LMS 4.1 (not just) for Dummies

Setting up an LMS server to manage your network can be a daunting task. LMS has hundreds of features and options to choose from and sooner or later things will go wrong. This is a TAC guide on how to configuring the basic network management tasks on your LMS server. This guide will explain how to archive your device configurations, monitor the network performance and faults and how to troubleshoot some (most common) of the problems you may encounter along the way.

If you open this guide on your LMS server, the links below will take you directly to the corresponding pages on your LMS server.

Contents

Server Checklist

Check the server name resolution

The LMS services use the server hostname to talk to each other. If your name resolution is slow or broken, you LMS server will be slow or broken.

1. Open a DOS box on the server and resolve the ip address and hostname:

   # cd CSCOpx\bin
   # hostname
   # perl resolver.pl <server hostname>
   # nslookup <server ip address>
   # nslookup <server hostname>

2. The hostname and IP address should be the same in all 4 commands. Update the DNS server and hosts file if they do not match.

   Note: You can use the hosts file instead of DNS to resolve the server hostname, but then you need to make sure that DNS is disabled in your TCP/IP Settings. Otherwise, the DNS timeouts will slow down the LMS server and trigger errors in the logs.

3. Check the name resolution on the LMS clients.

Check the device name resolution

Perform the same check for the network devices. If the LMS server cannot perform the forward and reverse name resolution of the devices, strange things will happen.

1. Open a DOS box on the server and resolve the ip address and hostname:

   # nslookup <device ip address>
   # nslookup <device hostname>

   Note: You can use resolver.pl to resolve multiple hostnames at once:

   # cd CSCOpx\bin
   # perl resolver.pl <device1> <device2> <device3>

2. Add the DNS records and PTR records to the DNS server if the name resolution fails.

Verify if the server has enough swap

LMS needs a swap file that is twice the amount of RAM.

1. Right click on My Computer
2. Select Properties -> Advanced -> Performance -> Settings -> Advanced -> Virtual Memory
3. Click Change
4. Configure a custom swap that is twice the amount of RAM (minimum is 8 GB of swap).

Check the LMS process status

1. Go to Admin > System > Server Monitoring > Processes

2. Select Show only: “Administrator has shut down this server” from the pulldown.
3. Only DataPurge and DFMCTMStartup should be listed. If any other processes are listed, it means that service has not started. To resolve this, make sure that nothing is holding the ports that LMS requires. Take note of the ports that are used before LMS starts:

   # net stop crmdmgtd
   # netstat –noab

4. Compare the ports in the netstat to the ports that LMS requires:

   http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/install/guide/prereq.html#wp1075786

5. Uninstall the applications that are using any of the required ports. You can use the PID in the output of the netstat to find out what application is using the required port.

Check the server clock

LMS uses a certificate that has an expiration date, so we need to make sure that the server date is correct.

 # date /T
 # time /T

Troubleshooting

Problem	**Solution**
Users cannot log into LMS	If the date was incorrect during the LMS installation, the certificate may no longer be valid after you correct the date. To resolve this, you can recreate the certificate after correcting the date: **# net stop crmdmgtd** **# cd CSCOpx\MDC\Apache\conf\ssl** **# del server.*** **# cd CSCOpx\MDC\Apache** **# perl ConfigSSL.pl -disable** **# perl ConfigSSL.pl -enable (Enter the certificate data)** **# net start crmdmgtd**

Add the devices

We first need to add the devices to the LMS device repository before LMS can manage the network. For large scale deployments (100+ devices), you can have the LMS server discover automatically. If fewer devices need to be discovered, you can skip to "Add the devices manually" below.

Perform the Discovery

1. Go to Admin > Network > Discovery Settings > Settings > Configure
2. Click Module Settings: Configure
3. The discovery modules that you need to select here depend on what works best for your network. Here is a description on what the advantages and disadvantages are for each module.

Module	Advantage	Disadvantage
Address Resolution Protocol (ARP)	-No device side configuration is required.	-Can use a lot of resources on the network devices if the arp tables are big. -Network devices that do not originate traffic (like switches) may be missing from the arp table.
Border Gateway Protocol (BGP)	-Uses few network and device resources.	-Switches or routers that are not BGP neighbors will not get discovered
Open Shortest Path First Protocol (OSPF)	-Uses few network and device resources.	-Switches or routers that are not BGP neighbors will not get discovered
Routing Table	-No device side configuration is required.	-Can use a lot of resources on the network devices if the routing tables are big. - Switches and routers that are not a next hop in the routing table will not get discovered.
Cisco Discovery Protocol (CDP)	-Uses few network and device resources.	-CDP needs to be enabled on the interfaces. Tip: only enable cdp on interfaces that are directly connected to network devices that you own. Interfaces that are connect to your users or your service provider should not have cdp enabled.
Ping Sweep on IP Range	-No device side configuration is required.	-Uses a lot of LMS server and network resources if the IP ranges are big. - Can take a lot of time to complete (hours or days on large deployments)

		- IPS may see the ping sweeps as attacks and can deny the LMS server access to the server.
Cluster Discovery Module	-Uses few network and device resources.	- Routers and switches that are not cluster members will not get discovered.
Hot Standby Router Protocol (HSRP)	-Uses few network and device resources.	- Switches and routers that are not part of an HSRP group will not get discovered.
Link Layer Discovery Protocol (LLDP)	-Uses few network and device resources.	-LLDP needs to be enabled on the devices.

