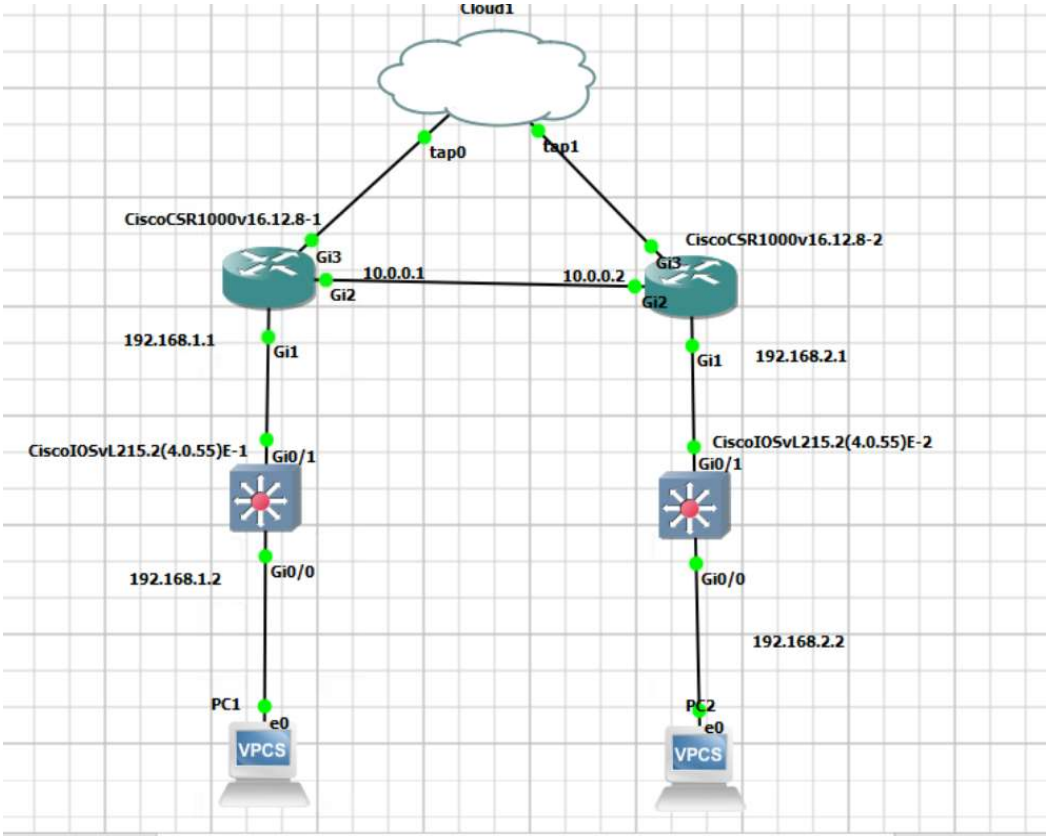
**OPEN NMS LAB (11-07)**

**Network topology:**




**Step 2 -**
**• Assign IP address to PC1 (192.168.1.2) and PC2 (192.168.2.2)**

PC1:
IP 192.168.1.2/24 192.168.1.1
Show IP
PC2:
IP 192.168.2.2/24 192.168.2.1
Show IP

**Step 3-**
**• Assign the IP address to R1 Gi1 (192.168.1.1) , Gi2 (10.0.0.1) and R2 Gi1 (192.168.2.1), Gi2 (10.0.0.2)**

**Router 1:**
Int gi1 Int gi 1
Ip address 192.168.1.1 255.255.255.0 ip address 192.168.2.1 255.255.255.0
No shut no shut
**Router 2:**
Int gi2 int gi 2
Ip address 10.0.0.1 255.0.0.0 ip address 10.0.0.2 255.0.0.0
No shut no shut

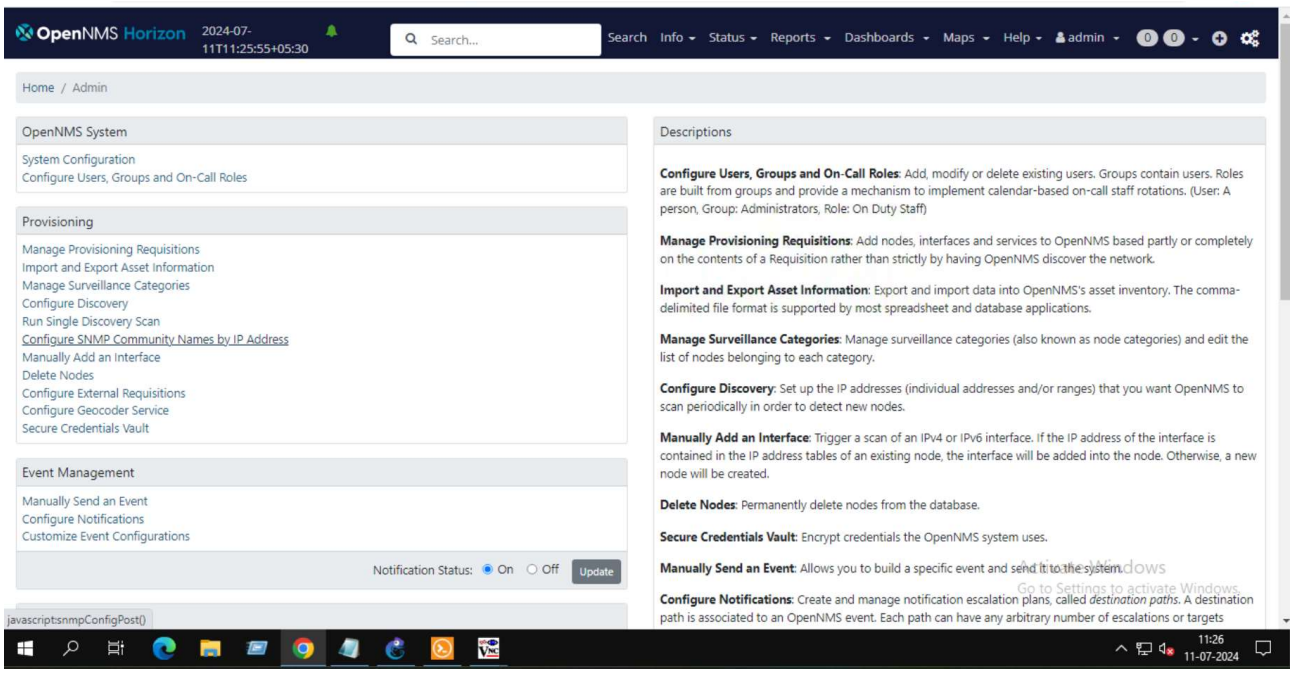
**Step 4:**
**• Run the OSPF protocol and advertise the routes**
**Router 1**
Router ospf 10
Network 192.168.1.0 0.0.0.255 area 1
Network 10.0.0.0 0.0.0.255 area 1

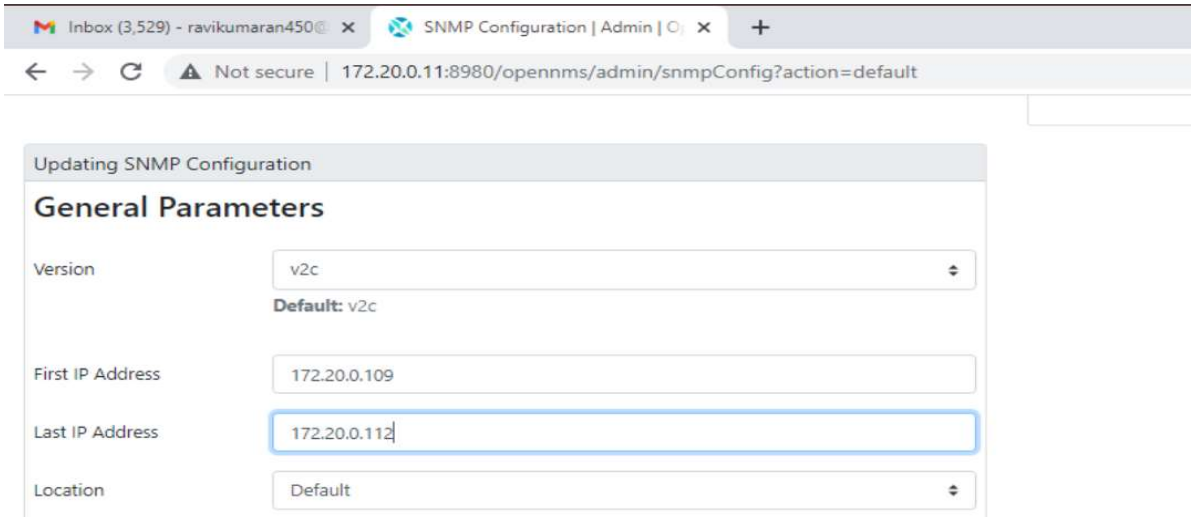
**Router 2**
Router ospf 10
Network 192.168.2.0 0.0.0.255 area 1
Network 10.0.0.0 0.0.0.255 area 1

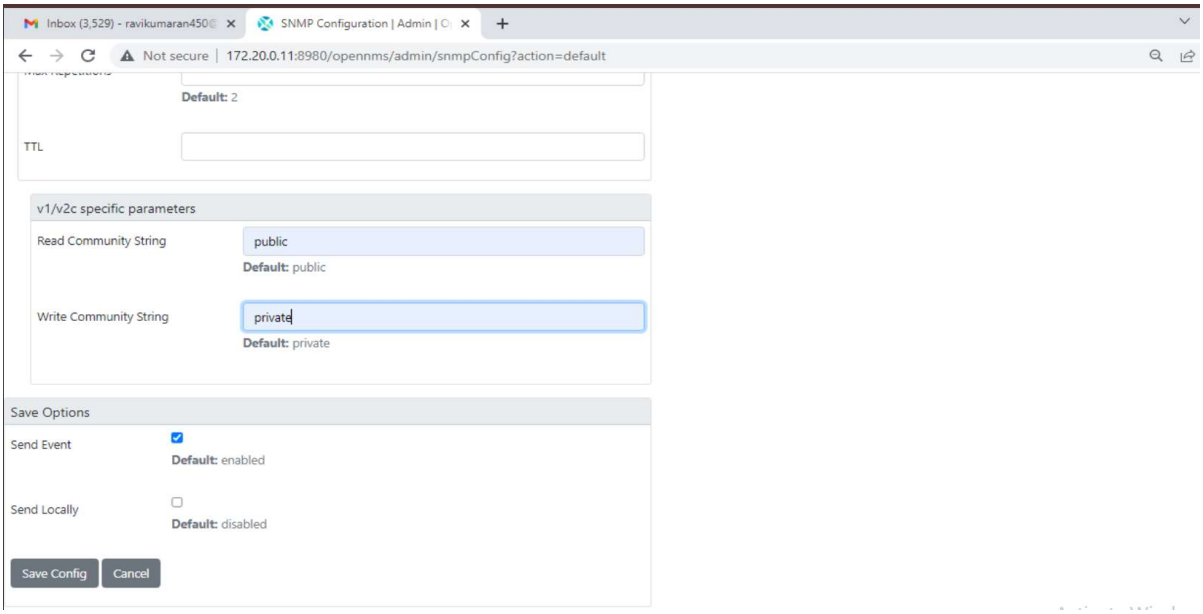
**Step 5:**
**• Configure the SNMP in both the router R1 and R2**
snmp-server community public ro
snmp-server community private rw
snmp-server enable traps
snmp-server host 172.20.0.11 traps version 2c public udp-port 1162
snmp-server manager
Show snmp host

