PiManager

Michael Wojtaszek[1], Corbin Hakimian[1], Sunjae Park[1], Magdy Ellabidy[1], and Mira Yun[2]

[1]School of Computing and Data Science, Wentworth Institute of Technology, Boston, USA

[2]Department of Computer Science, Boston College, Chestnut Hill, USA

{wojtaszekm, hakimianc, parks6, ellabidym}@wit.edu, mira.yun@bc.edu

Abstract

As cyber-attacks become more common in our digital age, it becomes more important that individuals and organizations can defend themselves against network attacks. Organizations can defend themselves against these kinds of attacks using network monitoring systems. However, these systems are often expensive and difficult to maintain and setup. We propose a solution, *PiManager*, involving off-the-shelf computing and communication devices and open-source software that allows the individual users or small organizations to protect their network against attacks at low cost. Network managers and learners of all levels can easily re-create our project and gain the ability to protect their network by monitoring network traffic and data flows.

Keywords – Network Management System, Raspberry Pi, Open-source Software.

I. INTRODUCTION

The Federal Bureau of Investigation reported 847,376 complaints of suspected internet crime in 2021, a 7% increase from 2020 that resulted in losses exceeding $6.9 billion [1]. In today's day and age, cyber-attacks are at an all-time high. To defend against these attacks, it is critical to first detect that such attacks are occurring; as a result, network monitoring tools and solutions are becoming an essential part to many organizations and individuals. Network monitoring tools allow network administrators to see incoming attacks as they are happening. Network administrators can then take preventative measures and determine the best strategy to block the attack.

A Network Management System (NMS) [1] is a set of applications that identifies, configures, monitors, updates, and troubleshoots network devices in the enterprise. NMSs have long been available to organizations and network engineers to handle a variety of network operations. However, most NMSs are not cost effective for individual users, and many of the high-end options tend to provide too many features that would not be useful for small scale networks. Industry organizations typically spend thousands of dollars a month on network monitoring tools to protect themselves against wireless attacks. They also want to ensure that their software runs 24/7 without having any issues. Network and system management companies such as SolarWinds [3] offer a diverse range in network nanagement software and monitoring tools. For instance, they offer performance prediction for bottleneck analysis and predict capacity usage. They offer tools that allow administrators to visualize complicated networks and identify unknown devices that may come and go in any large-scale network. These are all tools that can prove useful when managing multiple networks, with strict uptime requirements, and so on. The only issue with SolarWinds products is that they range in prices upwards of thousands of dollars. They fail to provide a cost-friendly alternative for people looking to implement an NMS into their private network or small business.

Our solution, *PiManager*, offers many of the same features as higher-end products, but achieves this at an affordable price. *PiManager* provides features such as network service and host resource monitoring, automatic log file rotation, parallelized service checks among others. *PiManager* uses open-source solutions such as Zabbix[4] with Raspberry Pi [5], an off-the-shelf low-cost computing device [6][7]. *PiManager* aims to provide is a network monitoring system that is both cost effective and easy to use.

II. NETWORK MANAGEMENT SYSTEM

An NMS is an application or set of applications that identifies, configures, monitors, updates, and troubleshoots network devices in the enterprise. Network engineers use a network monitoring system to handle a variety of operations:

- Monitor performance: NMS collects operating metrics through a series of polling, informs and or traps. Using software agents or Simple Network Management Protocol (SNMP) interfaces, an NMS can provide the visibility necessary to determine if network elements are operating correctly.
- Detect devices: NMS is used to detect devices on the network and to ensure the devices are recognized and configured correctly.
- Analyze performance: NMS is used to track performance data indicators, including bandwidth utilization, packet loss, latency, availability and uptime of routers, switches, servers, and other network components.
- Enable notifications: In the event of a system disruption, an NMS will proactively alert administrators about any performance issues.

NMS software can be installed either on premises on a dedicated server/s and managed on site, or accessed as a service on the cloud, where the vendor supplies the tools, the enterprise uses to administer and monitor its network. NMS software can manage a wide variety of network components, manufactured by multiple vendors.

NMS can be used to monitor both wired and wireless network elements. NMS software can also allow companies to track performance throughout their own networks, as well as through external networks, such as those operated by cloud and as-a-service providers. Visibility is enabled through APIs and other means through which an enterprise can access performance flow data, or logs, to analyze security or performance.

