GENESYS

Configurations Options Reference Manual

[general] Section

4/24/2025

Contents

[general] Section

This section contains information about the SCS operational mode and relevant settings.

This section must be called **general**.

alive_timeout

Default Value: 30
Valid Values: Any value from 15–300
Changes Take Effect: After restart

When SCS operates in Distributed mode (**distributed_mode** is set to on), specifies the time interval, in seconds, that this SCS waits for a response from other instances of SCS. When using a Message Server to allow the Solution Control Servers in the Distributed SCS network to communicate with each other, this option must be considered when setting the Advanced Disconnect Detection Protocol (ADDP) timeout values.

Refer to the Distributed Solution Control Servers section in the *Framework Deployment Guide* for details about Distributed Solution Control Servers.

app-switchover-timeout

Default Value: 60
Valid Values: 0 or any positive integer
Changes Take Effect: Immediately

Specifies the time interval, in seconds, that Solution Control Server waits for the switchover of an HA application to complete. When the timeout expires, Solution Control Server logs that the switchover operation has failed and allows the next switchover operation. When set to 0, the timer is disabled and Solution Control Server does not allow the subsequent switchover of an HA application in case of a switchover failure.

cfglib-connect-tmout

Default Value: 20
Valid Values: Any integer from 0 to 65536 seconds
Changes Take Effect: After restart

Sets a timeout (in seconds) for SCS to expect a TCP success or failure response from the Configuration Server to which it is connecting. If the connection has not been made when the timeout expires, all pending connection requests are canceled.

When set to 0 (zero), this timeout is disabled.

The value of this parameter overrides that of the **-cfglib-connect-tmout** command-line parameter.

default-audit-username

Default Value: GAX_backend

Valid Values: Name of any configured Application
Changes Take Effect: After restart

Specifies the default login username for GAX in SCS audit logs when connecting to an Application of type CFGSCI with a username of NULL. This option is required in this case because there is no provided username when connecting to SCS.

detailed-alarm-log

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After restart

This parameter enables or disables the generation of detailed alarm log statements as both SCS log file and user-defined SCS alarm log file.

- If set to `true`, logs the alarm events in a detailed format in log files.
- If set to `false`, logs the alarm events in the existing format in log files.

By default, detailed alarm log statements are generated in both the SCS log file and the user-defined alarm log file when the parameter **detailed-alarm-log** is not set.

disable-switchover

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: Immediately

Specifies if all switchover activity is to be disabled. Set this option to `true` to avoid false switchovers during dynamic migration. When dynamic migration is complete, set this option to `false` (the default) to restore normal behavior, enabling all switchover activity.

disconnect-switchover-timeout

Default Value: `0`
Valid Values: `0` or any positive integer
Changes Take Effect: Immediately

Specifies the time interval, in seconds, that SCS waits for an LCA connection to be restored before switching operations over to the backup server of an application installed on the host running LCA. When the timeout expires, SCS determines whether the switchover condition still exists:

- If the LCA remains disconnected (because, for example, the LCA host is down) and the status of the application installed on the LCA host remains `Unknown`, SCS switches the backup server configured for the application to `Primary` mode.
- If the LCA connection is restored (because, for example, a temporary network problem no longer exists) and the status of the application installed on the LCA host becomes `Started`, SCS does not perform a switchover to the application's backup server.

Use this option when the network linking SCS and a monitored host is slow (such as a WAN).

distributed_mode

Default Value: `off`
Valid Values: `on, off`
Changes Take Effect: After restart

Specifies whether SCS operates in Distributed mode, to support a distributed management environment. When set to on, SCS verifies the existence of the appropriate license at startup and, if the license is found and valid, starts operating in Distributed mode.

distributed_rights

Default Value: `default`
Valid Values:

default	SCS controls the objects associated with it in the Configuration Database.
main	SCS controls all objects that are not associated with any SCS in the Configuration Database.

