Framework Deployment Guide

Configuration Server Proxy

4/13/2025

Configuration Server Proxy

Contents

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 is configured, existing clients can continue, and new clients start, their operations when Configuration Server fails. In addition, after Configuration Server recovers, the client reconnect takes far less time than if all clients were directly connected to Configuration Server.

Configuration Server Proxy is an Application of Configuration Server type operating in a special mode. As such, it seemlessly replaces Configuration Server for the clients. You can also configure Configuration Server Proxy permissions so that clients of a particular proxy access only the part of the configuration environment relevant to their site. See User Authorization or the *Genesys Security Deployment Guide* for more information about setting permissions.

How it Works

In a distributed configuration environment, the master Configuration Server is running at the site where the Configuration Database is located. Configuration Server Proxies at multiple remote sites are connecting to the master Configuration Server.

Instead of sending all the requests to Configuration Server, Configuration Server clients that require read-only access to Configuration Server can operate with one or more Configuration Server Proxies. Configuration Server Proxy passes messages to and from Configuration Server. Moreover, the proxy keeps the configuration data in its memory and responds to client data requests. 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.

Configuration Server Proxy Functions

- Receives subscription requests from clients and handles them without passing the requests to Configuration Server.
- Stores in internal memory all configuration data it receives from Configuration Server.
- Receives notifications on data changes from Configuration Server, updates internal memory, and passes notifications to clients.
- Receives read-data requests from clients and responds to them using the data stored in the internal memory.

> **Important**
>
> - Always run Configuration Server Proxy under the default account **Environment\default**.
> - A hierarchical configuration of Configuration Server Proxies—for example, a Configuration Server Proxy application working with another Configuration Server Proxy that operates directly with Configuration Server—is not supported.

Deploying Configuration Server Proxy

Important

- To ensure faultless operation, all Configuration Servers in the configuration environment must be running the same release. Configuration Server Proxy may start with a master Configuration Server running a later release, but only during the migration process. Refer to the *Framework Migration Guide* for more information.
- When deploying Configuration Server Proxy, keep in mind that redundancy type is critical. Specifically:
  - If Configuration Server Proxy is running as a single proxy server, set the redundancy type to `Not Specified`.
  - If Configuration Server Proxy is part of a HA pair and/or is configured as a primary or backup, set the redundancy type to `Warm Standby`.

Prerequisites

- The Configuration Layer components, including the master Configuration Server, are installed and running as described in Deploying Configuration Layer.
- You are logged in to Genesys Administrator.

Installation and Configuration

1. Configure as many instances of Configuration Server Proxy as needed.

Prerequisite

- You are logged in to Genesys Administrator.

Procedure

a. Go to **Provisioning > Environment > Applications**, and select **New** in the toolbar. This opens a **Browse** dialog box that lists available application templates. If a Configuration Server Proxy template file is not listed, do one of the following:
   - Import the **Configuration Server Proxy_*current-version*.apd** file from the Management Framework 8.5 product CD.
   - Create a new template using the procedure in Application Templates, and repeat this step.

b. In the **Browse** dialog box, select the Configuration Server Proxy template file.

c. In the **General** section of the **Configuration** tab:

   i. Enter a descriptive name in the **Name** text box.

ii. In the list of **Connections**, add a connection to the master Configuration Server Application object. If redundant master Configuration Servers are configured, specify a connection to the primary Configuration Server.

d. In the **Server Info** section:

i. Select the **Host** object on which this Configuration Server Proxy runs.

ii. Specify the **Listening Ports** that Configuration Server Proxy clients must use to connect to this Configuration Server.

iii. In the **Working Directory**, **Command Line**, and **Command Line Arguments** text boxes, do one of the following:

- Enter the appropriate information in each of the text boxes. For information about command-line parameters, see Starting Configuration Server Proxy.
- Type a period (`.`) in the **Working Directory** and **Command Line** text boxes, and leave the **Command Line Arguments** text box blank. The information will be filled in automatically when you install Configuration Server Proxy, but only if the Installation Package can connect to the master Configuration Server.

iv. Enter appropriate values for the other mandatory fields (those indicated by red asterisks).

v. In the **Log On As Account** field, you must use the default account, **Environment\default**.