As network hardware vendors continue to make their systems more open, NMS software is enabling interoperability as enterprises use network monitoring systems tools to control and add features across a wider variety of devices. NMS is also serving as the framework for Intent-based networking, a developing methodology in which network oversight, configuration and troubleshooting is automated.

III. PIMANAGER

There are a lot of competitive options when it comes to selecting an NMS. Open-source solutions are attractive from the cost perspective, and because they are able to freely receive updates from a community-maintained project. In addition to cost, there are other motives in which networking professionals would choose another NMS. Most of those motives come down to ease of use and learnability of the platform. Some open-source solutions we considered implementing in our project include Cacti [8] and Nagios Enterprise Monitoring Server (NEMS) [9], and finally, Zabbix [4].

Cacti is an open-source network graphing solution that provides robust operational monitoring and fault management framework. It was our original choice of implementation when considering NMS platforms. However, it had compatibility issues with the wireless access point we use. While Cacti has been deemed to run faster queries compared to Zabbix, Zabbix is more of a mature platform making it more reliable in other ways [9].

NEMS Linux [9] is a well-regarded enterprise monitoring server. In addition to free enterprise services, they provide free offsite backups. The platform also comes with a wide variety of features and plugins. However, when it comes to ease-of-use and user experience, this is where Zabbix performs much better than NEMS.

We ultimately decided to go with using an open-source program called Zabbix [4]. Figure 1 shows Zabbix website displaying main features of Zabbix. We use Zabbix because it is open-source and it provids a relatively easy installation process, which is crucial for inexperienced users trying to implement an NMS in their home networks. Although open-source and freely available, Zabbix still provides features similar to the large-scale products like SolarWinds. It includes features such as metric collection, auto discovery, flexible and extendable data gathering, templating, flexible problem definition, proactive network monitoring and much more.