4. Click Next
5. Click on each discovery module and add and enter at least one IP address of a device that can be used to start the discovery.
6. Check the "Use DCR as Seed List" and "Jump Router Boundaries" boxes
7. Next
8. Select SNMPv2 or SNMPv3
9. Click Add
10. Enter Target: *.*.*.*
11. For SNMPv2, you can find out the read only community string with:

    # sh run | i community

    For SNMPv3, you conf find out the Auth and Privacy Algorithm with:

    # sh snmp user

12. Finish
13. Go to Inventory > Device Administration > Discovery > Launch / Summary
14. Click Start Discovery

Validate the Discovery

Refresh the Discovery Summary page. When the discovery status changes from running into finished, click on the "Reachable Devices:" link and check if all the devices have been discovered.

Add the devices manually

If any devices are still undiscovered after the discovery, you can add them manually.

1. Go to Inventory > Device Administration > Add / Import / Manage Devices
2. Click Add
3. Make sure that the LMS server can resolve the hostname into an IP address and the IP address into the hostname.

   # nslookup <device ip address>
   # nslookup <device hostname>

LMS only works correctly when the forward and reverse name resolution of the devices is correct. Add the DNS records and PTR records to the DNS server if they do not match.

4. Enter the Hostname in the hostname field
5. Click “Add to list”
6. Do the same for the remaining devices
7. Click Finish

Validate the result

1. Go to Inventory > Device Administration > Add / Import / Manage Devices
2. Check the “All Devices” box.
3. The “device(s) selected” at the bottom of the device selector should show the number of devices you have in your network.

Troubleshooting

Problem	**Solution**
LMS reports duplicate devices	-Go to Inventory > Device Administration > Add / Import / Manage Devices -Click on the Export button and export “All Devices” to csv file. -Check in the csv file if the device IP address, hostname or display name has already been assigned to another device.
Devices are not discovered or are listed as unreachable	- Check and update the SNMP credentials in Admin > Network > Discovery Settings > Settings > Configure - Rediscover - If that does not resolve the problem, try adding the devices manually.

Add the device credentials

LMS needs to know the Telnet/SSH and SNMP credentials before it can manage the devices.

Update the credentials

1. Go to Inventory > Device Administration > Add / Import / Manage Devices
2. Check the "All Devices" box.
3. Click "Edit Credentials".
4. Next
5. Manually Telnet/SSH to one of the devices from the LMS server and take note of the prompts that you get while entering enable mode. For example:

   # telnet foo.cisco.com
   Username:
   Password:
   foo> enable
   foo#

6. Verify that the device hostname is displayed at the prompt (foo in the example). You can change the hostname with the "hostname <hostname>" command in IOS.
7. Make sure that the devices only prompts for "Username" or "Password". LMS does not accept custom prompts like "User" or "username" (lower case u). You can add any non-default prompts to CSCOpx\objects\cmf\data\TacacsPrompts.ini
8. Enter the same Username, Password and Enable password that you entered when manually logging into the device. Only add those fields that were required.
9. Next
10. Enter the snmp credentials. For SNMPv2, you can find out the read only community string with:

    # sh run | i community

    For SNMPv3, you conf find out the Auth and Privacy Algorithm with:

    # sh snmp user

11. Click Finish
12. Go to Inventory > Job Browsers > Device Credentials Verification
13. Create a new job.
14. Check the "All Devices" box
15. Enable the "SNMP Read Community String" and "SNMP Read Write Community String" boxes or the SNMPv3 box
16. Check the "Telnet/SSH" and "Telnet/SSH Enable Mode User Name and Password" boxes.
17. Schedule the job to run daily during the night.

Validate the device credentials

1. Go to Inventory > Job Browsers > Device Credentials Verification

2. Click Create
3. Check the “All Devices” box
4. Check the “SNMP Read Community String” and “SNMP Read Write Community String” boxes or the SNMPv3 box.
5. Check the “Telnet/SSH” and “Telnet/SSH Enable Mode User Name and Password” boxes.
6. Uncheck the “Report type” box.
7. Enter a Job Description and submit.
8. Refresh the page until the job finishes.
9. Click on the job id.
10. All the devices should be listed as “Successful Devices”.

