Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2021, 8(1):120-122

Research Article ISSN: 2394 - 658X

Monitoring Network Devices Using Zabbix with Remedy Integration for Auto-Ticketing Functionality

Mohit Bajpai

ABSTRACT

The rapid growth and complexity of computer networks pose significant challenges for network administrators in maintaining network health and ensuring seamless operations. This paper presents a detailed technical approach to monitoring network edge devices using the Zabbix open-source monitoring platform, integrated with the Remedy ticketing system to enable automated incident management and dispatch functionality. The proposed architecture outlines the integration of Zabbix with Remedy, enabling real-time monitoring, intelligent alert handling, and automated ticket generation for swift incident response and resolution.

Keywords: Network monitoring, Zabbix, Remedy, Auto-ticketing, Integration, devices

INTRODUCTION

The proliferation of network-connected devices, such as routers, switches, and access points, coupled with the increasing complexity of IT infrastructure and the growing reliance on network-dependent services, have made effective network monitoring a critical requirement for organizations. Traditional network monitoring approaches often rely on manual operations, which can be time-consuming, error-prone, and resource-intensive. To address these challenges, this paper explores the integration of the Zabbix open-source monitoring platform, a versatile network monitoring tool that offers real-time monitoring, alerting, and reporting capabilities, with the Remedy incident management system, a widely used solution for incident handling, change management, and service desk operations.

The Zabbix monitoring platform is capable of collecting data from network edge devices using a variety of protocols, including SNMP, ICMP, and syslog. Zabbix can analyze the collected data, identify anomalies, and trigger alerts based on pre-configured rules and thresholds. By leveraging Zabbix's monitoring capabilities, organizations can proactively identify and address network issues, ensuring the reliability and availability of their IT infrastructure. [1] [2] [3]

The integration of Zabbix with the Remedy incident management system presents an opportunity to enhance the efficiency and effectiveness of network monitoring and incident management. When Zabbix generates an alert, it can automatically create a corresponding incident ticket in Remedy, which includes relevant information about the issue, such as device details, alert severity, and potential root causes. The Remedy system then handles the incident through its standard workflow, including assignment, escalation, and resolution tracking, ensuring that network issues are promptly detected, documented, and addressed.

HIGH-LEVEL INTEGRATED ARCHITECTURE

The Zabbix monitoring platform is responsible for continuously collecting data from the network edge devices, analyzing the collected metrics, and generating alerts based on pre-defined thresholds.

The Remedy incident management system is integrated with middleware APIs and Zabbix to automatically create and manage incident tickets based on the triggers generated by Zabbix. [4] [5]

The proposed monitoring and incident management solution integrates the Zabbix monitoring platform with the Remedy service management system, providing a comprehensive approach to network edge device monitoring and incident response.

The high-level architecture depicts the key components and interactions within the integrated system:

The integrated architecture showcases the seamless interaction between the Zabbix monitoring platform and the Remedy incident management system via middleware APIs. When the Zabbix detects an issue or anomaly on the network edge devices or network components a trigger is created.

The middleware/APIs then pulls the list of unacknowledged triggers from the Zabbix instances. And then process those triggers to create tickets in Remedy system based on the information provided by Zabbix, including device details, alert severity, and potential root causes. The auto-ticketing functionality streamlines the incident management process by eliminating the need for manual ticket creation, reducing response times, and improving the overall efficiency of the IT operations team.

The Remedy system then assigns the incident ticket to the appropriate team or individual based on pre-configured rules and escalation policies, ensuring that critical issues are addressed promptly.

The comprehensive solution presented in this paper leverages the strengths of both the Zabbix monitoring platform and the Remedy incident management system to provide a robust and efficient approach to network edge device monitoring.

The Zabbix monitoring platform collects data from network edge devices, such as routers, switches, and access points, using a variety of protocols, including SNMP, and ICMP.

Here is a diagram (Figure 1) depicting scenario where Zabbix and Remedy systems are integrated via middleware APIs to create a seamless issue detection and ticket creation and dispatch the technician based on the issue.

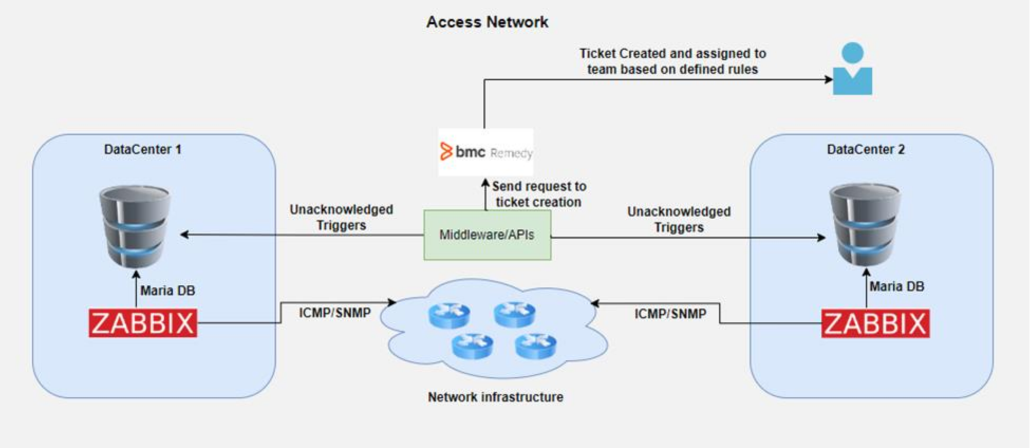
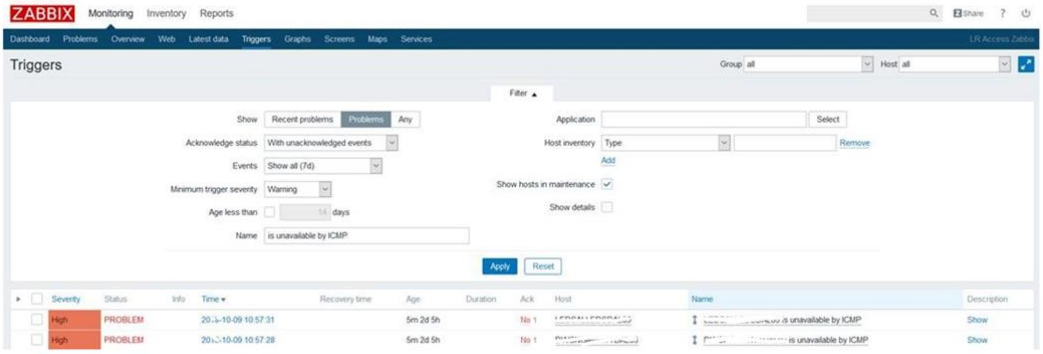


