citrix

TROUBLESHOOTING CITRIX ADC GSLB MEP & SYNC

OVERVIEW / PROTOCOLS & PORTS

- GSLB Metric Exchange Protocol (MEP) is a Citrix proprietary protocol used by Citrix ADC to exchange site and network metrics, persistence data, and other information to other sites participating in GSLB
- Communication process is accomplished between each GSLB site on TCP port 3011 (or 3009 for secure communication).
- MEP communication is initiated from the lower site IP address to the higher site address for site metrics exchange and higher to lower for network metrics.

Common GSLB MEP & SYNC Ports (open bi-directional)

TCP 3008	GSLB secure configuration sync
TCP 3009	Secure MEP communication process
TCP 3010	GSLB non-secure configuration sync
TCP 3011	MEP non-secure communication process

TROUBLESHOOTING CHECKLIST

MEP (most MEP issues are caused by networking-related or RPC config issues)

- Ensure TCP ports 3009 and/or 3011 are open bi-directional from MEP communication IPs (this IP could be MIP/SNIP and/or GSLB Site IP)
- Check GSLB rcpNode passwords, ensure they are same across GSLB sites
- Try to reset rpcNode passwords for all GSLB Site IPs
- Rule out “secure” being the issue of MEP. Disable secure option to force MEP to use TCP port 3011. Remember this port needs to be open.
- Check if monitors bound to GSLB service (monitors override MEP status)
- Reset MEP on all sites (disable MEP then re-enable MEP)
- Run shell command #nstcpdump.sh –an port <MEPport#> on both sites simultaneously to check the traffic. Or, take nstraces on both ADCs.

GSLB Sync

- Management Access and SSH needs to be enabled on all GSLB Site IP Addresses
- For GSLB Autosync, there needs to be symmetric configuration across all sites
- Ensure all RPC passwords are the same (Remember: All RPC node configuration is site specific and need to be re-applied if force sync is done).
- Use the following logs to help troubleshoot: /var/netscaler/gslb/logname.err and /var/log/ns.log.*
- If GSLB site is behind NAT, RPC port 3010 (non-secure) or 3008 (secure) needs to be opens.

GSLB MEP HEALTH-STATUS HANDLING

MEP ENABLED	If MEP is enabled, the GSLB MEP health-status is based on the MEP state (up or down)
MEP DISABLED	All services belonging to that site are marked down.
MONITORING (EXPLICIT MONITORS)	Health status is controlled by monitoring and not by the GSLB MEP state

HELPFUL GSLB COUNTERS

Common Command Usage: *# nsconmsg –K /var/nslog/newnslog -d stats –g <counterName>*
# nsconmsg –K /var/nslog/newnslog - s disptime=1 -d current –g <counterName> | more

_mep_state	MEP status counter (value 0 = down | value 1 = up)
sitemetric_mep_state	Indicates the status of the *site Metric Exchange connection* at the GSLB site.
nwmetric_mep_state	Indicates the status of the *network Metric Exchange connection* at the GSLB site.
gslb_err_sitemetric_mep_update_failed	Three great counters to indicate if MEP failed and/or timeout— they are similar to the counters above. The counters above will indicate the state of MEP. These counters will help troubleshoot GSLB errors and MEP failing. You can also use the ambiguous string to capture all GSLB error counters, -g gslb_err
gslb_err_nwmetric_mep_update_failed	
gslb_err_sitemetric_mep_timedout	
lb_cur_gslb_rpc	Check this counter if there are any RPC password related issues
gslb_tot_gslb_msg_sent	Whether MEP is being sent or received; if it’s being sent on one end, but counter, gslb_tot_gslb_msgs_rcvd, is not incrementing on the other, take a trace and follow the traffic on ports 3009 or 3011—depending on whether secure is enabled or disabled.
gslb_tot_gslb_msg_rcvd	

IMPORTANT INFORMATION / USE CASES

How do I know which IP Address is sourcing my MEP traffic?

- The appliance needs a NetScaler-owned IP address to use as the source IP address when communicating with other GSLB sites. By default, the RPC nodes use either a subnet IP (SNIP) address or a mapped IP (MIP) address, but you might want to specify an IP address of your choice.
- set rpcNode 192.0.2.4 -password mypassword
- set rpcNode 192.0.2.4 -srcIP 192.0.2.3

Failing MEP Scenario:

- First check to see if there are any monitors bound to GSLB services. If there are monitors bound, then troubleshoot why they are down, or you can unbind the monitors and set up GSLB MEP communication properly.
- Check to see if the rpcNode secure option is set to YES. If it is, disable secure option to NO, disable MEP, re-enable MEP.
  - Disable secure option from rpcNode, for all the GSLB site IPs—command below:
    - CLI Command: > set rpcNode <GSLB Site IP> -secure No (repeat this command on all the site nodes and for the Site IPs)
    - Then, disable and re-enable MEP
- If MEP is secured, check the following:
  - Does it work with default SSL ciphers?
  - Double check if there are any custom ciphers or a custom SSL profile and revert to default, if needed.
  - Check specific SSL protocols such TLS 1.1 vs. 1.2 vs. 1.3?
  - Take a NetScaler trace, or run the shell command, nstcpdump for live debugging: #nstcpdump.sh –an port 3011

Failing GSLB Sync due to password differences:

- Log entries in /var/log/ns.log:

```
ns.log.3:180:May 5 13:30:09 <local0.info> citrix_adc_name nsgslbautosync: sync started
May 9 17:42:59 <local0.info> citrix_adc_name nsgslbautosync: Error executing command on gslb site...Reason: ERROR: Invalid user-name or password
May 9 17:43:00 <local0.info> citrix_adc_name nsgslbautosync: unable to establish master SSH connection: master process exited unexpectedly
May 9 17:43:00 <local0.info> citrix_adc_name nsgslbautosync: Aborting ...
```

GSLB Sync Fails With Following Error:

- Error executing command on gslb site...ERROR: Connection failed Trying to connect using SSH... unable to establish master SSH connection: login timeout
- Fix:
  1. Enabled the management access on GSLBSITEIP
  2. Configured the firewall to accept autosync connections by specifying the remote site IP (clip for cluster setup) and port (3010 for RPC and 3008 for secure RPC).