Changes Take Effect: After restart

When SCS operates in Distributed mode (**distributed_mode** is set to on), specifies what objects SCS controls. Use this option when you run SCS in a distributed management environment and you want to grant this SCS instance control permissions over all configuration objects (such as, Hosts, Applications, and Solutions) that you have not configured other SCS instances to control.

distributed_sync_timeout

Default Value: `0`
Valid Values: `0` or any positive integer
Changes Take Effect: Immediately

Specifies a time interval, in seconds, after which a distributed Solution Control Server sends to other Solution Control Servers a request for the status of objects controlled by them, while also sending the statuses of objects that it controls. This enables all Solution Control Servers in the configuration to synchronize object statuses and report them accordingly. If this option is set to zero (`0`, the default) or is not defined, synchronization attempts are not sent in a timely manner.

Set this option in each Solution Control Server.

> ## Important
>
> - Genesys recommends that, if you want to enable this synchronization, you set this option to a value of no less than 60 seconds to reduce network traffic.
>
> - With this option enabled, Solution Control Server processes a higher number of messages, and may disconnect from Local Control Agent if the Advanced Disconnect Detection Protocol (ADDP) timeout is too small. Before using this option, ensure that the

> ADDP timeout between Solution Control Server and Local Control Agent is large enough.

enable-nonserver-app

Default Value: `false`
Valid Values: `true, false`
Changes Take Effect: After restart

Specifies whether SCS detects the non-server application(s) and sends change request as **configured** through the **change application option** alarm reaction.

- If set to `true`, SCS sends a change request through the **change application option** alarm reaction for the non-server application's option.

- If set to `false` (default), SCS does not request any option change for the non-server application(s).

haflip-detect-timeout

Default Value: 10
Valid Values: `-1`,10–2147483647
Changes Take Effect: Immediately

Specifies the time interval, in seconds, for which Solution Control Server detects the flipping of the monitoring applications from Primary–Backup–Primary or Backup–Primary–Backup mode and prints the standard 10327 log message.

When set to `-1`, this timeout is disabled.

ha_service_unavail_primary

Default Value: `true`
Valid Values: `false, true, on off, yes, no`
Changes Take Effect: Immediately

Specifies if an application in the HA pair is promoted to the primary mode when it is in a Service Unavailable state. If set to `true` (the default), the application is promoted to primary. If set to `false`, the application is not promoted. This setting prevents a race condition of HA scripts, which occurs when both SIP Servers are started almost at the same time and go into the primary mode for a brief period of time.

hostinfo-load-timeout

Default Value: 10
Valid Values: 10–120
Changes Take Effect: After restart

Specifies the time interval (in seconds) for which Solution Control Server waits to upload host information from any host it controls and with which the Local Control Agent on that host has a

secure connection with Solution Control Server. If the timer expires before the host information is uploaded, Solution Control Server disconnects from the Local Control Agent on that host's machine.

lookup_clienthost

Default Value: `false`
Valid Values: `true, false, on, off, yes, no`
Changes Take Effect: After restart

Specifies whether to look up the host name of the connected client. If set to `false` (default), SCS does not look up the host name and uses the IP address of the connected client in audit logs. If set to `true`, SCS looks up the host name and uses that in audit logs.

max-req-per-loop

Default Value: 20
Valid Values:0–32767
Changes Take Effect: After restart

Specifies the maximum number of requests that SCS will process without pausing to scan its connection with LCA and respond appropriately, therefore preventing the connection from closing because of ADDP timing out. When it is set to 0 (zero, disabled), the SCS processes all LCA requests in the queue without pausing. Set this to a non-zero value if SCS manages a large set of hosts and applications, and ADDP is used between SCS and LCA.

> ### Important
> Use this option only when requested by Genesys Customer Care.

service-unavailable-timeout

Default Value: 0
Valid Values: Any value from 0–5
Changes Take Effect: Immediately

Specifies the amount of time, in seconds, that SCS waits before applying the criteria for switchover if the primary and backup T-Servers report `Service Unavailable` simultaneously.