Troubleshooting Essentials

How to add a new MAC Vendor to macvendor table

To insert mac value in macvendor table:

insert into system.macvendor(prefix, vendor,hi, lo) values ('90:6C:AC','ARUBA NETWORKS', -1, -1);

Once done, import a macvendor pattern with expression set to ‘ARUBA NETWORKS’ (vendor name that you inserted with above sql) along with other profiling attributes.

Example:

```
<patterns xmlns="urn:lumeta:pattern:6.0" user-provided="true" version="3.2.7.10623">
<pattern priority="10000">
<source>macvendor</source>
<expression>ARUBA NETWORKS</expression>
<attributes>
<attribute type="Model" confidence="69">(Aruba Networks)</attribute>
<attribute type="OS" confidence="69">(Aruba Networks)</attribute>
<attribute type="DeviceType" confidence="83">Firewall</attribute>
<attribute type="Version" confidence="69">(Aruba Networks)</attribute>
<attribute type="Vendor" confidence="83">Aruba Networks</attribute>
</attributes>
</pattern>
</patterns>
```

Steps to take when discovery is not happening

1. Check the /var/log/lumeta-webapp.out file and see if there are entries “skip adding devices”. These entries mean that your rescan interval for collector is too small and your collector is not able to finish up its discovery phase. In this case, you need to increase your collector’s rescan interval.
2. If your CC is connected to a Scout, then check the CC <-> Scout connectivity:
    a. Ping the Scout from CC to verify that we can ping the Scout (or to see if Scout is up and running and CC can get a response back from it). On CLI, run:
        i. system ping <interface> <Scout IP> (please choose CC interface)
    b. If ping returns you 0% packet loss, then try to delete and reconnect the scout back. On CLI, run:
        i. spectre delete <Scout name>
        ii. spectre connect <Scout IP>
3. If the above error is "ERROR: connect timed out" then we don't seem to have full connectivity between the CC and Scout. In this case, please send /var/log/discovery-agent.log file and /var/log/lumeta-webapp.out file to Lumeta.

Steps to take when one cannot login to the Spectre CC box

1. First thing to verify is that the license has not expired due to license IP count exceeding the limit. Login to your CC via console as root or login to your CC as admin user and then become root:
    a. type db to enter the database
    b. Run the query: select name, message, time, details, priority from event.notification_all where type like 'LICENSE%' order by time desc limit 1;
    c. This will show you if you got any warnings or alerts regarding license expiration. If so, then continue on and find the number of IPs that were discovered by your CC.
    d. select zone_id, count(distinct ip) from zone.device group by zone_id;
    e. That will show the number of devices in each zone
    f. To find the name of zone associated with the zone_id:
    g. select * from system.zone;
    h. to exit the database
    i. \q
    j. Please verify the number of IPs that your license was generated for by logging in to CLI and running the command: certificate spectre view. If your number of IPs have exceeded, contact Lumeta for further information.

Steps to take when VM runs out of disk space

If your Spectre CC VM is running out of disk space, there are certain tables in the database that can be cleaned up to make more space. Please login to your CC as admin and run “support db” or login to your CC as root from console and run “db” (in both cases, you will be entering database mode). Then execute:

- select count(*) from event.notification_all;
- truncate table event.notification_all;
- select count(*) from event.notification_all; (just to confirm that we were able to delete all those records)
- select count(*) from event.event_all;
- truncate table event.event_all;
- select count(*) from event.event_all; (just to confirm that we were able to delete all those records)

How to force deleting of a zone (when deleting a zone from GUI/CLI fails)

If for some reason, you cannot delete the zone via GUI or CLI (because it is timing out or resulting in an error), you will need to login to db and delete it

- Login to your CC as admin and then run support db (to enter database mode) OR Login to your CC and su to root. Then run db (to enter database mode)
- Find the zone_id associated with your zone by running select * from system.zone; This will give the name of the zones and their id. Then run the following commands based on your zone id.
- select * from zone_0023 config;
- drop schema zone_0023 cascade;
- delete from system.zone where id=35;
- \q

NOTE: In the above example, even though the zone id is 35, in hex it becomes 0023.

How to manually disable NTPD on Spectre boxes

Here are the manual steps to disable NTP for Spectre:

1. Log into the CLI as admin (or any superuser)
2. Get a bash shell using command "support bash"
3. Become root by running "su" and giving the root password
4. Stop the NTP daemon: "service ntpd stop"
5. Make sure daemon won't be started on reboot: "chkconfig ntpd off"

How to verify open ports for a device (similar to how Spectre verifies)

Command to check if port on a device is open. From command center

1. echo "foo\n\n" > /dev/tcp/ip/port
2. You'll get 3 types of responses: Connection refused, timeout (or hang), and finally a successful connection displayed by line return.
3. When we get a "Connection timed out" reply, we consider that port to be neither open or closed.
4. When we get a "Connection refused" reply from a port, we consider that port to be closed.
5. When we get a "Connection success" reply from a port, we consider that port to be open.
6. If a port comes up as open and later on we get a "Connection timed out" reply from that port we do not clear up that port from open port list. This is the functionality in ESI 3.2.6 and prior. (Spectre 3.2.7 will introduce a data retention policy that will allow clear up data based on the reply that we get back).

How to change Spectre's hostname

1. On a CentOS box, hostname comes from /etc/sysconfig/network. You can display the hostname by running the command: hostname
2. Spectre prompts user for a host name during postinstall. This is saved in the db at system.system table. When user runs "system hostname" command at CLI prompt, the above is retrieved and displayed.

If for some reason, the hostname under database and application filesystem is not in sync, then you will need to reboot the system.

In more depth, here's a bit more about the two names, how to see them, and how you might change them (these assume you're at a root shell prompt)

1) CentOS

1. Edit the file /etc/sysconfig/network and change the HOSTNAME= line. Restart network: service network restart" for the hostname to be changed.
2. Run "hostname <new host name>" to make the change immediately (otherwise CentOS would pick it up next time the network restarts)

2) Spectre

1. Run at bash prompt: sudo -u postgres psql observer -c 'select name from system.system'
2. hostname will be displayed. This can be changed manually:
3. sudo -u postgres psql observer -c "update system.system set name='<new system name>' where name='<old system name>'"

All these changes should occur automatically via the "system hostname" CLI command, but that's where you can look if that doesn't work out.

How to disable PKI from bash prompt

As root, run the command: /usr/local/lumeta/bin/observer_pki enable false

Steps to disable FIPS mode on Spectre 3.2.7 (and later) CC/Scout when it is configured with BGP with MD5

1. Make a copy of the grub.conf file
    a. cd /etc
    b. cp grub.conf grub.OLD
2. Edit the grub.conf file
    a. vi grub.conf
    b. change fips=1 to fips=0
    c. Reboot system

Steps to perform if Scout runs out of memory during upgrade

While Upgrading a Scout, if you see the error message "Out of memory!", please perform the following steps:

1. On command line as su type the following commands. One per line
    a. dd if=/dev/zero of=swapfile bs=1024 count=2621440
    b. mkswap -L swapfile swapfile
    c. swapon swapfile

DO NOT REBOOT.

Via CLI continue with the upgrade.

You can monitor the upgrade if you have a second ssh session window. Cd/var/log..there will be an esi-update file; Tail -f /var/log/esi-update.log

If successful the Spectre system will reboot, and when it comes back online verify via CLI (system version spectre) or login in through the UI that the installation was successful