Name: Harsh Dalvi
Roll No: 13

Experiment No. 10

Aim: To compute Port, Service monitoring, Windows/Linus server monitoring using Nagios. **(LO1, LO5)**

Theory:

Windows Service Monitoring with Nagios:

Capabilities:

Nagios provides complete monitoring of Microsoft Windows services. Nagios is capable of monitoring the state of any Windows service (IIS, Exchange, DHCP, etc) and alerting you when the service is stopped or crashed.

Benefits:

Implementing effective Windows service monitoring with Nagios offers the following benefits:

- Increased server, services, and application availability.
- Fast detection of network outages and protocol failures.
- Fast detection of failed services and batch jobs.

What is Continuous Monitoring in DevOps?

Continuous Monitoring (CM), sometimes called Continuous Control Monitoring (CCM), is an automated process by which DevOps personnel can observe and detect compliance issues and security threats during each phase of the DevOps pipeline. It helps teams or organizations monitor, detect, study key relevant metrics, and find ways to resolve said issues in real-time.

Continuous Monitoring basically assists IT organizations, DevOps teams in particular, with procuring real-time data from public and hybrid environments. This is especially helpful with implementing and fortifying various security measures – incident response, threat assessment, computers, and database forensics, and root cause analysis. It also helps provide general feedback on the overall health of the IT setup, including offsite networks and deployed software.

Goals of Continuous Monitoring in DevOps:

- Enhance transparency and visibility of IT and network operations, especially those that can trigger a security breach, and resolve it with a well-timed alert system.
- Help monitor software operation, especially performance issues, identify the cause of the error, and apply appropriate solutions before significant damage to uptime and revenue.
- Help track user behavior, especially right after an update to a particular site or app has been pushed to prod. This monitors if the update has a positive, negative, or neutral effect on user experience.

Types of Continuous Monitoring:

1. **Infrastructure Monitoring:** Monitors and manages the IT infrastructure required to deliver products and services. This includes data centers, networks, hardware, software, servers, storage, and the like. Infrastructure Monitoring collates and examines data from the IT ecosystem to improve product performance as far as possible.
2. **Application Monitoring:** Monitors the performance of released software based on metrics like uptime, transaction time and volume, system responses, API responses, and general stability of the back-end and front-end.
3. **Network Monitoring:** Monitors and tracks network activity, including the status and functioning of firewalls, routers, switches, servers, Virtual Machines, etc. Network Monitoring detects possible and present issues and alerts the relevant personnel. Its primary goal is to prevent network downtime and crashes.

How to Implement Continuous Monitoring:

Software vendors create robust and versatile solutions that enable IT organizations to effectively monitor network traffic, detect anomalies or suspicious patterns of activity and develop actionable insights. The implementation of a continuous monitoring software solution can be described in five basic steps:

1. **System Definition:** The IT organization must determine the scope of its continuous monitoring deployment. Which systems are under the purview of the IT organization? Which systems should be subject to continuous monitoring?
2. **Risk Assessment:** The IT organization should conduct a risk assessment of each asset it wishes to secure, categorizing assets based on the risk and potential impact of a data breach. Higher-risk assets will require more rigorous security controls, while low-risk assets may require none at all and could even serve as a "honeypot.
3. **Choosing and Implementing Security Control Applications:** Once a risk assessment has been completed, the IT organization should determine what types of security controls will be applied to each IT asset. Security controls can include things like passwords and other forms of authentication, firewalls, antivirus software, intrusion detection systems (IDS) etc.
4. **Software Tool Configuration:** As the IT organization coordinates the desired security controls to protect key informational assets, it can begin to configure a continuous monitoring software tool to start capturing data from those security control applications. Continuous monitoring software tools incorporate a feature called log aggregation that collects log files from applications deployed on the network, including the security applications that are in place to protect information assets.
5. **Ongoing Assessment:** Collecting data from throughout the IT infrastructure is not the ultimate goal of continuous monitoring. With millions of data points generated and centralized each day through log aggregation, information must be assessed on an ongoing basis to determine whether there are any security, operational or business issues that require attention from a human analyst.

