DC/OS Networking - Troubleshooting

Overview

This document captures various troubleshooting that we have done so far or might be doing in future in DC/OS networking. Aim is to convert this doc into a user facing document so that our customer, support team and others could benefit from it. Besides, this document itself could be shared in case anybody interested in troubleshooting DC/OS networking.

Networking Components:

1. Marathon-LB
2. Edge-LB
3. Mesos-DNS
4. Spartan (or dcos-dns)
5. Minuteman (or dcos-l4lb)
6. Navstar (or dcos-overlay)

Connectivity issues with DC/OS overlay:

Scenario: Container A on host A is not able to access container B on host B
Troubleshooting Steps:

- Check DCOS jira for known issues
    - https://jira.mesosphere.com/browse/COPS-44
- Check Container A and Container B are healthy
    - For docker: (On the agent node) “docker exec -it <container-id> /bin/bash”
    - For UCR: (From CLI) “dcos task exec -it <task-id> /bin/bash”
- Check vtep interfaces are present on both the hosts
- Check d-dcos (for docker) and m-dcos (for UCR) have IP addresses
- Check for any iptables firewall rules
- Check ping from host A to host B
    - Issue in customer network, mostly it is Firewall
- Check ping from host A to vtep interface on host B
    - Issue in customer network, mostly it is Firewall
- Check ping from host B to Container B

VIP issues:

Scenario: Connection refused when accessing service via VIP

Troubleshooting Steps:

- Check DCOS jira for known issues
- Check if the VIP DNS is getting resolved. # host <vip-dns>
- Check if the backend services are up and accessible via the service IP and Port
- Check if the VIP configuration is correct
    - You would need to install `ipvsadm` tool or a docker container. You could use: docker run -it --net=host --privileged mesosphere/net-toolbox /bin/bash
- Check if there are any errors in the logs
    - For DC/OS 1.10, 1.9, # sudo journalctl -u dcos-navstar -f
    - For DC/OS 1.11, # sudo journalctl -u dcos-net -f

Scenario: Connection timeout when accessing service via VIP

Troubleshooting Steps:

- Check if the connections are long lived. Any connection that remain idle for more than 15 min will be terminated by IPVS. This is the default setting that comes with linux distro
- If yes, then two solutions:
    - Enable keep-alive on the client to avoid idle timeout
    - Manually increase the default timeout setting of IPVS
        - # ipvsadm --set tcp tcpfin udp

Issues accessing *.directory:

Please run the following command on node that explores any issues with DNS

- Check if /etc/resolv.conf contains spartan/dcos-dns ip addresses 198.51.100.[123]
    - If it doesn't please check dcos-gen-resolvconf
- Check if dns forwarder works fine
    - resolv.conf configured correctly
        - dig ready.spartan
    - spartan/dcos-dns is available
        - dig ready.spartan @198.51.100.1
    - mesos-dns is reachable
        - dig leader.mesos @198.51.100.1
- Check if you can find your dns record using spartan/dcos-dns http api
    - See networking run book, /v1/records
- Check if spartan/dcos-dns has the same issue on leader node
- Check mesos state and mesos logs
- Check exhibitor

Issues accessing *.mesos:

Please run the following command on node that explores any issues with DNS

- Check if /etc/resolv.conf contains spartan/dcos-dns ip addresses 198.51.100.[123]
    - If it doens't please check dcos-gen-resolvconf
- Check if dns forwarder works fine
    - resolv.conf configured correctly
        - dig ready.spartan
    - spartan/dcos-dns is available
        - dig ready.spartan @198.51.100.1
    - mesos-dns is reachable
        - dig leader.mesos @198.51.100.1
    - If no, on leader node check mesos-dns and its logs
        - dig master.mesos @127.0.0.1 -p 61053
- Check if mesos-dns knows master nodes
    - dig master.mesos @$(dig +short leader.mesos @198.51.100.1) -p 61053
- Check if you can find your dns record using mesos-dns http api
    - on leader node: curl http://localhost:8123/v1/enumerate
- Check mesos state and mesos logs

Issues with Marathon-LB:

Scenario: Unable to access VHOST via HTTPS (503/504)
Example: https://mesosphere.zendesk.com/agent/tickets/9384
Troubleshooting Steps:

- Check that the vhost exists and take note of the backend name
    - curl http://<marathon-lb-ip>:9090/_haproxy_getvhostmap
- Check that there are servers present in the haproxy.cfg backend
    - curl http://<marathon-lb-ip>:9090/_haproxy_getconfig
- Check that the VHOST / SNI mapping is working correctly by spoofing SNI
    - curl -kvv --resolve <vhost>:443:<marathon-lb-ip> https://<vhost>
- Check that the VHOST is correctly configured to route to <marathon-lb-ip>
    - curl -kvv https://<vhost>
    - If this step fails with 5XX but the previous step gives 2XX, it is likely a misconfiguration on the linkage between the VHOST and the <marathon-lb-ip>

Scenario: No server available to fulfil request when accessing VHOST (503)
Troubleshooting Steps:

- Check that the HAPROXY_0_VHOST label is set correctly on the app definition
- Check that the vhost exists and take note of the backend name

        - curl http://<marathon-lb-ip>:9090/_haproxy_getvhostmap
- Check that there are servers present in the haproxy.cfg backend
    - curl http://<marathon-lb-ip>:9090/_haproxy_getconfig

Issues with Edge-LB:

Scenario: No server available to fulfil request when accessing VHOST (503)
Troubleshooting Steps:

- Check that the pool.haproxy.frontend.linkBackend.map.hostEq contains the correct VHOST
- Check that the VHOST exists and that there are servers present in the haproxy.cfg backend
    - curl http://<marathon-lb-ip>:9090/_haproxy_getconfig

Scenario: haproxy.cfg not updated after backend tasks have changed / stale haproxy.cfg
Troubleshooting Steps:

- Check the /dcos-edgelb/api stderr log for failed attempts to request ".../deploy/...sidecar"
    - If the response code is 403 / 401, the service account is lacking permissions
    - Try adding either of these:
        - dcos security org users grant edgelb-principal dcos:adminrouter:service:dcos-edgelb/pools/<POOL-NAME> full
        - dcos security org groups add_user superusers edge-lb-principal
- Check that the scheduler is running and healthy at /dcos-edgelb/pools/<POOL-NAME>
    - Check the stdout logs for that task for failed references to sidecar (failed attempts to reserve resources required for sidecar)
- Check that the edgelb-pool-0-server task is running
- Check for failed edgelb-pool-0-sidecar tasks and inspect the errors

Scenario: Edge-LB failing to start
Example: https://jira.mesosphere.com/browse/COPS-2307
Troubleshooting Steps:

- Check the apiserver stderr at /dcos-edglb/api for fatal log messages
    - If messages like error="could not make request: Failed to create HTTP POST request for http://leader.mesos/package/install because no service account or auth token were found" exist, Check that the service account is correctly configured in the edgelb-options.json (field is named secretName, not secret-name)
- Check that any other marathon app can successfully use service accounts with a test app