Make a backup of the device list and credentials

You will want to make a backup of your hard work at this point in case something goes wrong later on. To save your work:

1. Go to Inventory > Device Administration > Add / Import / Manage Devices
2. Check the “All Devices” box.
3. Check the “Export Device Credentials” box. (Don’t forget this!!!)
4. Export the device list to csv file.
5. Copy the csv file to a safe location.

To restore the device list and credentials when things go wrong, go to Inventory > Device Administration > Add / Import / Manage Devices and click the “Bulk Import” button.

Troubleshooting

Problem	**Solution**
Device Credentials Verification shows failed devices.	-You can use the LMS Packet Capture tool to troubleshoot snmp or login problems. 1. Go to Monitor > Troubleshooting Tools > Troubleshooting Workflows 2. Open the device 3. Select Tools > Packet Capture 4. Start the Packet Capture 5. Run the Inventory > Job Browsers > Device Credentials Verification report again. 6. Open the packet capture in a packet decoder 7. Check if LMS is using the correct snmp credentials and look for errors messages on the device cli.

Collect the device inventory

We will now make sure that LMS collects all the hardware, software, serial number, etc data that are required for the Inventory reports.

Configure the inventory collection

1. Go to Admin > Collection Settings > Inventory > Inventory System Job Schedule
2. Under “Inventory Collection” , select Run Type: Weekly
3. Select a date in the future.
4. Select a time that is somewhere during off peak hours.
5. Click Apply
6. Under “Inventory Polling” , select Run Type: Daily
7. Select a date in the future.
8. Select a time that is somewhere during off peak hours.
9. Click Apply

If the LMS server does not accept the scheduled date, or if you would like to exclude certain devices from the Inventory Collection, you can also configure these jobs manually from the job browser:

1. Go to Inventory > Job Browsers > Inventory Collection
2. Click Create.
3. Check the “All Devices” box.
4. Select the “Inventory Polling” option.
5. Select Run Type: Daily
6. Select a time that is somewhere during off peak hours.
7. Enter Job Description: Daily Polling
8. Submit
9. Go to Inventory > Job Browsers > Inventory Collection
10. Click Create.
11. Check the “All Devices” box.
12. Select the “Inventory Collection” option.
13. Select Run Type: Weekly
14. Select a time that is somewhere during off peak hours.
15. Enter Job Description: Weekly Collection
16. Submit

Validate the inventory collection

1. Go to Inventory > Job Browsers > Inventory Collection
2. Click Create.

3. Check the “All Devices” box.
4. Select the “Inventory Collection” option.
5. Enter a Job Description
6. Submit
7. Refresh the page until the job status changes from Running to Successful or Failed.

We are now ready to run the Inventory reports.

1. Go to Reports > Inventory > Detailed Device
2. Select a device
3. Run the report.

You should be able to see the device and card hardware types, descriptions, serial numbers, etc.

Troubleshooting

Problem	Solution
Inventory Collection job fails with “Transport session to device failed.” Error	-Run a Inventory > Job Browsers > Device Credentials Verification report. -Make sure LMS has the correct SNMP read only credentials.
Inventory Collectionjob fails with generic error.	1. Go to Monitor > Troubleshooting Tools > Troubleshooting Workflows 2. Open the device 3. Select Tools > SNMP Walk 4. Enter OID: 1.3.6.1.2.1.47 5. Click OK. 6. The snmpwalk output should show the device inventory. For example: ENTITY-MIB::entPhysicalDescr.1 = STRING: 3640 chassis, Hw Serial#: 1234567, Hw Revision: 0x00 ENTITY-MIB::entPhysicalDescr.2 = STRING: 3640 Chassis Slot ENTITY-MIB::entPhysicalSerialNum.1 = STRING: 1234567 ENTITY-MIB::entPhysicalSerialNum.2 = STRING: ENTITY-MIB::entPhysicalName.1 = STRING: 3640 chassis ENTITY-MIB::entPhysicalName.2 = STRING: 3640 Chassis Slot 0 ENTITY-MIB::entPhysicalSoftwareRev.1 = STRING: 1.45 ENTITY-MIB::entPhysicalSoftwareRev.2 = STRING: ... 7. Check the ENTITY-MIB to see what the output should look like.

	8. If any of the values are incorrect, search the cisco.com Bug ToolKit for known device defects.

Archive the device configurations

We will now configure LMS to periodically make a backup of the device configurations in case we need to replace a device in the network or someone messes up our device configs.