**Save the configuration**
Wr

**Node Discovery on Open NMS**

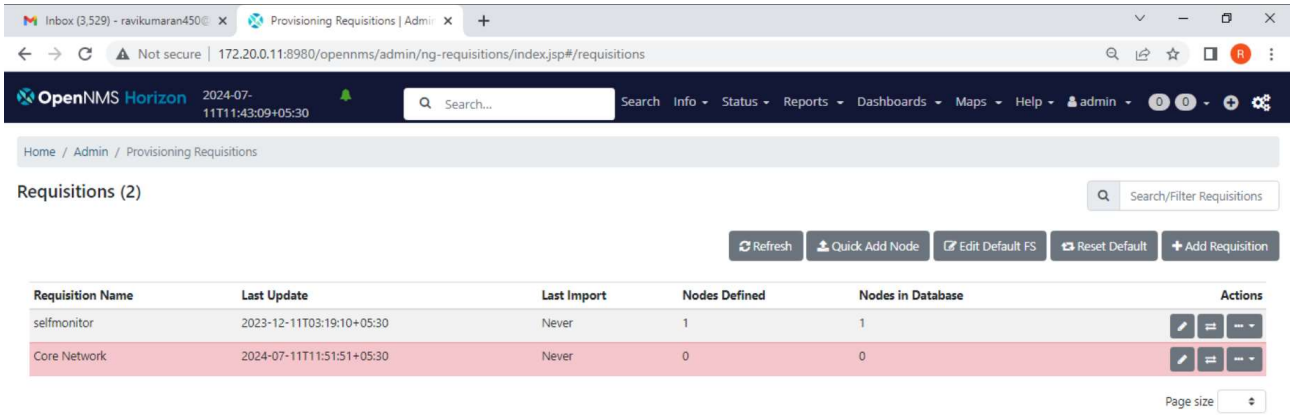


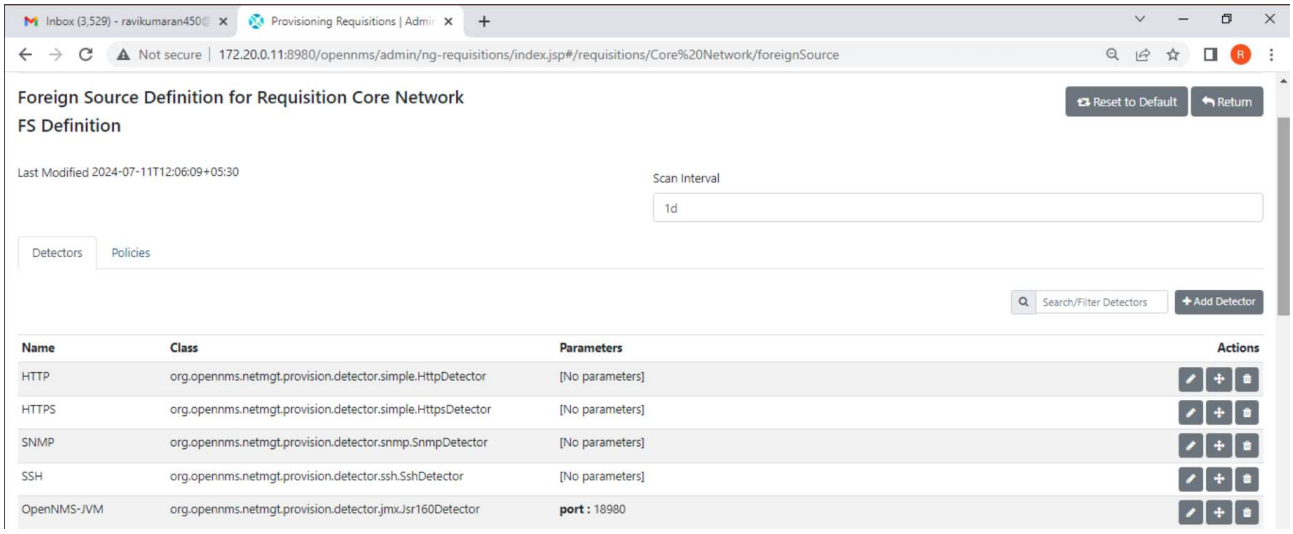


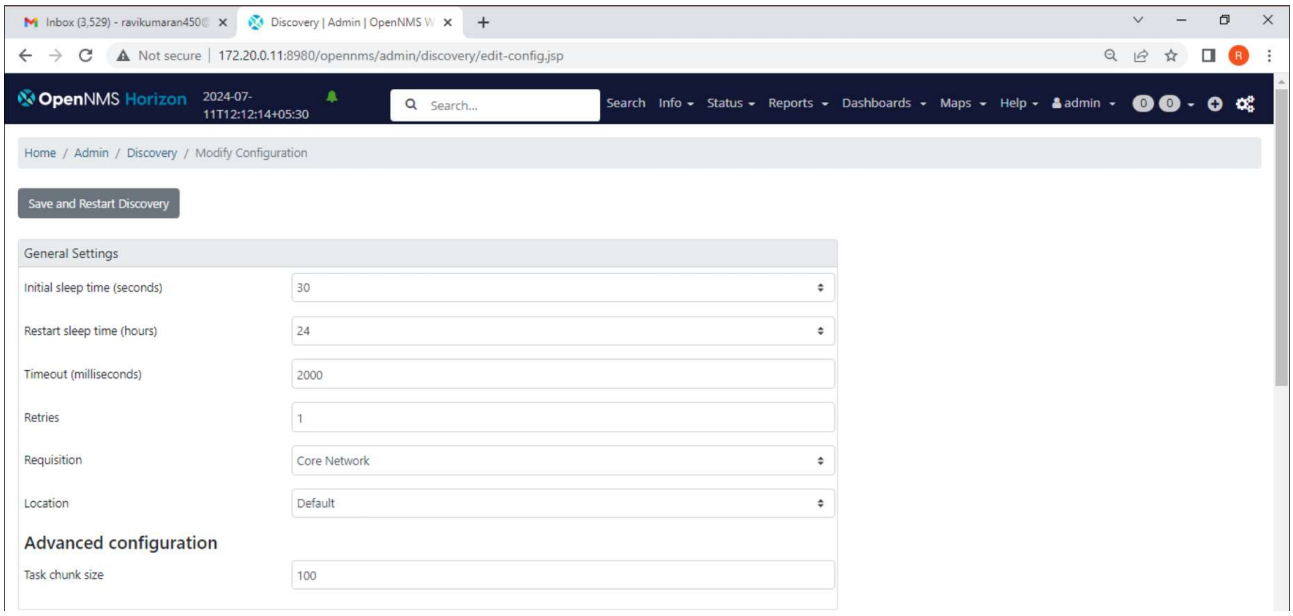

- **Home/admin/provisioning requisition**
- **Add requisition**

**Edit the Core network requisition and delete the source definition which are not needed like DNS, FTP, IMAP, ICMP, LDAP, NRPE, POP3,SMTP,WS-MAN**

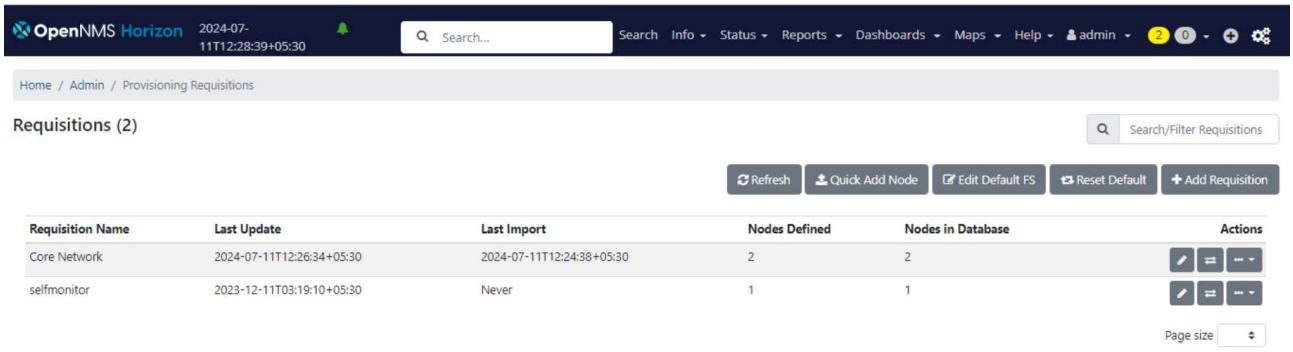



**Discovery configuration to discover the Router 1 & Router 2**

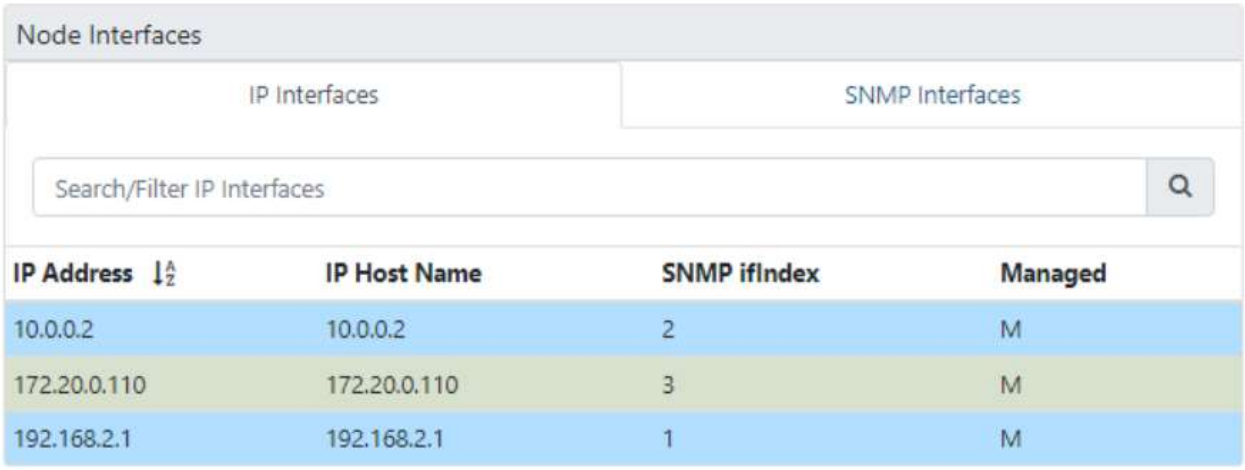


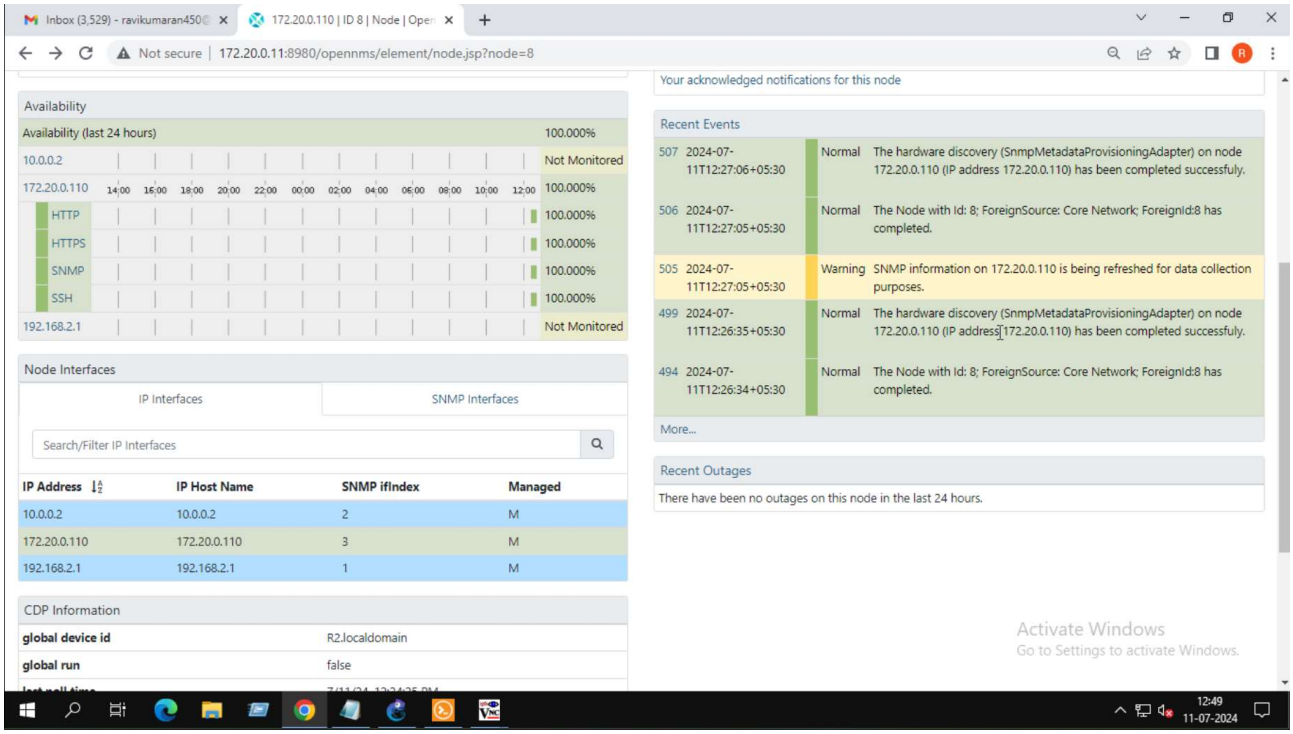
## Sync the discovered nodes:



