

Contents

Module Objective	1
Module Topics	1
1.1 Introduction to Monitoring	2
1.2 Definition of Monitoring	2
What did You Grasp?	3
1.3 What is Key Performance Indicators?	3
What did you Grasp?	4
1.4 Goals of Monitoring	4
What did You Grasp?	6
1.5 DevOps approach to Monitoring	6
1.6 Continuous Monitoring	7
1.7 Network Operation Center (NOC)	8
1.8 Role of NOC in DevOps World	8
What did You Grasp?	10
1.9 Telemetry and Metrics	10
1.10 Types of Monitoring	11
1.10.1 Types of Monitoring: End User Monitoring	12
1.10.2 Types of Monitoring: Infrastructure Monitoring	12
1.10.3 Types of Monitoring: Application Monitoring	13
1.10.4 Types of Monitoring: Log Monitoring and Analysis	13
What did You Grasp?	14
In a Nutshell	14

Module 1

DevOps and Monitoring

You will learn about the 'End User Monitoring' in this module.

Module Objective

At the end of this module, you will be able to:

- Define the monitoring
- Identify the need of monitoring
- Explain the approach of monitoring with respect to DevOps
- Define the Network Operations Center
- List the roles and responsibilities of NOC in DevOps world
- Describe the telemetry and metrics used for monitoring
- Explain the various aspects of monitoring



Module Topics

This module covers the following topics:

- Introduction to monitoring
- Goals of monitoring
- DevOps approach to monitoring
- Network operations center
- Role of NOC in DevOps world
- Telemetry and metrics
- Types of monitoring: end user, infrastructure, application, log monitoring and analysis



1.1 Introduction to Monitoring

What is monitoring?



To understand monitoring, let us get back to school days when teachers used to appoint a student as "Monitor" who used to keep an eye on the class in teachers absence and maintain the decorum of class.

Monitoring in IT infrastructure:



Similarly, In IT infrastructure, where the applications are running on servers and being used by customers need to be watched 24/7 to avoid any outage or revenue loss.

With equivalent roles and responsibilities, the monitoring system in IT plays a vital role in enhancing the availability, responsiveness of a platform.

1.2 Definition of Monitoring

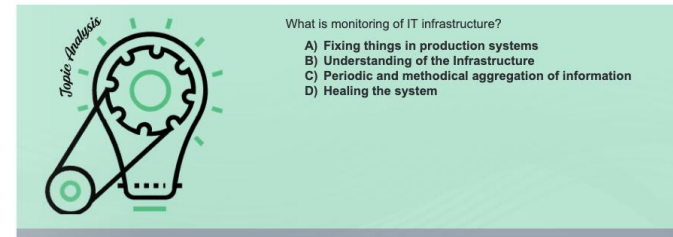
Monitoring in IT infrastructure:



Monitoring is the periodic and methodical aggregation of information of an IT environment. The information could be of events, infrastructure, users, applications, which are part of revenue generating machinery.

So, we can say that the act of collecting metrics and/or metadata of an IT environment, either directly or indirectly from the applications, servers, operating systems, application logs, private and public cloud hypervisors, network devices, SDN and SD-WAN controllers, and any other IT infrastructure or application data source is called Monitoring.

What did You Grasp?



1.3 What is Key Performance Indicators?

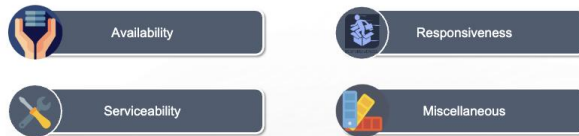
The Key Performance Indicators (KPIs) are the identifiers for the health of a system:



Source: <https://efmireland.ie/wp-content/uploads/2020/01/Key-Performance-Indicators-and-why-they%E2%80%99re-good-for-any-business.png>


To begin with monitoring, one should understand the Key Performance Indicators (KPIs) that are required for managing one's applications; and aggregating those KPIs in the most efficient manner. Monitoring is about the metrics that matter a prerequisite step in a series of steps that may include data normalization, storage, visualization, alerting, analysis through applications of machine learning and artificial intelligence, which in turn may support a range of disciplines from operations management to capacity planning.