Choose the Transport Protocols

1. Go to Admin > Collection Settings > Config > Config Transport Settings
2. Under Config Fetch, remove any of the protocols that are not configured on the devices. Here are some recommendations:
    a. Remove TELNET if the devices are configured to only use SSH
    b. Remove SSH if only TELNET is used.
    c. RCP and SCP require a user on the device that LMS can use. Remove RCP and SCP if they are not used.
    d. Some configurations like the vlan configuration (vlan.dat) can only be archived using TELNET or SSH, so make sure you leave either TELNET or SSH enabled.
    e. Leave TFTP in the protocol list as a backup in case TELNET/SSH fails.
3. Under Config Fetch, move TFTP to the top of the list as it takes the least amount of resources from the network.

    Note: TFTP requires SNMP write access to the devices, as the TFTP transfer is triggered by an snmpset request, so make sure LMS has the correct SNMP write credentials.
4. Click Apply

Set up the Configuration Archive

1. Go to Admin > Collection Settings > Config > Config Collection Settings
2. Under Periodic Polling , select the enable option
3. Click Schedule
4. Select Run Type: Daily and configure a time that is during off peak hours.

    Note: The Periodic Polling polls the CISCO-CONFIG-MAN-MIB to find out if the device configuration changed since the last archive. Periodic Polling only archives the configuration if the device reports that a configuration change took place, so you can use a short polling interval.
5. Click Apply
6. Under Periodic Collection , select the enable option and click Schedule
7. Select Run Type: Weekly and configure a time that is during off peak hours.

    Note: The Periodic Collection is a backup in case the Periodic Polling fails, so it can be scheduled at a longer interval.
8. Click Apply

Validate the Configuration Archive

1. Go to Configuration > Configuration Archive > Synchronization
2. Check the “All Devices” box.

3. Check the “Fetch startup config.” Box.
4. Enter a job description
5. Click Submit
6. Go to Configuration > Job Browsers > Configuration Archive
7. Refresh the page until the Status is Successful or Failed
8. We are now ready to view and compare configurations. Go to Configuration > Configuration Archive > Views > Version Tree .
9. Select a device
10. Click OK.
11. Open the tree and click on one of the configuration versions. You should see the device configuration.

Troubleshooting

Problem	**Solution**
Config Archive job shows “**Partially Failed Devices**” Error.	“Partially failed” means that LMS was able to archive either the startup, the running or the vlan configuration, but not all three. 1. Open the Configuration > Job Browsers > Configuration Archive job 2. Click the “failed” link to find out the reason. Note: some configurations like the vlan configuration (vlan.dat) can only be archived using TELNET or SSH, so make sure LMS have the correct TELNET/SSH credentials.
Config Archive job shows: “**config Fetch Operation failed for TFTP**.” Error.	1. Check if the LMS server is listening to the tftp 69/udp port: **# netstat –noab** Proto Local Address Foreign Address State PID UDP 0.0.0.0:69 *:* 1252 [crmtftp.exe] The process that listens to 69/udp should be crmtftp.exe. If another process is listening to the tftp port, uninstall the other tftp application and restart the CWCS tftp service. 2. Create a test config file on the LMS server: **# cd CSCOpx\tftpboot** **# echo > testconfig** 3. Telnet/SSH to the device and try to manually archive the configuration: **# copy startup-config tftp** Address or name of remote host []? <enter the LMS server IP address> Destination filename []? testconfig !!!

	6677 bytes copied in 0.148 secs (45115 bytes/sec) 4. If the tftp transfer fails, open the 69/udp port on firewalls or access lists that exist between the devices and the LMS server.
Config Archive job shows: "**Failed to establish TELNET connection**" error.	1. Manually Telnet/SSH to the device from the LMS server 2. Log in with the same credentials that you entered as primary credentials when adding the device 3. Go to enable mode 4. Check the privilege level 5. Attempt to show the configuration. For example: **# telnet foo.cisco.com** **Username:** **Password:** **foo> enable** **foo# show privilege** **Current privilege level is 15** **foo# terminal length 0** **foo# terminal width 512** **foo# show running-config** **Building configuration...** 6. If the "show privilege" does not show level 15, change the privilege of the LMS user on the TACACS server. **7.** If you see any errors during the terminal or show running commands, search the cisco.com Bug ToolKit for known device defects.

Monitor Performance

Set up the performance polling

1. Go to Monitor > Performance Settings > Setup > Automonitor
2. For Device Availability and CPU Utilization, you can use a short interval (i.e. 5 minutes.) as there will be less devices than links in the network.
3. For Interface Availability, Interface Errors and Interface Utilization use a longer interval (i.e. 15 or 30 minutes) as there will be more links than devices in the network.
4. Click Apply
5. Go to Monitor > Dashboards > Monitoring
6. In the "Device Performance Management Summary" portlet, verify if the "No. of Objects Monitored" is below 100,000.

