A10 ADC System Health Check

Customer: *Buying A10*

Date Performed:

A10 Engineer:

Donkey Kong, [dkong@a10networks.com](mailto:dkong@a10networks.com), 111-111-1111

Partner:

Rock Solid Partner, Inc.

Partner Engineer(s):

Patty Partner, [ppartner@rsp.com](mailto:ppartner@rsp.com), 987-654-3210

Customer Engineers:

Captain Customer, customers@buyingA10.com, 123-456-7890

**Table of Contents**

[1) Kick-off 3](#_Toc505090817)

[2) Topology review 3](#_Toc505090818)

[3) Capture & save original/current configuration 3](#_Toc505090819)

[4) Redundancy Check 4](#_Toc505090820)

[5) Health Check 4](#_Toc505090821)

[a) General check items 5](#_Toc505090822)

[i) Memory 5](#_Toc505090823)

[ii) HW/DISK/CF 5](#_Toc505090824)

[6) Interface/Trunk/Vlan status 5](#_Toc505090825)

[7) System Resources 6](#_Toc505090826)

[a) CPU 6](#_Toc505090827)

[b) Utilization/capacity 6](#_Toc505090828)

[c) Spikes/peg 6](#_Toc505090829)

[8) Sessions 7](#_Toc505090830)

[a) IP 7](#_Toc505090831)

[b) TCP 7](#_Toc505090832)

[c) UDP 7](#_Toc505090833)

[d) SSL 7](#_Toc505090834)

[e) L4 session 8](#_Toc505090835)

[f) CPS (connections per sec) 8](#_Toc505090836)

[9) System Errors 8](#_Toc505090837)

[10) Health monitor status 8](#_Toc505090838)

[11) Performance numbers (TH3030S) 9](#_Toc505090839)

[12) Application Services 9](#_Toc505090840)

[a) Latency 9](#_Toc505090841)

[13) Monitoring Review 10](#_Toc505090842)

[14) Security Check 10](#_Toc505090843)

[15) New code/version release consideration 10](#_Toc505090844)

[16) Closing Comments/Recommendations 10](#_Toc505090845)

[a) Additional Resources 12](#_Toc505090846)

# Kick-off

Start the meeting by discussing goals. The primary goal is to review the current configurations and determine current ADC health and if look for any indicators to determine if there are any immediate issues or something than may lead to eventual issues with the ADC. An additional goal included with the review will be to look at the security and determine if there are areas that can be improved through best-practices or new configuration to help protect system resources.

**NOTE**: This health check was written & verified using ACOS v4.1.0-P10 & v4.1.1-P7. While the procedures covered here are valid for all ACOS v4.x versions, this document is still germane for previous ACOS versions (e.g. v2.7.1, v2.7.2), however, commands may differ (or not available).

# Topology review

Review the network topology and discuss the expectations of the ADC. High-availability should be a big part of the discussion. Include global redundancy as well. Depending on architecture, dynamic-routing (bgp/ospf/isis) may also be of concern.

Include in this conversation the physical topology, such as physical links and the connections to the network with requirements (lags/lacp/vlan trunking/etc).

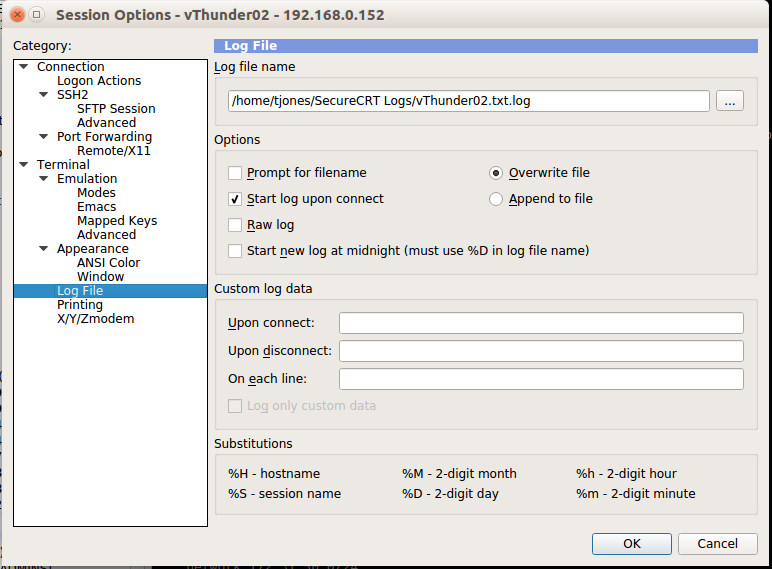
# Capture & save original/current configuration

