital channels (chat, email, social-media, etc.) utilize the Interaction Server to determine agent availability for handling digital interactions. Interaction Server uses an Interaction Proxy clustered layer to multiplex connections from clients and digital server to the corresponding Interaction Servers. Interaction Servers themselves can also be clustered – cluster can be configured to handle all digital

media across one or more data centers; or they can be partitioned around media types.

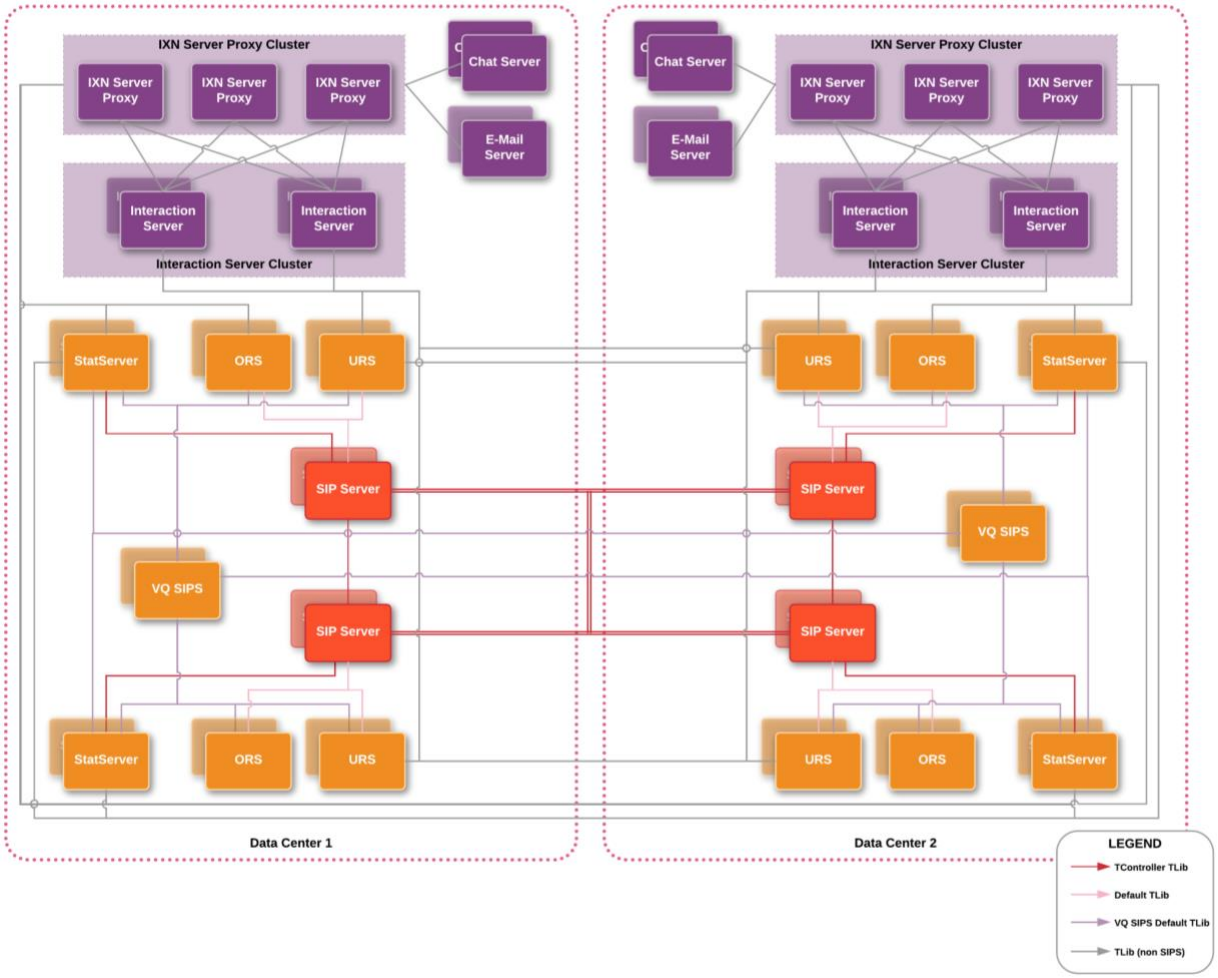

Figure 14: Digital Layer

Interaction Servers will need to connect to all URS being used by SIP Server cluster nodes. [Why]

A connection is required to all Routing StatServer connected to SIP Server cluster nodes. These can be managed by the Interaction Proxy cluster layer. This enables Interaction Server to reserve agents that may be used on SIP Server cluster nodes….

For more details on the architecture of Digital please see [Digital Solution Blueprint]. For configuration information on Interaction Server and the digital channels please see [docs.genesys.com/]

4.1.9.1 High Availability

Interaction Server uses a primary-backup failover HA mechanism. In addition, the cluster of Interaction Server HA pairs can share the load from the various digital channels and users.

Interaction Server Proxy cluster layer …

For more details, please see the Digital Solution Blueprint and docs.genesys.com

4.1.9.2 Disaster Recovery

For discussion on Disaster Recovery of the Digital channels, please consult the [Digital Solution Blueprint] and docs.genesys.com.

4.2 Database Layer

Genesys supports a wide variety of databases. Please consult the Supported Operating Environment documentation here [https://docs.genesys.com/Documentation/System/Current/SOE/Welcome] to see which databases are supported.

Replication between data centers is also required for various components of the data layer. This may require installing additional database products and licenses and ensuring the databases are properly configured for replication between data centers.

Cassandra and Elasticsearch are open source data layer products that are also incorporated into this solution and need to be deployed and administered within the environment.

5 Interaction View

5.1 Agent Experience

Workspace Web Edition is the desktop supported by SIP Cluster. It is a browser based thin client. For voice channel, Genesys Softphone is the recommended SIP endpoint. Other SIP phones may be supported – please see the [Supported Media Interface] guides. Agents using PSTN phones are also supported.

5.1.1 Agent Login

The agent should be provided with a URL that points to the WWE FQDN defined for their preferred data center. A second URL pointing to another data center should also be provided in case WWE is not available in the preferred data center.

If the browser disconnects from WWE/GWS for a configured amount of time (1 minute default), the user will be requested to refresh their browser and login again. They can alternatively use the URL for the other data center.

The login experience is based on agent provisioning and is similar to a typical WWE deployment. Note that the EmployeeID for the agent is used as the value of AttrAgentID in the TAgentLogin request – a separate Agent Login configuration object is not required.

5.1.2 Genesys Softphone

The Genesys Softphone can run in one of two modes – Standalone or Connector mode. In Connector mode, WWE controls the softphone. Standalone mode enables the softphone to be used in parallel with WWE; the agent can use the softphone independently, but WWE is integrated so that it can also control the phone and report on events.

The Genesys Softphone should be provisioned with a geo-aware SRV FQDN address that points to the SIP Cluster SIP access point. DNS should be configured to prefer the local data center's SIP access point over the other data centers' access point. The SIP access point can be either an SBC, or a SIP Proxy.

Note that the Genesys Softphone can automatically switch to the available SIP Cluster data center if there is an outage with the data center it is currently using. This is based on the proper configuration of DNS SRV addresses for the SIP Cluster access point and is based on SIP REGISTER timeouts.

5.2 Call Flows

5.2.1 Login and SIP Registration

The following diagram depicts the agent login and SIP phone registration.