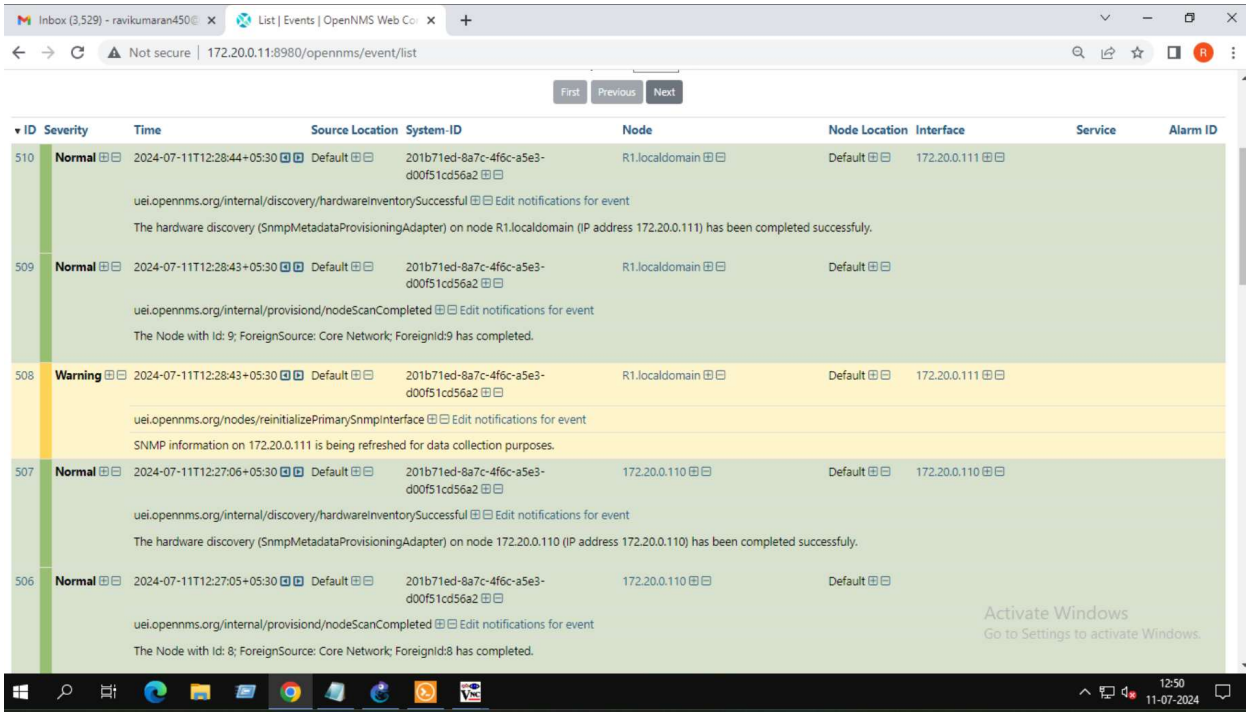

## Node Management on Open NMS

## Go to info -→ nodes → select node

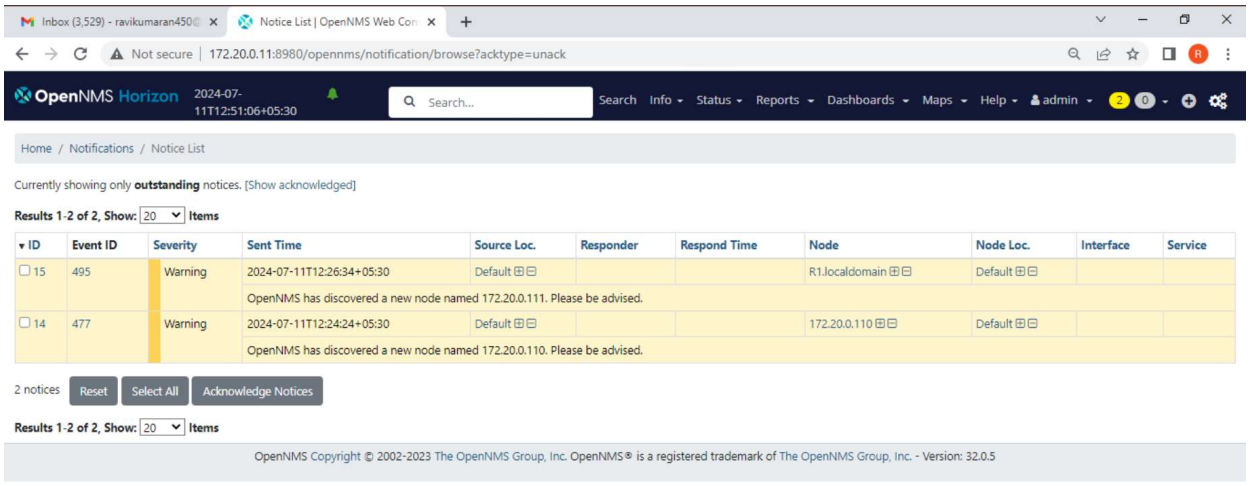


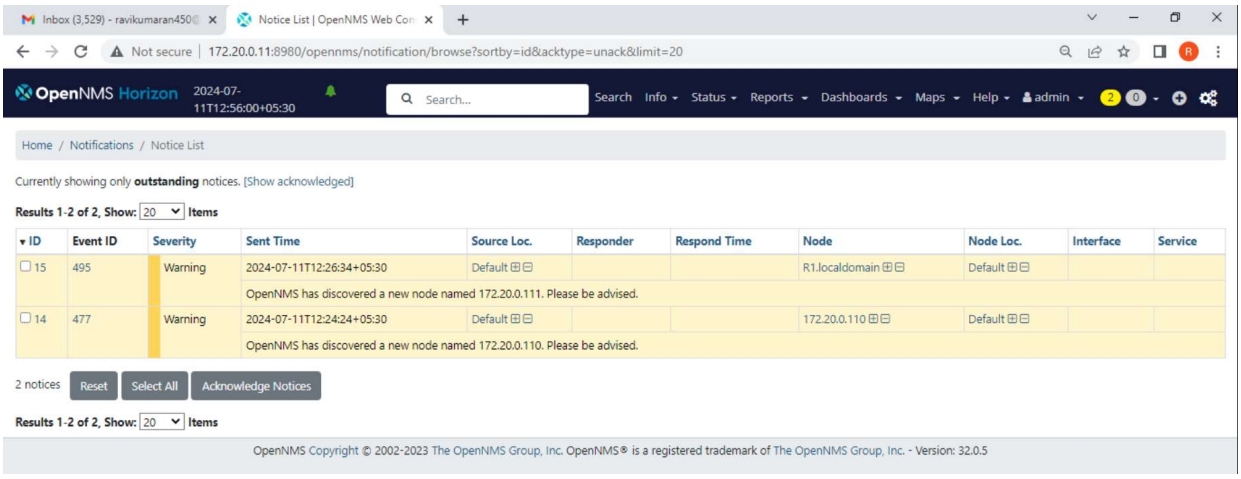
## Go to Status -→ Events → All Events]



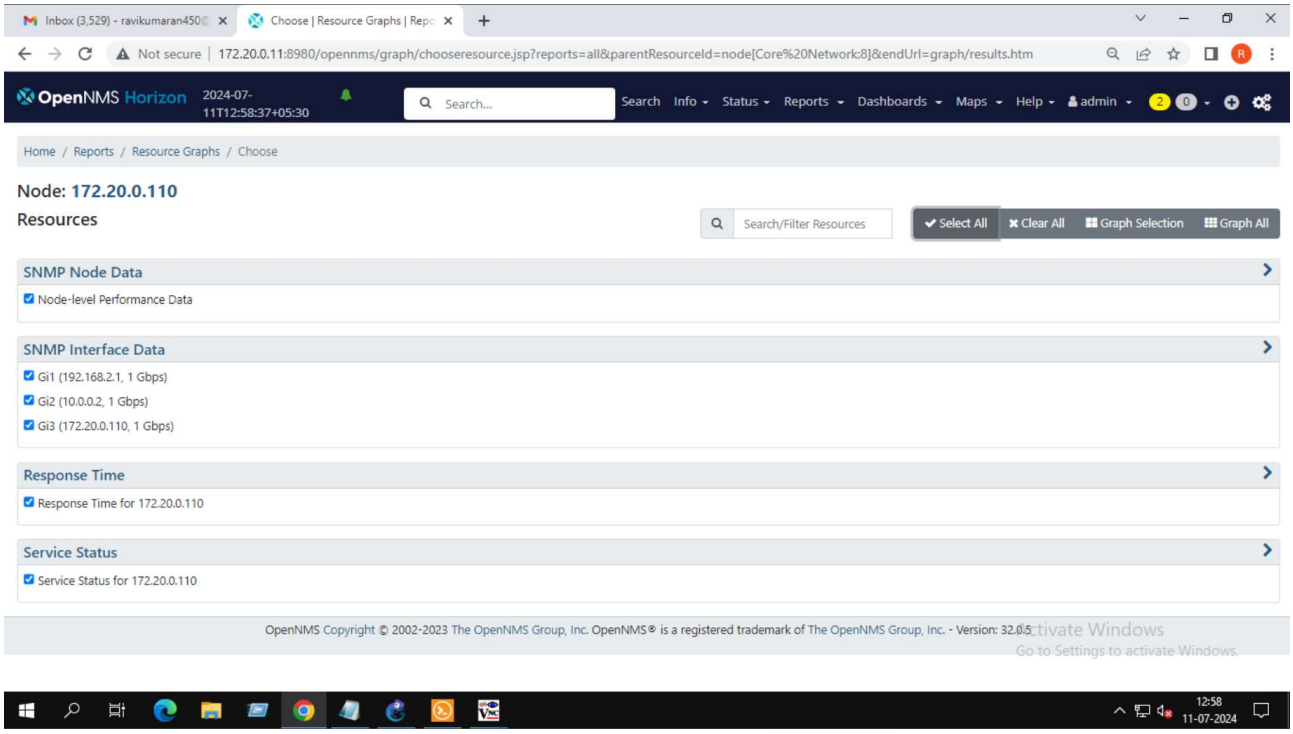

## Go to Status → Notifications → All outstanding notices and acknowledges notices



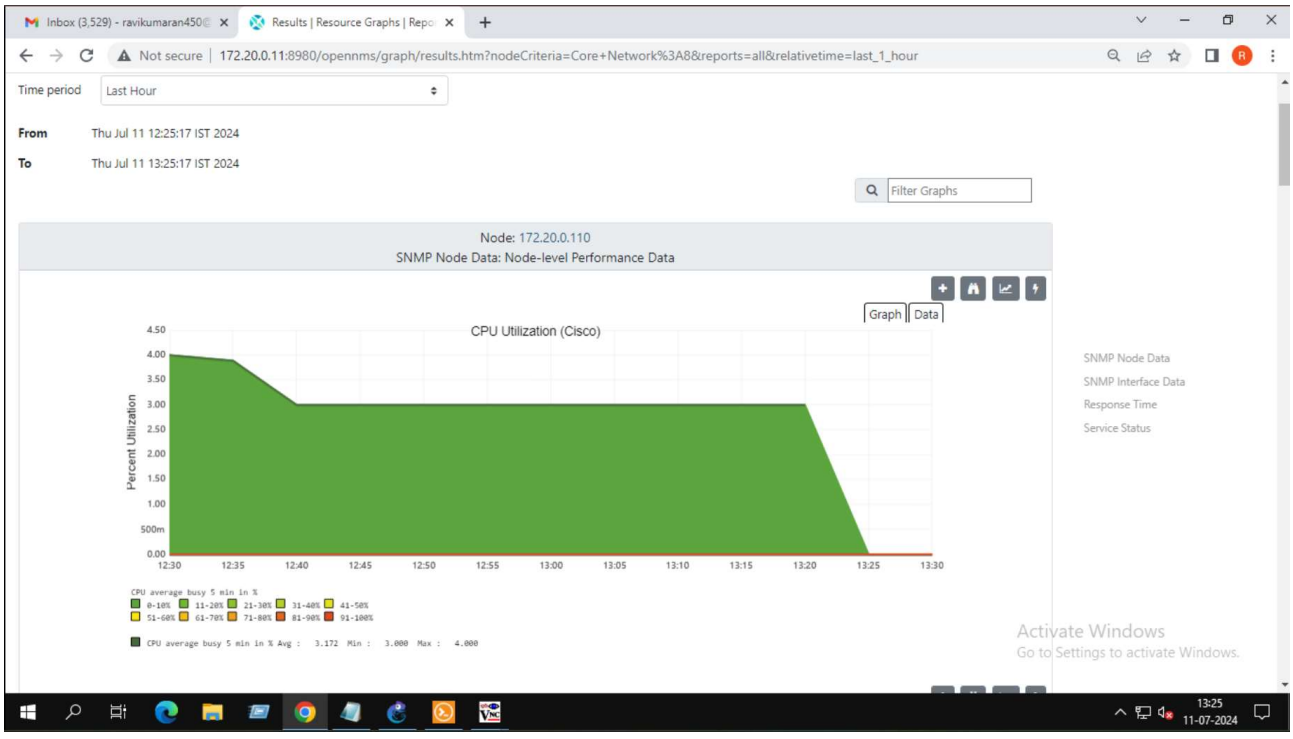

## Go to Status → Notifications -→ all acknowledged notices

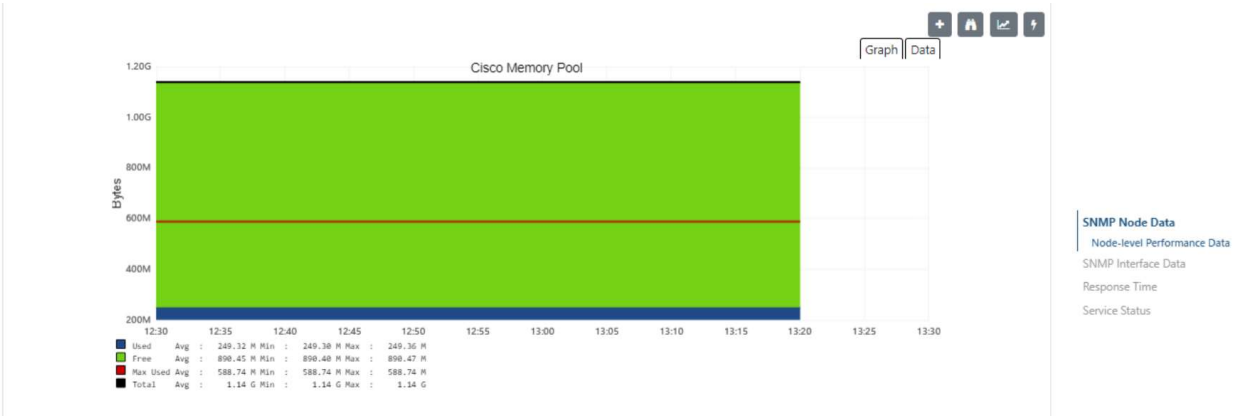


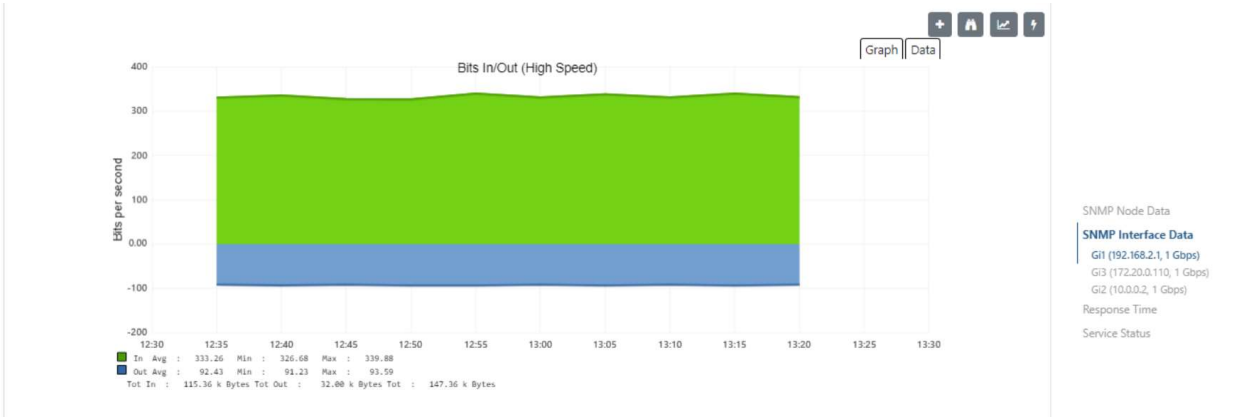
## Go to Reports -→ Resource Graphs -→ select Node and select all



