Workspace Desktop Edition Deployment Guide

Load Balancing using clusters

5/11/2025

Load Balancing using clusters

[**Added:** 8.5.108.11] [**Modified:** 8.5.111.21, 8.5.126.07]

A Cluster is pool of Genesys Servers of the same type to which Workspace connects. Workspace connects to a single node of a cluster at a time. The node is selected by a client-side or server-side logic, depending on the clustering model. The Genesys servers that Workspace supports through the clustering model are: Statistic Server, Configuration Server Proxy, Universal Contact Server Proxy (8.5), Universal Contact Server Node (9.1), and Interaction Server Proxy.

There are two Configuration models to defined clusters for Workspace:

1. Stat Server, Interaction Server Proxy, and UCS Proxy (8.5) or UCS Node (9.1) clusters
2. Configuration Server Proxies

> **Important**
>
> For information about UCS 9.1 Nodes architecture, refer to the 9.1 Architecture topic in the *Universal Contact Server Deployment Guide*. [**Added:** 8.5.126.07]

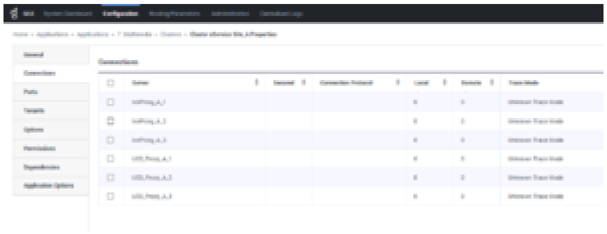
Please refer to the Business Continuity page for details about how to provision as many clusters as business continuity sites.

Contents

Provisioning clusters for Stat Servers, Interaction Server Proxies, and UCS proxies or nodes

Using clusters, Workspace can enable Load Balancing between each server of same type.

To enable Load Balancing through clusters, Workspace takes advantage of the Application Cluster in Genesys Management Framework (a pool of servers that can be of different types; for example, UCS Proxies (8.5) or UCS Nodes (9.1), Interaction Server Proxies and Statistic Servers). This model provisions server pools for the Interaction Server Proxy, UCS Proxy (8.5) or UCS Node (9.1), Stat Servers connections types. The Application Cluster model also enables the support of various scale factors that depend on the application type (for example, three Interaction Server Proxy nodes for eServices agents and six UCS Proxy (8.5) or UCS Node (9.1) clusters for eServices agents and Voice agents). The following figure shows an example of how an application cluster might be configured in Genesys Administrator Extension:



Connections

□	Server	Secured	Connection Protocol	Local	Remote	Trace Mode
□	IxnProxy_A_1			0	0	Unknown Trace Mode
□	IxnProxy_A_2			0	0	Unknown Trace Mode
□	IxnProxy_A_3			0	0	Unknown Trace Mode
□	UCS_Proxy_A_1			0	0	Unknown Trace Mode
□	UCS_Proxy_A_2			0	0	Unknown Trace Mode
□	UCS_Proxy_A_3			0	0	Unknown Trace Mode

> **Important**
>
> Workspace employs a Cryptographically secure pseudo-random number generator (CSPRNG) to select the next node to ensure the best load balancing between all Workspace instances.

Procedure

Creating a cluster for Workspace

Purpose:

To enable Business Continuity for Statistic Server, Interaction Server Proxy, or Universal Contact Server Proxy (8.5), or Universal Contact Server Node (9.1) clusters in Workspace.

Start

1. Be sure to have ApplicationCluster template in Genesys Administrator Extension. if you don't have such application template, either import it from eService Interaction Management CD or create an empty template from scratch using "Application template" type.
2. Create a new application based on application cluster template

3. In connections, add all Stat Servers, Interaction Server Proxies, and UCS Proxies (or UCS Nodes) you want to load balance
4. In Server Info tab, select the tenant (ignored by Workspace) and a fake host and port (this information will not be used by Workspace), also working directory and command line can be filled with some fake chars
5. Save Application Cluster
6. Add this Application Cluster to the Connections of your Workspace Desktop Edition application.

