SIP Server HA Deployment Guide

Other HA Enhancements

4/14/2025

Other HA Enhancements

SIP Server supports several additional capabilities related to high-availability deployments.

Single Host HA Deployment

Starting with version 8.0, SIP Server supports deploying both primary and backup SIP Server applications, as well as the Stream Manager or Media Server application, on the same physical host. Benefits of using the single host HA configuration include the following:

- Efficient use of the hardware equipment.
- Less complex configuration: Virtual IP address control scripts, Alarm Reactions, and Alarm Conditions are not required.

However, this type of HA configuration is supported only for small-size deployments—100 seats or less.

Synchronization of Contact Between SIP Server HA Pair

SIP Server 8.x synchronizes the SIP registration `Contact` header for a particular device across both primary and backup instances of SIP Server. The primary SIP Server sends the contact information to the backup SIP Server using the HA link, as well as through the Configuration Server.

SIP Traffic Monitoring

SIP Server 8.x supports SIP traffic monitoring for enhanced reliability. When configured, SIP Server monitors incoming SIP traffic and can initiate a switchover after a configurable length of time during which no SIP messages are received.

In deployments where two NICs are used, one NIC is dedicated to SIP communication, while the second NIC is used for other kinds of communication with various components. Solution Control Server (SCS) manages and monitors the SIP Server application through the second NIC.

The SIP traffic monitoring feature allows the primary SIP Server to monitor the network connectivity through the NIC that is responsible for SIP communication, to recognize connectivity issues that impact the SIP service, and to initiate reactions that result in recovery of the service.

An Application-level configuration option, **sip-pass-check**, must be configured to enable this functionality. In addition, at least one service device must be configured for Active Out-Of-Service Detection by using **oos-check** and **oos-force** configuration options. See the *Framework 8.1 SIP Server Deployment Guide* for information about the Active Out-Of-Service Detection feature description.

When it is set to `true`, the **sip-pass-check** option enables tracking of SIP messages that reach the primary SIP Server, including responses from SIP devices (DNs) that are monitored by SIP Server by using the **oos-check** and **oos-force** options.

The primary SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS when all devices configured with the Active OOS check have failed and no other SIP messages have been received for a period of time. The period of time is calculated as the maximum of the sums of the **oos-check** and **oos-force** option values configured for service DNs (if **oos-force** is less than 5, 5 is used). When SIP Server reports the SERVICE_UNAVAILABLE status to LCA/SCS, SCS switches the primary SIP Server to the backup role, and SIP Server reports the SERVICE_RUNNING status to LCA/SCS. The backup SIP Server becomes the primary, and starts monitoring SIP traffic.

If both the primary and backup servers receive no SIP traffic, a switchover would occur each time that the effective out-of-service timeout expires. To prevent frequent switchovers in this case, SIP Server detects the "double switchover" condition and doubles the effective out-of-service timeout each time that the double switchover happens"up to four times greater than the initially calculated timeout, or until one of the two servers detects SIP traffic. As soon as SIP traffic is detected, the server that detected the traffic remains the primary SIP Server and continues normal operation.

Monitoring Critical Conditions

You can use Genesys Administrator to check the current running status of SIP Server. Starting in release 8.1.0, SIP Server displays its state as `Running` in Genesys Administrator in cases where it is unable to open a listening port, and it is configured as one instance in a High Availability (HA) pair. Prior to release 8.1.0, (release 8.0.4 and earlier), in this same scenario SIP Server displayed its status as `UNAVAILABLE`.

To monitor problems with binding a listener (SIP Server is running but unable to open a listening port), Genesys recommends that, for each SIP Server instance, you configure an Alarm Condition for the log event `00-04200`. For more information, consult the Solution Control Interface (SCI) help topic, "Using Log Events for Alarm Detection".

To ensure that administrators do not miss the alarm, Genesys recommends that you configure automatic clearing of the activated alarm in accordance with business processes and the schedule of the customer administrator.

The recommended configuration of an Alarm Condition for `00-04200` enables monitoring of a wide range of events that are critical for both SIP Server functionality and for service availability. This includes problems that might occur when binding a listener, unexpected terminations, or unauthorized terminations of the SIP Server process.

In Genesys Administrator, alarms that are detected and activated can be observed through a

dedicated view, providing a central location for observing all alarms that occurred in the entire environment.

If required, an alarm reaction can be configured to notify administrators automatically when a critical condition occurs.

After the administrator investigates and resolves the problem, they must manually clear the alarm condition.

If the problem occurred due to a temporary outage (for example, a network switch reboot), SIP Server remains in the `Running` state, ensuring availability of the HA pair once the network switch is recovered; in release 8.0.4, SIP Serer required a manual restart to return to the Running state.

In release 8.0.4, if both SIP Server instances encountered a problem when binding a listener, both instances in the HA pair remained in `UNAVAILABLE` status, requiring a manual operation to resume the service. In release 8.1.0, SIP Server instead switches the primary role between the two HA instances and resumes the service as soon as one of the instances is able to open a listening port.

Network Status Monitoring

SCS connection monitoring

To enable monitoring of the SCS connection status, set the value of the SIP Server Application option **control-vip-scripts** to `true`. If the connection to SCS is not available and both SIP Servers in the HA pair are running as primary, one of them will enforce switching its role to the backup.

Virtual IP address monitoring

To enable Virtual IP address monitoring for the IP Address Takeover configuration, set the value of the SIP Server Application option **sip-iptakeover-monitoring** to `true`. The primary SIP Server monitors the presence of the Virtual IP address on its host. The backup SIP Server monitors the absence of the Virtual IP address on its host. The corresponding Virtual IP script is executed if misconfiguration is detected. If the problem persists, SIP Server reports the `Service Unavailable` status. The Standard-level log event 00-52029 or 00-52030 is generated when the failure or success, respectively, of a Virtual IP address is detected.

NIC status monitoring

To enable NIC status monitoring, set the value of the SIP Server Application option **tlib-nic-monitoring** to `true`. Both primary and backup SIP Servers monitor the status of the NIC associated with their Application objects in the configuration environment. This allows SIP Server to enforce switching to backup in case of NIC failure.

SIP NIC status monitoring

To enable SIP NIC status monitoring in scenarios where a dedicated NIC is used for SIP communication (the two-NIC configuration), set the value of the SIP Server Application option **sip-nic-monitoring** to `true`. The IP address of the SIP NIC must be configured using the **sip-nic-address** option. SIP Server reports the `Service Unavailable` status if failure is detected. The Standard-level log event 00-52027

or 00-52028 is generated when the failure or success, respectively, of a SIP NIC is detected.