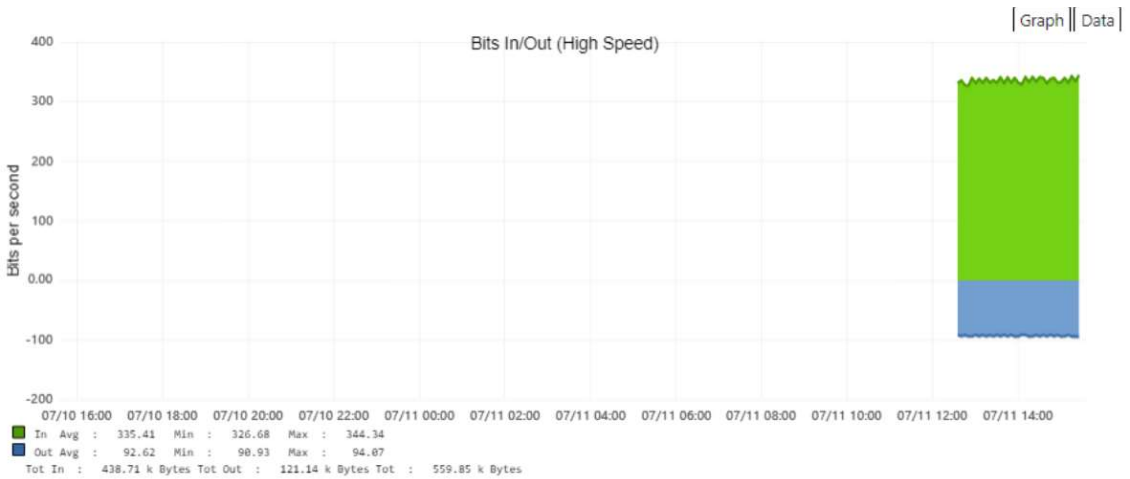

## Click on Graph Selection and select time period last hour






**Ping PC1 to PC2 and observe more packets bits in Out**

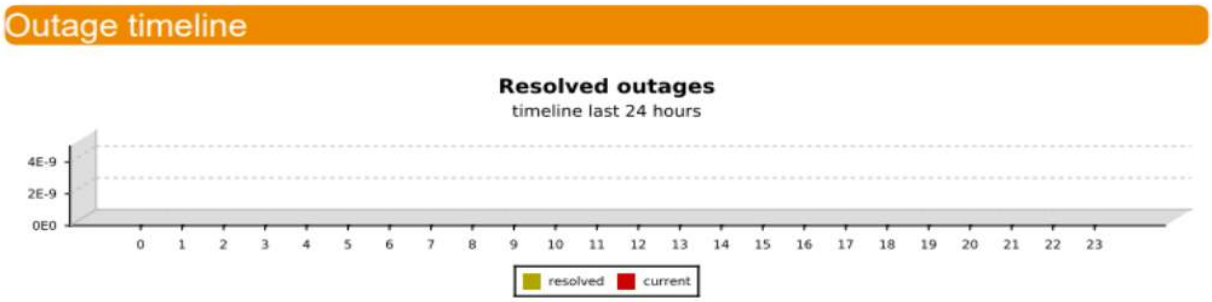


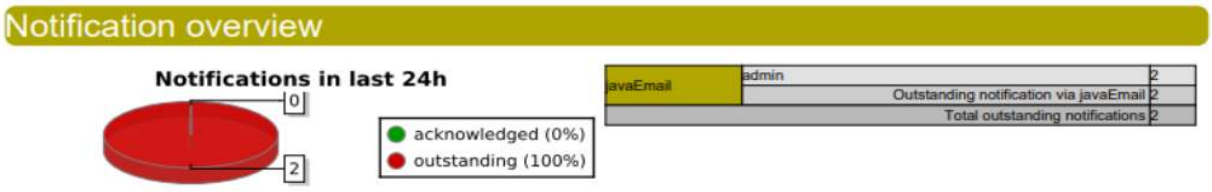

Graph | Data

Raw values

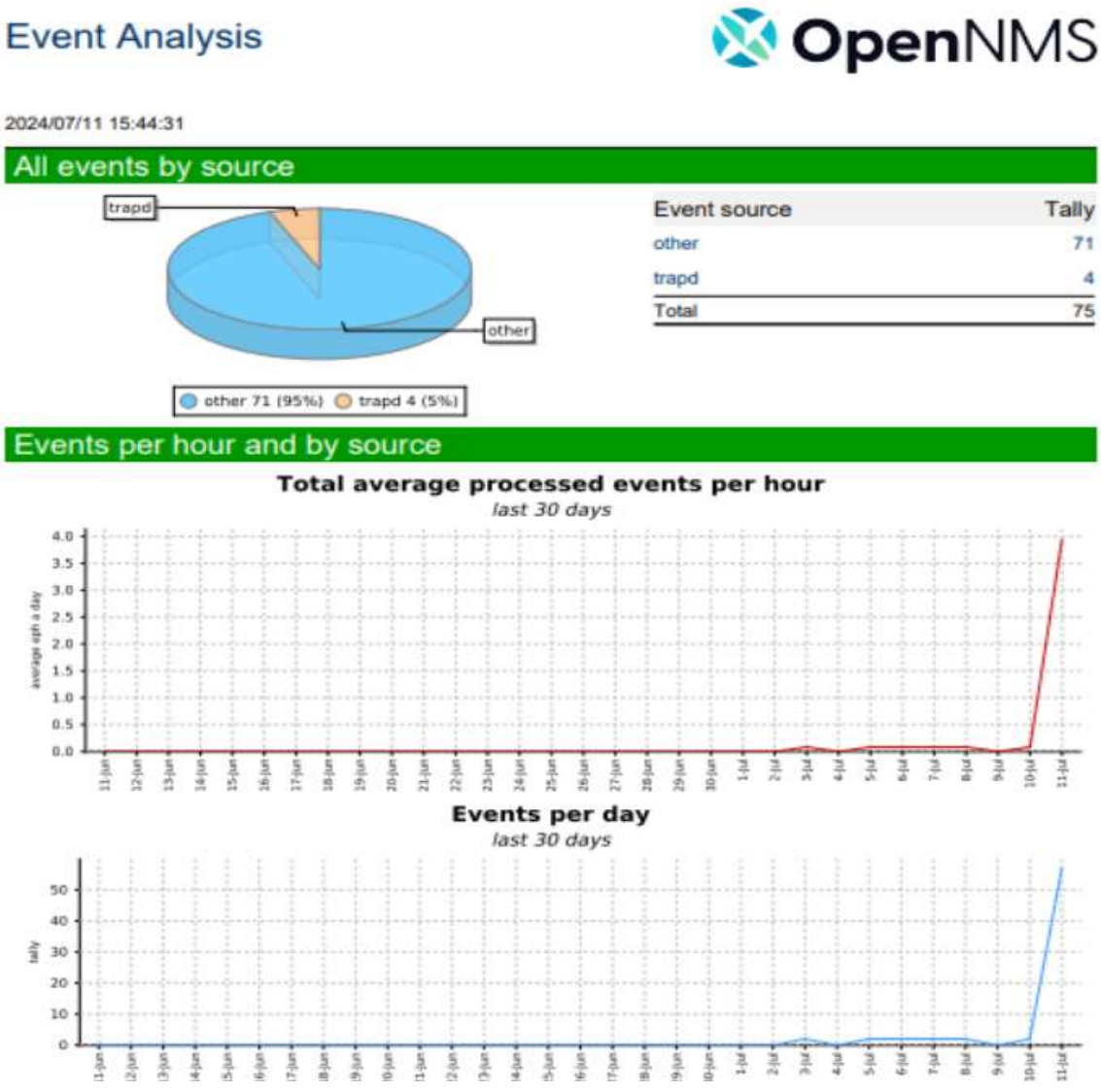
| Date/Time | In | Out |
|---|---|---|
| Thu Jul 11 15:35:00 2024 | NaN | NaN |
| Thu Jul 11 15:30:00 2024 | NaN | NaN |
| Thu Jul 11 15:25:00 2024 | 344 | -94.1 |
| Thu Jul 11 15:20:00 2024 | 334 | -93.8 |
| Thu Jul 11 15:15:00 2024 | 343 | -93.9 |
| Thu Jul 11 15:10:00 2024 | 332 | -91.3 |
| Thu Jul 11 15:05:00 2024 | 340 | -93.5 |
| Thu Jul 11 15:00:00 2024 | 333 | -93.9 |
| Thu Jul 11 14:55:00 2024 | 332 | -91.3 |
| Thu Jul 11 14:50:00 2024 | 340 | -93.5 |
| Thu Jul 11 14:45:00 2024 | 338 | -91.0 |

**Go to Reports → Dashboard Reports → Early Morning report**
**Check Outages, Alarm, Notifications and events summary reports..**