   Note: LMS allows you to monitor up to 100,000 objects (cpu, memory, interfaces, etc.). You probably won't have 100,000 cpus in your network, but for the interfaces, this limit can easily be reached. Monitor the inOctets, OutOctets, inErrors, OutErrors, on 250 devices with 100 interfaces each and you've already reached the limit.
7. If "No. of Objects Monitored" is getting close to 100,000, manually create an Interface Utilization and Interface Errors poller for your critical links:
   a) Go to Monitor > Performance Settings > Setup > Automonitor
   b) Set the Interface Availability, Interface Errors and Interface Utilization to "Don't Monitor"
   c) Apply.
   d) Go to Monitor > Performance Settings > Setup > Pollers
   e) Click Create
   f) Select your critical devices (core devices and access devices that are connected to business critical applications).
   g) Select a Polling Interval of 30 minutes.
   h) Add "Interface Errors" and "Interface Utilization".
   i) Uncheck the "Poll all Instances" box.
   j) Next
   k) Select the critical interfaces in your network
   l) Finish

Validate the performance polling

1. Go to Monitor > Performance Settings > Setup > Pollers
2. Click on the Link Ports_Interface Utilization link.
3. Check if your critical links are monitored.
4. If some of the critical links are missing, you can add them manually:
   a) Go to Monitor > Performance Settings > Setup > Pollers

b) Click Create

c) Select your critical devices (core devices and access devices that are connected to business critical applications).

d) Select a Polling Interval of 30 minutes.

e) Add “Interface Errors” and “Interface Utilization”.

f) Uncheck the “Poll all Instances” box.

g) Next

h) Select the critical interfaces in your network

i) Finish

6. Go to Monitor > Dashboards > Monitoring.
7. You should now be able to view the cpu, memory and interface utilization in the portlets.
8. Go to Monitor > Performance Settings > Setup > Pollers
9. In the “Status” column, none of the pollers should show a “with errors” link.

Troubleshooting

Problem	Solution
The pollers are showing a “**with errors**” link.	1. Click on the link to see which MIB objects failed. 2. Take note of the device and MIB object that is causing the error. 3. Go to Monitor > Troubleshooting Tools > Troubleshooting Workflows 4. Open the device 5. Select Tools > SNMP Walk **6.** Enter OID: 1.3.6.1.2.1.2.2.1, and click OK. You should see something like: RFC1213-MIB::ifIndex.1 = INTEGER: 1 RFC1213-MIB::ifIndex.2 = INTEGER: 2 RFC1213-MIB::ifDescr.1 = STRING: "Ethernet0/0" RFC1213-MIB::ifDescr.2 = STRING: "Port-channel1" RFC1213-MIB::ifSpeed.1 = Gauge32: 10000000 RFC1213-MIB::ifSpeed.2 = Gauge32: 1544000 RFC1213-MIB::ifInOctets.1 = Counter32: 1082348318 RFC1213-MIB::ifInDiscards.1 = Counter32: 14928 RFC1213-MIB::ifInErrors.1 = Counter32: 12518 … In this example, the device does not have the ifInOctets, ifOutOctets, ifInDiscards and ifInErrors counters for "Port-channel1", so LMS cannot monitor the Interface Utilization and Interface Errors. 7. For the Interface Utilization, LMS needs the correct ifSpeed,

	ifInOctets and ifOutOctets. **Note:** If the ifspeed is greater than 20,000,000, also check the 1.3.6.1.2.1.31.1.1.1.6 (ifHCInOctets) and 1.3.6.1.2.1.31.1.1.1.10 (ifHCOutOctets) OIDs. LMS uses the ifHCInOctets and ifHCOutOctets counters to calculate the utilization on high speed interfaces to make sure that it does not miss a counter wrap. 8. For the Interface Errors, LMS needs ifInDiscards and ifInErrors. 9. If any of these counters are missing or incorrect, search the cisco.com Bug ToolKit for known device defects.

Manage Faults

Set the LMS server as trap destination

LMS frequently polls the cpu, memory, temperature, fan status, etc. MIB objects to find out if any faults have occurred in the network. As the default polling interval for most of these objects is 4 minutes, it may take a few minutes for an alarm to appear in LMS. To make the alarms immediate, we will now configure the network to notify the LMS server through SNMP traps that a fault has occurred.

1. For snmp v2c, the managed devices need the following configuration:

   # snmp-server host <ip address of the LMS server> <community string>

2. If you are only using SNMP v3 traps, you can skip to the next step "Validate the device discovery". LMS does not support SNMP v3 traps.
3. You can use a Netconfig job to check if all the devices have the LMS server as their trap receiver:
   a) Go to Configuration > Compliance > Compliance Templates > Templates
   b) Click Create
   c) Select the "Routers" and "Switches and Hubs" groups
   d) Enter a name and click Next
   e) Under the Compliance Block, enter the required snmp-server command. For example:

      + snmp-server host 1.1.1.1 public

   f) Click Finish
   g) Go to Configuration > Compliance > Compliance Templates > Direct Deploy
   h) Select the template we just created
   i) Click Deploy
   j) LMS will now check all the device configurations for the existence of the "snmp-server host" command and deploy the command where needed. If you would like LMS to just check for the existence without deploying the command, go to Configuration > Compliance > Compliance Templates > Compliance Check instead of Direct Deploy.
   k) Go to Configuration > Compliance > Compliance Templates > Jobs to check the result of the compliance job.
   l) If any of the deployments failed, add the snmp-server host command manually through the device cli.