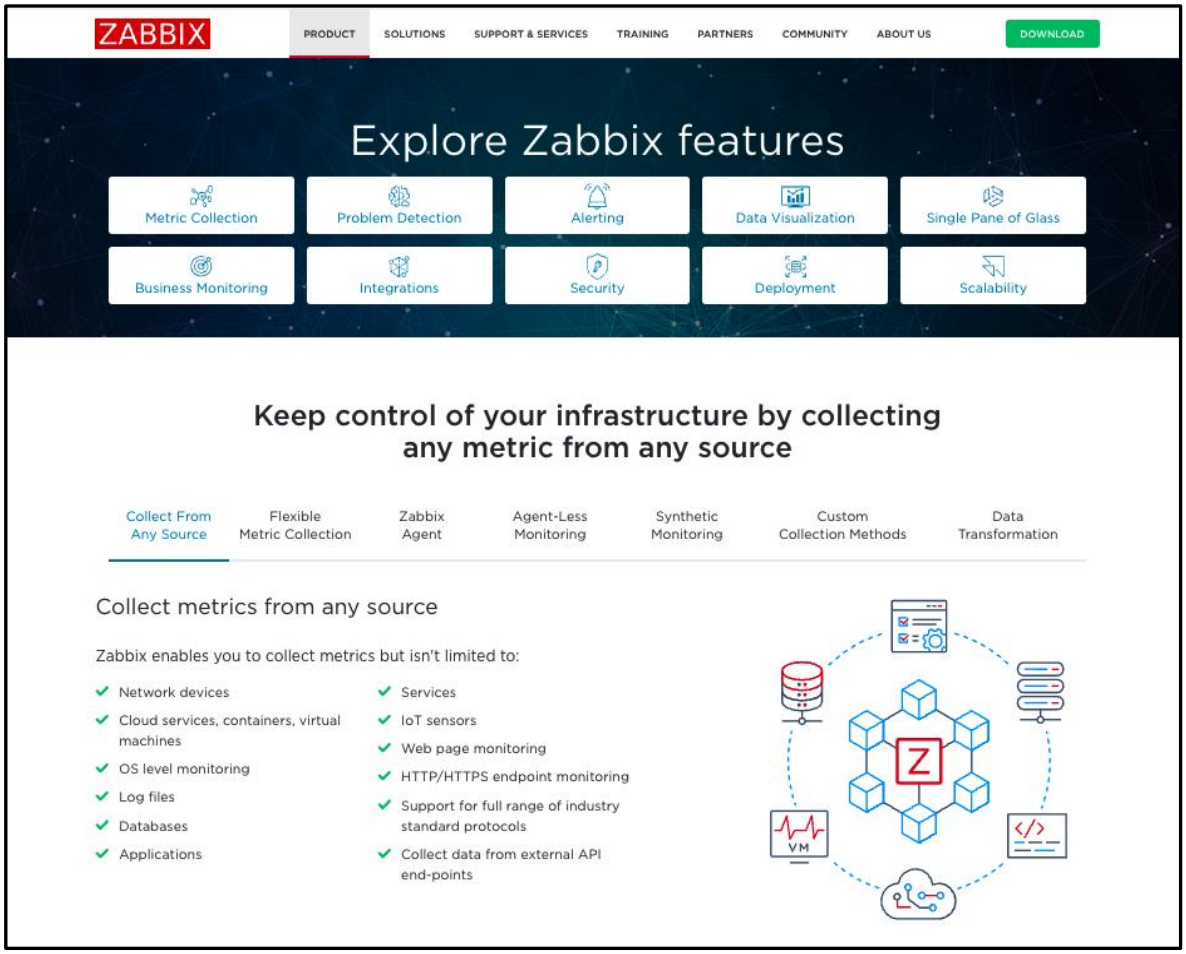

Figure 1: Zabbix website displaying main features of Zabbix

3.1 Hardware

PiManager uses a Raspberry Pi 3. The Raspberry Pi is a portable off-the-shelf computing device that is widely used for a variety of monitoring activities [6][7]. In addition, it is cost effective, ranging for around $40-50 USD that offers all the necessary hardware features for Zabbix to run efficiently. Any Secure Digital (SD) card with 16GB available can be sufficient enough for installing Zabbix. *PiManager* uses a Linksys WRT54GL wireless access point and a Lenovo P51 ThinkPad to work as the SNMP host.

3.2 Installation

Before installing Zabbix onto the Raspberry Pi, the board requires that the most up to date Operating System (OS) be installed along with Secure Shell (SSH) being enabled. Install the SD card into the Pi and connect the power source and Ethernet cable into the Pi. The Ethernet cable is then plugged directly into one of the switch ports on the Linksys WRT54GL router. Once the hardware setup is complete, complete the OS installation and enable SSH.

Next, Zabbix needs to be installed. When it comes to Zabbix, users do need to understand a fair bit of technical knowledge before delving into the platform. Zabbix provides a relatively straight forward installation guide that lists all the needed commands to get the Zabbix server up and running [4]. One of the key features in the development process is the creation of the MySQL database management system which provided the enablement of data warehousing. Figure 2 shows Zabbix dashboard functioning on the Raspberry Pi.

After the installation of Zabbix on our Raspberry Pi, we then moved onto setting up SNMP for our Windows 10 Host device. SNMP is a protocol designed for collecting and organizing information about managed devices on IP networks. As shown in Figure 3, we enabled SNMP on windows10 machine and it allows the acceptance of SNMP packets form the host aka the Zabbix server.