> **Warning**
> Always run Configuration Server Proxy under the default account **Environment\default**.

e. (Optional) On the **Options** tab:

- If you want this Configuration Server Proxy to be writable, set the option **proxy-writable** in the **[csproxy]** section to `true`.
- Set the values of the log configuration options.

f. Click **Save & Close** to save the configuration.

2. Install the corresponding number of Configuration Server Proxies.

Prerequisite

- The Configuration Server Proxy Application object is created.

On UNIX

Installing Configuration Server Proxy on UNIX

a. On the Management Framework 8.5 product CD, go to **configuration_layer/configserver/**

operating_system.

b. Type `install.sh` at the command prompt, and press **Enter**.

c. For the installation type, type 3 to select Configuration Server Proxy, and press **Enter**.

d. To specify the host name for this Configuration Server Proxy, do one of the following:

- Type the name of the host, and press **Enter**.
- Press **Enter** to select the current host.

e. Enter the Master Configuration Server host name, and press **Enter**.

f. Enter the Master Configuration Server network port, and press **Enter**.

g. Enter the Master Configuration Server user name, and press **Enter**.

h. Enter the Master Configuration Server password, and press **Enter**.

i. The installation displays the list of Application objects of the specified type configured for this Host object. Type the number corresponding to the Configuration Server Proxy Application object you configured in step 1, and press **Enter**.

j. To specify the destination directory, do one of the following:

- Press **Enter** to accept the default.
- Enter the full path of the directory, and press **Enter**.

k. If the target installation directory has files in it, do one of the following:

- Type 1 to back up all the files in the directory, and press **Enter**. Specify the path to which you want the files backed up, and press **Enter**.
- Type 2 to overwrite only the files in this installation package, and press **Enter**. Then type y to confirm your selection, and press **Enter**. Use this option only if the application already installed operates properly.
- Type 3 to erase all files in this directory before continuing with the installation, and press **Enter**. Then type y to confirm your selection, and press **Enter**.

The list of file names will appear on the screen as the files are copied to the destination directory.

l. Specify the full path to, and the exact name of, the license file that Configuration Server Proxy will use, and press `Enter`.

When the installation process is finished, a message indicates that installation was successful. The process places Configuration Server Proxy in the directory that you specified during installation.

On Windows

Installing Configuration Server Proxy on Windows

> **Warning**
> Genesys does not recommend installation of its components via a Microsoft Remote Desktop connection. The installation should be performed locally.

a. On the Management Framework 8.5 product CD, **configuration_layer/configserver/windows**.

b. Locate and double-click **setup.exe** to start the Genesys Installation Wizard.

c. Use the **About** button on the wizard's **Welcome** page to review the **read_me** file. This file also contains a link to the server's Release Notes file.

d. Click **Next**.

e. On the **Configuration Server Run Mode** page, select **Configuration Server Proxy**.

f. On the **Connection Parameters to the Genesys Configuration Server** page, specify the host name, port, user name, and password for the Master Configuration Server, then click **Next**.

g. On the **Select Application** page, select the name of the Configuration Server Application object that you created in step 1, and click **Next**.

h. On the **Access to License** page, specify the license access type and the appropriate parameters, and click **Next**.

i. On the **Choose Destination Location** page, the wizard displays the destination directory specified in the **Working Directory** property of the server's Application object. If the specified path is invalid, the wizard generates a path to **c:\Program Files\GCTI*Singletenant or Multitenant* Configuration Server**. If necessary, click:

   - **Browse** to select another destination folder. In this case, the wizard will update the Application object's **Working Directory** property in the Configuration Database.
   - **Default** to reinstate the path specified in the **Working Directory** property.

   Click **Next** to proceed.

j. On the `Ready to Install` information page, click:

   - **Back** to update any installation information.
   - **Install** to proceed with the installation.

k. On the **Installation Complete** page, click **Finish**. When the installation process is finished, a message indicates that installation was successful. The process places Configuration Server Proxy in the directory that you specified during the installation process.

3. Modify each Configuration Server Proxy client to work with Configuration Server Proxy.

Prerequisites

- The Configuration Server Proxy Application object is created.

- You have identified the client applications that are to operate with this particular Configuration Server Proxy.
- You are logged in to Genesys Administrator.

> **Important**
> Repeat this procedure for each application that is to be a client of Configuration Server Proxy.