Use this step to capture the original configuration. No changes should be made in the process of this health-check, however, having an artifact will ensure the post-health-check configuration matches the pre-post-check configuration.

Also ensure logging is enabled on all CLI sessions to the ADC. How to do this will differ based on application used.

Below is an example on how to save session logs using SecureCRT. Putty is very similar.

Open the properties for the client by right-clicking on the client in the Session Manager, the add a location & filename for the log.



*Run the following commands on both ADC’s:*

show running with-default partition-config all

show startup-config all-partitions

# Redundancy Check

This step will check the redundancy for both the data plane (vrrp-a) and the control plane (avcs), if applicable.

Look at the vrrp configuration and verify proper/best practice setup for proper data plane failover. Verify vrrp-a interface is ensure for data plane.

Verify vrrp-a functionality ( no erros/mismatch/etc).

Verify vcs chassis members, state match configuration.

*Run the following commands on master ADC:*

show running vrrp-a

show vrrp-a detail

show running vcs

show vcs summary

# Health Check

The following steps are going to go through the various functions of the ADC configurations and operational data to look for clues of any possible health issues the ADC may experience or could be experiencing. Also look for opportunities to optimize configuration or use best practices to help improve the health of the ADC as well as the functionality and performance of the services being load-balanced.

This health-check is a minimum baseline for slb (server load-balancing) services being utilized on the ADC. This health-check does not cover the features: GSLB, AAM, WAF.

## General check items

### Memory

Check the memory usage on ADC. Memory is allocated to resources, so the amount of memory remaining can be indicator of resources available (if increase is required).

A memory usage above 90% indicates the ADC is at the upper limits or operation. Look at solutions (tech refresh to larger ADC, scale-out, clean-up, etc) to try to alleviate memory burden.

*Run the following commands on both ADC’s:*

show memory

### HW/DISK/CF

Check the ADC hardware & storage. Review the output and verify things like temperatures, free disk space, fans, etc all look to be within acceptable ranges.

*Run the following commands on both ADC’s:*

show hardware

show disk

show slb hw-compression

show environment

# Interface/Trunk/Vlan status

For each interface, review: actual speed, actual duplex, output errors, & % utilization.

Verify the trunk members and ensure the status is enabled (not blocking).

Check lacp for the trunks to confirm sync.

Verify that the trunk/interfaces are members of appropriate vlans

*Run the following commands on both ADC’s:*

show interfaces transceiver (if using fiber)

show interfaces

show trunk

show lacp counter

show lacp trunk detail

show vlans

# System Resources

Verify the output for each command below. Check the utilization, peak, and exceeded values to determine if close to resource exhaustion.

*Run the following commands on both ADC’s:*

show system resource-usage

show slb resource-usage

show resource-accounting all-partitions summary

show resource-accounting global

show resource-accounting resource-type app-resources

show resource-accounting resource-type network-resources

## CPU

Review the CPU’s for the system. Expected are reasonable levels of cpu utilization, understanding that the data plane should distribute load across data plane cpus.

*Run the following commands on both ADC’s:*

show cpu

## Utilization/capacity

Review the overall cpu statistics to determine the sustained load of ADC. High, sustained levels may indicate more capacity is needed. (Look at scale-out or upgrade of hardware as possible solutions).

*Run the following commands on both ADC’s:*

show cpu overall

## Spikes/peg

Look for spikes or longer periods of sustained high cpu levels. Look for drivers for such spikes (important time for service?)

Think about using multi-ctrl-cpu if the control cpu(s) continually run high.

*Run the following commands on both ADC’s:*

show cpu history

# Sessions

Check the session output for to review total sessions. Look for any anomalies like high number of half open tcp sessions. Look for any anomalies like high number of half open tcp sessions.