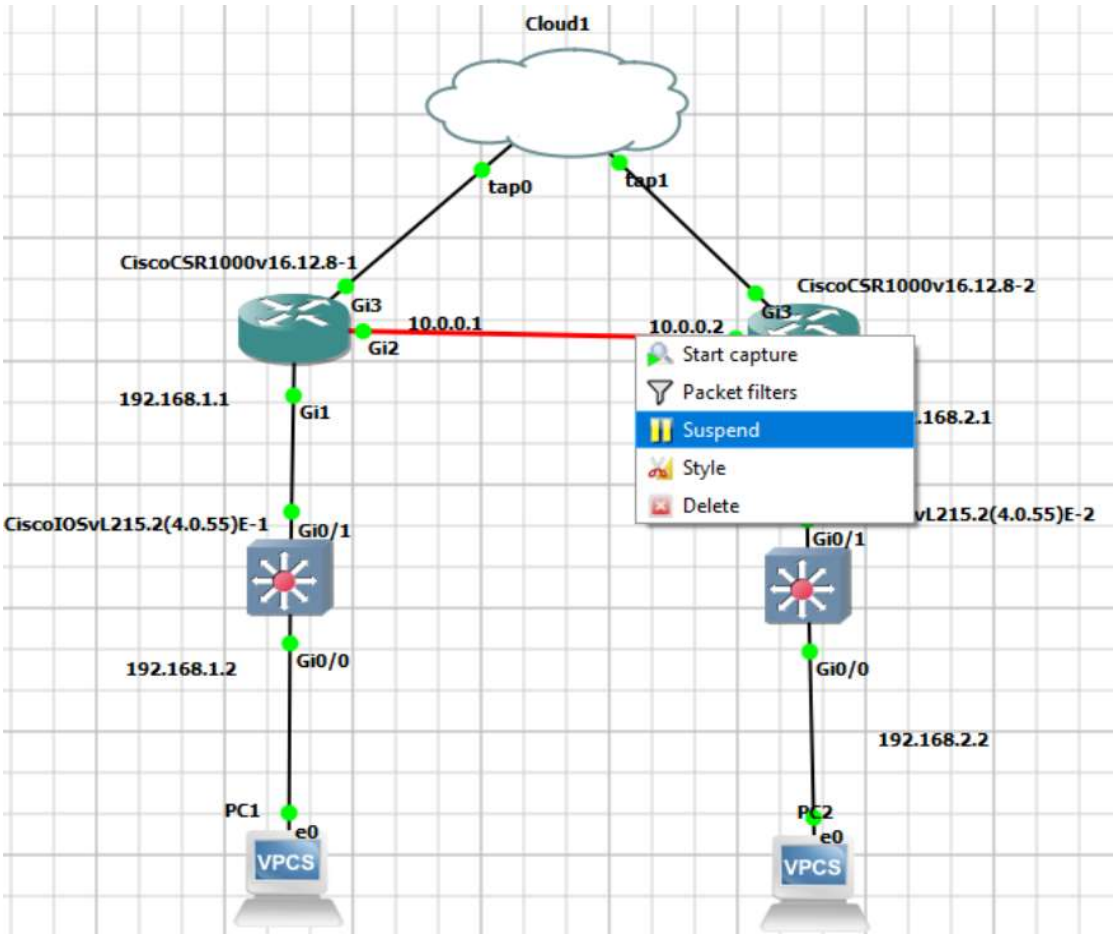




**Go to Reports → Dashboard Reports → Event analysis report**
**Validate the event based on source and hour**

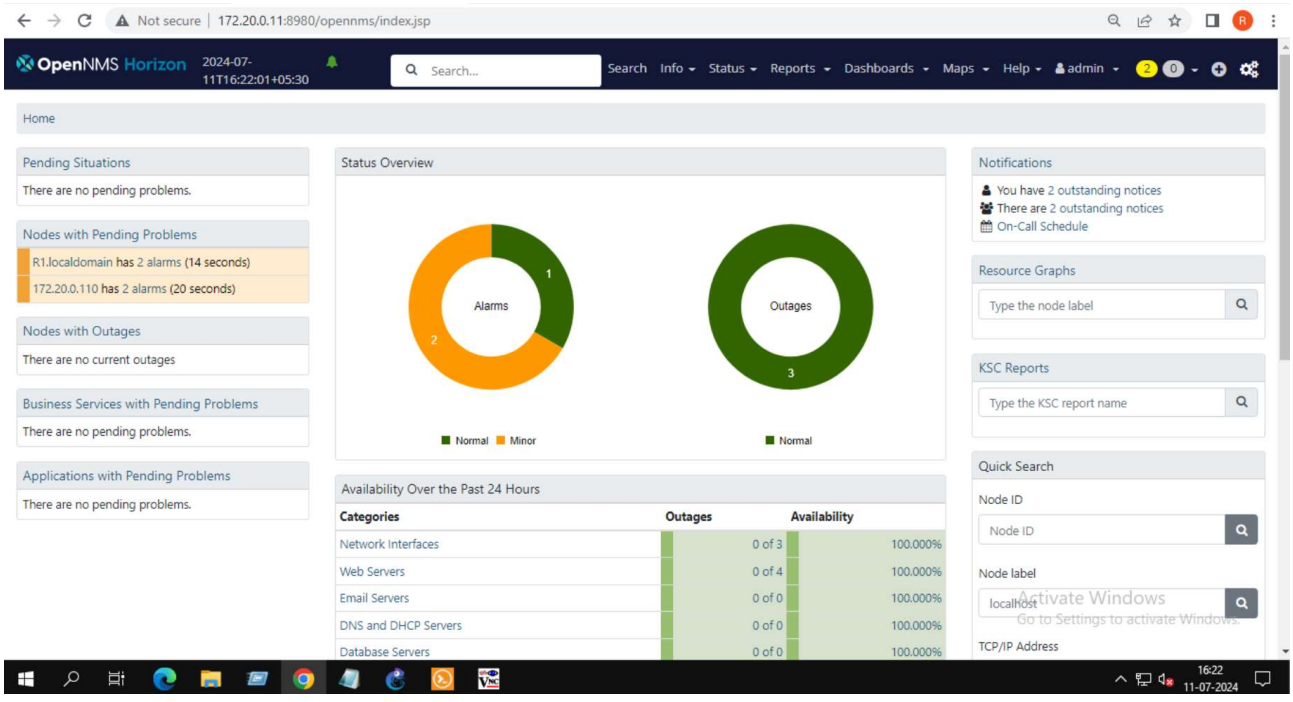


## Generate the SNMP Traps

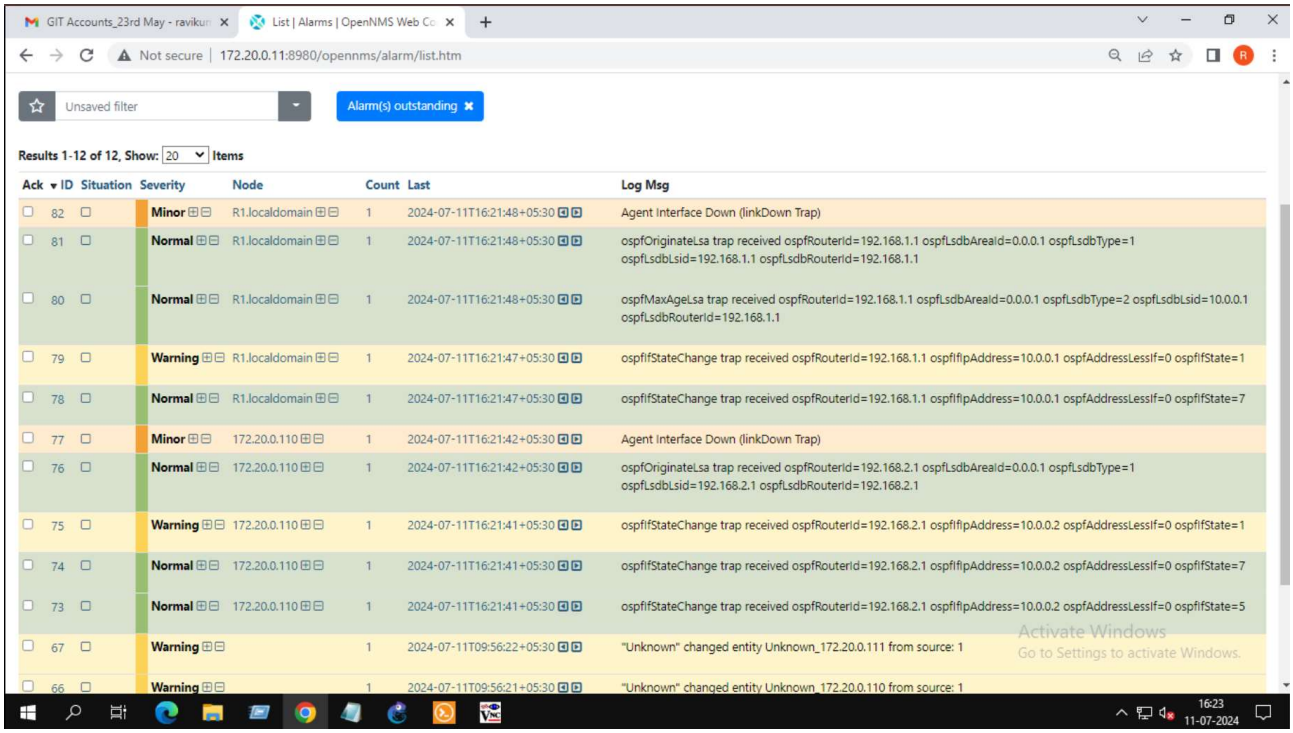
Generate the SNMP traps via suspend the link between Router 1 and Router 2, it will generate the SNMP alarms for link down and OSPF state change traps



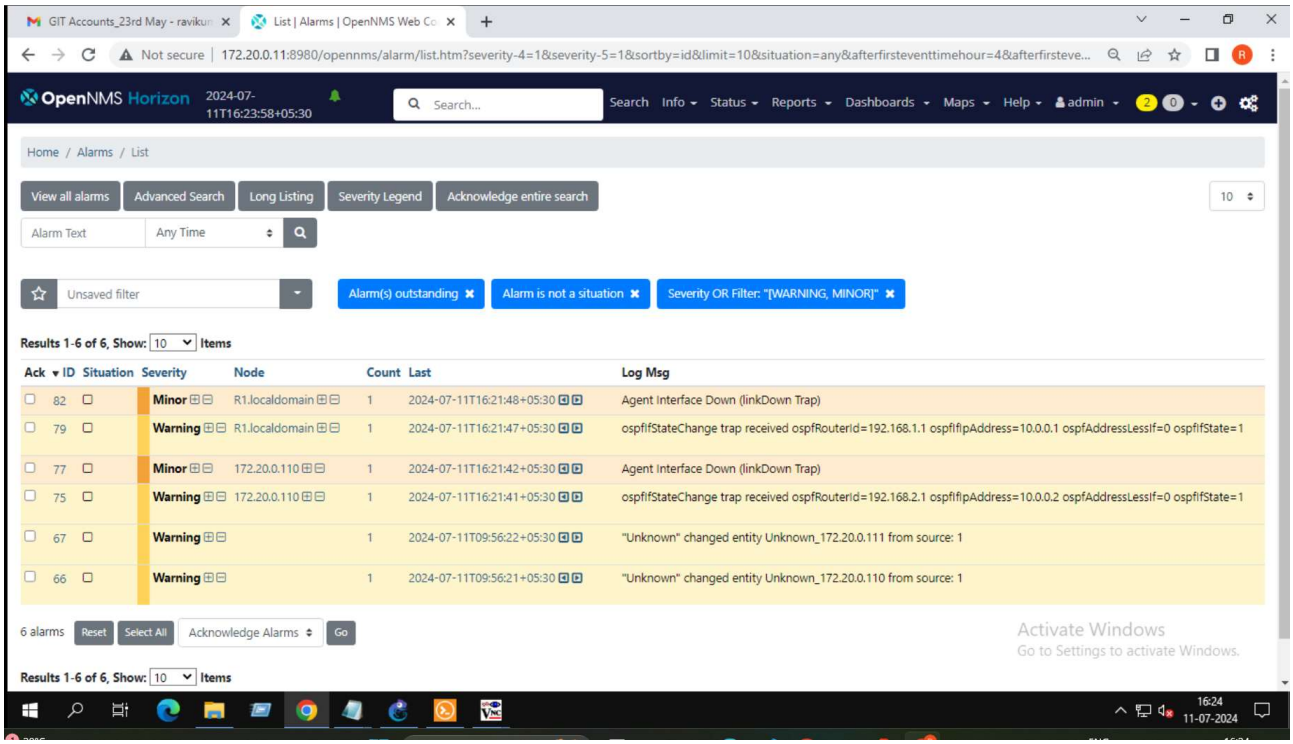

## Dashboard View:



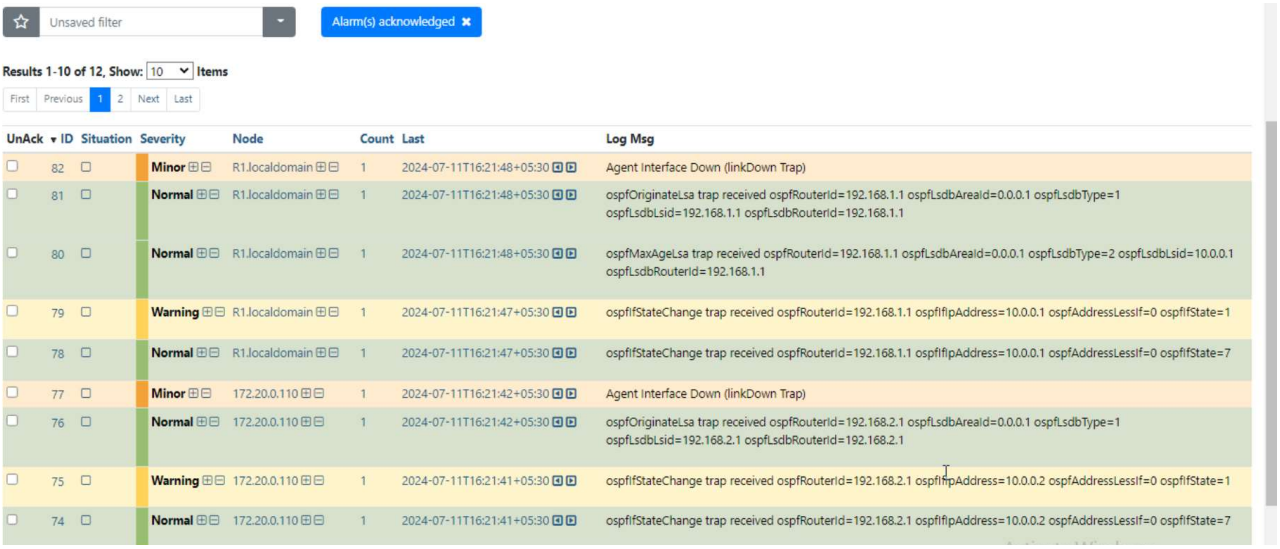
**Check the alarms in NMS , Interface down and OSPF state change alarms would be appeared on NMS.**