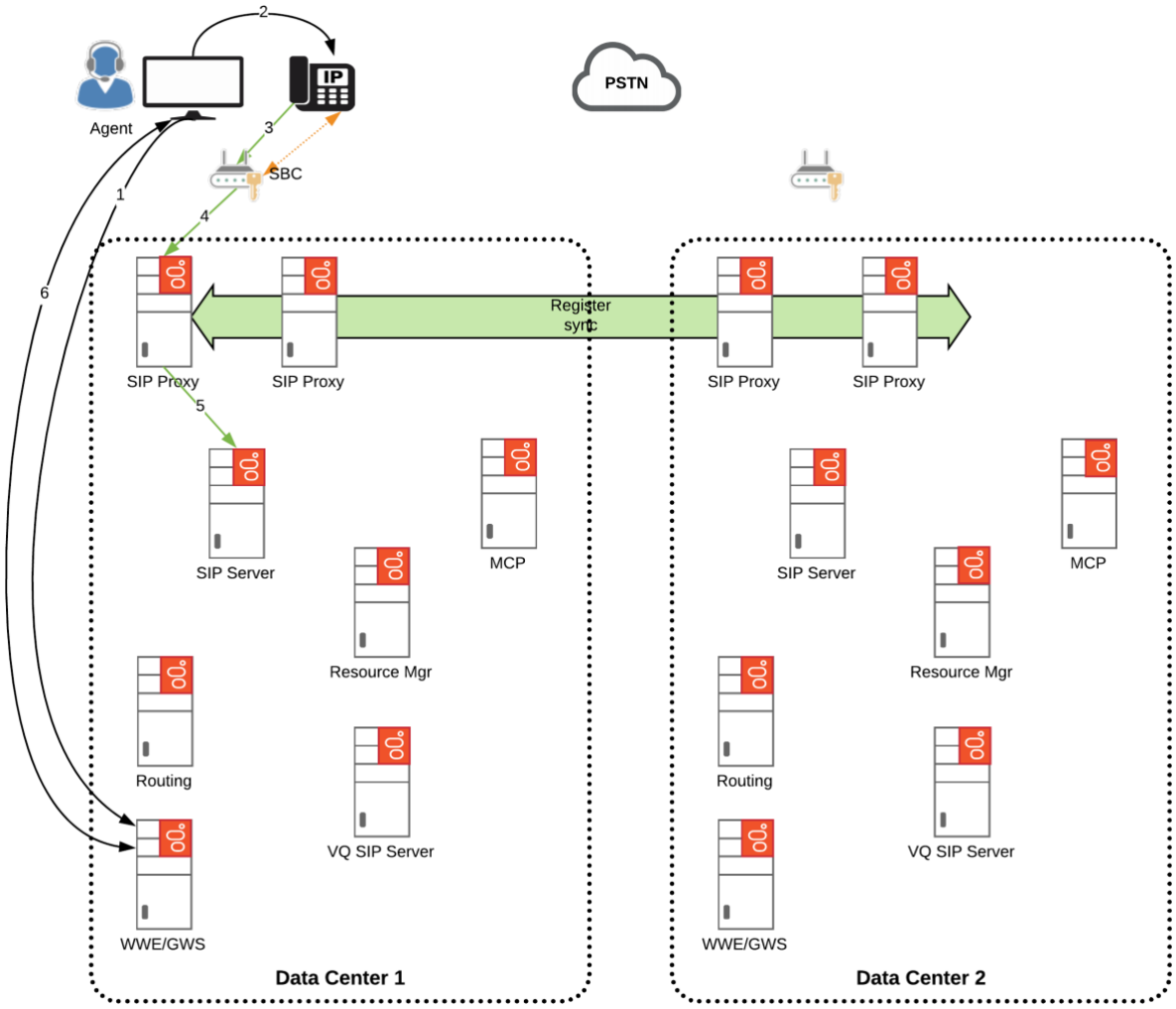

Figure 15: Login and Register

1. Agent starts WWE, get authenticated and receives the softphone configuration (if applicable).
2. Softphone is configured and activated (if applicable).
3. SIP phone sends REGISTER message to the SIP access point (SBC).
4. SIP REGISTER sent from SBC to a SIP Proxy based on round robin.
5. REGISTER sent from SIP Proxy to any SIP Server within the Data Center based on geo-location. DN is now in service.
6. GWS starts the session for the agent.

5.2.2 SIP Inbound

The following diagram depicts Agent Registration and an Inbound call routed to an agent.

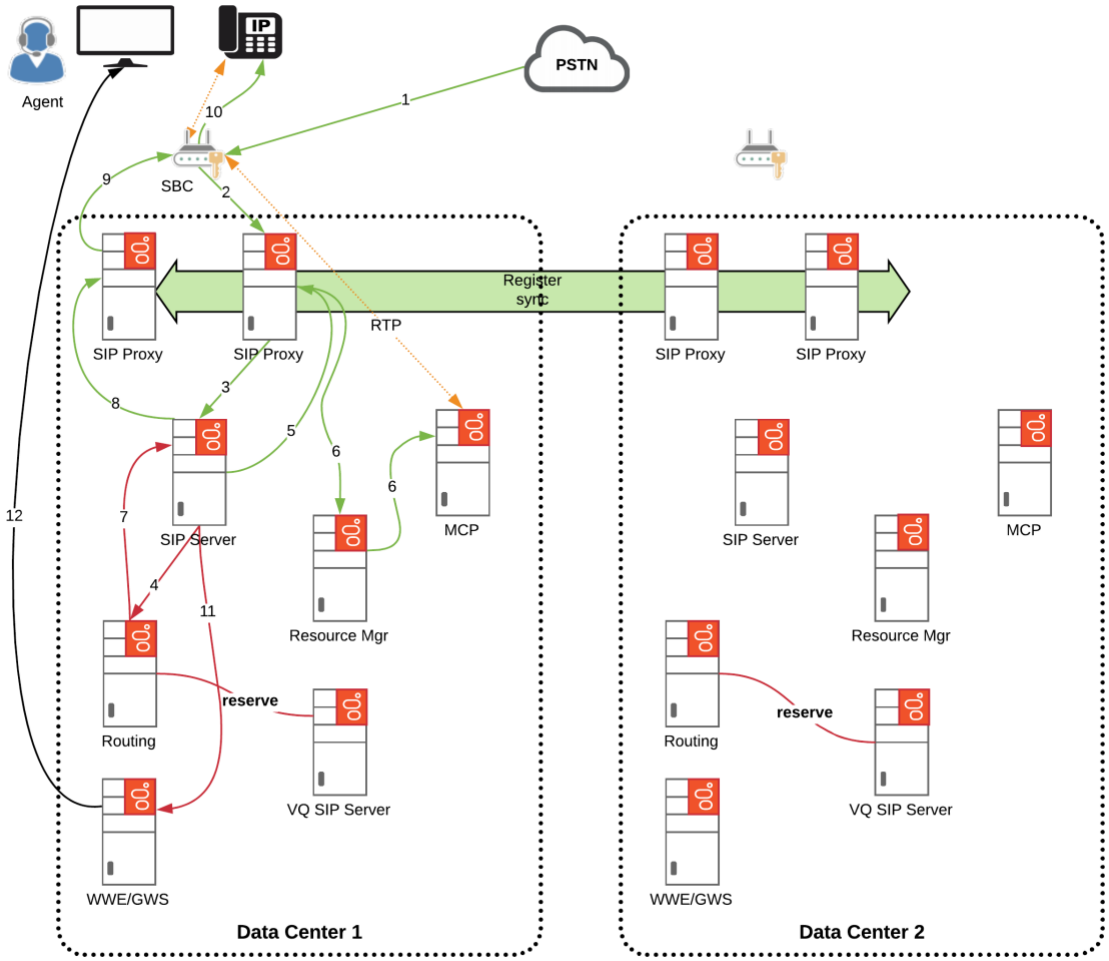

Figure 16: Inbound Call Flow

1. Inbound call from PSTN or SIP Trunk received by the SBC.
2. SBC forwards INVITE to a SIP Proxy (based on DNS SRV round robin).
3. INVITE forwarded from SIP Proxy to any SIP Server within the Data Center.
4. EventQueued/EventRouteRequest sent to the Routing layer from SIP Server. ORS strategy is executed – in this case a Treatment is requested.
5. INVITE sent to SIP Proxy.