Procedure

a. Go to **Provisioning > Environment > Applications**, and double-click the client Application object that you want to connect to Configuration Server Proxy.
b. In the **General** section of the **Configuration** tab, add a Connection to the Configuration Server Proxy to which the client application should connect.
c. Click **Save & Close** to save the configuration changes. Now, when you start the client application, it will operate with the given Configuration Server Proxy.
d. Start the client application using one of the following methods:
    - From Genesys Administrator.
    - From the command line. In this case, you must use the parameters **-host** and **-port** to point to the Configuration Server Proxy with which the application will be operating.
e. Click **Save & Close** to save the changes.

4. (Optional) Configure redundant Configuration Server Proxies.

Prerequisites

- A primary Configuration Server Proxy Application object already exists.
- You are logged in to Genesys Administrator.

Procedure

a. Configure an Application object for the backup Configuration Server Proxy as described in step 1, above.
b. Install a backup Configuration Server Proxy as described in step 2, above.
c. In Genesys Administrator, go to **Provisioning > Environment > Applications** and double-click the primary Configuration Server Proxy client Application object.
d. On the **Configuration** tab, open the **Server Info** section.
e. In the **Backup Server** field, specify the Configuration Server Proxy application you want to use as the backup server.
f. Open the **Properties** dialog box of the Configuration Server Proxy application that you want to configure as a primary server.
g. In the **Redundancy Type** field, select `Warm Standby`.
h. Select `Auto-Restart`.

i. Click **Save & Close** to save the configuration changes.

Configuring a Dedicated Port for Client User Interface Applications

Warning

- Genesys strongly recommends that you do not restrict the default port to accept only client UI applications. Because the backup Configuration Server communicates with Configuration Server via the default port, and because many other Genesys Server applications cannot operate properly with being connected to the default port, restricting the default port would disable you from using these additional beneficial components.
- Ports that have been dedicated as **HA sync** (in the **Server Info** section of the port's **Configuration** tab in Genesys Administrator) cannot be provisioned to accept only client UI applications.

Dedicated ports can also be configured on Configuration Server Proxy in the same way that they are configured on the master Configuration Server. Like the master server, the proxy server must sit inside the firewall, as shown in the following illustration: thumb|center|Dedicated Port on Master Configuration Server Proxy

Use the instructions here to configure the dedicated port.

Starting Configuration Server Proxy

Important

- Always run Configuration Server Proxy under the default account **Environment\default**.
- If using a primary-backup pair of Configuration Server Proxies, follow the same starting procedure for both primary and backup applications but make sure you specify the correct application name for each.

The startup command line for Configuration Server Proxy must identify the:

- Configuration Server Proxy executable file
- Configuration Server Proxy application name (the **-app** parameter)
- Configuration Server host (the **-host** parameter)
- Configuration Server port (the **-port** parameter)
- Configuration Server Proxy license file or license server location (the **-l** parameter)

Configuration Server Proxy supports the command-line parameters common to Genesys server applications, as described in Starting and Stopping Manually.

> **Tip**
> If you want to generate logs logging during startup and initialization (referred to as *bootstrap logging*) of Configuration Server Proxy, start the server from the command line and include the **-log-<log option name> <log-type>** parameter. Optionally, you can store these logs in a file separate from the operations logs—also include the **-log-<log-type> <filename>** parameter in the startup command.

On Unix

Starting Configuration Server Proxy on UNIX

Go to the directory in which Configuration Server Proxy is installed, and do one of the following:

- To use only the required command-line parameters, type the following command line: `sh run.sh`
- To specify the command line yourself, or to use additional command-line parameters, type the following command line:
  ```
  confserv -host <Configuration Server host> -port <Configuration Server port> -app <CS proxy application objects name> [<additional parameters and arguments as required>]
  ```

On Windows

Starting Configuration Server Proxy on Windows

Do one of the following:

- Use the **Start > Programs** menu.
- To use only the required command-line parameters, go to the directory in which Configuration Server Proxy is installed, and double-click the **startServer.bat** file.
- To specify the command line yourself, or to use additional command-line parameters, open the MS-DOS

window, go to the directory in which Configuration Server Proxy is installed, and type the following command line:

```
confserv.exe -host <Configuration Server host> -port <Configuration Server port> -app
<CS proxy application objects name> [<additional parameters and arguments as
required>]
```

Writable Configuration Server Proxies

By default, Configuration Server Proxy provides read-only access to configuration data. Configuration Server clients that require write access to Configuration Server must still connect directly to Configuration Server. Some of Genesys Supervisor- and Agent-facing applications (such as Workspace Desktop Edition), while deployed in high numbers, require write access to configuration data and should be deployed against Configuration Server Proxy in Writable mode.