There are basically four Key Performance Indicators, which are:



- **Availability:** One of the most important indicator of performance is availability of site. The end user facing site should always be available and must being watched 24/7. A high level monitoring should always be enabled to fetch the metrics of site availability.
- **Responsiveness:** The minimum rate at which a platform needs to resolve queries, receive and acknowledge requests to the end user should be monitored. To ensure customer satisfaction the response should be immediate and if it is below the critical threshold then it should be highlighted.
- **Serviceability:** Serviceability is the supinity with which a running system or infrastructure can be maintained. In case of any outage or downtime of a standalone system or complete infrastructure, the healing process should be easy enough to bring the system up and running in a bare minimum period of time. The process should be automated to avoid any human error during vulnerable times.
- **Miscellaneous:** These are the indicators which are specific to use cases with respect to the project, platform. Generally, these pointers are customized in accordance to business requirements.

What did you Grasp?



Why KPIs are required?

- A) For system to run fine
- B) For monitoring
- C) For the visibility of management
- D) Alerting the NOC team

1.4 Goals of Monitoring

Goals of monitoring:

- Continuous observation
- Maintaining discipline
- Note down the issues and concerns
- Report the issues and concerns



To understand the goals of monitoring, we will use the same analogy of class monitor with the IT monitoring. So going back to our analogy, we can briefly expect a couple things from a class monitor.

- Continuous observation of class students.
- Maintaining discipline in the teacher's absence.
- Note down the issues and concerns of students in class.
- Report the issues and concerns to the attention of class teacher.


There are basically four goals of monitoring:



- **Learning:** To achieve this goal, we aggregate data of the advancement of your project or programme, about the planned or unplanned repercussions, about growth in the environment and about hurdles that you encounter. You use this data to mirror on your points of retreat and your expectation about the problem or about the possible solutions or the knowledge needed to find solutions. This might lead to the conclusion that you have to revisit your previous assumptions.
 - Target audience: This point directly impact those teams or groups who are directly engaged in conducting the project or programme. The other important team or groups are the people who are carrying out related experiments, managers and financiers. Policymakers should be convoluted in the process, particularly when mirroring on organisational barriers.
- **Accountability:** The team or group is considered accountable on the basis of the goals achieved that have been set for a period or time, in accordance with the resource provided if they have been wisely used.
 - Target audience: In this case, the audience is usually the client or financier of a project or programme. For eg: in case of country wide programme or project the government and bureaucrats will be the target audience.
- **Intervention or adaptation:** The farther we go with monitoring we learn from the metrics and data which we have aggregated and realise that some of the points need to be improved considering the vulnerability scanned during the monitored period. This leads to the transition of the project or programme needs to be modified, and this somehow becomes one of the critical goal of monitoring. This step is an integral part of reflexive monitoring.
 - Target audience: In case of intervention or adaptation the target audience is the stakeholders and the team handling the project usually management. Also, this can be initiated by the clients/financiers because they could also have the same visibility, which makes them the most important target audience.

- **Transferring knowledge:** Inspiring the team and transferring knowledge can accord to the lictness of system innovations and help increase support for imbed them in an organisation.
 - Target audience: The target audience of this are client/financiers and potential or existing fellow innovators, possible future financiers and insurers, regulators or a wider public.

What did You Grasp?



Why we need monitoring?

- A) To keep an eye on health of the system
- B) To define the KPIs
- C) To design the system
- D) To increase business revenue

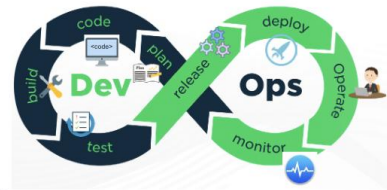
1.5 DevOps approach to Monitoring

The key factor, which impacts the DevOps lifecycle:

- Continuous Integration
- Continuous Testing
- Continuous Delivery
- Continuous Deployment
- Continuous Monitoring
- Continuous Business Planning

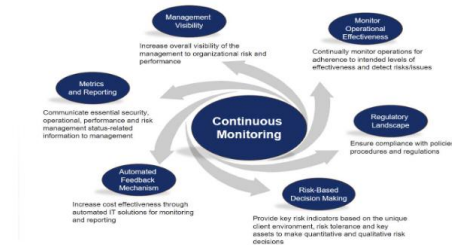
The key factor, which impacts the devops lifecycle is "being continuous", if we consider all of the aspects of devops.

- Continuous Integration
- Continuous Testing
- Continuous Delivery
- Continuous Deployment
- Continuous Monitoring
- Continuous Business Planning



1.6 Continuous Monitoring

The following diagram displays some facts of the continuous monitoring.