6. INVITE forwarded from SIP Proxy through RM to MCP. RTP is established and the treatment is played.
7. Once an agent is available, URS signals SIP Server to route the call to the designated Agent.
8. INVITE sent from SIP Server to a SIP Proxy.
9. INVITE forwarded by SIP Proxy to SBC.
10. INVITE forwarded to the Agent's SIP Phone and RTP is established.
11. EventRinging TLib message is sent to all TLib clients including GWS at the same time that the INVITE was sent from SIP Server (11).
12. GWS forwards the ringing notification to the Agent's Workspace.

5.2.3 Outbound

A typical Outbound call flow is shown below.

1. The Administrator configures an Outbound campaign on the OCS server.
2. OCS retrieves the set of numbers to dial.
3. OCS sends a request for SIP Server to dial the next number in the campaign.
4. Assuming CPD is required on the Outbound call, SIP Server sends and INVITE through SIP Proxy and Resource Manager to attach an MCP to monitor the outbound call.
5. Outbound call is made through the SBC towards the external number.
6. RTP is established between the SBC and the MCP used for CPD.
7. Agent is requested as it is determined that the call is valid.
8. Agent is registered via the VQ SIP Server.
9. Router sends request to add the agent into the call.
10. SIP Server sends and invite through SIP Proxy towards the agent's phone.
11. EventRinging is sent towards GWS and is forwarded to the Agent's workspace.

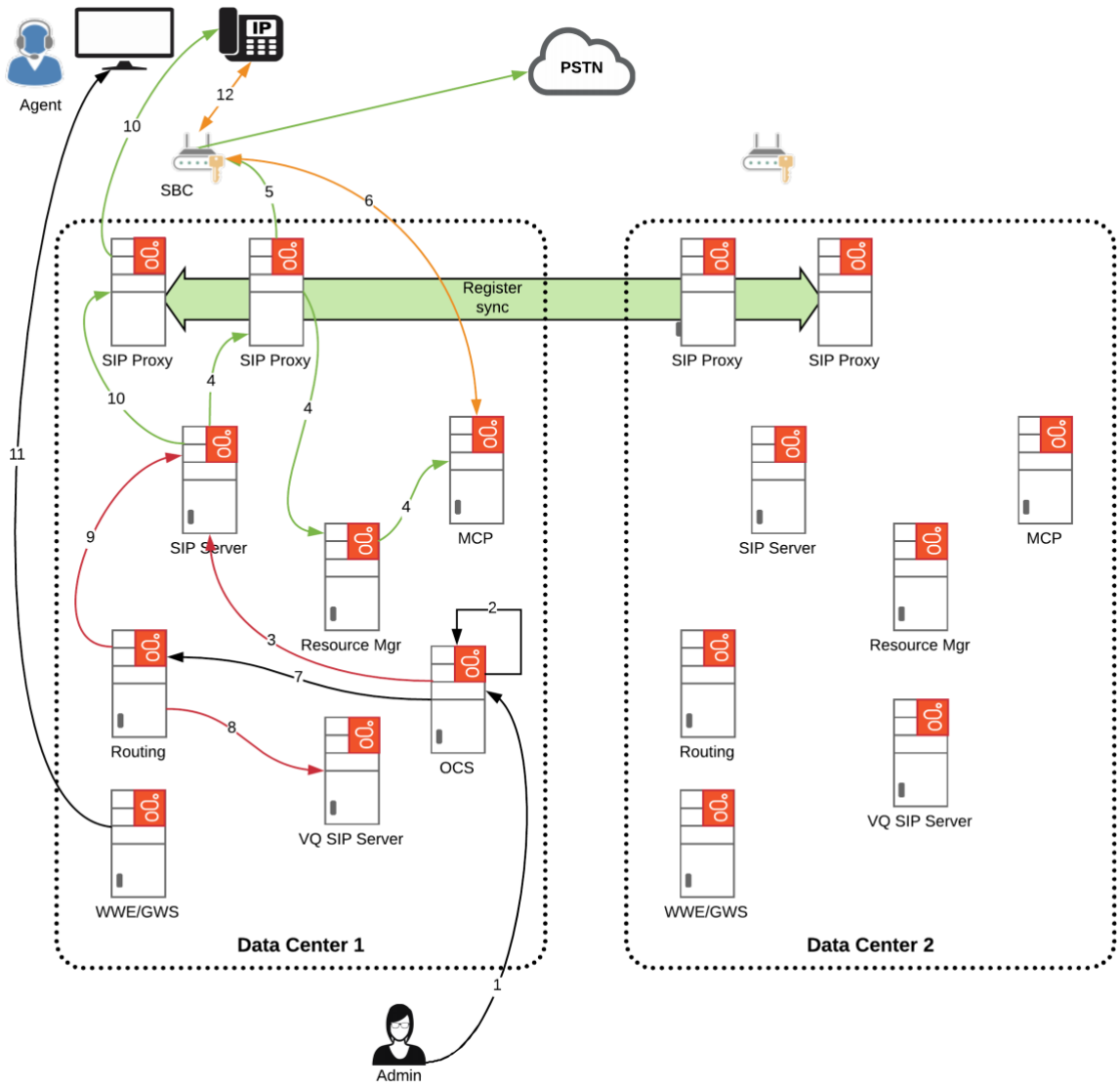

Figure 17: Outbound Call Flow

5.2.4 Screen Recording

Screen and voice recording call flows are depicted in the following diagram.