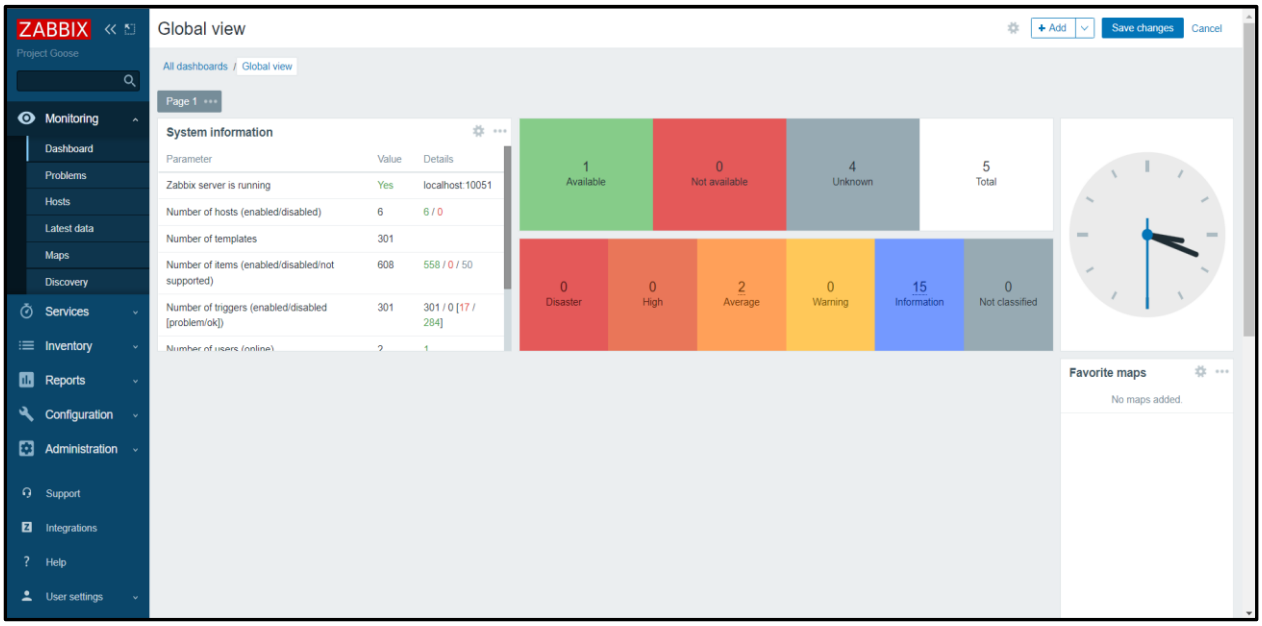

Figure 2: Zabbix Dashboard

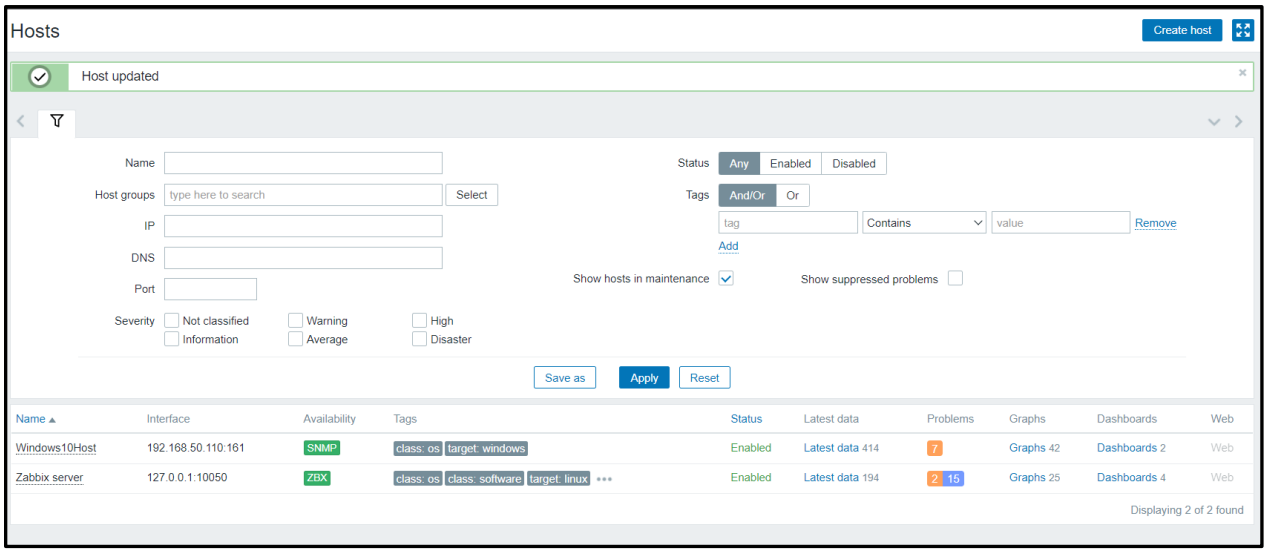

Figure 3: SNMP on Window10 Host

After we successfully setup and enabled SNMP to work with our Windows 10 host device, we can monitor traffic that flows through our network. Figure 4 shows our wireless traffic that flows through our Linksys wireless access point. A long with the option to view current traffic, we can also view previous traffic history that may be proven useful when looking for spikes in traffic in the network as shown in Figure 4.