*Run the following commands on both ADC’s:*

show session

## IP

Verify all IP information from the output. Verify all routes are in route table.

NOTE: Commands not shown, but also verify dynamic routes if dynamic protocol is used.

*Run the following commands on both ADC’s:*

show ip route

show ip stats

show ip anomaly-drop statistics

## TCP

Check for TCP anomalies.

*Run the following commands on both ADC’s:*

show slb switch | i TCP

show slb tcp stack

## UDP

Check for UDP anomalies.

*Run the following commands on both ADC’s:*

show slb switch | i UDP

## SSL

Review output and look for anomalies. Pay particular attention to ‘HW ring full’ to determine load on SSL chip. A high value equates to slower/dropped SSL traffic due to encrypt/decrypt. Look at client/server template ciphers w/o ECDSA to lesson load. New hardware recommended for high SSL chip load.

*Run the following commands on both ADC’s:*

show slb ssl error

show slb ssl stats

## L4 session

Review the output and look for any excessive drop values or uneven traffic distribution across data plane cpus.

*Run the following commands on both ADC’s:*

show slb l4 detail

## CPS (connections per sec)

Check the CPS for exceeded values.

*Run the following commands on both ADC’s:*

show resource-accounting resource-type system-resources

# System Errors

Check the logs and look for errors. Determine source of errors and determine resolution.

*Run the following commands on both ADC’s:*

show log | i Error

show errors (available in some ACOS versions)

# Health monitor status

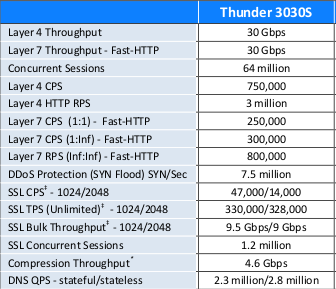
This section will verify the status for the health-check of all real-servers and the associated health monitor. If a status shows down, verify the reason for the downed state.

*Run the following commands on both ADC’s:*

show health stat

show health down-reason <##>

# Performance numbers (TH3030S)



This section will review the ADC statistics and determine how the system is performing versus the maximum available for the system. (Note: The performance numbers show above are provided for guidance based on the best possible scenario under lab conditions. In production, typically a mix of services will lead to lower maximum values for an individual service).

*Run the following commands on both ADC’s:*

show slb performance interval 1 (run for 1 minute)

# Application Services

This section is to ...

*Run the following commands on both ADC’s:*

show slb server <$SVR\_NAME>

show slb service-group <$SVC\_GRP\_NAME>

show slb virtual-server <$VIP\_NAME> detail

## Latency

This section will check the latency for both server side.

*Run the following commands on both ADC’s:*

show slb server <$SVR\_NAME>

# Monitoring Review

Review the output to determine how/if logging is being performed.

*Run the following commands on master ADC:*

show logging

# Security Check

Check for

*Run the following commands on both ADC’s*

show management

show slb conn-rate-limit src-ip statistics

show ip anomaly-drop statistics

# New code/version release consideration

Discuss current code options versus upgrade options. A push to v4 is the recommend path always.

If a move to ACOS v4, discuss plan to get there.

*Run the following commands on both ADC’s:*

show version

show bootimage

# Closing Comments/Recommendations

Clouse the meeting with a review of the steps and answer any questions based on the output of each step in the preceding steps. Take actions for follow-up on any unanswered questions.

Ensure a copy of outputs for all ADC’s are captured and distributed.

An expected result will be a list of recommendation changes the customer should consider making. Should assistance be requested, the partner engineer or A10 engineer should follow-up with anticipated hours required and who can provide services (ie. A10 ProServ or partner ProServ).

# Additional Resources

* A10 Documentation: <https://documentation.a10networks.com/signin.html>
* A10-DG-DDoS\_Protection\_for\_Web\_and\_DNS\_Servers (Provided).

## Summary of A10 Deployment Guide - DDoS Protection for Web and DNS Servers

!

!

Recommendations:

When using the A10 ADC to deal with DDoS attacks, the following key features are recommended:

 DDoS Protection should be enabled.