Validate the device discovery.

LMS performs a separate device inventory collection to discover the objects that it needs to monitor. We will now check if all the device have been discovered correctly.

1. Go to Admin > Collection Settings > Fault > Fault Monitoring Device Administration
2. All the devices should be listed under "All Known Devices in Inventory Services"

Troubleshooting

Problem	Solution
Fault Monitoring shows devices under "All **Unknown** Devices in Inventory Services"	LMS does not know the device type. 1. Check the Supported Devices Table. 2. If the Supported Devices Table says that you need a device package update, you can install the device packages from Admin > System > Software Center > Device Update.
Fault Monitoring shows devices under "All **Questioned** Devices in Inventory Services"	Either LMS was not able to resolve the device hostname, the device was ICMP unreachable or SNMP unreachable. 1. Click on the device name (do not check the checkbox, click on the name itself) and check the Error Code. 2. Ping the device 3. Check the name resolution: **# nslookup <device ip address>** **# nslookup <device hostname>** 4. Go to Inventory > Job Browsers > Device Credentials Verification 5. Check the snmp read only credentials
Fault Monitoring shows devices under "All **Learning** Devices in Inventory Services"	LMS has started the discovery, but the discovery is not finished yet. If the device is stuck in the "learning" state, a) manually delete the device from Inventory > Device Administration > Add / Import / Manage Devices (you will lose all the historic config archive, syslogs etc.) or b) disable and enable the Fault Management from Admin > System > Device Management Functions (you will lose all the custom polling, thresholds, etc).

Discover the Topology

Start the Data Collection

1. Go to Admin > Collection Settings > Data Collection > Data Collection Schedule
2. Click Start

Validate the Data Collection.

1. Go to Configuration > Topology
2. Your browser may prompt you to install the java plugin. Install the plug-in and restart your browser.
3. Go to Configuration > Topology again
4. Your browser may prompt you to download a file. Download the file.
5. Topology Services should now open.
6. Open Network Views
7. Right click on "Layer 2 View" and select Display View
8. Topology Services should show all your devices with a green icon and the lines between the devices should be full black.
9. Select "Unconnected Device View" and select Display View
10. Topology Services should not show any devices in the "Unconnected Device View".

Troubleshooting

Problem	**Solution**
I'm getting a "**Cannot connect to ANI Server**" error when I open Topology Services	1. Check the name resolution on the client. The client should be able to resolve the LMS server hostname and IP address. 2. Try opening Topology Services in a browser on the LMS server itself. If you only see the error on the clients, but not the server, a firewall or access list may be blocking the communication ports between the client and server.
LMS keeps prompting me to "**Please launch Topology Services again to work properly**".	Clear the java cache: 1. Go to Control Panel > Java 2. Under "Temporary Internet Files", click Settings 3. Click "Delete Files" > OK 4. Restart your browser and try again
You got an error "**ANI Server is down**"	1. On the server, verify that status of ANIServer is :Running with busy flag set": **pdshow ANIServer** 2. The ANIServer.properties file could be corrupted. Try to restore it:

	a) Stop the ANIServer process: **pdterm ANIServer** b) Copy ANIServer.properties.orig ANIServer.properties. Edit the ANIServer.properties: **DEVICESROOT=.** Into **DEVICESROOT=NMSROOT\\campus\\lib\\classpath** (replace NMSROOT with the correct directory where NMS is insralled. Default location is C:\PROGRA~1\CSCOPX. Note the use of two backslashes in the DEVICEROOT properties.) c) Start the ANIServer: **pdexec ANIServer**
The "Layer 2 View" does not show my **links**.	Make sure that CDP is enabled on the devices. LMS uses CDP to discover the links. 1. Connect to the device and check if it has any neighbors: **# show cdp neighbors** 2. Connect to each of these neighbors and make sure that they are sending cdp hello packets: **(config)#cdp run** **(config)#interface <interface that connects to the unconnected device>** **(config-if)#cdp enable**
The "Layer 2 View" does not show my **devices.**	Check if your devices are hiding in the "Unconnected Device View".
My devices are listed in the "**Unconnected Device View**"	"Unconnected Device" means that LMS did not discover any neighbors on the device that LMS manages. 1. Connect to the device and check if it has any neighbors: **# show cdp neighbors** 2. Connect to each of these neighbors and make sure that they are sending cdp hello packets: **(config)#cdp run** **(config)#interface <interface that connects to the unconnected device>** **(config-if)#cdp enable**
My device icon is **red**	The device is unreachable or LMS does not have the correct SNMP read-only credentials.

