

Innovative Cyber-Range Solution for W.L.S. Are The Best LLC.

By: Mason Riley, Sujay Kanwar, Muhammad Adeel, Huzaifah Majid



Meet our Team: Mitnick Mavericks

Adeel

- Cybersecurity expert with background in SIEM and Incident response.



Sujay

- Cybersecurity Graduate from Rutgers University
- Experience With Industry Standard Network Analysis Tools



Mason

- Assistant System Administrator at Rutgers University New Brunswick
- Cloud Architect Enthusiast with a focus on Cybersecurity



Huzaifah

- Security+ Certified
- Double Major CS & ITI
- Linking secure solutions

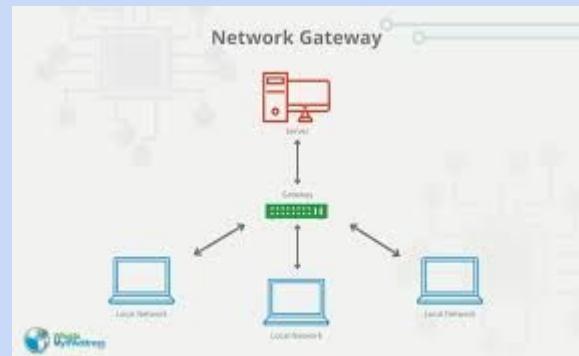


Executive Summary

- Objectives
- Standards
- Our Solution

Executive Summary

OBJECTIVE:



- Network gateway



- Company website



- Service uptime

Executive Summary contd.

Standards:

Compliant with WEF (Warren's Exciting Framework)

Our Commitment to You

By the end of this project we guarantee a solution that allows for monitoring of the following W.L.S services:

- **Network Gateway**
- **Website**
- **Uptime**



What do we need from you?

- Selection of virtual environments to monitor for log purposes



Project Assumptions



Rules:

- Adherence to predefined timelines
- Maintaining communication
- Ensuring quality



Our Needs:

- Collaboration and accessibility to necessary resources and information from W.L.S.

Our Resources:

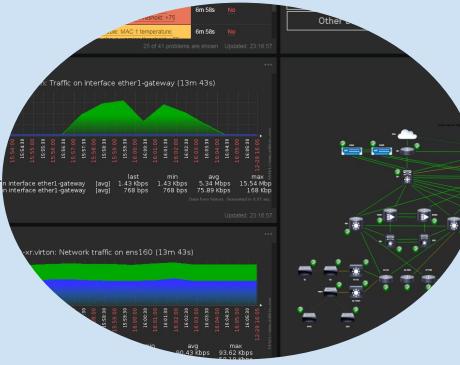
- Expert team, advanced mon dedicated support.



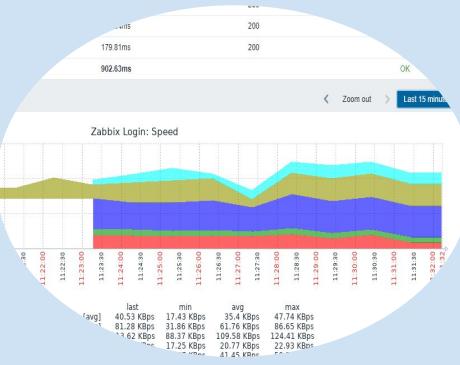
OUR SOLUTION:



Improved Network Security

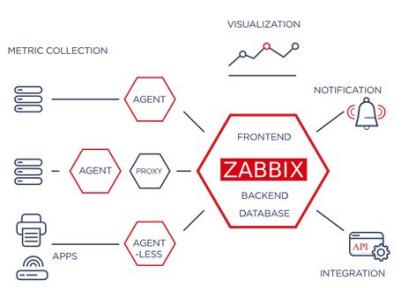


Reliable Website Monitoring



Thorough Gateway Analysis

HOW?