 Hardware-based SYN Cookies should be enabled.(if supported on your model - TH6430S,TH6430,TH5430S,AX2200,AX2200-11,AX3100,AX3200,AX 3200-11,AX 3200-12,AX3400, AX5100, AX5200,AX5200-11)

 IP Anomaly filters should to be turned on along with system-wide PBSLB using dynamic Black/White List entries (IP address 0.0.0.0/0).

 IP Limiting should be configured.

 DNS Firewall feature should be enabled and applied to virtual ports configured for service type UDP-DNS.

!

!

FLOOD ATTACKS

!

!

ICMP FLOODS (Mitigation - ICMP Rate Limit - Packets Per Sec)

icmp-rate-limit 20000 lockup 30000 60

Notes: Below are ranges for each

icmp-rate-limit ?

<1-65535> Normal rate limit. If exceeds this limit, drop the ICMP packet that goes over the limit.

icmp-rate-limit 20000 lockup ?

<1-65535> Maximum rate limit. If exceeds this limit, drop all ICMP packet for a time period.

icmp-rate-limit 20000 lockup 30000 ?

<1-16383> Lockup period (second)

!

UDP ATTACK (Mitigation - Source IP Based Connection-rate Limiting)

slb conn-rate-limit src-ip udp 2000 per 100 shared exceed-action log lock-out 30

Notes:

slb conn-rate-limit src-ip ?

tcp tcp conn rate limit

udp udp conn rate limit

<1-1000000> Max connections per period

slb conn-rate-limit src-ip udp ?

<1-1000000> Max connections per period

slb conn-rate-limit src-ip udp 100 per ?

100 100 ms

1000 1000 ms

slb conn-rate-limit src-ip udp 2000 per 100 ?

exceed-action Threshold exceed action

shared Threshold shared amongst all Virtual Ports

<cr>

slb conn-rate-limit src-ip udp 2000 per 100 shared ?

exceed-action Threshold exceed action

<cr>

slb conn-rate-limit src-ip udp 2000 per 100 shared exceed-action ?

lock-out Lockout period in seconds if threshold exceeded

log Send log if threshold exceeded

slb conn-rate-limit src-ip udp 2000 per 100 shared exceed-action lock-out ?

<1-3600> Lockout period in seconds if threshold exceeded

!

!

SMURF ATTACK (Mitigation - ICMP Rate Limit - Packets Per Sec)

A10 ADCs do not forward (and flood) such directed broadcasts to the local network by default (if directed to VIP). If destination is backend server, use ICMP Rate Limit

!

!

NETWORK ATTACKS

!

!

IP OPTION EXPLOIT (Mitigation - DDoS Protection "IP Option")

ip anomaly-drop ip-option

!

LAND ATTACK (Mitigation: DDoS Protection "Land Attack")

ip anomaly-drop land-attack

!

PING OF DEATH (Mitigation: DDoS Protection "Ping-of-Death")

ip anomaly-drop ping-of-death

!

IP FRAGMENTATION ATTACK (Mitigation: DDoS Protection "Frag")

ip anomaly-drop frag

!

TCP NO FLAG EXPLOIT (DDoS Protection “TCP No Frag”)

ip anomaly-drop tcp-no-flag

!

TCP SYN+FIN EXPLOIT (Mitigation: DDoS Protection "TCP SYN Fin")

ip anomaly-drop tcp-syn-fin

!

TCP SYN FRAGMENT ATTACK (Mitigation: DDoS Protection "TCP SYN Frag")

ip anomaly-drop tcp-syn-frag

!

OUT OF SEQUENCE ATTACK (Mitigation: IP Anomaly Filter "Out of Sequence" with System-wide PBSLB)

ip anomaly-drop out-of-sequence 10

\*\*Note: 10 is the threshold of out-of-sequence packets that can be seen before dropping. Can be 1-127.

\*\*Note: Must also configured PBSLB. BW-List must be previously defined and imported

bw-list BW-LIST tftp://192.168.0.7/BW-list.txt period 86400 load

system pbslb bw-list BW-LIST

system pbslb over-limit lockup 5 logging 10

!

