NetOp

The Ultimate Network Operations & Monitoring Checklist | 2023

www.netop.cloud

Contents

Introduction

Enterprise networks are becoming increasingly complicated, with devices from multiple vendors, distributed networks across multiple locations, and little way to keep tabs on it all. It's no wonder that network operations team members often feel that their users are telling them where the problems are, rather than being able to discover and fix them themselves, before the users ever know about them.

Wifi slowdowns, video conferences that stutter or disconnect, and the inability to be productive are just some examples of end-users' experience. It all comes down to the fact that NetOps teams are too reactive, since they often do not have the right network operations and monitoring solution to give them the information they need to take a proactive approach.

Relying on outdated network operations and monitoring solutions force network operations teams to face challenges such as:

Lack of clear visibility of the physical and logical/service level network topology

Due to the network complexity, each member of the Network Operations team may not have a complete understanding of the network's layout and how all the devices, connections, and services are connected to each other. This lack of visibility can make it difficult to monitor the network effectively and respond quickly to issues that arise. Note that the physical layout of devices in the network differs from the logical or service level network topology, which refers to the way in which services and applications are connected to the network and how they interact with each other.

Siloed dashboards

Often each network device has its own management tool and dashboards, meaning that NetOps teams do not have a comprehensive overall view of what is happening in the network. Besides the inefficiency of having to look at multiple dashboards to see the full picture, it makes it challenging to identify and diagnose issues that affect the network as a whole.

Lack of correlation between different performance metrics and input streams

Available data is often not correlated across multiple devices, making it almost impossible to gain a complete understanding of how different aspects of the network are related and how they impact each other. Identifying and solving problems in such an environment is challenging at best.

Manual, time consuming incident and resolution analysis

Incident and resolution analysis may involve tasks such as manually reviewing logs and alerts, troubleshooting individual devices and connections, and coordinating with other teams and vendors to identify and address issues. These tasks can be time-consuming, require significant expertise and experience, and are prone to human error.

Lack of predictability of network behavior

Without a holistic network operations and monitoring solution, it can be impossible to identify event trends, or to establish the necessary baselines in order to predict future events. This means NetOps teams are always going to be in reaction mode, rather than being able to take proactive measures.

Alert noise and flooding

With multiple monitoring tools and a lack of context for many alerts, it can be difficult to prioritize and filter for the most urgent ones. This makes triaging events problematic.

Skills gap in ever-evolving and scaling complex network management

The rapid pace of technological change, the increasing scale and complexity of networks, and the demand for higher levels of network availability, security, and performance have all contributed to a growing skills gap in the network operations field.

The future of network operations and monitoring is AI - the whole world has discovered AI most recently through the popular rise of ChatGPT and other AI tools, however in the IT world AI has been used to overcome many of the challenges described above by providing real-time analysis, automation, prediction and correlation between alerts. It would be nice if it were as simple as plugging in an AI engine and all your problems are solved. In contrast, even for solutions that say they are AI based, it is still important to look out for the key features described below..

1. Monitor Network Metrics

The basic functionality of your network operations and monitoring solution is to monitor the metrics and thresholds across all relevant domains that ensure the health and performance of the network. This should help NetOps personnel identify and respond to potential network issues before they become critical. While it's important for your solution to monitor metrics in an ongoing way, performance thresholds are predefined levels of acceptable performance; when a metric exceeds a threshold, it can trigger an alert or notification, indicating that there may be an issue that requires attention. The monitoring solution should adapt to individual networks and allow customization of thresholds per network, and the best solutions can do that automatically.

Cross-domain data ingestion and analytics for ongoing monitoring and alerts help NetOps teams identify potential network issues, optimize network performance, and ensure that the network remains reliable and available to support the needs of the organization.