Administrative applications, such as Genesys Administrator, should still connect to the Master Configuration Server to perform complex configuration updates, because Configuration Server Proxy in writable mode is not designed to handle all types of configuration updates. Updates made in bulk might result in a significant extra load on the system when done by the Proxy server rather than the Master server.

To configure a Configuration Server Proxy as writable, use the Configuration Server Proxy configuration option **proxy-writable**. For more information about this option, refer to the *Framework Configuration Options Reference Manual*.

Redundant Configuration Server Proxies

The high-availability (HA) architecture implies the existence of redundant applications, a primary and a backup, monitored by a management application.

Like Configuration Server, Configuration Server Proxy supports the Warm Standby redundancy type between redundant Configuration Server Proxies. For more information, refer to Redundant Configuration Servers.

HA Configuration Server Proxy supports ADDP between the pair of proxy servers if ADDP has been enabled between the master Configuration Server and Configuration Server Proxy in the Connections tab of the proxy server. The primary and backup Configuration Server Proxies also use these ADDP settings to communicate with each other.

Prior to release 8.1.3, when a switchover occurred between the primary and backup Configuration Server Proxies, Configuration Server Proxy clients had to read configuration information anew and reestablish the connections to the backup server themselves. Especially in large configuration environments, this often led to detrimental effects on system performance, leading clients to question the usefulness of the backup proxy server.

Starting in release 8.1.3, client connections are restored automatically to the backup Configuration Server Proxy when it switches to primary mode, if the connection between the client and primary Configuration Server Proxy is lost, because the primary proxy server is stopped. This makes the switchover practically invisible to clients, and essentially eliminates the performance impact on the

system. This restoration is made possible by the backup Configuration Server Proxy keeping its own record of client connections and disconnections. Under normal conditions, the primary proxy server notifies the backup proxy of client connections and disconnections, which the backup stores in its History Log Database. When the backup switches to primary mode, it is able to restore client connections based on the connection and disconnection information it has stored.

If the connection between the primary and backup servers is lost, prior to switchover, the session is not restored. Clients of the Configuration Server Proxy must reregister and read all data from scratch.

> **Important**
>
> You cannot separate two Configuration Server Proxies configured as an HA pair into two standalone servers at runtime. You must stop, re-configure, and then restart each server.

Limiting the Number of Proxy Servers Loading and Reloading Data

This feature limits the number of Configuration Server Proxies that can load or reload data from the master Configuration Server and also provides an option to delay the actual moment when each Configuration Server Proxy attempts to reload its cached data after master Configuration Server becomes available following a prolonged disconnect or downtime.

This feature can be implemented on both master Configuration Server and each of Configuration Server proxies, with both implementations complementing each other. On Configuration Server Proxy side, it can delay sending first read request to the master Configuration Server after the connection has been re-established and it has been confirmed that full reload is required to get the system in-sync. This delay can future be tailored for primary and backup instances of each Configuration Server proxy HA pair. On Configuration Server master side, it can delay responses to a Configuration Server Proxy requests attempting full data re-reads, based on current load the server and number of proxies already performing re-read. This feature will not affect default behavior of master and proxy servers during short connection loss, as session restoration does not involve client disconnects and data reload; it only works in the case when synchronization require re-reading of entire configuration data by some or all proxy servers.

Implementation

To specify the maximum number of Configuration Server Proxies allowed to concurrently load or reload data from the master Configuration Server, use the following options in the **system** section of the master Configuration Server Application object:

1. Ensure that transaction serialization is enabled (serialize-write-transactions is set to `true`). If transaction serialization is not enabled, you cannot use this feature.
2. Set proxy-load-max to the maximum number of proxy servers allowed. If this option is not configured or is set to `false`, there is no limit.

3. Set the delay reload period for Configuration Server Proxies using the delay-reload and delay-reload-backup options. If these options are set to `0` (the default), the delay reload feature is disabled.