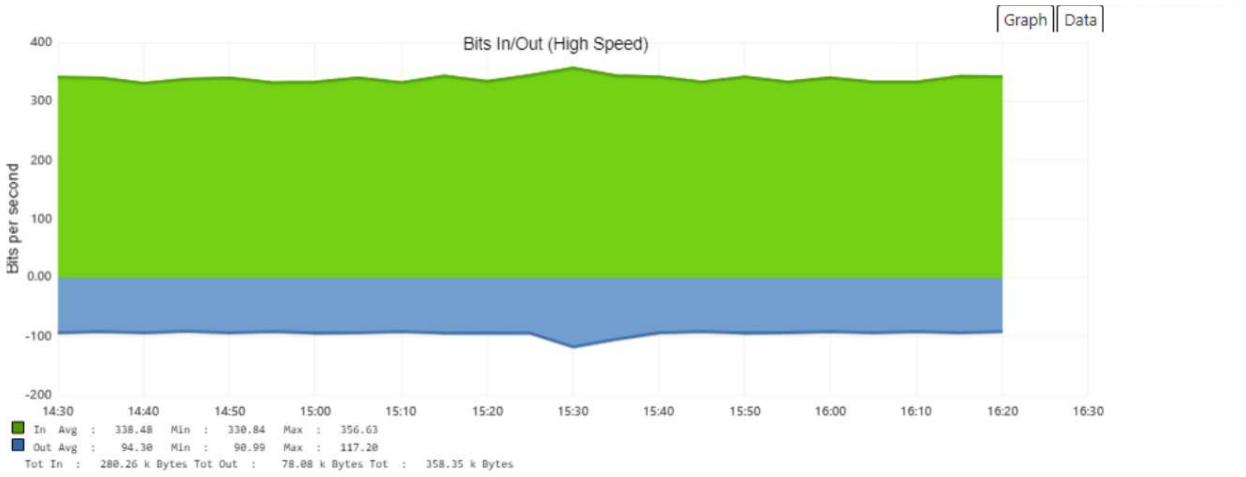

**Click on Advance alarm search and select Minor and Warning alarm**



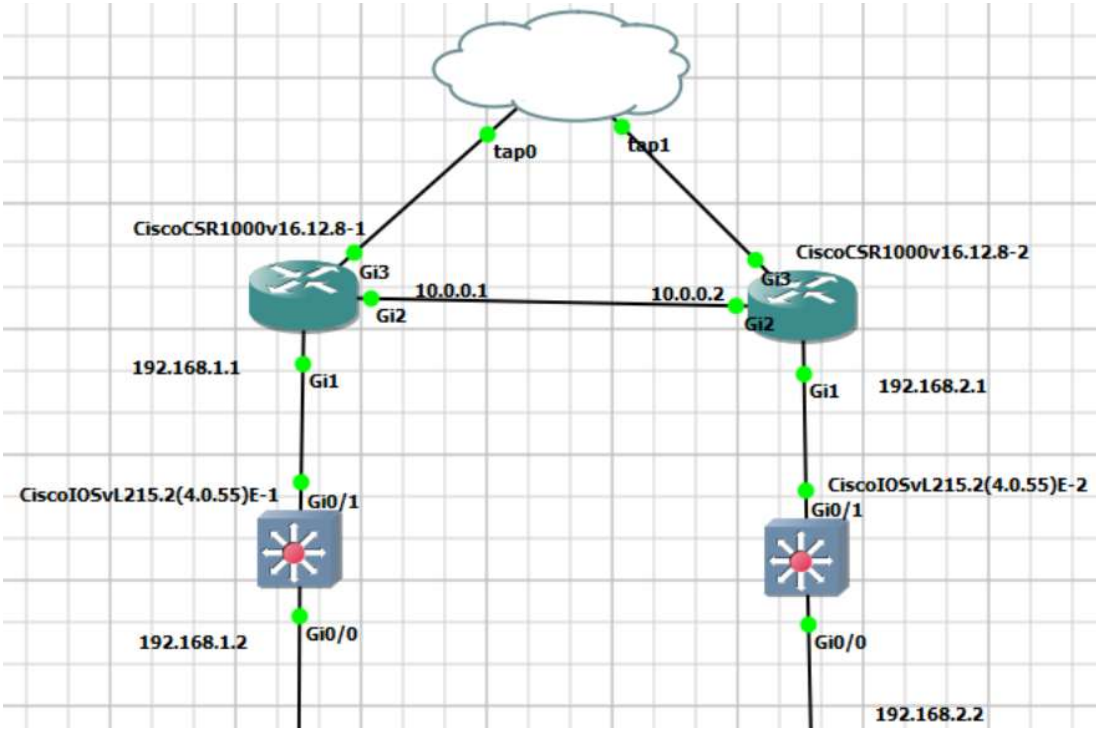
## Acknowledge all the alarms



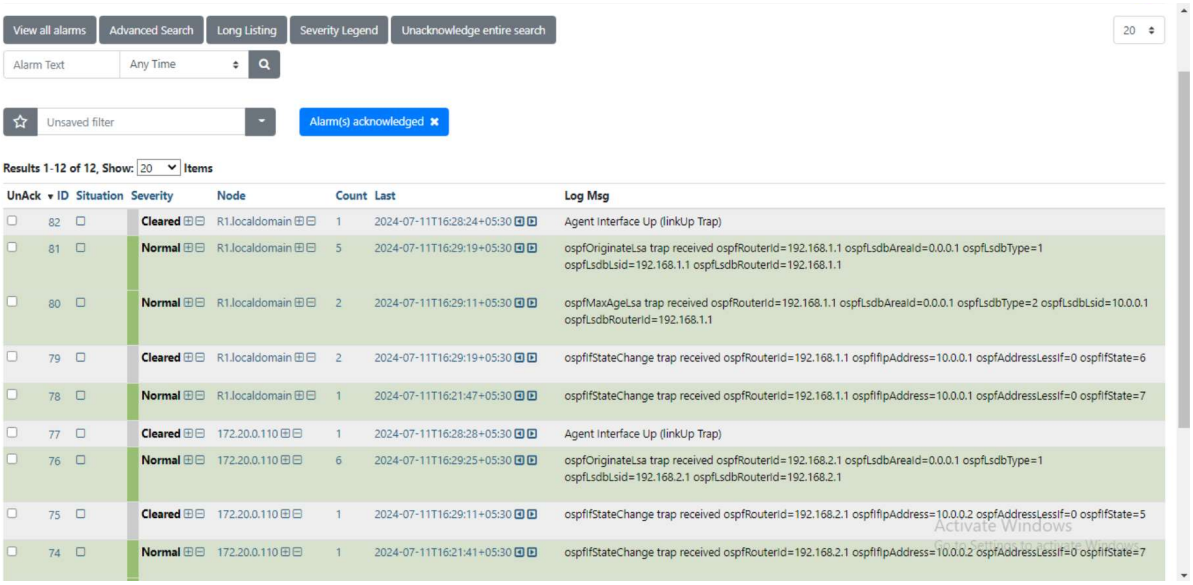

## Ping PC1 and PC2 and observe the Bits In/Out reports



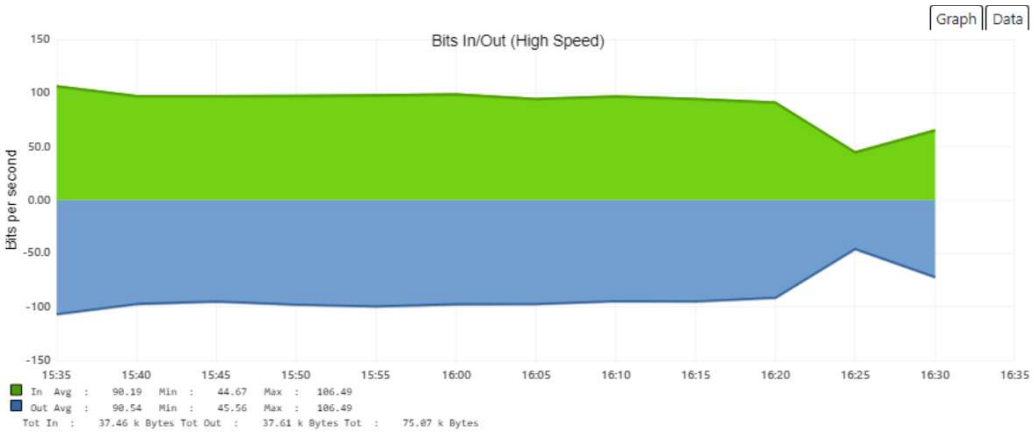

## Recover the link status



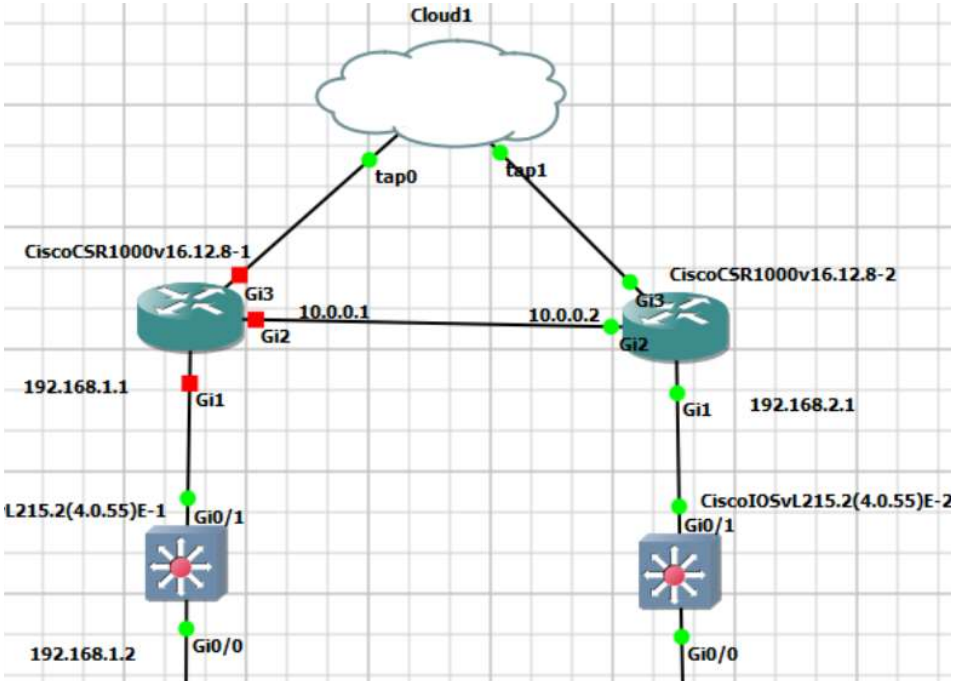
## Check the alarms in NMS, all the alarms will be cleared