ZABBIX

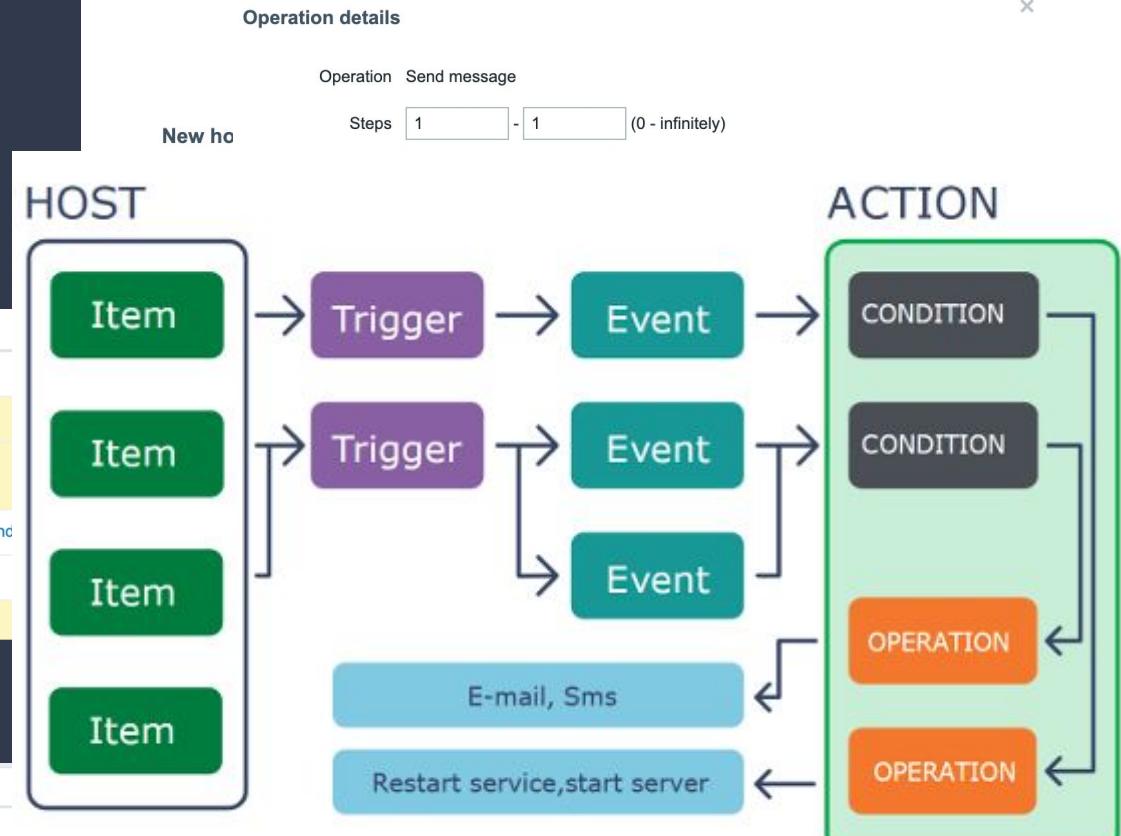
- Real-time insights
 - Network Health
 - Website Performance
- User-friendly interface
- Scalability

Zabbix Guide

- Step 1:
- Step 2:
- Step 3:
- Step 4:

Create a Host
Adjust hosts
Create Triggers
Create Alerts

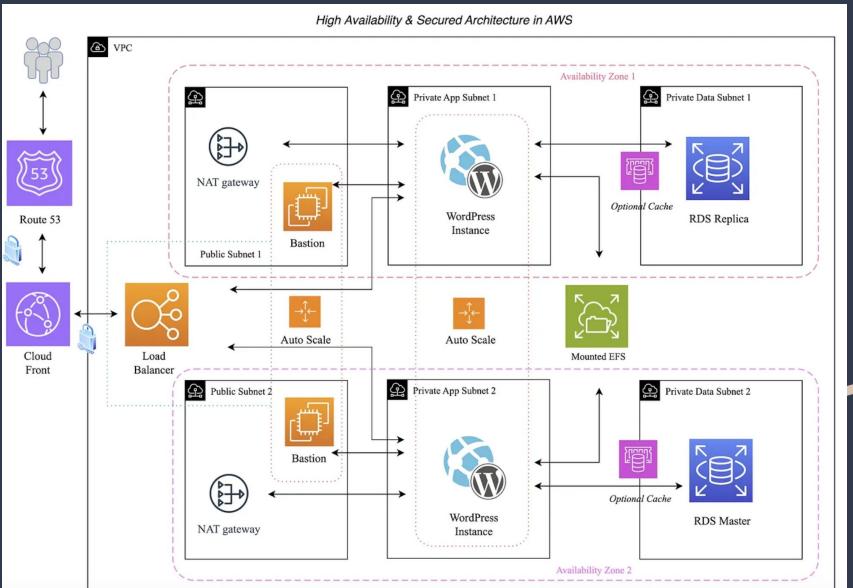
Severity	Value	Name ▲	Operational data
<input type="checkbox"/>	Information	OK	Linux by Zabbix agent: Linux: /etc/passwd has been changed
<input type="checkbox"/>	Name ▲		Conditions
<input type="checkbox"/>	NOTIFY DR. ALLAN		Trigger equals 8aa0e2f0d052: Docker: Service is down