TCP ZERO WINDOW ATTACK {Mitigation: IP Anomaly Filter "Zero Window" and system-wide PBSLB}

ip anomaly-drop zero-window 10

\*\*Note: 10 is the threshold of 0 window size packets to accept before dropping. Can be 1-127.

\*\*Note: Must also configured PBSLB. BW-List must be previously defined

system pbslb bw-list BW-List

system pbslb over-limit lockup 5 logging 10

!

TEARDROP ATTACK (Mitigation: DDoS Protection "Frag")

ip anomaly-drop frag

!

COMPHRESIVE (Enable drop-all to turn on all IP anomaly-drop features)

ip anomaly-drop drop-all

!

!

APPLICATION / HTTP ATTACKS

!

!

INVALID PAYLOAD PACKETS (HTTP/SSL) {Mitigation: IP Anomaly Filter "Bad Content" with system-wide PBSLB}

ip anomaly-drop bad-content 10

\*\*Note: 10 is threshold of invalid payload packets to accept before dropping. Can be 1-127.

\*\*Note: Must also configured PBSLB. BW-List must be previously defined

bw-list BW-LIST tftp://192.168.0.7/BW-list.txt period 86400 load

system pbslb bw-list BW-List

system pbslb over-limit lockup 5 logging 10

!

HTTP GET/POST FLOOD {Mitigation: IP Limiting (Policy Template)}

class-list HTTP-RL

10.100.0.0 /16 lid 1

10.255.0.0 /16 lid 2

0.0.0.0 /0 glid 10

192.168.0.0 /16

exit

glid 10

request-limit 150

request-rate-limit 20 per 1

over-limit-action lockout 60

exit

slb template policy POLICY-HTTP-RL

class-list name HTTP-RL

class-list lid 1

request-limit 300

request-rate-limit 100 per 1

exit

class-list lid 2

request-limit 500

request-rate-limit 200 per 1

exit

exit

slb virtual-server VIP\_01

port 80 http

template policy POLICY-HTTP-RL

exit

exit

!

SLOWLORIS {Mitigation: HTTP Template with "HTTP Request Header Time Out"}

slb template http Policy-HTTP-Slowloris

req-hdr-wait-time 7

exit

slb virtual-server VIP\_01

port 80 http

template http Policy-HTTP-Slowloris

exit

exit

slb enable-ddos

!

SLOW POST ATTACK {Mitigation: HTTP Template "HTTP Request Header Time Out"}

\*\*same first as Slowloris

!

SOCKSTRESS ATTACK {Mitigation: System-wide PBSLB (with IP Anomaly Filter) and IP Limiting}

\*\* Enabled via Out of Sequence Attack, TCP Zero Window Attack, Invalid Payload Packets & HTTP GET/POST Flood.

!

!

DNS SERVER ATTACKS

!

!

DNS FLOOD ATTACK {}

class-list CL-DNS

10.0.0.0 /8 lid 1

0.0.0.0 /0 lid 10

192.168.0.0 /16 lid 2

exit

glid 20

conn-limit 50000

conn-rate-limit 1000 per 10

request-limit 50000

request-rate-limit 1000 per 10

over-limit-action log 10

exit

slb template dns Policy-DNS

malformed-query drop

class-list name CL-DNS

class-list lid 1

conn-rate-limit 500 per 10

over-limit-action log 10

exit

class-list lid 3

conn-rate-limit 2000 per 10

over-limit-action log 10

exit

exit

slb virtual-server DNS-VIP 1.1.1.53

port 53 dns-udp

template dns Policy-DNS

exit

exit

exit

!

DNS AMPLIFICATION ATTACK {Mitigation: Combination of DNS Firewall Template, IP Limiting and System-wide PBSLB}

\*\*Note: DNS Flood Attack, Out of Sequence Attack, HTTP GET Flood

!

!

OTHER DDoS CLI Cmds

!

slb hw-syn-rr <1-500000>

Note: Enable distribution of client SYNs across multiple CPUs. This feature protects against CPU overload due to SYN floods, a common symptom of DDoS attacks.

!

system attack log

Note: Enable logging for DDoS attacks.

!

system anomaly log

Note: Enable logging system anomalies.

!