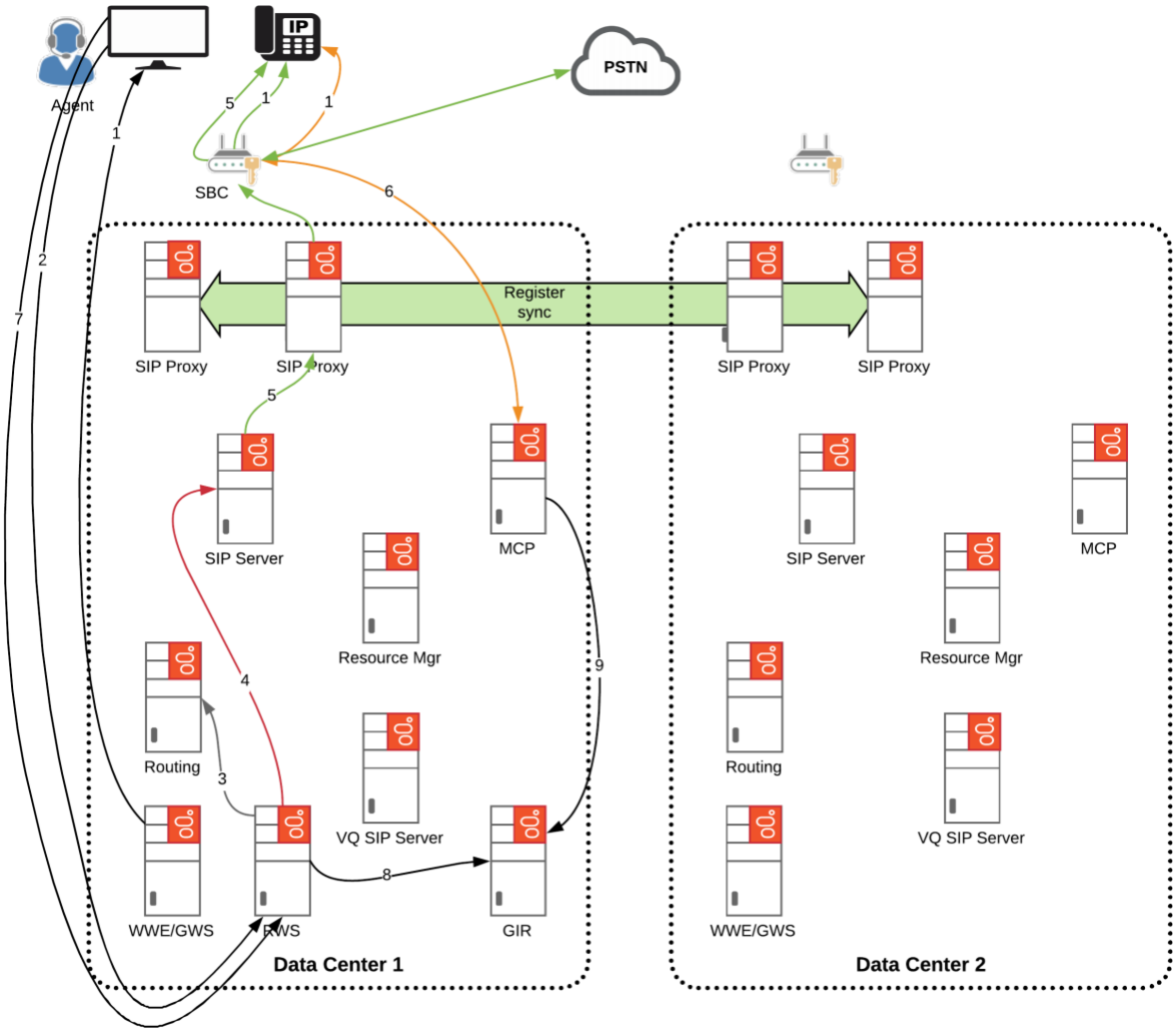

Figure 18: Screen Recording

1. Starting criteria, phone is registered and the agent is logged in and available for a call. PSTN call is being routed to the agent.
2. Screen Recording Service registers with RWS at the time the agent logs into WWE. The service is also responsible for recording video of the screen within the agent's desktop computer once activated.
3. RWS monitors DN for voice recording. If the voice call is recorded, it will trigger additional rule on RWS for the agent (ie. Percentage recording).

4. RWS sends a request to record the call for this agent.
5. SIP Server sends an INVITE through SIP Proxy to SIP Phone (SBC?) to send RTP to the MCP for recording.
6. RTP is established with the MCP. Note that its IVR Profile will specify that the recording should be encrypted with the keys specified in that IVR Profile.
7. Call concludes and the Screen Recording plug-in sends the video of the agent's screen to RWS.
8. RWS send the video to GIR for muxing the audio and storing the final encrypted video file.
9. MCP stores the encrypted audio file in the appropriate file storage and notifies GIR that the audio is ready for further processing.

5.2.5 Disaster Recovery

The following diagram depicts a disaster scenario.

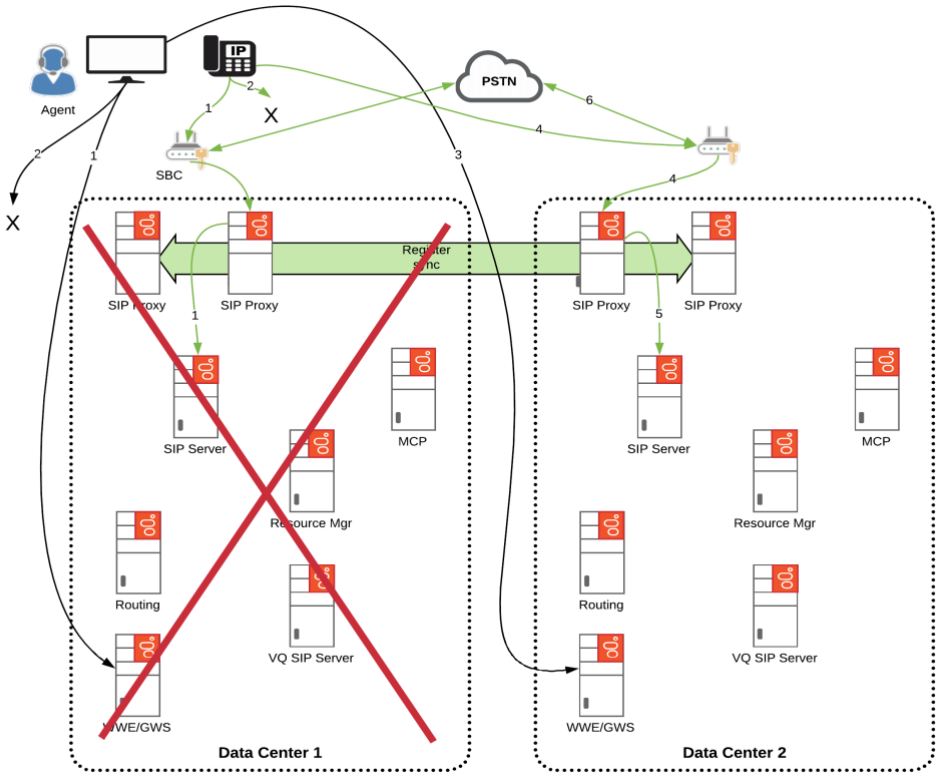

Figure 19: Disaster Call Flow

1. Initial scenario – the agent is logged into WWE and her phone is registered within Data Center 1.
2. An outage occurs. WWE's connection times out and the SIP phone's regular REGISTER messages stop returning 200OK.
3. The Agent will eventually use the URL that points to WWE in the other data center. The agent will be authenticated. Screen Recording Service will also re-register with RWS to ensure that the proper DN is monitored for recording.
4. The SIP phone should REGISTER using the DNS SRV record which should point to the SIP access point in the other data center.
5. The SIP Phone's DN can now be put into service on the SIP Server in Data Center 2.
6. It is assumed that the service provider will distribute calls the the available SBCs which should ensure that new calls will be directed towards Data Center 2.

Note that during catastrophic failures, calls will be lost that were established in Data Center 1.

5.2.6 Call Back

One of the typical call back scenarios is depicted in the call flow below.