Using Configuration Server Proxy with External Authentication Systems

In distributed systems prior to release 8.0, external authentication was configured only on the Master Configuration Server, and each Configuration Server Proxy passed authentication requests to it. Now, RADIUS and LDAP external authentication, starting in release 8.0 and 8.1 respectively, can be configured on the Master Configuration Server and on each Configuration Server Proxy. Therefore, each Configuration Server Proxy can process authentication requests itself, and does not need to pass them on to the Master Configuration Server. For more information about setting up external authentication on Configuration Server Proxy, refer to the *Framework External Authentication Reference Manual*.

Load-Balanced Configuration Server Proxies for Agent-Facing Applications

Starting in release 8.5.1, you can integrate load balancing into a system of Configuration Server Proxies. This enables a group of Configuration Server Proxies to share the processing load (client connections).

The benefits of load-balancing are two-fold:

- Deploying a pool of Configuration Server Proxies enables you to easily manage environments in which the capacity of a single proxy server is not enough to handle all agent-facing clients (such as with the Workspace Desktop Edition).

> **Important**
>
> Refer to the Hardware Sizing Guide to determine the capacity of maximum incoming connections for a single Configuration Server Proxy.

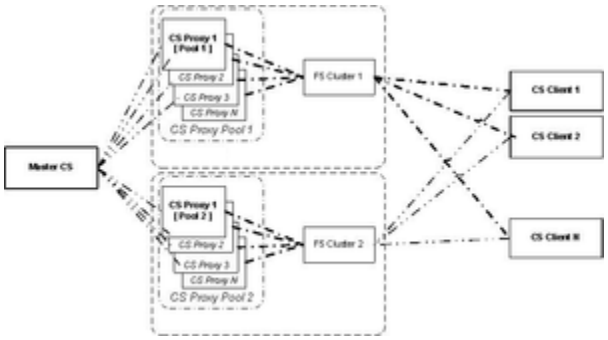
- If any Configuration Server Proxy is not operational, new client connections are not distributed to that proxy server automatically.

High Level Architecture

This solution requires the use of a third-party load balancer (F5). A set of standalone Configuration Proxy Instances are deployed on several hosts, subject to limitations noted in the Hardware Sizing Guide. The resources of each host (memory and number of CPUs) must be sufficient to allow the launching of, and running under load, all instances of Configuration Server Proxy assigned to it. The

master Configuration Server maintains a connection to each Configuration Server Proxy. An F5-based hardware load balancer is connected to all of the proxy servers in the group, and provides a single virtual IP address and port to which the clients of those proxies connect.

This can be extended to multiple groups of Configuration Server Proxies, each group served by a different load balancer. This is shown in the following diagram.



Load-Balanced Configuration Server Proxies

Support of Agent-Facing user Interface Applications

The following Genesys application supports working with a pool of Configuration Server Proxies behind a hardware load balancer: Workspace Desktop Edition (formerly called Interaction Workspace).

Limitations

This solution also has these limitations:

- Session restoration on the Connection Server Proxy side is not supported in this type of deployment.
- The built-in Kerberos protection against ticket sniffing by caching used tickets is turned off. Clients are connecting to a pool of servers, and each proxy server has a separate ticket cache.

Warning

Support for this solution has been tested by Genesys on a limited number of applications. Connecting unsupported applications to Configuration Server Proxy using a hardware load balancer may result in performance issues and feature degradation. Refer to the documentation for a particular application to confirm that it supports the Configuration Server Proxy load-balancing architecture.

Configuration

To set up the load-balanced solution, do the following:

1. Install and configure F5 with VIP, and use the round-robin methodology to distribute connections to clients.

2. Install and configure the Configuration Server Proxies as individual **Application** objects of type ConfigurationServer. Do not specify any backup instance, to ensure that all instances are independent from each other.
3. Create a Host object for the machine associated with the External Configuration Server Proxy, and set its LCA port to `0` (zero).
4. Configure another Application object of type ConfigurationServer, to create an External Configuration Server Proxy that represents the F5 load balancer. Set its host and port to the values for F5.
5. Provision all client applications with a connection to the External Configuration Server Proxy. If required, configure ADDP on those connections.
6. In the **[csproxy]** section of each Configuration Server Proxy in the proxy pool, set **proxy-cluster-name** to the name of the External Configuration Server Proxy object. For more information about this option, refer to the *Framework Configuration Options Reference Manual*.
7. If you are planning to use Kerberos authentication, do the following:
   - Configure all Configuration Server Proxies in the pool to use the same SPN and the same .keytab file.
   - Set the **KRB5RCACHETYPE** environment variable to `none`.
8. Set each of the proxy servers in the pool to autorestart, to enable Solution Control Server (SCS) to detect application failure and/or host unavailability. Configure any other monitoring features, such as hangup detection, as required. The External Configuration Server Proxy object, representing the F5 load balancer, is not monitored by SCS.