Name: Harsh Dalvi
Roll No: 13

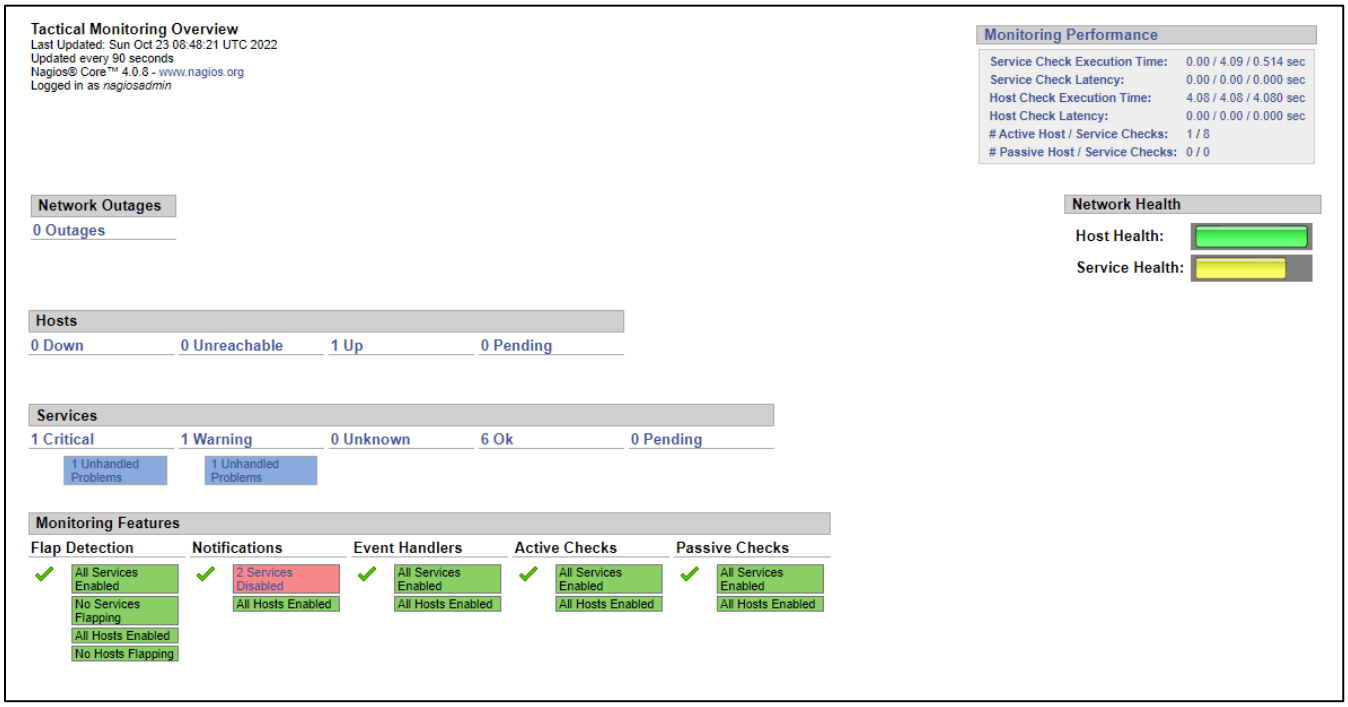
Subject: Advance DevOps , Sem: SEM V
Class / Batch: TE-IT / Batch B

Benefits of Continuous Monitoring:

1. **Better Network Visibility and Transparency:** CM offers DevOps teams clarity on the state of the IT infrastructure by automatically collecting and analyzing data to reflect possible outages and important trends.
2. **Facilitates Rapid Responses:** A primary aspect of CM is implementing an alert system that immediately notifies the right people the minute an IT incident emerges. This enables timely response to security threats or functional stop-gaps, minimizing damage and allowing faster restoration of the system to optimal operational levels.
3. **Minimizes System Downtime:** Consistent system monitoring and quick, necessary alerts help maintain system uptime by raising the alarm when there is a service outage or any application performance issues.
4. **Assists with Healthy Business Performance:** Reduction in system downtime also minimizes negative impact on customer experience, thus safeguarding the organization against losses in revenue or credibility. As mentioned before, Continuous Monitoring tools can also be used to track user reactions to software updates, which is useful for several teams – development, QA, sales, marketing, customer service, etc.