Source: https://fedrampcompliance.com/wp-content/uploads/2016/01/service_7.png

Continuous monitoring refers to the availability, responsiveness and serviceability of the platform.

- **Management Visibility:** The monitoring setup should provide visibility of a bird eye view of the running infrastructure to the higher authority. A high level view should always be visible to the management to measure risk and vulnerability.
- **Monitor Operational Effectiveness:** The system which is continuously monitoring the stack should be effective enough to identify the possible risks and vulnerability in the infrastructure.
- **Regulatory Landscape:** Since the stack requires certain access to aggregate data from the infrastructure, those access should be regulated with compliance policies. The procedure of collecting metrics should be regulated to avoid any security vulnerability.
- **Risk-Based decision Making:** Provide key risk indicators based on the unique client environment, risk tolerance and key assets to make quantitative and qualitative risk decisions.
- **Automated Feedback Mechanism:** Increase cost effectiveness through automated IT solutions for monitoring and reporting.
- **Metrics and Reporting:** Communicate essential security, operational, performance and risk management status-related information to management.

1.7 Network Operation Center (NOC)

The following image displays the Network Operation Center (NOC).



The NOC stands for Network operations center, it is a body who is the first line of defense against any attack, failure or malfunction in the IT environment like Services, Databases, External firewalls, Network etc. They are responsible for keeping an eye on the visual medium to observe the health of system and fixing issues.

Basically, a NOC is a group of people who keeps an eye on the monitoring dashboards to have a visibility of the infrastructure, also they get alerted for every issue occur in the system, they are responsible for resolving those issue with the best of their knowledge and standard operating procedure (SOP) provided to them.

1.8 Role of NOC in DevOps World

Roles of NOC:



The following are the roles of NOC in DevOps world:

- 24X7 coverage:** The network infrastructure is a combination of complex subunits and platform which keeps on evolving. Since the teams which are working to develop these system are constantly striving to improve and evolve their focus is more on going further on the path of evolving the systems. The issues which occur in the system need to be fixed by a team who is dedicated to this particular role so that the development and the operation teams can strive for further development of the project. The skilled staff of NOC team takes care of system 24X7 without budging.

- Advanced Expertise:** An engineer is likely to be an expert in many areas which are many like networking, server administration, database administration, applications, e-commerce, or some other specialty. Since the NOC team is the first line of defence they require to be expert in the problem solving field with respect to the project. A Network Operations Center must transcend these other areas to provide an integrated "single pane of glass" view into the health and operation of those critical systems.
- Focus:** The role of NOC is critical in terms of keeping the health of platform healthy, they need to be reliable to the service to the customers. Their focus should be on the running state of the applications. Monitoring and evaluation requires to have a focus audience which is constantly looking to the system in a systematic way with having any loss in focus to evade failures.
- Customized, flexible monitoring solutions:** It is not possible to always have a plug in play monitoring solution which will look after every exclusive process running. At times we need to have a customised solutions for the exclusive problem which occurs in a system. These problems require custom scripts to properly detect failure and fix them. The NOC team responsible to design such solutions/scripts which can take those unique requirements as per the business.
- Eliminating Noise:** At times the monitoring solution has an extension called alerting, whose purpose is to alarm for the issues. But the problem arises when the number of alarms being sent becomes staggering, then the critical alarms are ignored and outage occurs. The NOC team act as a filter, who promotes only important and critical alarms which needs the attention of administrators and operations team. With all of these capabilities in place, your IT staff will not be distracted with false alarms. More importantly, they won't miss the real ones.
- Eliminating busy work:** The computing environment is always evolving and improving with the constant efforts of engineers working towards it. In order to keep the ball running they need to be focused and not getting disturbed by alarms triggered by monitoring stack. Hence, this busy work is taken care by the NOC teams. Freeing your staff from this busy work and allowing them to focus on the activities that generate value for your organization.
- Added Value:** A top-tier NOC partner operates as an extension of your staff, providing value to your organization by minimizing outages in your network and decreasing the mean time to repair (MTTR). You can expect increased uptime of your network and more staff hours dedicated to other projects, as their time will no longer be spent on the care and feeding of a monitoring platform. Your NOC partner will maintain the monitoring platform 24x7, keep eyes on your network around the clock, and allow you to leverage their expertise for a fraction of the cost of monitoring in-house.
- Peace of Mind:** The ultimate benefit of partnering with a NOC services provider is peace of mind. Knowing your network is under constant watch by a highly skilled NOC is invaluable. No matter what time of day or day of the week, you can expect your NOC partner to be on duty, focusing on your network, and responding to all alerts. No more missed alerts while someone sleeps through a page or misses an email. Can it get any better? Yes it can! It's nice to be alerted of an outage in your network at two in the morning, but it's GREAT to sleep through it and find out the next morning your NOC partner fixed the issue, following a specific set of steps that you want followed, while you had a good night's rest.