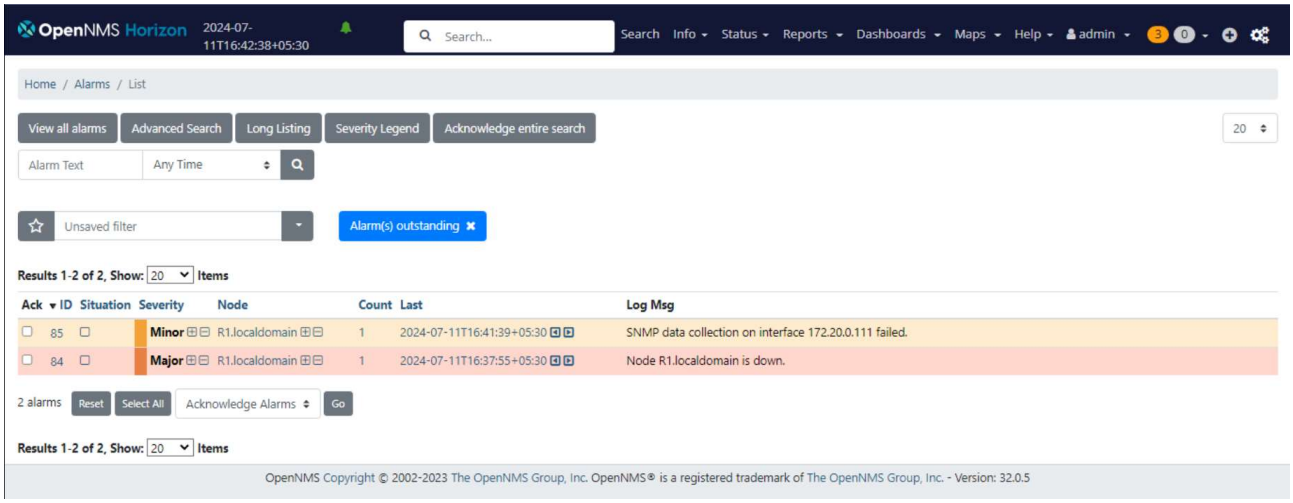

## Ping PC1 and PC2 and observe the Bits In/Out reports



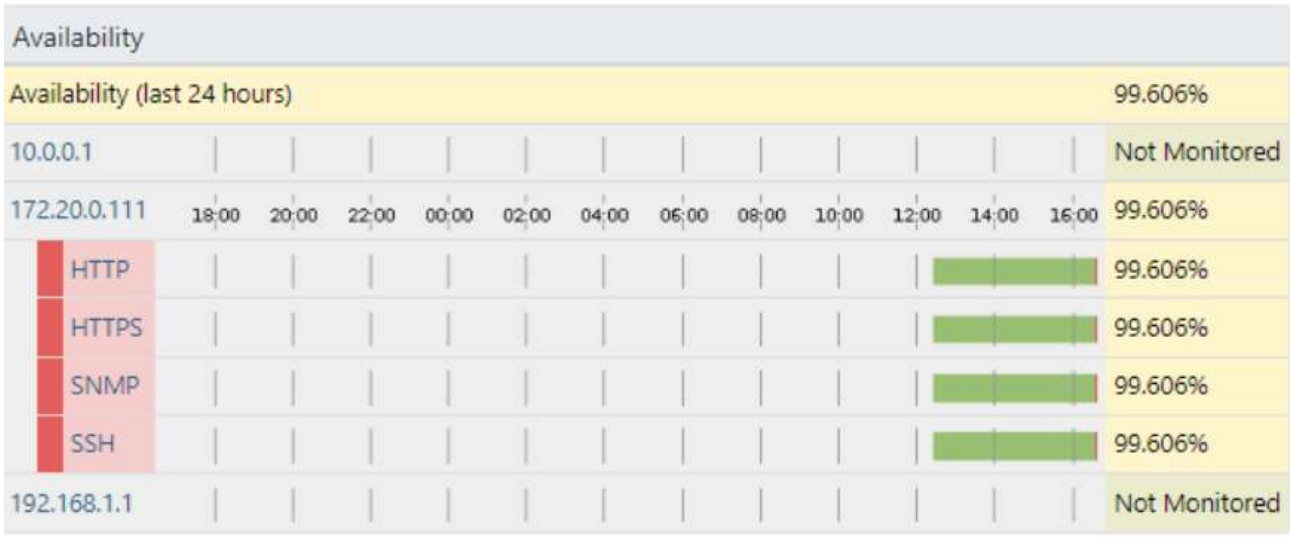

## Generate the Outage-
## Stop the Router 1, communication between Node and NMS server get stopped

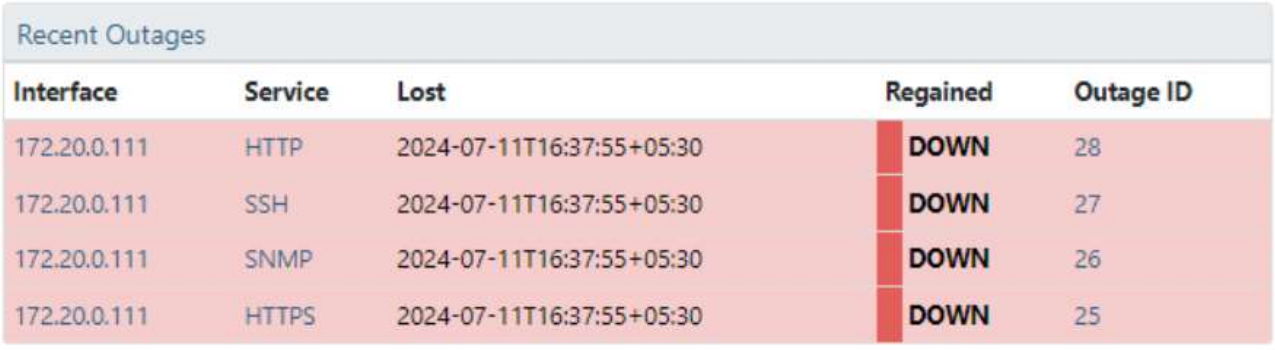


**Alarms will be generated at NMS server**

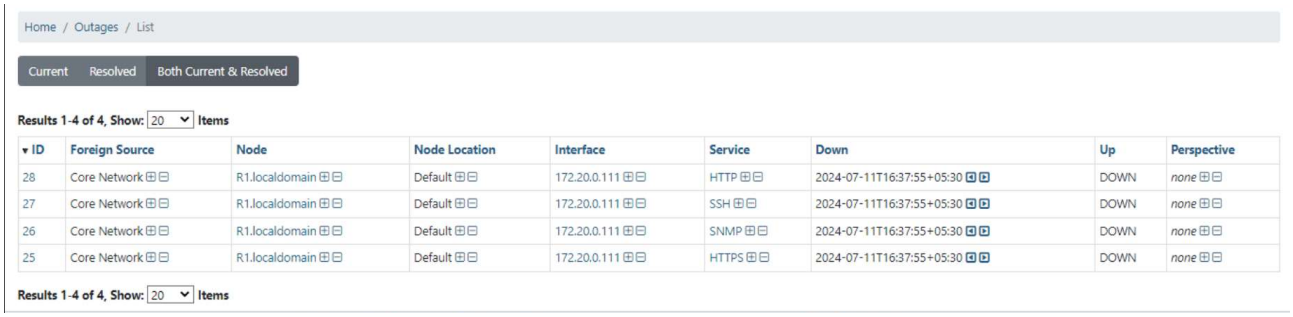



**Check the SNMP availability for the node, it get reduced from 100% and keep decreasing...**

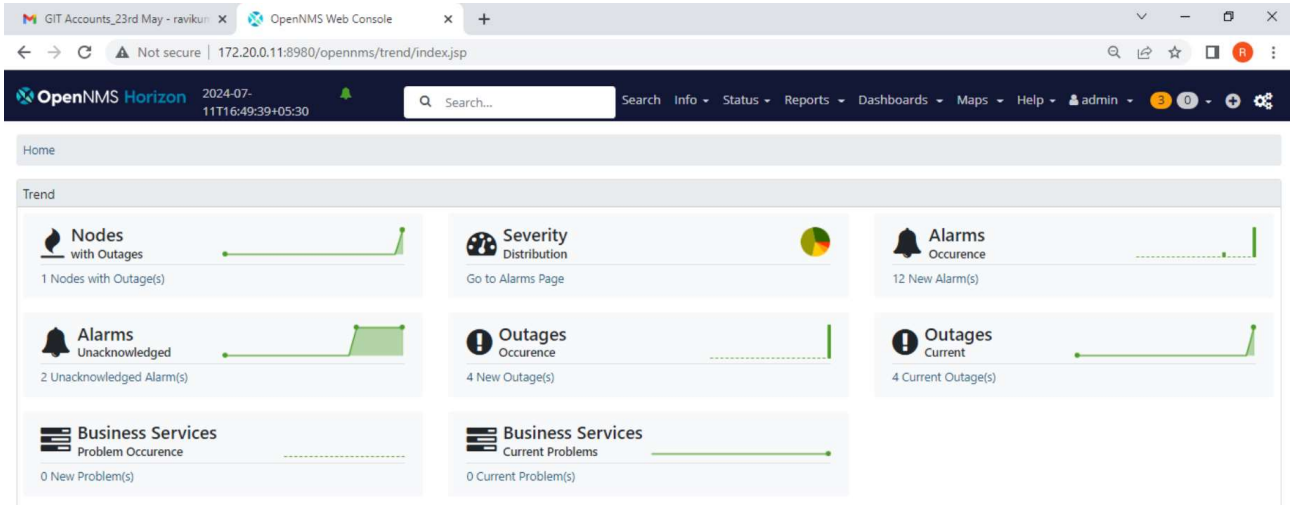


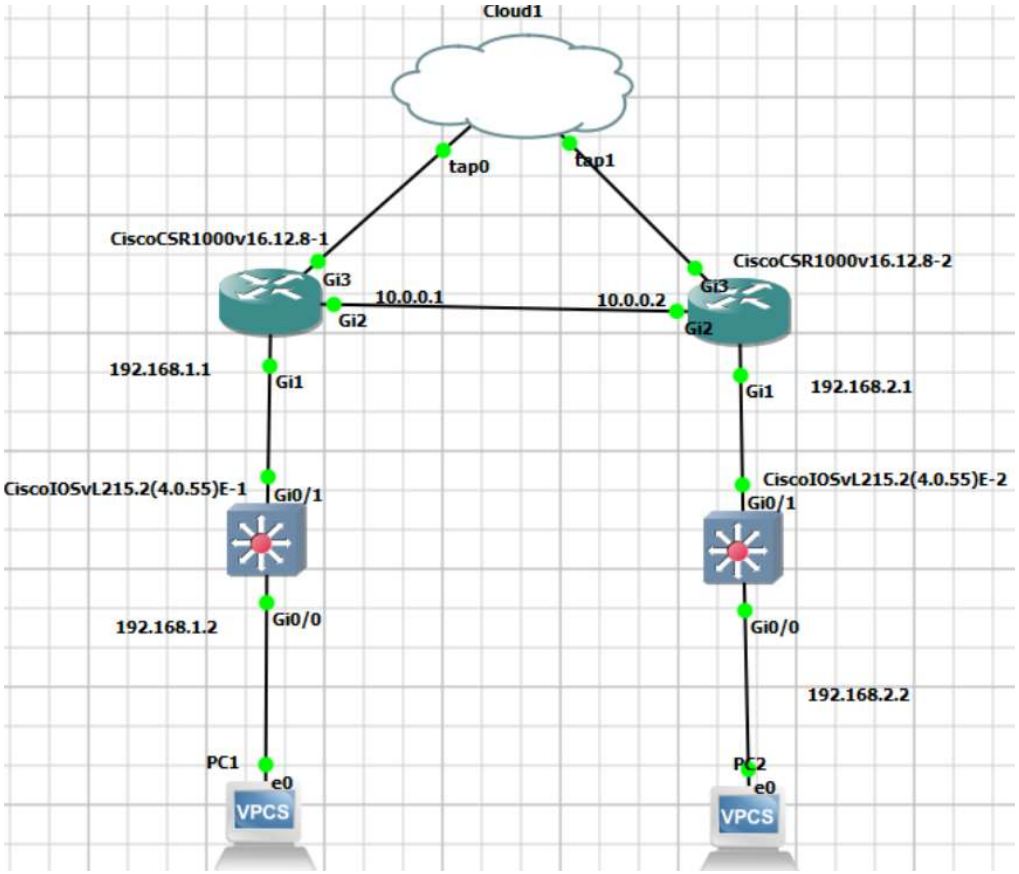
## Click on Status → Outages → all outages




## Click on Status → Trend



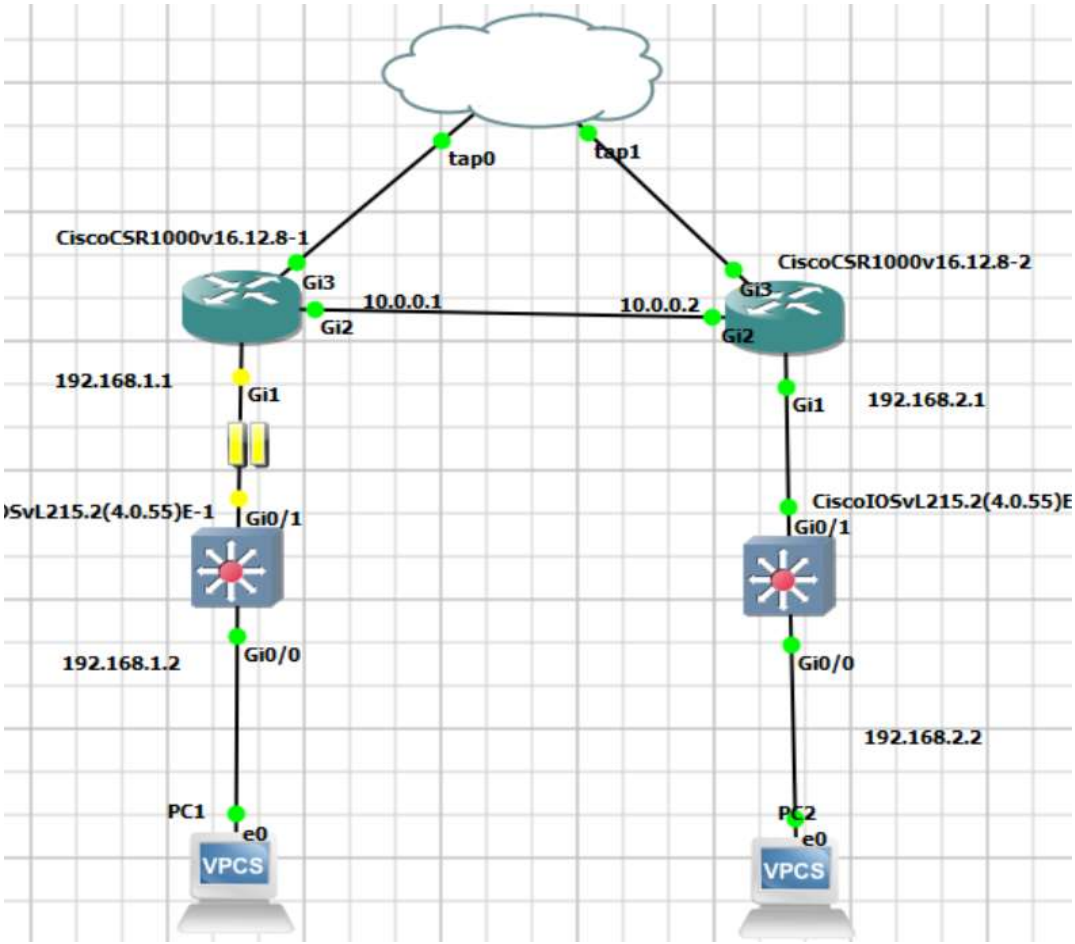

## Recover the Faults



## Check the alarms in NMS, all the alarms will be cleared

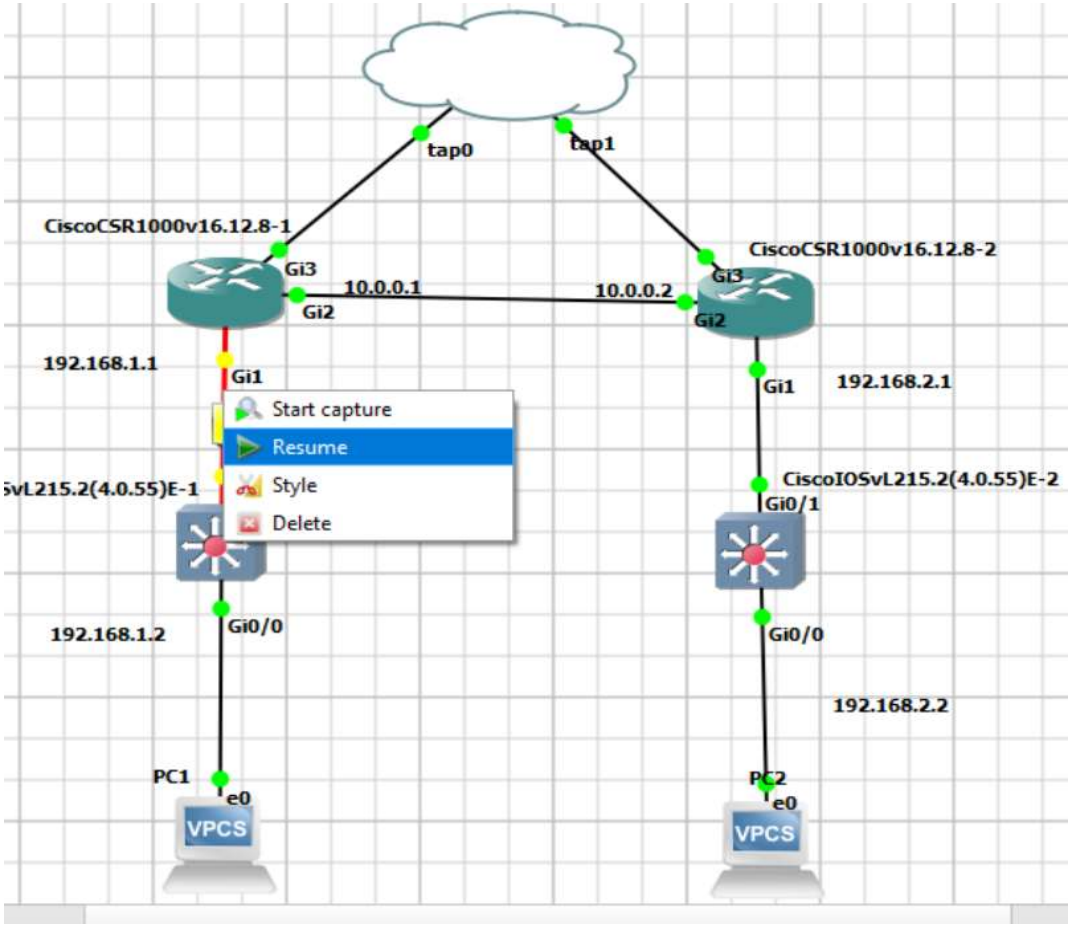
| UnAck | ID | Situation | Severity | Node | Count | Last | Log Msg |
|---|---|---|---|---|---|---|---|
| ☐ | 82 | ☐ | Cleared | R1.localdomain | 1 | 2024-07-11T16:28:24+05:30 | Agent Interface Up (linkUp Trap) |
| ☐ | 81 | ☐ | Normal | R1.localdomain | 5 | 2024-07-11T16:29:19+05:30 | ospfOriginateLsa trap received ospfRouterId=192.168.1.1 ospfLsdbAreaId=0.0.0.1 ospfLsdbType=1 ospfLsdbLsid=192.168.1.1 ospfLsdbRouterId=192.168.1.1 |

## Generate Trap by suspending link between router and SW




| Ack | ID | Situation | Severity | Node | Count | Last | Log Msg |
|---|---|---|---|---|---|---|---|
| ☐ | 89 | ☐ | Minor | R1.localdomain | 1 | 2024-07-11T17:21:30+05:30 | Agent Interface Down (linkDown Trap) |
| ☐ | 88 | ☐ | Warning | R1.localdomain | 1 | 2024-07-11T17:21:29+05:30 | ospfIfStateChange trap received ospfRouterId=192.168.1.1 ospfIfIpAddress=192.168.1.1 ospfAddressLessIf=0 ospfIfState=1 |