Steps to perform the Experiment:

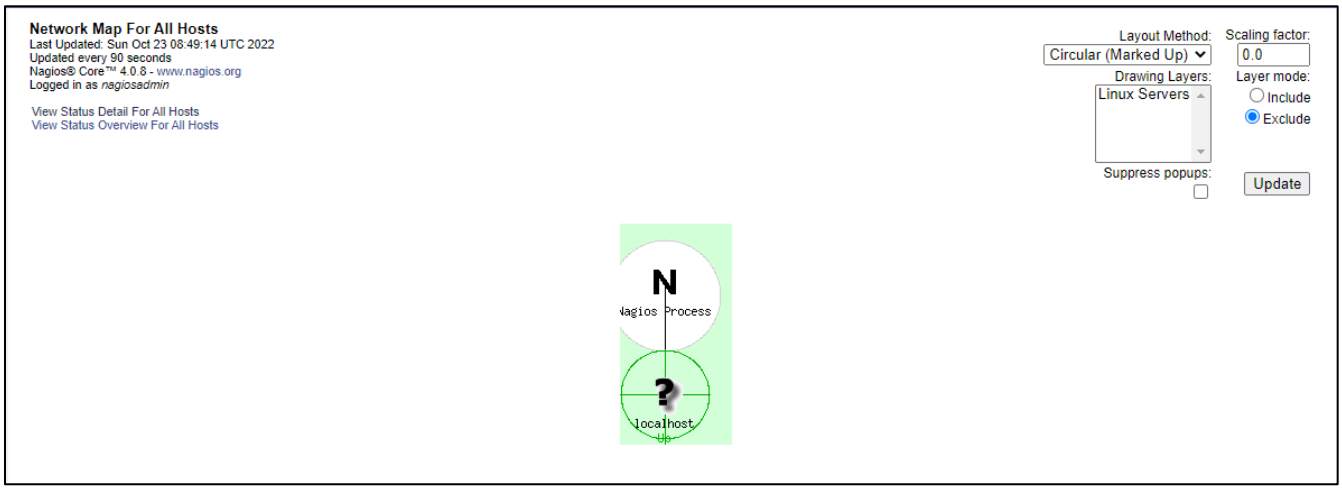
Step 1: Tactical Overview



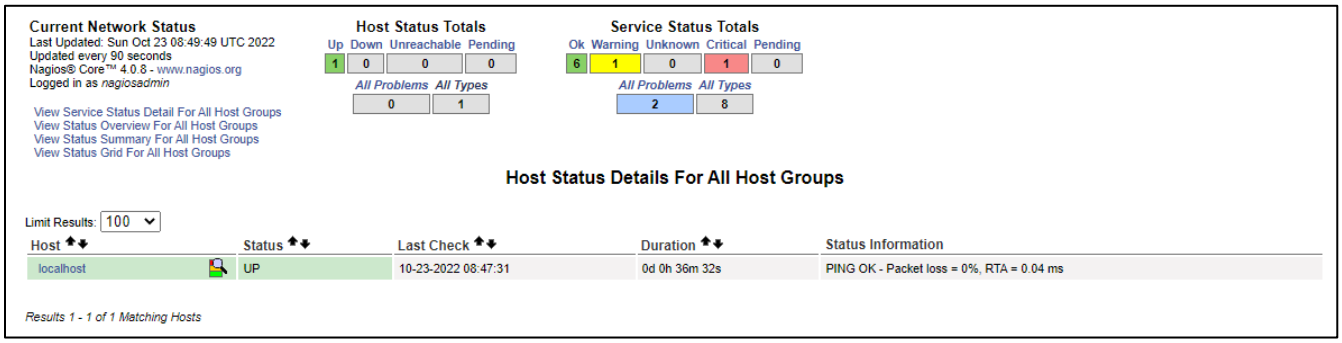
Name: Harsh Dalvi
Roll No: 13

Subject: Advance DevOps , Sem: SEM V
Class / Batch: TE-IT / Batch B

Step 2: Map

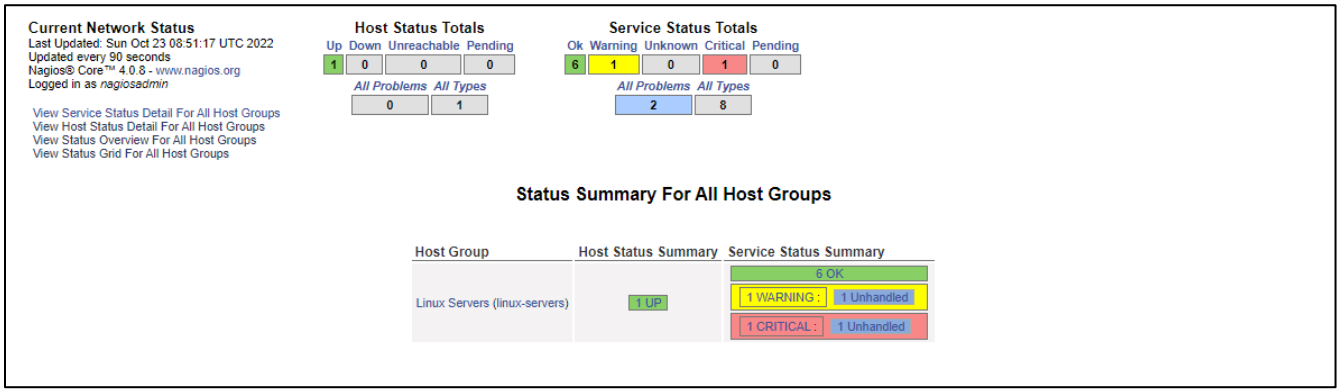


Step 3: Hosts



Step 4: Hosts group