TLS Configuration

To configure TLS between agent-facing Applications and Configuration Server Proxy clusters using the F5 load balancer, do the following:

1. Obtain Certification Authority (CA) security certificates for each Configuration Server Proxy host and agent-facing client host. Store the certificates in the **Trusted Root Certification Authorities Certificates** folder. Refer to the Microsoft article Installing a Root Certificate.
2. Request and obtain security certificates for Server authentication. Make sure that the name in the **Subject** field of the certificates matches the Fully Qualified Domain Name (FQDN) of the F5 host name registered in DNS. The certificate must also have a private key that corresponds to that certificate. Host names are case-sensitive and must match DNS and Active Directory records. Refer to the Microsoft article Obtain a Certificate and to the *Genesys Security Deployment Guide*.
3. To enable key archival and recovery, set the following in the certificate template and on the CA:
   - The specific certificate template must be configured to allow key archival.
   - At least one key recovery agent must be identified on the CA, and a key recovery agent certificate must be issued to that agent.
   - Key archival must be configured on the CA.
4. Import the F5 host certificate to each host running Configuration Proxy Servers, storing the certificate in the Personal Certificates folder of the Computer account. Refer to the Microsoft article Import a Certificate.
5. On each Configuration Server Proxy, set the Listening Mode of the ports used for TLS communications to **Auto-detect** or **Secure** and attach the F5 host certificate. Refer to the *Genesys Security Deployment Guide*.

F5 Configuration

To ensure that replies from servers always traverse the load balancer on the way back to the client, SNAT (Secure Network Address Translation) is used. One of the most popular SNAT modes is the automap feature that allows mapping of all original client IP addresses to the self address of the F5 unit. The SNAT pool allows mapping of all the original client IP addresses to the IP addresses of the SNAT pool.

SNAT with a single IP address has a limit of 65535 ports. The SNAT connections might fail if a large number of client requests are traversing the SNAT. To mitigate port collisions, create SNAT pools or use SNAT automap with an appropriate number of self IP addresses on the Virtual LAN to support the expected level of concurrent connections using SNAT.

The following sample configuration is for a deployment where two IP addresses are used for the pool. In the sample, the following placeholders are used:

	<vsCSP IP>	Virtual Server of Configuration Server Proxies
	<node1 IP address>	Host 1 IP address
	<node2 IP address>	Host 2 IP address
	<F5 IP address>	F5 box IP address
	<default GW IP>	Default GateWay IP address

```
vlan vlanPerfExternal {
   tag 4094
   interfaces 1.2
}
self <F5 IP address> {
   netmask 255.255.255.0
   vlan vlanPerfExternal
   allow default
}
route default inet {
   gateway <default GW IP>
}
monitor TCP-9070 {
   defaults from tcp
   dest *:9070
}
monitor TCP-9075 {
   defaults from tcp
   dest *:9075
}
profile tcp tcp-idle600 {
   defaults from tcp
   idle timeout 600
}
node <node1 IP address> {
   monitor icmp
   screen MFfirstNode
}
node <node2 IP address> {
   monitor icmp
   screen MFsecondNode
}
pool poolCSP01 {
   monitor all TCP-9070 and TCP-9075
```

```
   members
      <node1 IP address>:9070
         monitor TCP-9070
      <node1 IP address>:9075
         monitor TCP-9075
      <node2 IP address>:9070
         monitor TCP-9070
      <node2 IP address>:9075
         monitor TCP-9075
}
virtual vsCSP {
   snat automap
   pool poolCSP01
   destination <vsCSP IP>:9070
   ip protocol tcp
   profiles tcp-idle600 {}
}
```

Business Continuity

Genesys Workspace Desktop Edition integrates load-balanced Configuration Server Proxies into a Business Continuity solution, by keeping a pool of proxy servers at each Site (active and stand-by) of the configuration. In this case, a separate application and host object that represent the F5 load-balancer at each site must be created. Refer to Genesys Workspace Desktop Edition documentation for more information about how to set up Business Continuity for Agent Desktop when using Configuration Server Proxy objects from preferred and backup sites.