	1. Go to Inventory > Job Browsers > Device Credentials Verification 2. Run a credentials verification job.
My device icon has a green **question mark**	LMS was able to connect to the device, but the device type is not recognized. Check if the device is listed in the supported device list: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/device_support/table/lms41sdt.html

Discover the Hosts

Start the Host Acquisition

1. Go to Admin > Collection Settings > User Tracking > Acquisition Schedule
2. Click Start

Validate the Host Acquisition

1. Go to Reports > Inventory > User Tracking > All Host Entries
2. Select Layout: All Columns
3. Click Submit
4. The report should show all the host Hostnames, IP addresses, MAC addresses and should show where your hosts are connected to the network.

Troubleshooting

Problem	Solution
The Host **MAC addresses** are not discovered.	1. Make sure that the switch that is directly connected to the host has been added to Inventory > Device Administration > Add / Import / Manage Devices. Note: LMS only supports Cisco access switches. 2. Connect to the switch cli and check if the host is listed in the switch forwarding table: **# show mac-address-table** 3. If the host MAC address is not listed, ping the host to make sure it is active. 4. Take note of the port where the host is active 5. Go to Reports > Switch Port > Ports > Port Attributes 6. Select the switch that is directly connected to the host 7. Run the report 8. Look up the port where the host is active and verify that the isTrunk state is false. Note: LMS ignores any host that is connected to a trunk as it assumes that the port is part of the backbone. 9. If the isTrunk state is true, go to Admin > Collection Settings > User Tracking > Acquisition Configuration in Trunk and enable the "Enable End Host Discovery on all Trunks" option or add the port to the "Enable End Host Discovery on selected Trunk(s)" list. 10. Go to Admin > Collection Settings > User Tracking > Acquisition Schedule

	11. Run a fresh acquisition.
The Host **IP Addresses** are not discovered.	1. Make sure that the Default Gateway of the host has been added to Inventory > Device Administration > Add / Import / Manage Devices. Note: LMS only supports Cisco default gateways. 2. Connect to the Default Gateway cli and check if the host is listed in the ARP table: **# show ip arp** **Note**: LMS does not support show arp vrf 3. If the host IP address is not listed, go to Admin > Collection Settings > User Tracking > Ping Sweep and make sure that the host subnet has been added to the "Selected Sources". Then run a fresh acquisition. 4. Go to Reports > Inventory > User Tracking > All Host Entries 5. Select Layout: All Columns 6. Click Submit 7. The report should list the Default Gateway in the "Associated Routers" column. 8. If the Default Gateway is not listed, delete and read the Default Gateway from Inventory > Device Administration > Add / Import / Manage Devices. Then run a fresh Data Collection and Host Acquisition
The **Host Names** are not discovered.	1. Make sure that the LMS server can resolve the host IP address into a hostname: **# nslookup <host ip address>** 2. Go to Admin > Collection Settings > User Tracking > Acquisition Schedule 3. Run a fresh acquisition.
The **User Names** are not discovered.	1. Make sure that the utlite.exe script is running on the host as described in the utlite installation guide: http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/4.1/user/guide/admin/appendixcli.html#wp1032284 2. Make sure nothing is blocking the 16236/tcp port between the host and LMS server. 3. Use the LMS Packet Capture tool to check if the host is sending its username. The username is sent in clear text.
The hosts reports show false **duplicates**	1. If the duplicate host is a DHCP client, go to Admin > Collection Settings > User Tracking > Acquisition Settings and enable the "Enable User Tracking for DHCP Environment" option.

	Note: Make sure that the LMS server can ping the hosts when using this option. The DHCP discovery relies on ICMP to learn which IP addresses are new and which IP addresses can be ignored. 2. Connect to the switch cli and check if the forwarding table shows the same duplicates: **# show mac-address-table** 3. LMS uses the bridge tables as source, so any duplicates here will also be shown in the Usertracking reports. 4. Run a Usertracking report and check the "Last Seen" column. 5. If the duplicate shows an old "Last Seen" date, go to Admin > Network > Purge Settings > User Tracking Purge Policy and decrease the "Delete entries older than" values. 6. Run a fresh acquisition.

Maintain the LMS server

Now that we've configured our LMS server, we will want to make sure that it runs correctly for some time. Here are some steps that will make sure that the server does not reach its capacity limit and that we have a backup in case things go wrong.

Schedule the Backup

1. Go to Admin > System > Backup
2. Enter Backup Directory: C:\Progra~1\CSCOpx\backup

Note: Do not store the backup in C:\. This will result in errors during the restore.