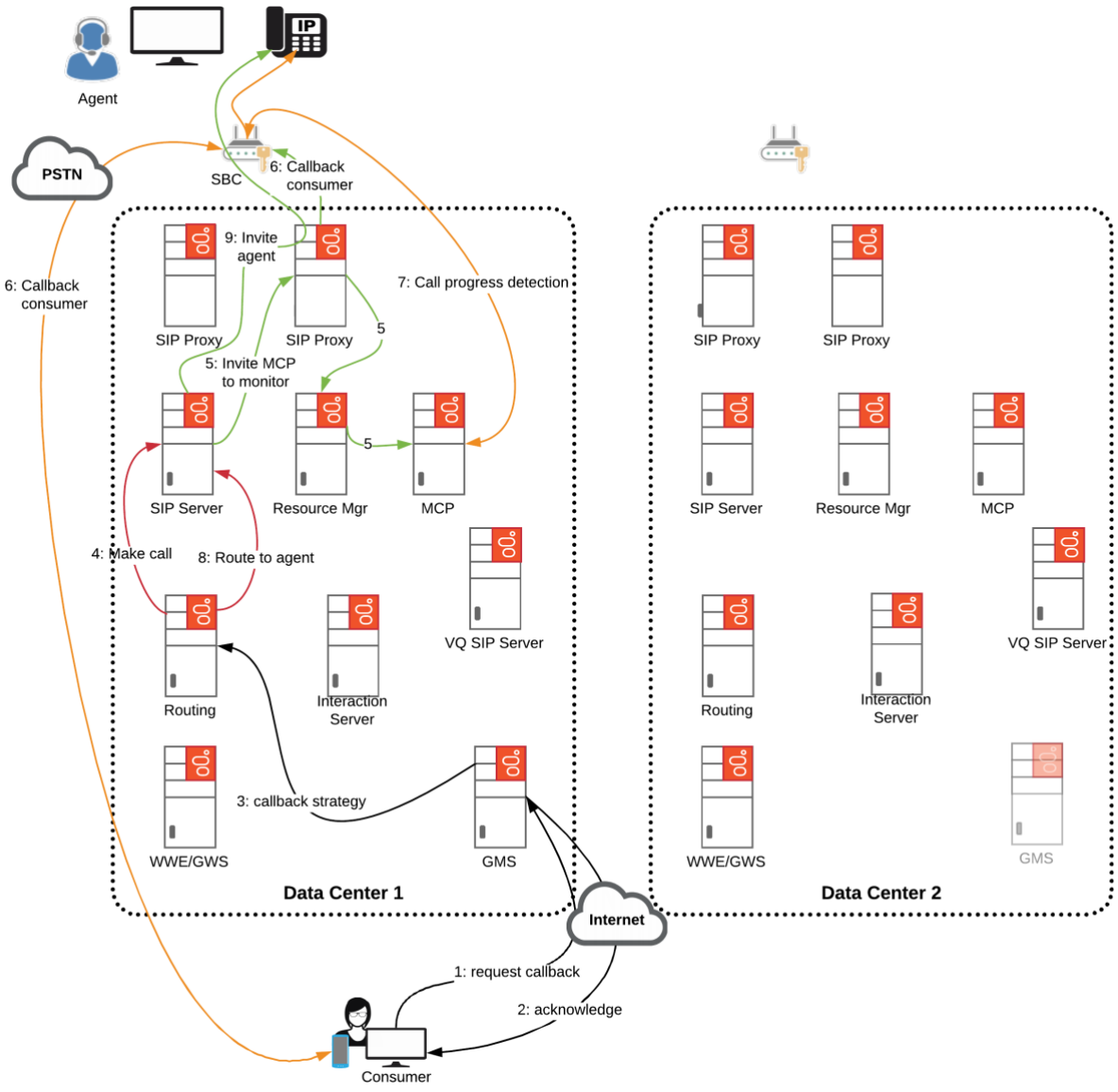

Figure 20: Call Back Call Flow

1. A request for a callback is sent from the web or mobile app to GMS (through appropriate firewalls and load balancers).

2. GMS will send back an acknowledgement to the web/mobile app.
3. GMS sets up the Callback strategy within the routing components (URS/ORS).
4. At the appropriate time, a MakeCall request will be sent from the Callback strategy to SIP Server in order to callback the customer.
5. An MCP can be invited to the call for progress detection.
6. The consumer will be called back.
7. The MCP will use CPD to determine that the call has been successfully answered.
8. The strategy will then route the call to an agent on SIP Server.
9. SIP Server will then send the Invite to the agent.

Note that there are several other ways to use callback. As an example, the user or mobile app call make the call (steps 4-6) into the contact center and the callback strategy will ensure that the call is immediately forwarded to the best agent without queueing.

5.2.7 Voicemail

The following diagram depicts a customer leaving a voicemail in the system.

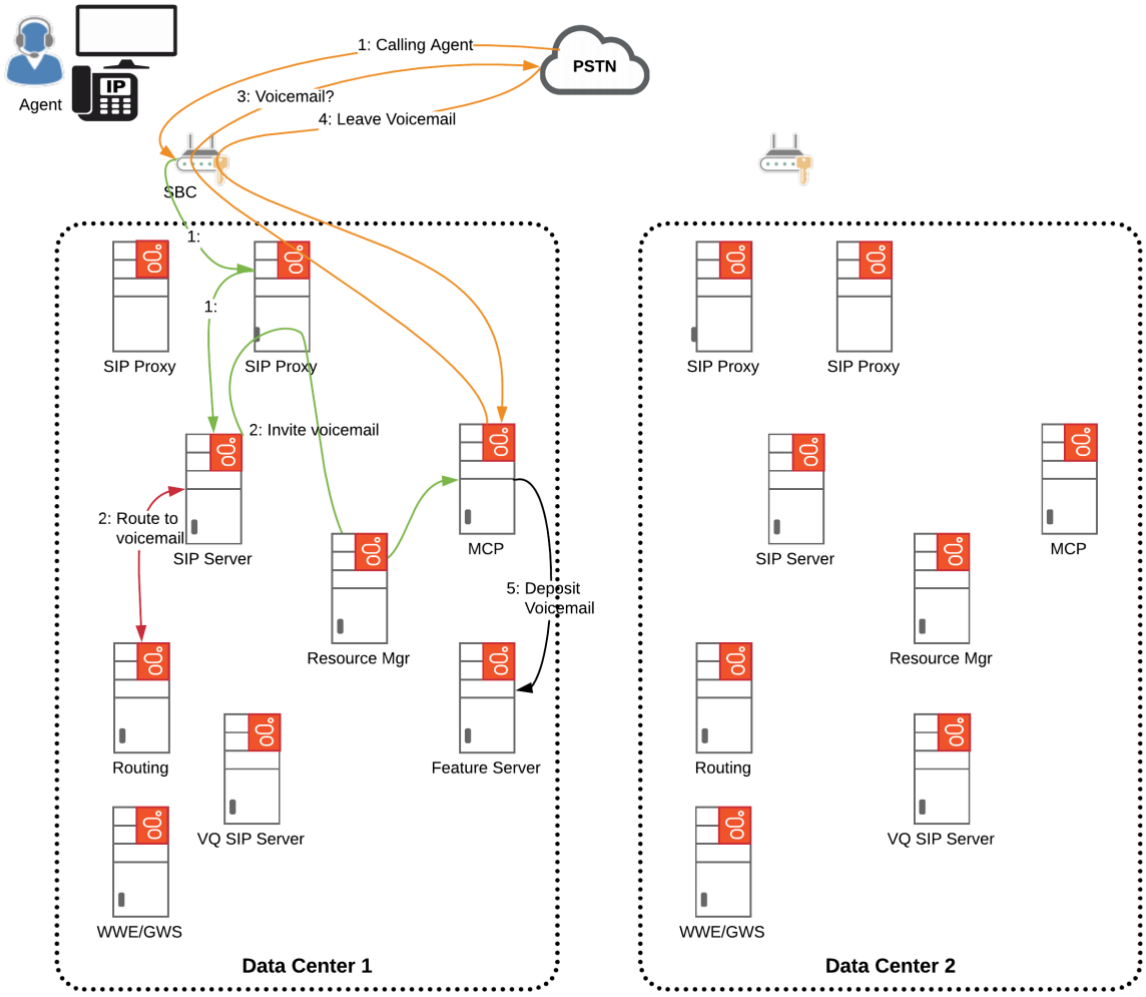

Figure 21: Leaving a Voicemail

1. Consumer calls into the contact center – call will be sent to a SIP Server.
2. Based on conditions (e.g. no agent availability), the strategy will route the call to voicemail. SIP Server will invite the consumer to the voicemail application within GVP/MCP.
3. The consumer will interact with the voicemail application.
4. The consumer then leaves a voicemail within the IVR application.
5. The voicemail audio is then deposited within the voicemail box in Feature Server.

The agent then retrieves the voicemail.