What did You Grasp?

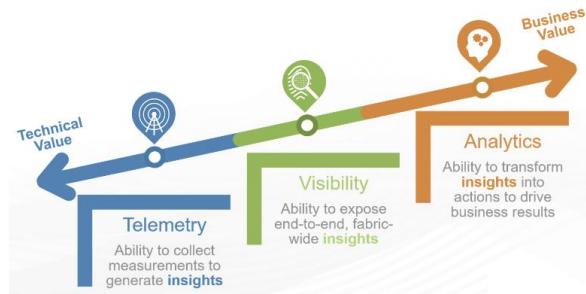


Why do we need NOC?

- A) To determine the business target
- B) To maintain the discipline
- C) To have market statistics
- D) To have a peace of mind

1.9 Telemetry and Metrics

The following image illustrates the concept of telemetry and metrics.



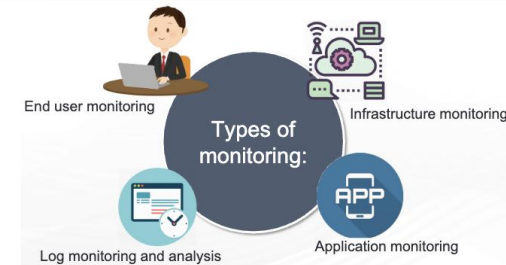
- **Telemetry** is a means by which data is collected from remote or inaccessible devices, or to be more accurate, a means by which it is transmitted by those devices to receivers. We have a lot of devices in the Edge network which operate in a similar fashion; which sit in all manner of inaccessible locations and operate on an egress-only basis. This article will introduce you to how we collect measurements from these devices. collects basic system measurements such as load averages, memory usage, disk space utilisation and network activity. It also collects some other less interesting statistics such as system fork count, active process count, and established TCP connection counts.

This data is then packaged up and sent securely to the network's telemetry receiver servers, which sit outside of the main network infrastructure — critical to remaining accessible during possible outages — before being verified and stored alongside the metrics of all other devices.

- **Metrics** represent the raw measurements of resource usage or behavior that can be observed and collected throughout your systems. These might be low-level usage summaries provided by the operating system, or they can be higher-level types of data

tied to the specific functionality or work of a component, like requests served per second or membership in a pool of web servers. Some metrics are presented in relation to a total capacity, while others are represented as a rate that indicates the "busyness" of a component. Metrics are useful because they provide insight into the behavior and health of your systems, especially when analyzed in aggregate. They represent the raw material used by your monitoring system to build a holistic view of your environment, automate responses to changes, and alert human beings when required. Metrics are the basic values used to understand historic trends, correlate diverse factors, and measure changes in your performance, consumption, or error rates.

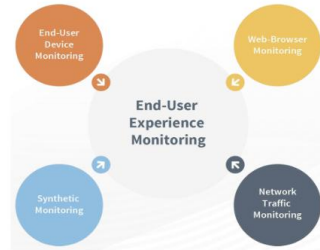
1.10 Types of Monitoring



Monitoring & evaluation has been classified in various types, which is dependent on motive, pivot, timing and target audience.

- **End User Monitoring:** It is an important aspect where the site availability is monitored from the perspective of end user.
- **Infrastructure Monitoring:** The platform from where the applications are being served must be constantly monitored basically the hardware.
- **Application Monitoring:** keeping an eye on the performance of the applications is sacrosanct to meet the industry standards for customer satisfaction.
- **Log Monitoring & Analysis:** It is a type of monitoring where the logs of applications, web-servers and app servers are monitored recording all the events happening across the system.

1.10.1 Types of Monitoring: End User Monitoring



End user monitoring is considered as the monitoring outside of the IT environment from the customer point of view, the parameters which are considered in this are the health of user device, the performance of browser, the health of the network via which the service is being served.

End user monitoring has been classified into four parts:

- End user device monitoring
- Web browser Monitoring
- Network Traffic Monitoring
- Synthetic Monitoring

1.10.2 Types of Monitoring: Infrastructure Monitoring

The following image displays the infrastructure monitoring.