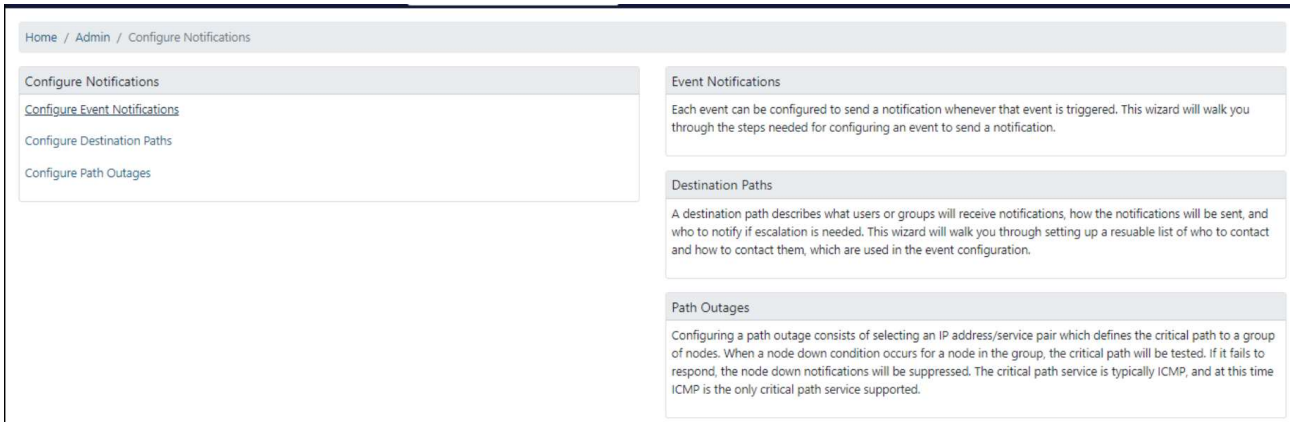
## Recover the fault

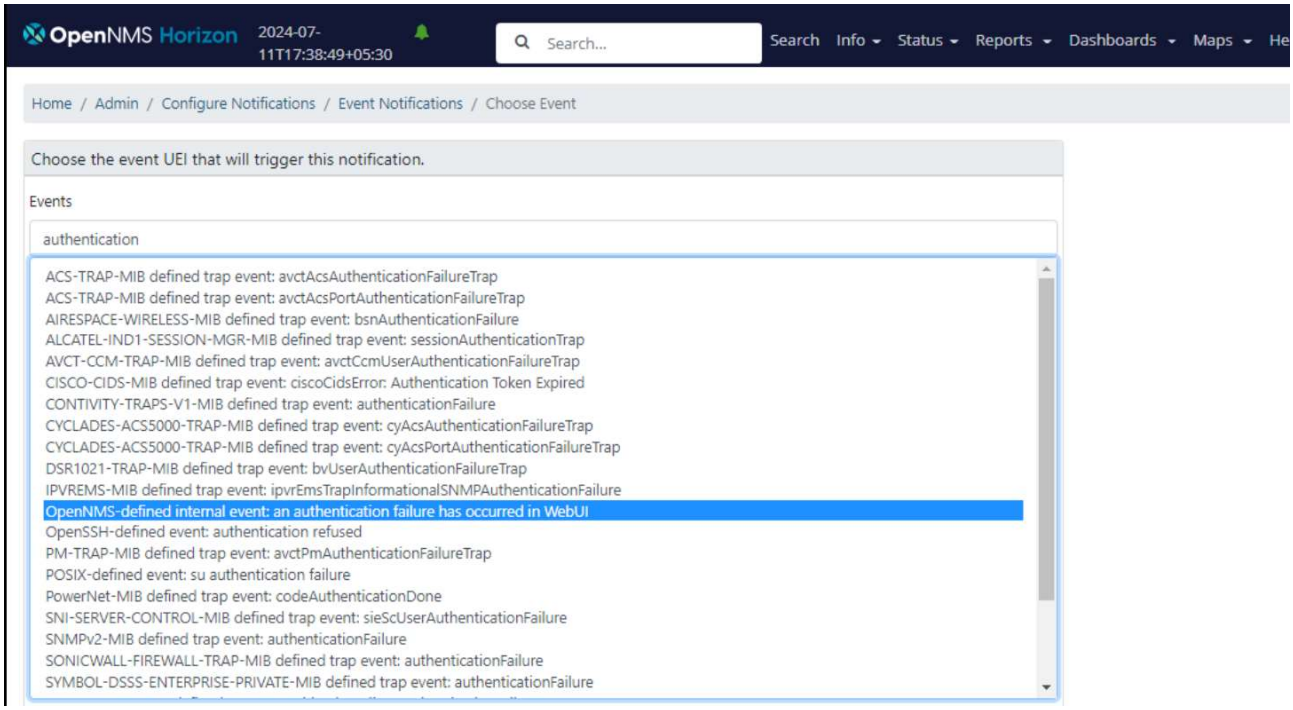



## Check the alarms in NMS, all the alarms will be cleared

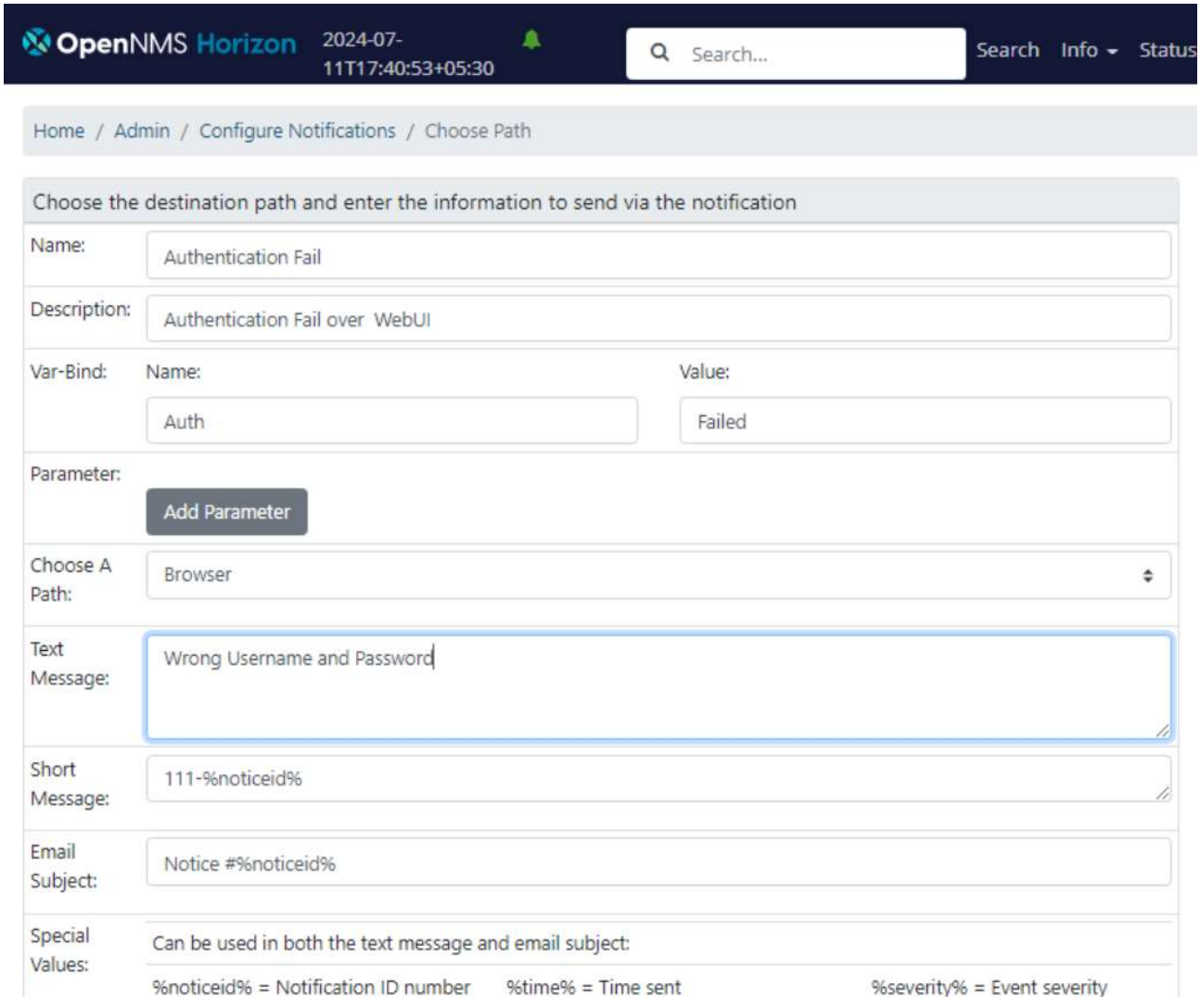
| UnAck | ID | Situation | Severity | Node | Count | Last | Log Msg |
|---|---|---|---|---|---|---|---|
| ☐ | 82 | ☐ | Cleared | R1.localdomain | 1 | 2024-07-11T16:28:24+05:30 | Agent Interface Up (linkUp Trap) |
| ☐ | 81 | ☐ | Cleared | R1.localdomain | 8 | 2024-07-11T17:30:30+05:30 | ospfOriginateLsa trap received ospfRouterId=192.168.1.1 ospfLsdbAreaId=0.0.0.1 ospfLsdbType=1 ospfLsdbLsid=192.168.1.1 ospfLsdbRouterId=192.168.1.1 |

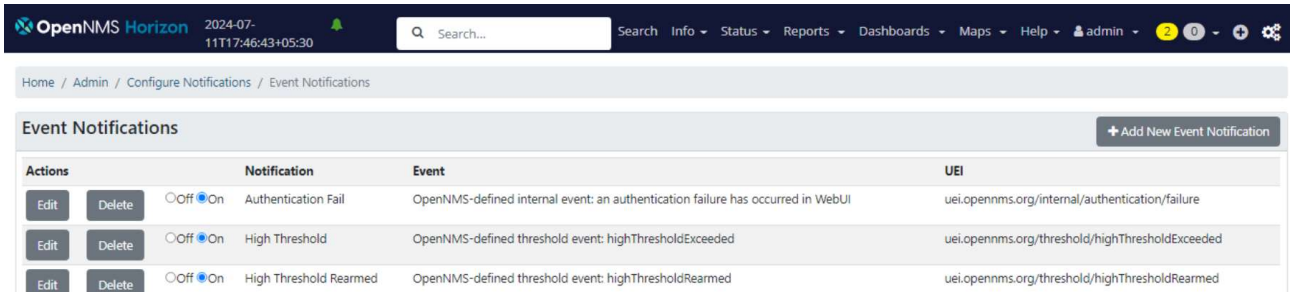
## Configure Notification - Event notification to be generated when some one try accessing OpenNMS with incorrect credentials on WebUI

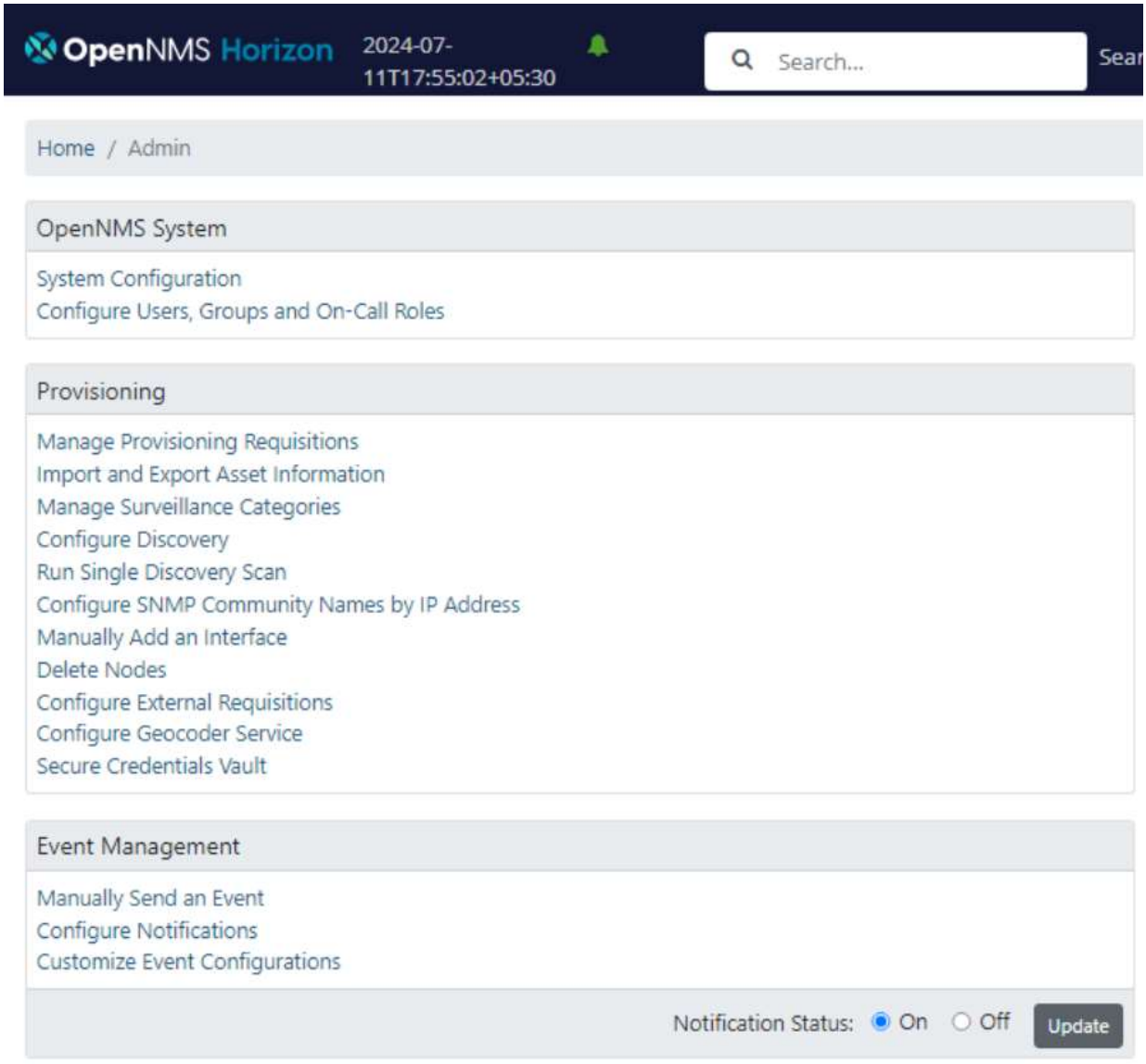





**Click Next → Skip Result Validation**






## Go to Status → Events → all events