End

ADDP

In Genesys Administrator Extension, you can define the cluster addp parameter for all applications in the cluster application from the Workspace application connections table. These parameters can be overridden in each server application.

IP Version

You can define the `ip-version` option for all applications of the cluster from the Workspace application connections table. The `ip-version` option can be overridden in each server application object. For example, you could set the value of the `ip-version` options for each application of the cluster to `4,6`.

Time interval for reconnection

Use the following two options (in Workspace application to make it global to all clusters or in Application Cluster annex, in section 'interaction-workspace') to specify the time interval for reconnection:

- `warm-standby.reconnection-random-delay-range`
- `warm-standby.retry-delay`

Provisioning cluster for Configuration Server proxies

There are two approaches to provisioning Cluster for Configuration server, Cluster based on Network Load Balancer F5 BIGIP and Cluster based on Client Side Load Balancing.

Cluster based on Network Load Balancer F5 BIGIP

This approach involves a hardware network load balancer that achieves a server-side load balancing and fault detection to equally distribute the connection load between up and running Configuration Server Proxies configured in a pool. In this approach Workspace applications physically connect to the Network Load Balancer, which is connected to all the Configuration Server Proxies of the pool.

Refer to Load-Balanced Configuration Server Proxies for Agent-Facing Applications in the Genesys

Management Framework documentation. In an F5 BIGIP environment, Workspace is configured to connect to one or several External Configuration Server Proxy applications; these External Configuration Server Proxies are not connected to an actual Configuration Server, but instead point to the hardware network load balancers.

> Important
>
> - This approach requires Config Server 8.5.1
> - The `CSProxy/proxy-cluster-name` option should be set with the name of the External CS Proxy in each of the CS Proxy application that simulate a real CS Proxy executable
> - In this approach, the selection of the node of the cluster is done by the Network Load Balancer.

Cluster based on Client-Side Load Balancing

Unlike network load balancing, the client-side random balancing approach relies on the statistical Law of Large Numbers to achieve equal distribution of Workspace instances between the Configuration Server Proxies. In this approach, Workspace instances are directly connected to the Configuration Server Proxy instance selected by the random algorithm.

Procedure

Creating a CS Proxy Cluster for Workspace

Purpose:

To enable Business Continuity for CS Proxy in Workspace.

Prerequisites

- The Configuration Server Proxies are created as individual Application objects of type ConfigurationServer Provisioning Configuration Server proxies. They do not have any backup instance, to ensure that all instances are independent from each other.

Start

1. Create a Fake Host object and set its LCA port to 0 (zero). It will not be used at runtime.
2. Configure another Application object of type `ConfigurationServer`, to create a Virtual Configuration Server Proxy that represents the Configuration Server Proxy cluster. Set its host using the fake host and assign it a fake port. `Host` and `Port` are not used at run-time. The Virtual Configuration Server Proxy object, representing the Configuration Server Proxy cluster, is not monitored by SCS.
3. In the options of the virtual Configuration Server Proxy application, create in the Section `interaction-workspace`:
    - A key-value pair for each Configuration Server Proxy that composes the cluster where:
        - Key is `cluster.nodes.<CS Proxy name>`, where <CS Proxy name> refers to a static name, used internally for reference to that node.

- Value is `host:port` that represents the Configuration Server Proxy host and port.

- The `cluster.environment-name` option with a name that represent the configuration environment name.

4. Add a connection in the Workspace application to this Virtual Configuration Server Proxy.
5. If you are using Configuration Server Proxy version 8.5 or higher, in the [csproxy] section of each Configuration Server Proxy in the proxy cluster, set the value of `proxy-cluster-name` to the name of the Virtual Configuration Server Proxy object. For more information about this option, refer to the *Framework Configuration Options Reference Manual*.

TLS

To enable TLS, if available, specify `autodetect` Configuration Server Proxy ports in the definition of the cluster nodes through options `cluster.nodes.*`.

Kerberos

To enable authentication of Workspace users through Kerberos, all Configuration Server Proxies must be configured with the same SPN and the same `.keytab` file.