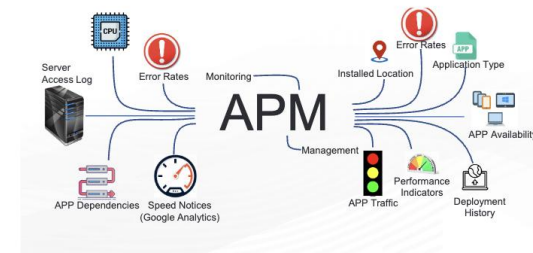


To understand Infrastructure monitoring one needs to understand what is Infrastructure in IT. It is nothing but the hardware on which the application runs, servers, storage devices, network hardware etc. It needs to be monitored because it is the layer below the application and if something is messed up in it then it will ultimately impact the users.

The metrics, which are aggregated from the infrastructure are like CPU, Memory, Network I/O rate. And if these resources are spiking above threshold then the monitoring stack will report the issue. Adequate infrastructure monitoring would have prevented the loss of time, money, and space associated with maintaining unproductive servers.

1.10.3 Types of Monitoring: Application Monitoring

The following image displays the application monitoring.



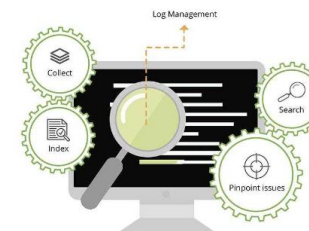
Application performance monitoring is a type of monitoring in which the performance of an application is watched to optimize response time, identify errors and exceptions, proper functioning of components and integration. The main goal is to ensure the application is performing well enough to handle client requests/response.

With the help of Application Monitoring one can watch whether the application is meeting the performance standards or not. It also helps in identifying bugs and potential risks. An APM solutions provides the insight of resource utilisation in application and how the application is handling requests, which helps in identifying the performance issues before they impact the end user.

Application performance monitoring is often confused with "application performance management". The AP management is a strategy of managing performance excellence and Monitoring is a part of it.

1.10.4 Types of Monitoring: Log Monitoring and Analysis

The following image displays the log monitoring and analysis.



Log monitoring is a type of monitoring which keeps an eye over the events aka logs occurring in a system. A system could be servers, applications, network and security devices which generate log files having events based on timestamp. Errors, Info, and debug logs are constantly logged and further saved for analysis.

To identify problems automatically before hand, system administrators and operations team enable monitoring on the generated logs. The log monitoring setup/system skim the log files and search for known text patterns and rules that indicate important events. Once an event is detected, the monitoring system will send an alert, either to a person or to another software/hardware system usually to the NOC team. Monitoring logs help to identify security events that occurred or might occur.

What did You Grasp?



Which one is monitoring of events in a system?

- A) End user monitoring
- B) Infrastructure Monitoring
- C) Application monitoring
- D) Log Monitoring

In a Nutshell



In this module, you learnt:

- Basics of Monitoring
- Need of monitoring
- Approach of monitoring with respect to DevOps
- What is Network Operations Center
- What is the roles and responsibilities of NOC in DevOps world
- What is telemetry and metrics used for monitoring.
- Various aspects of Monitoring

Release Notes

B. TECH CSE with Specialization in DevOps Semester Eight -Year 04

Release Components.
Facilitator Guide, Facilitator Course Presentations, Student Guide, Mock exams and relevant lab guide.

Current Release Version.
1.0.0

Current Release Date.
2nd Jan 2020

Course Description.
Xebia, has been recognized as a leader in DevOps by Gartner and Forrester and this course is created by Xebia to equip students with set of practices, methodologies and tools that emphasizes the collaboration and communication of both software developers and other information-technology (IT) professionals while automating the process of software delivery and infrastructure changes.

Copyright © 2021 Xebia. All rights reserved.

Please note that the information contained in this classroom material is subject to change without notice. Furthermore, this material contains proprietary information that is protected by copyright. No part of this material may be photocopied, reproduced, or translated to another language without the prior consent of Xebia or ODW Inc. Any such complaints can be raised at sales@odw.rocks

The language used in this course is US English. Our sources of reference for grammar, syntax, and mechanics are from The Chicago Manual of Style, The American Heritage Dictionary, and the Microsoft Manual of Style for Technical Publications.

Bugs reported

Next planned release

Not applicable for version 1.0.0

Version 2.0.0 Jan 2021