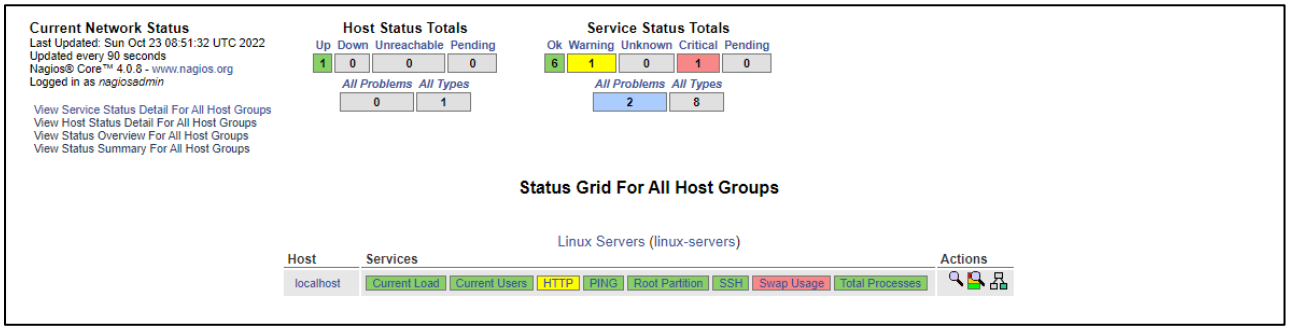
Summary



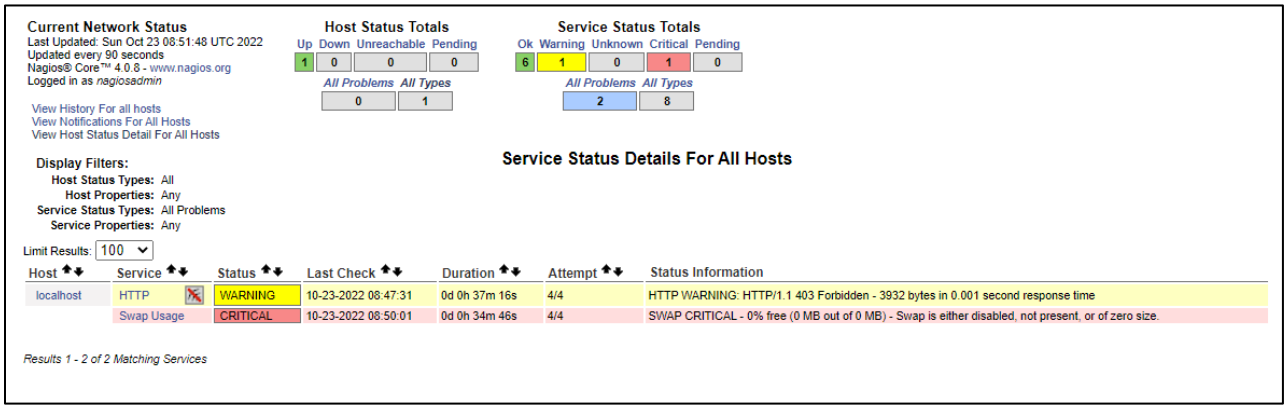
Name: Harsh Dalvi
Roll No: 13

Subject: Advance DevOps , Sem: SEM V
Class / Batch: TE-IT / Batch B

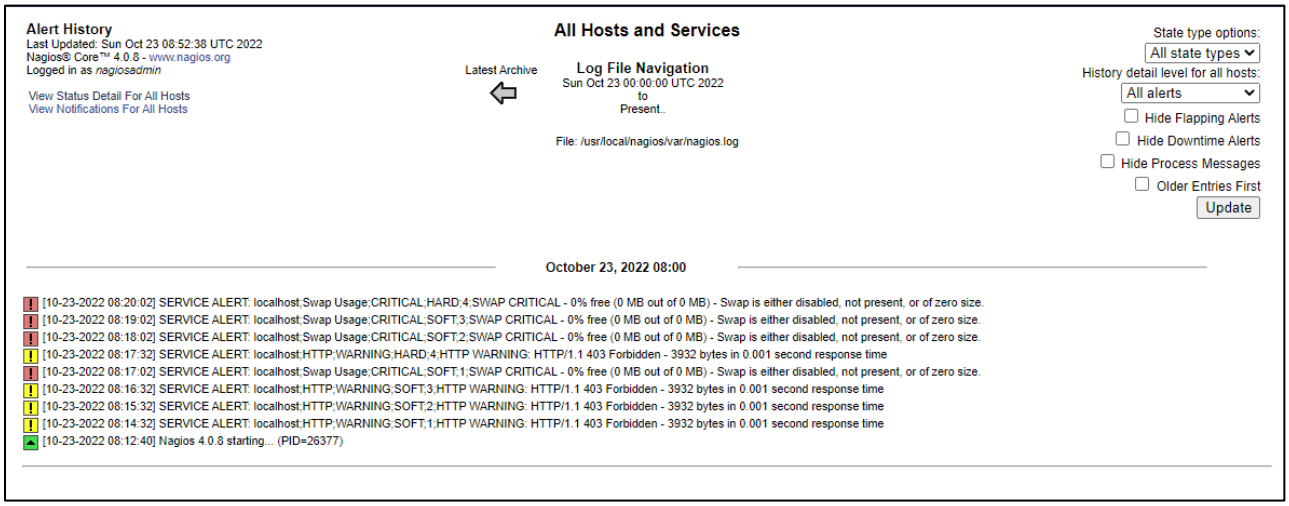
Grid



Step 5: Problems



Step 6: History



Conclusion: From this experiment, we have studied and understood about the concept of server monitoring using the Nagios tool on different ports and services which are being used and served by the server. Hence, we have successfully achieved the Lab Outcome One and Five (LO1 and LO5). Also, we have achieved PO1, PO2, PO3, PO4, PO5, PO9, PO10 and PO12 from this experiment.