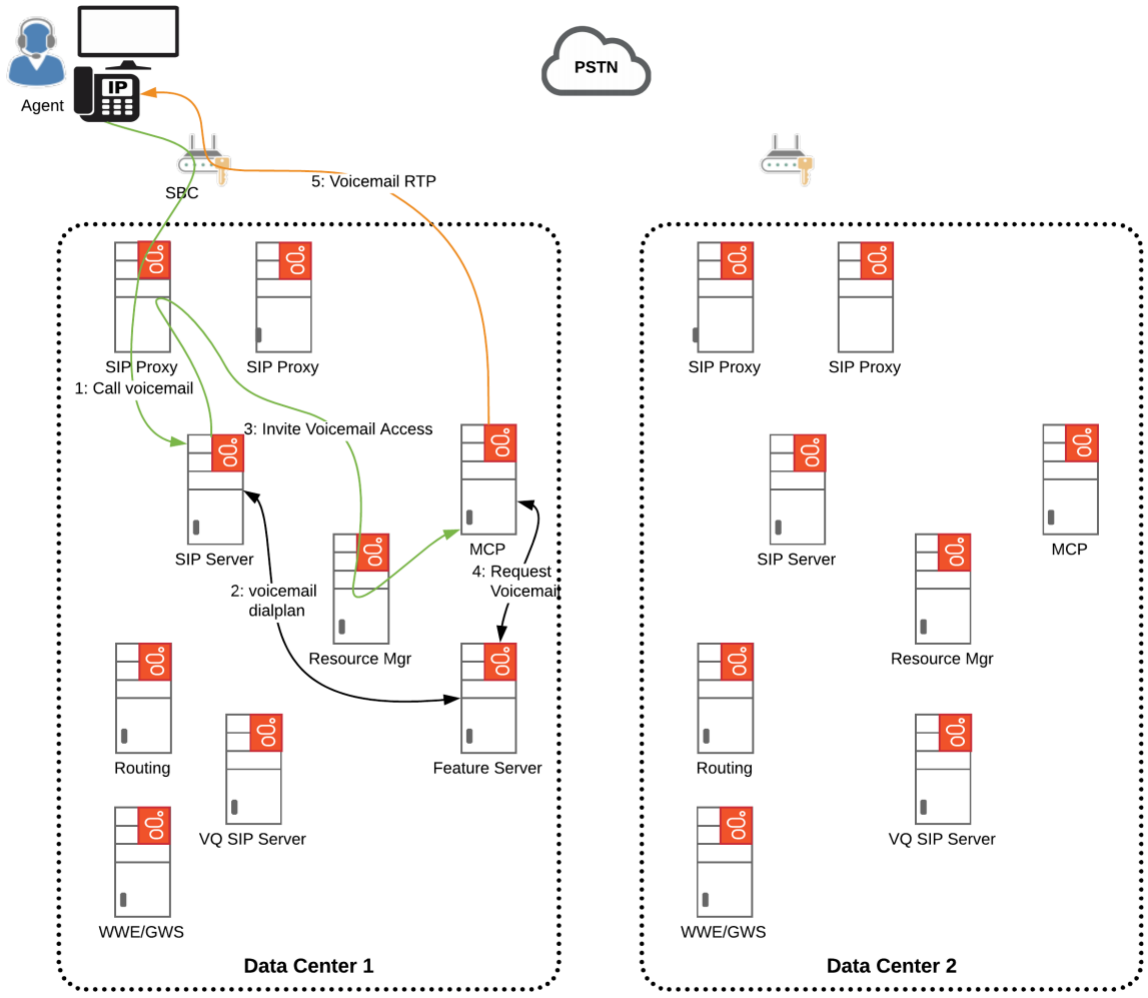

Figure 22: Accessing Voicemail

1. The agent dials the voicemail number.
2. SIP Server retrieves the voicemail dial plan from Feature Server.
3. The agent is then invited to the GVP voicemail access IVR application.
4. The IVR application retrieves the voicemail from the voicemail box on Feature Server.
5. Agent listens to the voicemail.

The agent could use WWE to make the voicemail request instead of dialling directly – this would result in a 3PCC call and SIP Server would then send an invite towards the agent once the Voicemail application is called (step 3).

5.2.8 Consultation Between Data Centers

The following diagram depicts an agent in DC1 consulting with an agent in DC2.

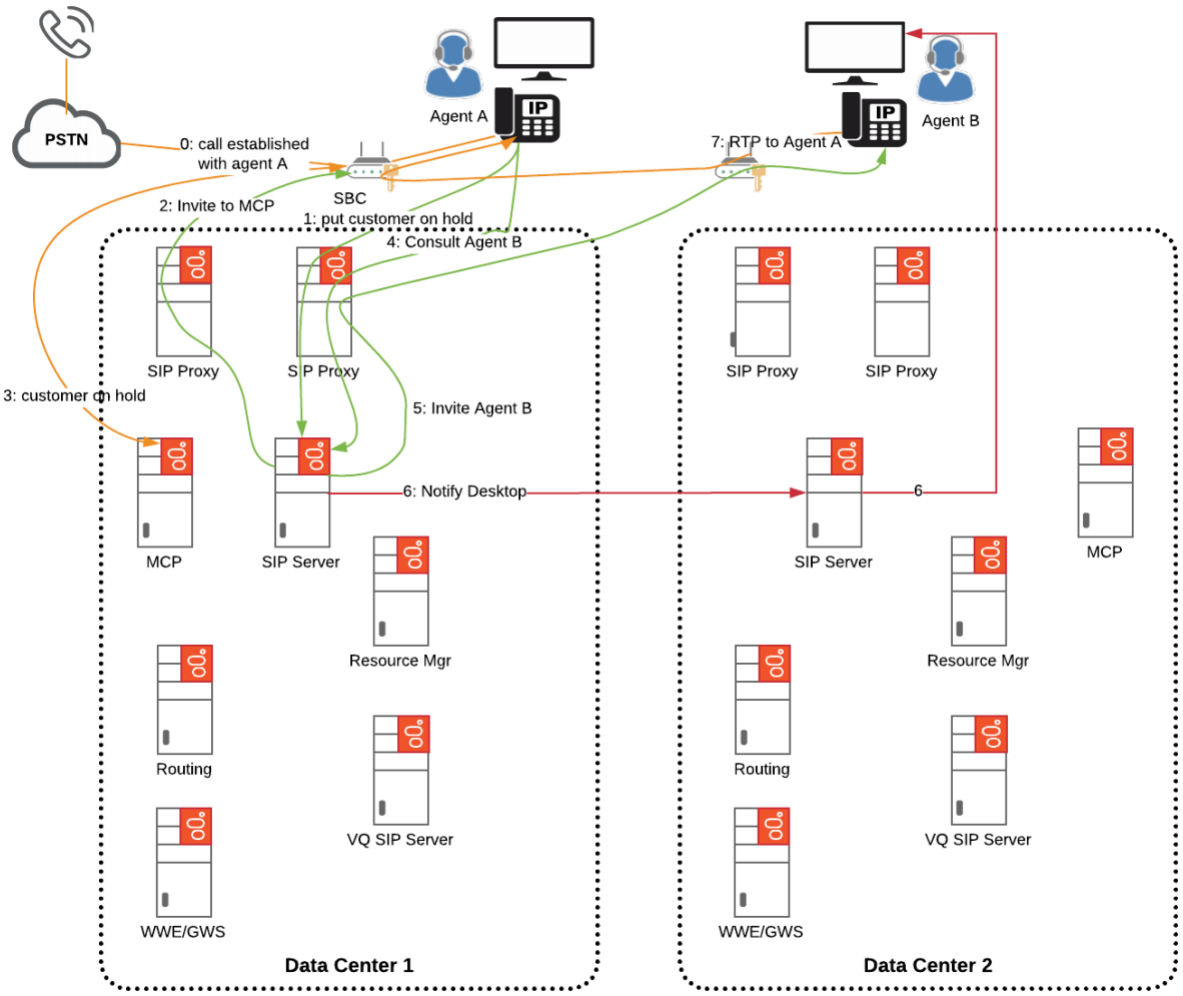

Figure 23: Geo Consult Call

Initially, Agent A in DC1 is on a call with a customer.

1. Agent puts the customer on hold.

2. An reInvite is sent to the customer for an MCP to handle the hold.
3. Customer is connected to the MCP and is now on hold.
4. Agent A makes request to consult with Agent B.
5. SIP Server send the Invite directly to Agent B.
6. SIP Server in DC1 knows that Agent B's DN is owned by SIP Server on DC2 and sends a notification. SIP Server in DC2 sends notification through GWS to the agent's desktop regarding the incoming consult call.
7. RTP is established between Agent A and Agent B.