3. Click OK
4. Select Frequency: Daily
5. Enter Generations: 7

Note: the backup requires twice the amount of space that is used in your CSCOpx directory (once the amount for the temporary tar file and once the amount for the backup itself). Reduce the number of generations if needed.

6. Click Apply

Validate the Backup

1. Go to Admin > System > Backup
2. Enter Backup Directory: C:\Progra~1\CSCOpx\backup
3. Click Apply
4. Open the backup log in a text browser:
5. # notepad C:\Program Files\CSCOpx\log\dbbackup.log
6. The last line in the dbbackup.log should be:

[<date><time>] Backup completed: at [<date><time>]

Troubleshoot the Backup

Problem	**Solution**
The backup does not start	1. Open a DOS box and check with the at command if the backupsch.bat script is listed in the Windows scheduler: **# at** Status ID Day Time Command Line---------- 1 Each M T W Th F S Su 5:00 AM C:\PROGRA~1\CSCOpx\objects\logrot\logrotsch.bat 2 Each M T W Th F S Su 12:00 AM C:\PROGRA~1\CSCOpx\conf\backupsch.bat If the backupsch.bat is not listed, you can manually edit the backupsch.bat and

	add it to Administrative Tools > Task Scheduler 2. Check if the backup is locked: **# dir C:\PROGRA~1\CSCOpx\backup.LOCK** The LMS backup creates a backup.LOCK in C:\PROGRA~1\CSCOpx to make sure that no two backups are run at the same time. If the previous backup did not create this backup.LOCK file, then no new backup can be performed. Delete the backup.LOCK if no backup is currently running.
The backup runs slow	LMS schedules the backup in the Windows Scheduler with priority 7. On large scale deployments this can cause the backup to take more than 24 hours. You can increase the priority in the Windows Scheduler: 1. Go to the Administrative Tools > Task Scheduler 2. Right click on the task that runs the backupsch.bat and "export" it. 3. Edit the <task>.xml file that you just exported. 4. Change the line **<Priority>7</Priority>** into: **<Priority>4</Priority>** 5. Save the <task>.xml. 6. Delete the task that LMS created. 7. Import the task from the XML file

Schedule the Config Archive Purge

LMS stores a new configuration file for every configuration change it detects in **CSCOpx\files\rme\dcma\devfiles.** If you have a lot of devices and a lot of configuration changes, these config files can quickly fill up your file system. To make sure that LMS does not fill up our file system, we will now configure the config archive purging.

1. Go to Admin > Network > Purge Settings > Config Archive Purge Settings
2. Select Enable
3. Click Change
4. Schedule the purge job daily at 7am
5. Check the “Maximum versions to retain: 5” box
6. Check the “Purge versions older than: 30 days” box
7. Click Apply

Schedule the Config Job Purge

Every Inventory Collection, Configuration Archive, Software Archive etc. that LMS performs, results in a new job. Over the years, this can easily add up to thousands of jobs. To make sure that the Job Browser won’t take too long to load, we will now configure the job purging.

1. Go to Admin > Network > Purge Settings > Config Job Purge Settings
2. Check the "Jobs/Archives" box to select all the jobs.
3. Click Schedule
4. Schedule the purge job daily at 7:30am
5. Enter Purge records older than: 7 days
6. Click Done

Schedule the Syslog Purge

LMS first adds each syslog to the CSCOpx\log\syslog.log file before it adds them to its CSCOpx\databases\rmeng\SyslogFirst.db, SyslogSecond.db and SyslogThird.db databases. As the managed devices can sometimes send hundreds of syslogs per second, the syslog.log and syslog databases can quickly reach their capacity limits. We will now make sure LMS purges the old syslogs.

1. Go to Admin > Network > Purge Settings > Syslog Force Purge
2. Enter Purge records older than: 7 days
   Note: do not set the purge to more than 13 days. LMS rotates the syslog database updates between the SyslogFirst.db, SyslogSecond.db and SyslogThird.db databases every 7 days. If you use a purge that is greater than 13 days, all three databases will be used at once and you will not be able to reclaim the database space with the CSCOpx\MDC\tomcat\webapps\rme\WEB-INF\debugtools\dbcleanup\DBSpaceReclaimer.pl script.
3. Make sure the job is schedule the job to run daily at 1am
4. Click Save
5. Go to Admin > System > Log Rotation
6. Click Add
7. Make sure the CSCOpx\log\syslog.log file is added
8. Click Schedule
9. Schedule the job to run daily at 5am.
   Note: do not check the "Restart Daemon Manager" box. Only the stdout.log log rotation requires a restart. However, tomcat has its own log rotation so there should be no need for this.

Schedule the VRF lite purge

1. Go to Admin > Network > Purge Settings > VRF Lite Purge Settings
2. Check the job purge box
3. Enter Purge Jobs older than 1 days
4. Click Save