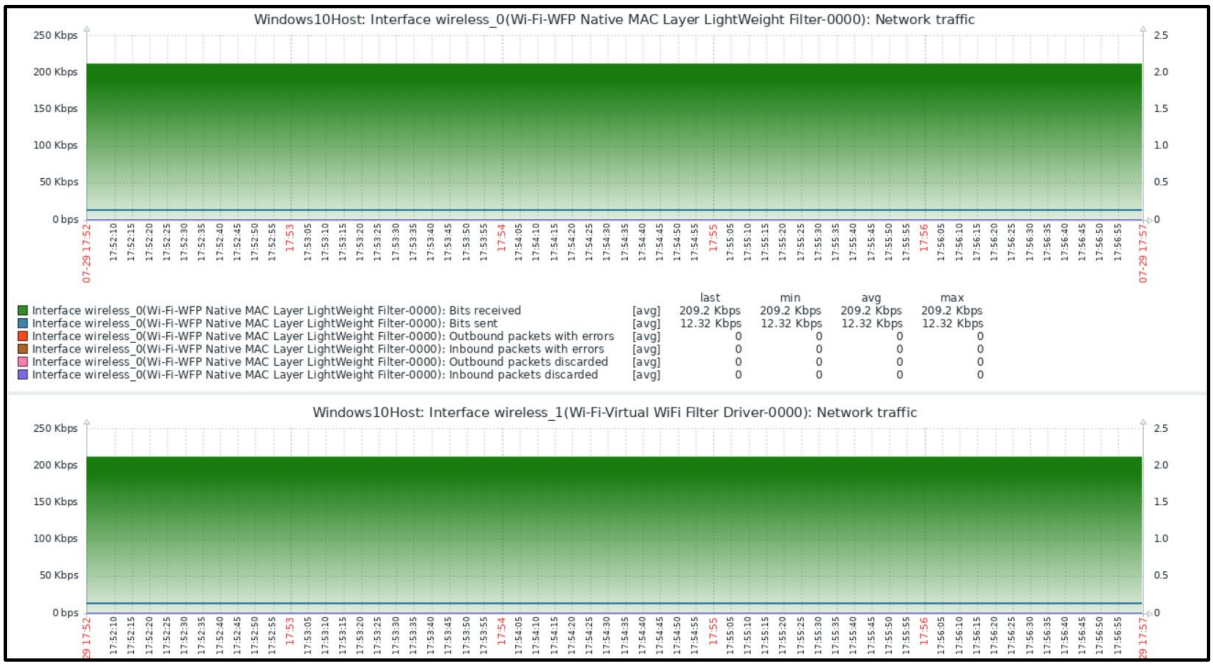

Figure 4: Shows a graph displaying the current traffic that is flowing through our network