Support for Multi-Language Environments

You do not need to perform any additional configuration to have Configuration Server Proxy support multi-language environments. If the master Configuration Server supports UTF-8 encoded data, all Configuration Server Proxies connected to that master Configuration Server also support UTF-8 encoding. See Multi-language Environments for more information about using UTF-8 encoding to enable multi-language environments.

Configuration Server Proxy and Configuration History Log

You can configure a history log with Configuration Server Proxy to store historical information about client sessions and changes to configuration objects. Refer to Configuration History Log for more information.

Failure of Configuration Server Proxy

When Configuration Server Proxy fails or disconnects from its clients, the clients attempt to reconnect to Configuration Server Proxy. If it is not available and if a backup Configuration Server Proxy is configured, the clients attempt to connect to the backup.

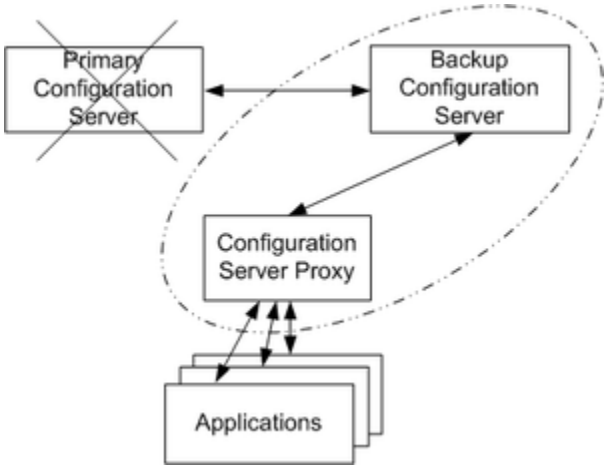
When Configuration Server Proxy fails, you must restart it manually or use the Management Layer for autorestart.

Failure of Master Configuration Server

When the master Configuration Server fails or the connection to it is lost, the clients of Configuration Server Proxy continue their normal operations. Configuration Server Proxy initiates reconnection attempts to the master Configuration Server. Meanwhile, Configuration Server Proxy responds to client requests using the configuration data stored in its memory.

When the master Configuration Server fails, you must restart it manually or use the Management Layer for autorestart.

The following diagram shows Configuration Server Proxy behavior when a primary-backup pair of master Configuration Servers is configured.



Distributed Installation

When the primary master Configuration Server fails or the connection to it is lost, Configuration Server Proxy tries to reconnect to the master Configuration Server and, if it is not available, to the backup Configuration Server. If the connection to the backup Configuration Server is established, Configuration Server Proxy remains connected to the backup server until:

- The connection to the backup Configuration Server is lost.
- The backup Configuration Server fails.
- Configuration Server Proxy fails or is restarted.

Configuration Server Proxy operation from persistent read-only database

Configuration Server Proxy remains operational during prolonged disconnect from master

Configuration Server. This comprises ability to restart Configuration Server Proxy using locally cached data. And, upon master Configuration Server's availability, Configuration Server Proxy can be restarted to re-read and restore full synchronization.

If the master Configuration Server is down/inaccessible during Configuration Server Proxy startup, then it CS Proxy makes a connection with DBMS and directly loads data from DB in persistent mode. Also, Configuration Server Proxy indicates in the log that it started in persistent mode. To enable this feature, Configuration Server Proxy (CSProxy) should be started with the command-line option **-proxy-persistent-mode**. The related options are:

- db-persistent-failover-tmout
- -cs-persistent-failover-tmout

To support this feature in Configuration Server Proxy’s host, DBMS client must be installed. Also, you must provide the **confserv.cfg/conf** file under Configuration Server Proxy working directory, as with master Configuration Server.

> ### Important
> Any instance of Configuration Server proxy that activated persistent mode will start as primary proxy and allow client connections, will ignore SCS requests except for stop and will periodically log out message indicating persistent mode is activated. Because proxy in this mode won't have connection to master Configuration Server, it cannot get aware of master Configuration Server going back online and require restart to re-syncornize data after master server is fully recovered.