KPIs and other metrics to track

NetOps teams should seek a rich set of metrics for each of these categories:

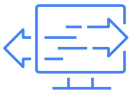
Device level indicators

Clients

Applications

Port and interface level metrics

Wifi



Sessions

Performance thresholds

For each performance threshold, your network operations and monitoring solution should recommend acceptable levels for the different metrics being tracked, as well as be able to define what constitutes an "alert" or "warning" level for each metric. Correlation among anomalies - often done by machine learning - makes it easier for NetOps personnel to determine the root cause of an issue, reduce alert noise, and reduce Mean Time to Resolution (MTTR).

Your network operations and monitoring solution should include:

Multiple severity level thresholds (warning level to critical level)

Ability to identify and track occurrences of events over time

Correlate anomalies

Device and application-specific monitoring needs

Each device and application has its own specific monitoring needs, and your network operations and monitoring solution should be flexible enough to identify each.

Ensure all possible parameters are collected from switch(es)

Ensure all possible parameters are collected from the router(s), SD-WAN and more

Ensure all possible parameters are collected from the firewall(s)

Alerting and notification systems

Alerting and notification systems are an important part of any network operations and monitoring solution, enabling NetOps teams to quickly identify and respond to potential network issues. Besides having different notification channels, it's critical to be able to customize and filter notifications based on severity and/or category, and to take necessary steps to prevent alert fatigue.

An anomaly is an event, behavior, or pattern that is outside of the expected or normal range. Anomalies can be caused by various factors, such as equipment failures, configuration errors, network congestion, or security breaches. Network operations and monitoring systems should have alerts not just on pre-set thresholds, but also on anomalies that pop up. And more advanced solutions – typically based on AI – can deduce that the source of an anomaly is related to several issues originating from one root cause. By automatically correlating these together, the total number of alerts can be significantly reduced.

Ensure highly accessible notification in channels such as email, Slack, WebEx, SMS, voice calls, beeper

Ability to filter any type of event or monitored KPI by severity (critical, high, medium, low) and by category (security, operations, performance, configuration)

Ability to aggregate alerts having the same root cause into a higher level anomaly to reduce alert noise

2. Analysis of network insights

Reporting and analysis tools

Reporting and analysis tools provide critical insights and visibility into network performance and trends. Ensure that your network operations and monitoring tool has these capabilities:

Dashboards
High level information should be available, such as how many issues there are, which networks need attention, how many critical errors there are.

Automated reports
You should be able to receive scheduled reports, comparisons between time frames and trends.

Automated root cause analysis tools
These should contain smart correlation capabilities .

Statistics drill down
You should be able to drill down from the reports into specific KPIs to investigate.

Ability to investigate connectivity between network entities
Ability to analyze events from multiple sources and identify areas that need human attention, automatically.

Prediction

To get ahead of the curve, it's not enough to report on what has already happened; advanced network operations and monitoring solutions should be able to analyze historical data and use machine learning/ artificial intelligence to predict future network performance metrics and even future anomalies.

This can help NetOps teams plan for future network growth, allocate resources more effectively, and avoid potential bottlenecks or issues. Key predictions that your network operations and monitoring solution should include are:

Network behavior prediction

Anomaly prediction

3. Data handling

How your network operations and monitoring solution handles data is important for ensuring compliance, as well as providing the peace of mind that you can recover critical functions in case of disaster. Configurations of network devices must be backed up on a schedule to ensure that they can be quickly restored if necessary, reducing downtime. Firmware and network device operating systems should be upgraded regularly, so they have the latest security patches, bug fixes, and performance enhancements, to perform at their peak capability. These are all things that your network operations and monitoring solution should be able to manage.