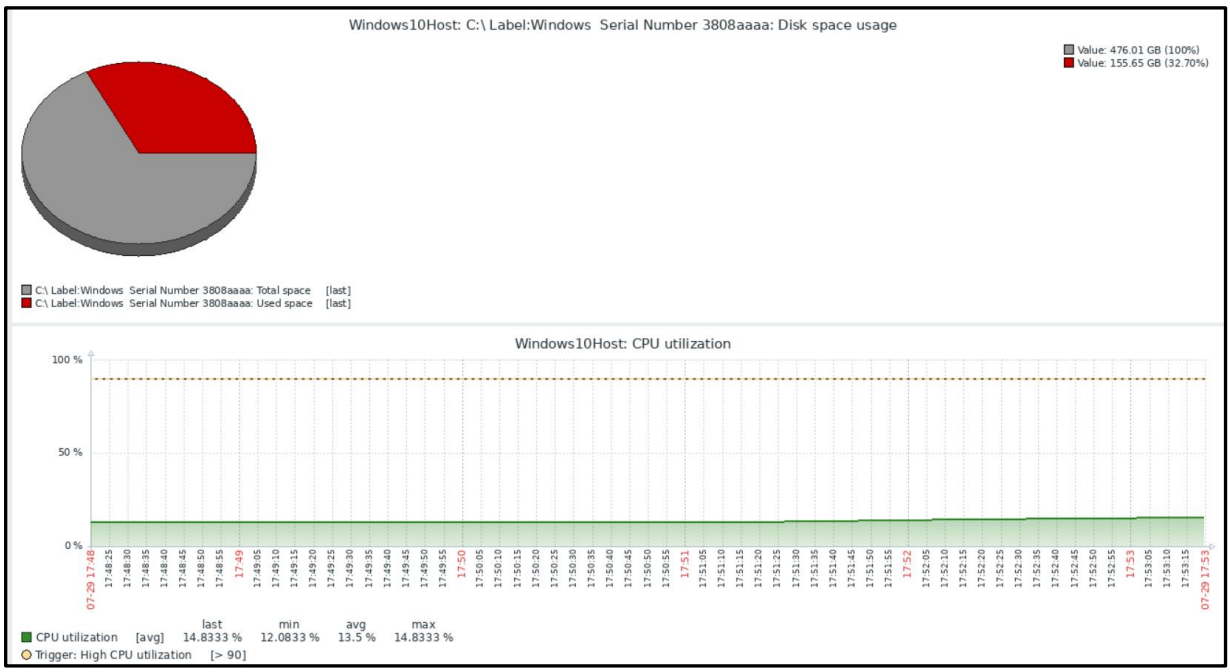

Figure 5: CPU utilization and disk space usage

As shown in Figure 5, *PiManager* also can show real-time CPU utilization and disk space usage status. This feature is beneficial when observing the physical stress on the hardware when the network comes under load.

In this paper, we showed only be a few examples of all the features *PiManager* offers. However, our *PiManager* has proven to be a low-cost alternative to large scale NMS products like SolarWinds. *PiManager* can allow small scale companies or home users the opportunity to upgrade their network security at a low cost. An NMS is a crucial system that every network should have when protecting against attacks. For example, when an attacker decides to start a distributed denial-of-service (DDoS) attack on a network, the network administrators can see the incoming traffic and data flows via *PiManager*, allowing for the opportunity to block the incoming attack.

IV. CONCLUSION

PiManager provides everyday consumers a more cost affordable NMS solution within any environment. Our project, PiManager, helps beginners who are new to utilizing network management tools to understand how to create an NMS. We also wanted to ensure open-source software was used to make sure costs were minimized. And levels of learners and network administrators can easily re-create our project using a Raspberry Pi, an SD card, a windows machine, and Zabbix. Once our solutions are installed properly, network administrators gain the ability to protect their network by monitoring: CPU utilization, disk space usage, and network traffic.

Compared to pricier competitors on the market, we provide a functional NMS that would only cost a consumer approximately $200 as a one-time payment. While on other hand solutions such as SolarWinds cost more than $1,000 to run monthly. Not to mention our solution is much easier to maintain and setup, that even people with limited networking experience can get it to work. Our main objective is to allow users to be able to find and use an affordable NMS.

REFERENCES

[1] WECT [Online]. Available: https://www.wect.com/2022/03/23/fbi-releases-2021-internet-crime-report/, Published: Mar. 23, 2022

[2] Lee, S., and Levanti, K., and Kim, H. S. "Network monitoring: Present and future." Computer Networks, Volume 65, 2014.

[3] SolarWinds [Online]. Available: https://www.solarwinds.com/[Accessed: 02-Mar-2022].

[4] Zabbix [Online]. Available: https://www.zabbix.com [Accessed: 02-Mar-2022].

[5] Raspberry Pi [Online]. Available: https://www.raspberrypi.org/ [Accessed: 02-Mar-2022].

[6] Mani Dheeraj Mudaliar and N. Sivakumar, "IoT based real time energy monitoring system using Raspberry Pi," Internet of Things, Volume 12, 2020.

[7] Sforzin, Alessandro, et al. "Rpids: Raspberry pi ids—a fruitful intrusion detection system for iot." 2016 Intl IEEE Conferences on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld). 2016.

[8] Cacti [Online]. Available: https://www.cacti.net/ [Accessed: 02-Mar-2022].

[9] Nagios Enterprise Monitoring Server [Online]. Available: https://nemslinux.com/vision/ [Accessed: 02-Mar-2022].

[10] Zabbix vs Cacti Comparison [Online]. Available: https://www.getapp.com/it-management-software/a/zabbix/compare/cacti/ [Accessed: 02-Mar-2022].