At this point, Agent A could disconnect Agent B after the consultation and take the customer off hold to complete the interaction. Or Agent B could be conferenced into the call in which case an MCP would be invited to mix the various RTP streams for the conference call.

5.3 External Interfaces

The following tables lists the external devices and components that will need to be integrated with the Genesys solution components.

Interface	Protocol	Solution Components	Integration Tasks	Description
Media Gateway/ Session Border Controller (SBC)	SIP and RTP	SIP Proxy, SIP Server, Resource Manager, MCP, SIP Endpoints	Add the necessary bandwidth to the network Provision the network infrastructure (e.g. DNS) for the new traffic Provision the MG and SBC appropriately for the integration Configure the codec list for supported codecs.	This interface is used to handle ingress and egress voice traffic from the network.
Configuration, Log, and Reporting Databases (Relational Database/RDBMS)	TCP/SQL	Genesys Info Mart, Interaction Concentrator, GVP Reporting Server, Config, Log, etc.	Provision the network infrastructure (e.g. DNS) for the new traffic	This interface is used to get configuration data about the solution and log alarms.

			Run the database scripts (.sql) Provision appropriate user access to required database tables	It also is used to store reporting data.
Corporate Backend Servers	HTTPS (REST or SOAP), RDMBS access methods (optional)	MCP, 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 can also be used to perform certain business actions.
Enterprise Authentication Service (Optional)	Active Directory	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. Genesys provides the option to have user passwords authenticated an external authentication service or authentication can be managed by Genesys.
Corporate Network Management System (Optional)	SNMP	Genesys 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.
Domain Name Servers	DNS	SIP Proxy, SIP Server, Workspace, Interactive Insights, SIP Endpoints, etc	Provision the DNS records along with appropriate weightings.	This interface is used by the clients to perform the

		(potentially any Genesys application).	Ensure that DNS SRV records are setup in a geo-aware manner to ensure that a requestor will be given local records with higher priority than those of the remote SIP Cluster data center sites.	name/IP address translation. DNS is a key technology used to support the SIP Cluster.

Table 3 - External Interfaces

5.4 Operational Management

5.4.1 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.

SIP Server and other components of the solution also have HTTP statistics monitoring. An NMS can use these HTTP ports to monitor and alert if statistics exceed threasholds.

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

5.4.2 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 can reduce the time to send logs to support. Configuring 3rd party components to log into the same location is ideal as well. Establishing a "log" directory in the root of the disk structure and logging there is recommended:

```
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 SIP messaging Genesys provides the SIP Span 2 utility which can provide an understanding of the SIP call flows within a Genesys environment.

In order to understand the logs and efficiently troubleshoot SIP Server issues, it is recommended to maintain a network architecture diagram showing the IP addresses of key components (including SIP Server(s), Resource Manager(s), Media Control Platform/Media Server(s), Media Gateway(s), Session Border Controllers, etc.) and information on typical call flows. This 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 Genesys Care together with the initial problem description and logs, to help reduce overall resolution time.

Genesys Care Workbench

The Genesys Care Workbench is a suite of troubleshooting tools that can quickly and easily identify and resolve issues in a 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 monitor log files from supported Genesys applications and display important events for troubleshooting.

Once Genesys Care Workbench is released it is recommended that it is included as a standard part of any deployment. For further information, please check out the following link:

https://docs.genesys.com/Documentation/ST/current/WorkbenchUG/Welcome

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.

6 Implementation View

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

6.1 Solution Sizing Guidelines

Describe sizing of the solution. If applicable link to the Solution Sizing Calculator.

Include input assumptions.

Input Assumptions	2,000 Agents
Agents	2,000
Agent utilization	80%
Call qualification time	60s
Queue time	120s
Talk time	180s
Log retention	Debug 2 weeks
Reporting History	2 years
Non-aggregated Reporting History	3 months
Calculated worst case values - Inbound	
Calls / agent / hour	16
Concurrent active calls	2000
Peak CAPS	8
Busy hour calls	28800
Calculated worst case values - Outbound	
Calls / agent / hour	48
Total Daily Records	50,000
Total Answer Rate	70%
Human Answer Rate	30%
Redial Attempts	1

For Log Retention, the logs should be moved from each hosts' local storage to an archival storage system such as a NAS or using a log/data mining tool. Retention periods for logs may vary due to legal requirements. From a support perspective, retaining logs and ICON data for two weeks is a recommended best practice.

As noted in the deployment section of this document, one ICON HA pair should be setup for each SIP Server cluster HA pair is also recommended.

6.1.1 Storage Sizing

Voice recording storage sizing should be based on:

- Average voice recording size: bitrate times the average file length in seconds divided by 8
  - 16 kbps for mp3 (stereo)
  - 8 kbps for mp3 (mono)
- Average recording size times the retention period

For Screen recording storage, refer to the [GIR Solution Blueprint] for further details.

6.1.2 Database Sizing

Database sizing for recordings is based on the:

- Number of recording per day
- The retention period for the recordings
- The baseline metrics for the database:
  - Initial size: 1 GB
  - Size increase per 100,000 records (recordings per day times the retention period) 0.1 GB
  - Index size per 100,000 records 0.3 GB

6.1.3 Network Sizing and Readiness

Network sizing for the SIP Cluster is based on many factors including:

- concurrent call volume
- audio codecs for calls
- attached data

There is additional network traffic between each data center to support the SIP Cluster.

For GIR there are three main considerations for network bandwidth:

- MCP Bandwidth: density of MCP times the bandwidth for bridging
  - The calculated density (number of recording sessions) of each MCP
  - The bandwidth required for G.711 (0.25 Mbps)

- File storage (WebDAV): voice plus screen
  - Voice (Mbps): busy hour total recording size (MB) divided by 3600 times 8
    - Busy hour recording size: busy hour calls time average call duration time bitrate divided by 8 divided by 1024
  - Screen: Depends on a number of factors including the upload window and the video quality. Please refer to the screen recording appendix for details.

6.2 Configuration Guidelines

The following section provides some high level guidelines on important SIP Cluster configurations. For detailed information and up-to-date information please consult the appropriate deployment and configuration guides at http://docs.genesys.com

6.2.1 SIP Server

Ensure DNS is configured with geo-aware SRV FQDN address. It should resolve to the SIP Cluster access point closest to the requestor. As an example, the SRV record would be:

