Article title: Troubleshooting Gateway application failures, performance concerns, and service outages

Article Id: 42511 **Status:** Published **Created Time:** 12-02-2018 16:25 **Updated Time:** 14-02-2018 07:39

Products
STARTER PACK-7 , CA Rapid App Security

Issue/Introduction:

Solution

Background

Under certain circumstances, the Gateway may fail to process message traffic. This may result in a loss or degradation of availability as one or more nodes in a cluster are unable to process adequate amounts of traffic.

Presentation

This behavior may present in one of the following ways:

1. A protected service is no longer receiving traffic from the Gateway.
2. One or more nodes are reported as *offline* or unknown via the Enterprise Service Manager.
3. One or more nodes are reported as *down* via the Layer 7 Policy Manager Dashboard.
4. The Gateway (SSG) service is not running.
5. The Gateway log files are not generating new log entries.

Troubleshooting

There are several pieces of information that should be obtained before the Gateway appliance or the Gateway service is restarted. Restarting the application or service may result in critical diagnostic data being lost. If a restart or reboot is performed then diagnostics may need to wait for the next occurrence of the issue. Please note that these commands can be run against live production environments without causing further downtime or availability concerns.

System statistics

The following are all commands that should be run from the privileged shell of the API Gateway. For more information on accessing the privileged shell of the API Gateway, please refer to the product documentation page titled "Privileged Shell for Root Commands".

1. top -n 1 -b > /home/ssgconfig/top
2. ps -e -o pid,args --forest > /home/ssgconfig/ps-forest
3. ps awwx -mo pid,lwp,stime,time,c,cmd > /home/ssgconfig/ps-lwp
4. egrep "8080|8443|9443" /proc/net/ip_conntrack > /home/ssgconfig/ip_conntrack_port
5. cat /proc/sys/net/ipv4/netfilter/ip_conntrack_count > /home/ssgconfig/ip_conntrack_count
6. ethtool -S ethX > /home/ssgconfig/ethtool-ethX (Note: The value "X" should correspond to one or more interfaces on the Gateway appliance)
7. iptables -nvL > /home/ssgconfig/iptables-counter
8. ss -o state established \(sport = :8080 or sport = :8443 or sport = :9443 \) \ dst 0.0.0.0/0 | egrep -v Recv-Q | wc -l
   The above command counts the number of *established* inbound connections. That command should be run on every node in the cluster.
9. ss -o state established \(sport = :8080 or sport = :8443 or sport = :9443 \) \ dst 0.0.0.0/0 | grep -v ^0 | egrep -v Recv-Q | wc -l
   The above command counts the number of *queued* inbound connections. That command should be run on every node in the cluster.
10. ss -o state established \(dport = :http or dport = :https \) \ dst 0.0.0.0/0 | egrep -v Recv-Q | wc -l
    The above command counts the number of *outbound* connections. That command should be run on every node in the cluster.

Garbage collection (GC)

1. sudo su gateway
2. /opt/SecureSpan/JDK/bin/jstat -gcutil `cat /opt/SecureSpan/Gateway/node/default/var/ssg.pid` 10s > ~/gc_output.txt
   The above command gathers the garbage collection data every ten seconds and puts it into the gc_output.txt file. That command should be left to run for as long as possible (5 to 60 minutes) and the file should then be provided to CA Support.
   If prescribed by a CA Support Engineer to collect this data over a longer period of time (i.e. days or weeks), the following steps should be completed *instead* of the command above:
   Edit the following file: */opt/SecureSpan/Gateway/node/default/etc/conf/node.properties*
   Add the following line to the file in step one above: *node.java.opts = -verbosegc -XX:+PrintGCDetails -Xloggc:/tmp/gc.log*
   Save the file after the modification in step two above.
   Restart the API Gateway service to implement the change: *service ssg restart*