Backup and upgrades

- Device periodic backup and restore
- Device firmware/version tracking
- Upgrade tracking and implementation

Data retention and archiving

- Ensure data is retained for some meaningful period (depending on organization needs)
- Ability to customize data retention per your compliance requirements and data recovery plan

4. Day to day adaptability

Your network operations and monitoring solution should be adaptable to your needs, rather than you having to adapt to it. As your organization's and network's demands grow, your solution should be scalable enough to grow with it. It must be able to seamlessly accommodate any additional devices (even from multiple vendors), applications, and new users that are added to the network. This is especially critical for distributed networks. Your solution should be able to deduce network topology changes from both implicit and explicit sources of asset relationships and dependencies - this can include physical connections, such as cables and switches, as well as logical connections, such as software dependencies and communication protocols. In addition, the user interface should be friendly and intuitive to use and customizable to the point where any member of the NetOps team can feel confident while they use the solution. Of course, this can be enhanced by user training, which should be offered by the solution provider.

Scalability

Unlimited devices per network site, with no problem to scale up the number of devices/nodes

Unlimited network sites with the ability to seamlessly add more network sites

User interface and ease of use

Simple drill down flow from customer level to device level

Ensure site level includes clear end-to-end topology from both implicit and explicit sources

Ensure view covers physical as well as service performance indicators, device inventory and device dashboards

Simple flow from notification to troubleshooting and finding root cause

Highlight the most important issues and prioritize them

Final thoughts

By implementing a network operations and monitoring solution that checks all the boxes, your NetOps personnel will remain productive and motivated, while keeping your network functioning optimally. The importance of observability for network operations is paramount, and data across the full stack should be correlated. This will help in the recognition of patterns, relationships and dependencies that when correlated correctly can indicate a probable root cause.

NetOp.cloud adopts the observability paradigm, and its proactive AI-powered network operations and monitoring solution lets you identify and resolve issues faster than users can report them. It gives you real-time visibility and control of your cloud-managed networks, providing you with all the information you need to troubleshoot with ease.

NetOp.cloud uses the latest AI-based technology to continuously learn and understand network behavior to proactively prevent issues while improving performance. NetOp eliminates alert fatigue and simplifies network operations by identifying anomalies, providing early warnings and predicting network behavior. Taking only minutes to deploy, NetOp agentless solution also allows you to easily automate multi-site, multi-vendor network configuration by providing point-and-click scenarios to fix, enhance and optimize the network performance.

Printable Checklist

Network Metrics and Monitoring

Types of metrics to be tracked / KPIs

- ☐ Device level metrics
- ☐ Port and interface level metrics
- ☐ Clients
- ☐ Wifi
- ☐ Applications
- ☐ Sessions

Performance thresholds

- ☐ Multiple severity level thresholds
- ☐ Ability to identify occurrences of event during a range of time
- ☐ Correlate anomalies

Device and application-specific monitoring needs

- ☐ Ensure all possible parameters are collected from switch(es)
- ☐ Ensure all possible parameters are collected from the router(s)
- ☐ Ensure all possible parameters are collected from firewall(s)

Alerting and notification systems

- ☐ Ensure highly accessible notification method
- ☐ Ability to filter by severity and/or category
- ☐ Ability to aggregate alerts with the same root cause

Analysis of Network Insights

Reporting and analysis tools

- ☐ Dashboards
- ☐ Automated reports
- ☐ Automated root cause analysis tools
- ☐ Statistics drill down into KPIs
- ☐ Ability to investigate connectivity between devices on-demand
- ☐ Ability to analyze events from multiple sources and identify areas that need human attention, automatically

Prediction

- ☐ Metric prediction
- ☐ Anomaly prediction

Data handling

Backup and upgrades

- ☐ Device periodic backup and restore
- ☐ Device firmware/ version tracking
- ☐ Upgrade tracking and implementation

Data retention and archiving

- ☐ Ensure data is retained for at least 6 months
- ☐ Customizable data retention policy

Day to day adaptability

Scalability

- ☐ Unlimited devices per network site
- ☐ Unlimited network sites

User interface and ease of use

- ☐ Simple drill down flow from customer to site level
- ☐ Clear topology at site level
- ☐ Ensure view covers physical and logical health, device inventory, device dashboards
- ☐ Simple flow from notification to troubleshooting and finding root cause
- ☐ Highlight most important issues for and prioritize