```
_sip.tcp.sipcluster.abc.com
_sip.udp.sipcluster.abc.com
```

This address should also be configured in the VoIP Service DN in the TServer section.

The DNS records in each data center should list all the SIP Proxies, giving priority to the proxies in the local data center versus the remote data center(s).

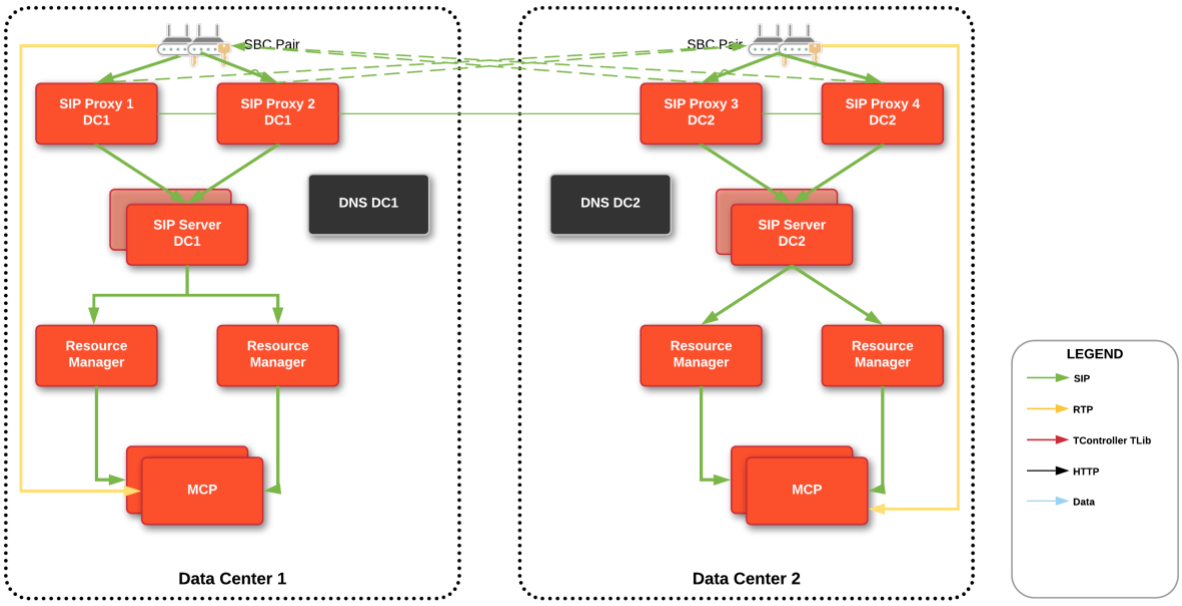

Figure 24: DNS Configuration

In the layout above, The DNS records would look something like this:

DNS DC1				DNS DC2			
Pri	Weight	Port	Target	Pri	Weight	Port	Target
1	50	5060	Sipprxy1.abc.com	2	50	5060	Sipprxy1.abc.com
1	50	5060	Sipprxy2.abc.com	2	50	5060	Sipprxy2.abc.com
2	50	5060	Sipprxy3.abc.com	1	50	5060	Sipprxy3.abc.com
2	50	5060	Sipprxy4.abc.com	1	50	5060	Sipprxy4.abc.com

Table 4: DNS Config example

A client requesting `sipcluster.abc.com` from DC1 will use the SIP Proxies with priority 1 (sipprxy1 and sipprxy2). Traffic will be delivered 50/50 to those proxies. If those proxies are unavailable, the client would then choose the next priority up (sipprxy3 & 4) on DC2.

6.2.2 ICON

See the configuration guidelines for setting up the ICON `[callconcentrator]` section. Note that a dummy application needs to be setup so that ICON will connect to the T-Controller port on SIP Server.

6.2.3 WWE Provisioning

Instructions for provisioning workspace web edition (WWE) can be found at the following links:

- https://docs.genesys.com/Documentation/HTCC/latest/IWWDep/Provisioning
- https://docs.genesys.com/Documentation/SIPC/latest/Solution/ConfiguringGWS

Proper configuring of the Genesys Web Services is a prerequisite.

Specific configuration options of WWE are made in the `[interaction-workspace]` section at various levels (agent, agent group, virtual agent group or cluster). Note that these are loaded at login; any changes are not during the session are not updated during.

Each agent will need two URLs to point to the WWE address within each data center. One will be their main WWE instance, the other their backup in case of a disaster scenario. For example:

`https://dc1.abc.com/ui/ad/index.html`

`https://dc2.abc.com/ui/ad/index.html`

The Genesys Softphone provisioning is also discussed in the links above. Need to ensure that the SIP Server address is set to the proper DNS address for the SIP Cluster. The DNS record for the SIP Cluster should point the softphone to the nearest SIP access point.

```
sipendpoint.sip-server-address: sipcluster.abc.com
```

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 following list some of the security features to consider for this solution:

- TLS connectivity between all components
- SRTP
- Encrypted recording files (default in GIR)
-

6.3.1 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.

6.4 Localization and Internationalization

Localization and Internationalization are topics for numerous Genesys components, especially user interfaces and reporting. Within the SIP Cluster Premise Solution, the main components to pay particular attention are:

- Media Files such as audio files
- Administration & Operation management user interfaces
- Agent desktop software
- Reports

Appendix A Migration Strategy

In traditional Genesys environments, migrating to a new environment could be accomplished by using the Genesys ISCC protocol. As the new T-Server or SIP Server came on-line, agents could be moved to the new environment and calls targeted for that agent would be routed with minimal or no modification to the routing strategies. ISCC would ensure that the call and all pertinent data was sent to the proper T-Server/SIP Server for that agent.

SIP Cluster does not support the use of ISCC between the cluster and other Genesys T-Server environments. This means that migration will not be based on the traditional ISCC methods, but rather the use of a platform agnostic approach as described below.

The following describes a new approach to migration utilizing GMS as a federation mechanism to transfer data between disparate Genesys environments.

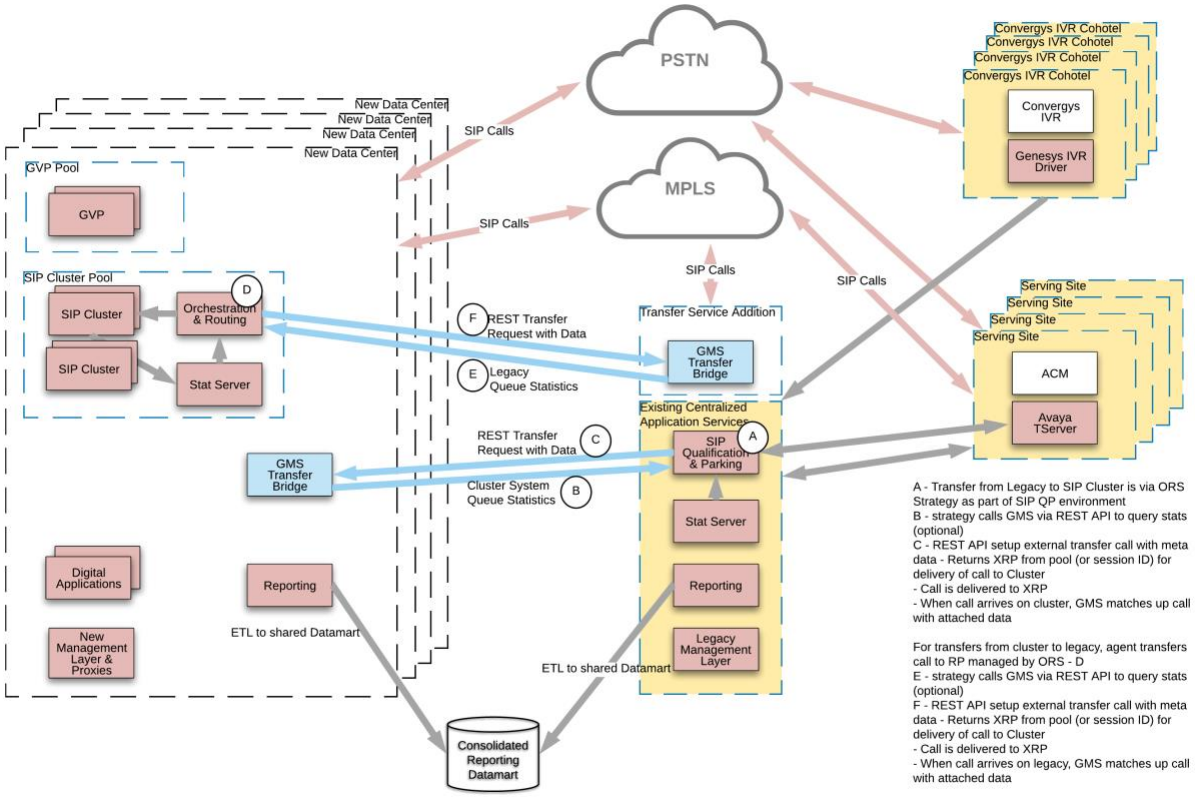

Figure 25: Migration Strategy

The diagram depicts legacy Avaya PBX environments and Convergys IVRs (on the right) connected to a Genesys traditional SQP and management layer in the middle. On the left is the new SIP Cluster environment.