> ## Important
>
> To run multiple Configuration Server Proxies configured with the same SPN on the same host, refer to Management Framework External Authentication Guide for details about how to set up redundant/clustered applications. This is not a restriction specific to the cluster model, but is applicable to any Configuration Server connection model from Workspace.

ADDP

In Workspace Application table connection, you can define the connection protocol ADDP by specifying the addp parameter for the Virtual Configuration Server Proxy application.

Time interval for reconnection

Use the following two options in Workspace Desktop Application to specify the time interval for reconnection:

- `warm-standby.reconnection-random-delay-range`
- `warm-standby.retry-delay`

`warm-standby.retry-delay` can be overriden in the Virtual Configuration Server Proxy

Provision Bootstrap Configuration Cluster Settings in Workspace Configuration File

Genesys recommends that you edit the `InteractionWorkspace.exe.config` file that you deliver to agents to provide Configuration cluster information to the client for the first time that Workspace is launched in a Configuration Server Cluster environment. This static provisioning is making the first connection of a user from a new workstation more safe. This file is in the Workspace installation directory.

Edit or add the following keys:

- For Stand-alone deployment:

  ```
  <appSettings>
    ...
    <add key="login.url" value="tcp://MyConfigurationEnvironment/ApplicationName" />
    <add key="login.cluster.nodes.MyConfigurationEnvironment"
   value="[CSP1Host:CSP1Port][CSP2Host:CSP2Port][CSP3Host:CSP3Port],Timeout=10" />
    ...
   </appSettings>
  ```

- For Business Continuity deployment:

  ```
  <appSettings>
    ...
    <add key="login.url" value="tcp://MyConfigurationEnvironment/ApplicationName" />
    <add key="login.cluster.preferred-site.nodes.MyConfigurationEnvironment"
   value="[CSP1Host:CSP1Port][CSP2Host:CSP2Port][CSP3Host:CSP3Port],Timeout=10" />
    <add key="login.cluster.peer-site.nodes.MyConfigurationEnvironment"
   value="[CSP4Host:CSP4Port][CSP5Host:CSP5Port][CSP6Host:CSP6Port],Timeout=10" />
    ...
   </appSettings>
  ```

  Where:

  - **MyConfigurationEnvironment**: The name of the Configuration Environment that is displayed in the **Login** window. For example: 'Production' or 'Staging'. This must be consistent with the `cluster.environment-name` configured in the Virtual Configuration Server Proxy application(s).
  - **ApplicationName**: The name of the Workspace Desktop application in Management framework
  - **CSP1Host:CSP1Port...**: The `host:port` pairs of your configuration server proxies defining the cluster.
  - **Timeout**: Specifies the delay, in seconds, that is applied after connections to primary and backup have been checked and failed. This parameter applies only after initial successful connection has been lost.

Summary of connection flow

A combination of three sources is used to define the connection logic to the Configuration Server Proxy nodes.

When an agent logs in to a workstation for the first time:

1. A pre-defined configuration is read from the `Interactionworkspace.exe.config` file.
2. Workspace tries to connect to one of the nodes of Configuration Server Proxy according to one of the following logic: Primary/Backup with Disaster Recovery, Cluster with Disaster Recovery, Primary/Backup without Disaster Recovery, Cluster without Disaster Recovery.
3. Once Workspace is connected, it reads the virtual Configuration Server Proxy connection(s) information.
4. Store the current configuration in the `localUserSettings.conf` file for the next login from this Workstation.

When an agent logs in to a workstation for the second and subsequent times:

1. Workspace reads the configuration information stored in the `localUserSettings.conf` file. Stored settings have a configuration environment name.
2. Workspace reads the predefined configuration stored in the `Interactionworkspace.exe.config` file, which has a configuration environment name.
3. Workspace compares the configuration environment name, if they match, then Workspace uses the stored settings from the `localUserSettings.conf` file. If they do not match, Workspace uses the `Interactionworkspace.exe.config` file as if this is a first login situation.

> ### Important
>
> - Workspace employs a Cryptographically secure pseudo-random number generator (CSPRNG) to select the next node to ensure the best load balancing between all Workspace instances.
> - In all cases, Workspace does not try to close the current Configuration Server Proxy node connection if it does not match the configuration.