Figure 1



Group: all
Host: all

Show: Recent problems | **Problems** | Any
Acknowledge status: With unacknowledged events
Events: Show all (7d)
Minimum trigger severity: Warning
Age less than: □ 14 days
Name: is unavailable by ICMP
Application:
Host inventory: Type
Show hosts in maintenance: ☑
Show details: □

Severity	Status	Info	Time ▾	Recovery time	Age	Duration	Ack	Host	Name	Description
High	PROBLEM		20[redacted]-10-09 10:57:31		5m 2d 5h		No 1	[redacted]	[redacted] is unavailable by ICMP	Show
High	PROBLEM		20[redacted]-10-09 10:57:28		5m 2d 5h		No 1	[redacted]	[redacted] is unavailable by ICMP	Show

Figure 2: above shows Triggers configurations setup for a given scenario.

ZABBIX CONFIGURATION AND MONITORING

Zabbix is configured to monitor various network edge devices, including routers, switches, and access points, using a combination of SNMP, ICMP, and syslog data collection methods.

The monitoring configuration includes the following key elements:

Device Discovery: Zabbix automatically discovers network devices based on IP ranges, SNMP community strings, or other identification criteria, ensuring comprehensive coverage of the network infrastructure.

Metrics Collection: Zabbix collects a wide range of metrics from the monitored devices, such as CPU utilization, memory usage, interface status, and error rates, providing a comprehensive view of the network's health.

Thresholds and Alerts: Zabbix is configured with pre-defined thresholds and alert rules to identify and notify on critical conditions, such as high CPU utilization, interface down events, or unusual traffic patterns.

Reporting and Dashboards: Zabbix provides robust reporting and visualization capabilities, enabling network administrators to monitor the overall health of the network, identify trends, and generate customized reports.

The integration of Zabbix with the Remedy incident management system ensures that network issues are automatically documented, assigned, and escalated, improving the overall responsiveness and efficiency of the IT operations team.

The comprehensive solution presented in this paper leverages the strengths of both the Zabbix monitoring platform and the Remedy incident management system to provide a robust and efficient approach to network edge device monitoring.

CONCLUSION

This paper has presented a detailed technical approach for monitoring network edge devices using the Zabbix open-source monitoring platform, integrated with the Remedy incident management system for auto-ticketing and dispatch functionality.

The proposed solution combines the real-time monitoring and alerting capabilities of Zabbix with the incident management and workflow automation features of Remedy, creating a comprehensive solution that enhances the efficiency and responsiveness of IT operations [6].

The integration of the Zabbix monitoring platform and Remedy incident management system enables organizations to enhance their network visibility, expedite incident response, and optimize incident resolution, ultimately contributing to improved network reliability and availability [4] [6] [2].

REFERENCE

[1]. Cong, P., Shenghua, B., Hongliang, Z., & Baoyu, T. (2020, June 1). Research on Cluster Monitoring and Prediction Platform based on Zabbix Technology. IOP Publishing, 512(1), 012155-012155. https://doi.org/10.1088/1755-1315/512/1/012155

[2]. Khan, R., & Khan, S U. (2018, March 1). Design and implementation of an automated network monitoring and reporting back system. Elsevier BV, 9, 24-34. https://doi.org/10.1016/j.jii.2017.11.001

[3]. Lee, S., Levanti, K., & Kim, H S. (2014, June 1). Network monitoring: Present and future. Elsevier BV, 65, 84-98. https://doi.org/10.1016/j.comnet.2014.03.007

[4]. Ljubojević, M., Bajic, A., & Mijić, D. (2018, March 1). Centralized monitoring of computer networks using Zenoss open source platform. https://doi.org/10.1109/infoteh.2018.8345528

[5]. Orrick, D., Bauer, J., & McDuffie, E. (2000, October 1). Remedial help desk 101 at Florida State University. https://doi.org/10.1145/354908.354958

[6]. Zhou, W., Tang, L., Zeng, C., Li, T., Shwartz, L., & Grabarnik, G Y. (2016, December 1). Resolution Recommendation for Event Tickets in Service Management. Institute of Electrical and Electronics Engineers, 13(4), 954-967 https://doi.org/10.1109/tnsm.2016.2587807

[7]. BMC Software. (2020). BMC Remedy ITSM Suite Overview. BMC Software. Retrieved from https://www.bmc.com/it-solutions/remedy-itsm.html

[8]. Zabbix (2020) https://www.zabbix.com/rn/rn5.0.0