Send message to users: Admin (Zabbix Administrator) via Email
Send message to user groups: Internal via Email

Enabled

Zabbix + Cloud



- On-site setup will limit
 - Scalability
 - Fault tolerance
 -

Never forget about security and a safety of your Zabbix. There are some ideas that you can employ on your Zabbix on a Clouds:

- Separating database and cluster infrastructure in a different VPC and control access between those VPC's;
- Secure access to your Zabbix internal VPC reserved for administrative personnel;
- Zabbix database holding lot's of sensitive data. Think about encryption of the database and/or volume.
- Use encryption for the traffic between Server and Proxies. Use the certificates, not PSK.
- Use Vaults for storing sensitive configuration files, such as zabbix_server.conf

Beyond Monitoring: Enhancing Cybersecurity

- **Enhanced Security**
 - Implement Intrusion Detection
 - Conduct Threat Analysis
- **Cybersecurity Awareness**
 - Workshops for W.L.S. Staff
 - Regular Training Sessions
- **Advance Monitoring solutions**
 - Insightful Lab Function Analysis
- **Hands On Training**
 - Lab Environments for Security Training
 - Focus on Common Web Exploits
- **Monitoring Skills Development**
 - Understanding Monitoring with Docker



Zabbix Agent Monitoring

ZABBIX					
SVR-ZABBIX					
Dashboards					
Monitoring					
Problems					
Hosts					
Latest data					
Maps					
Discovery					
Services					
Inventory					
Reports					
Data collection					
Alerts					
Users					
Administration					
Workstation	State of service "iphpsvc" (IP Helper)	189	Running (0)	component_system	name: IP Helper service: iphsvc
Workstation	State of service "InI_Service" (Intel(R) Dynamic Application Loader Host Interface)	179	Running (0)	component_system	name: Intel(R) Dyn... service: InI_Servic...
Workstation	State of service "LanmanServer" (Server)	168	Running (0)	component_system	name: Server service: LanmanServ...
Workstation	State of service "LanmanWorkstation" (Workstation)	158	Running (0)	component_system	name: Workstation service: LanmanWor...
Workstation	State of service "LSM" (Local Session Manager)	148	Running (0)	component_system	name: Local Session service: LSM
Workstation	State of service "mpssvc" (Windows Defender Firewall)	138	Running (0)	component_system	name: Windows Defe... service: mpssvc
Workstation	State of service "nsi" (Network Store Interface Service)	128	Running (0)	component_system	name: Network Sto... service: nsi
Workstation	State of service "NvContainerLocalSystem" (NVIDIA LocalSystem Container)	118	Running (0)	component_system	name: NVIDIA Local... service: NvContain...
Workstation	State of service "NVDisplay.ContainerLocalSystem" (NVID/A Display Container LS)	108	Running (0)	component_system	name: NVIDIA Disp... service: NVDisplay_C...
Workstation	State of service "PcaSvc" (Program Compatibility Assistant Service)	98	Running (0)	component_system	name: Program Com... service: PcaSvc
Workstation	State of service "Power" (Power)	88	Running (0)	component_system	name: Power service: Power
Workstation	State of service "Pro!SvC" (User Profile Service)	78	Running (0)	component_system	name: User Profil... service: Pro!SvC
Workstation	State of service "QBCFMonitorService" (QBCFMonitorService)	68	Running (0)	component_system	name: QBCFMonit... service: QBCFMonit...
Workstation	State of service "QBVS" (QBVSService)	58	Running (0)	component_system	name: QBVSService service: QBVS
Workstation	State of service "RpcEptMapper" (RPC Endpoint Mapper)	48	Running (0)	component_system	name: RPC Endpoi... service: RpcEptMappe...
Workstation	State of service "RpcSs" (Remote Procedure Call (RPC))	38	Running (0)	component_system	name: Remote Proc... service: RpcSs
Workstation	State of service "RtkAudioUniversalService" (Realtek Audio Universal Service)	28	Running (0)	component_system	name: Realtek Audi... service: RtkAudioUn...
Workstation	State of service "SamSs" (Security Accounts Manager)	18	Running (0)	component_system	name: Security Acco... service: SamSs
Workstation	State of service "Schedule" (Task Scheduler)	0	Running (0)	component_system	name: Task Scheduler service: Schedule
Workstation	State of service "SENS" (System Event Notification Service)	598	Running (0)	component_system	name: System Event service: SENS
Workstation	State of service "SqmBroker" (System Guard Runtime Monitor Broker)	588	Running (0)	component_system	name: System Guar... service: SqmBroker

Sample Dashboards



Phases

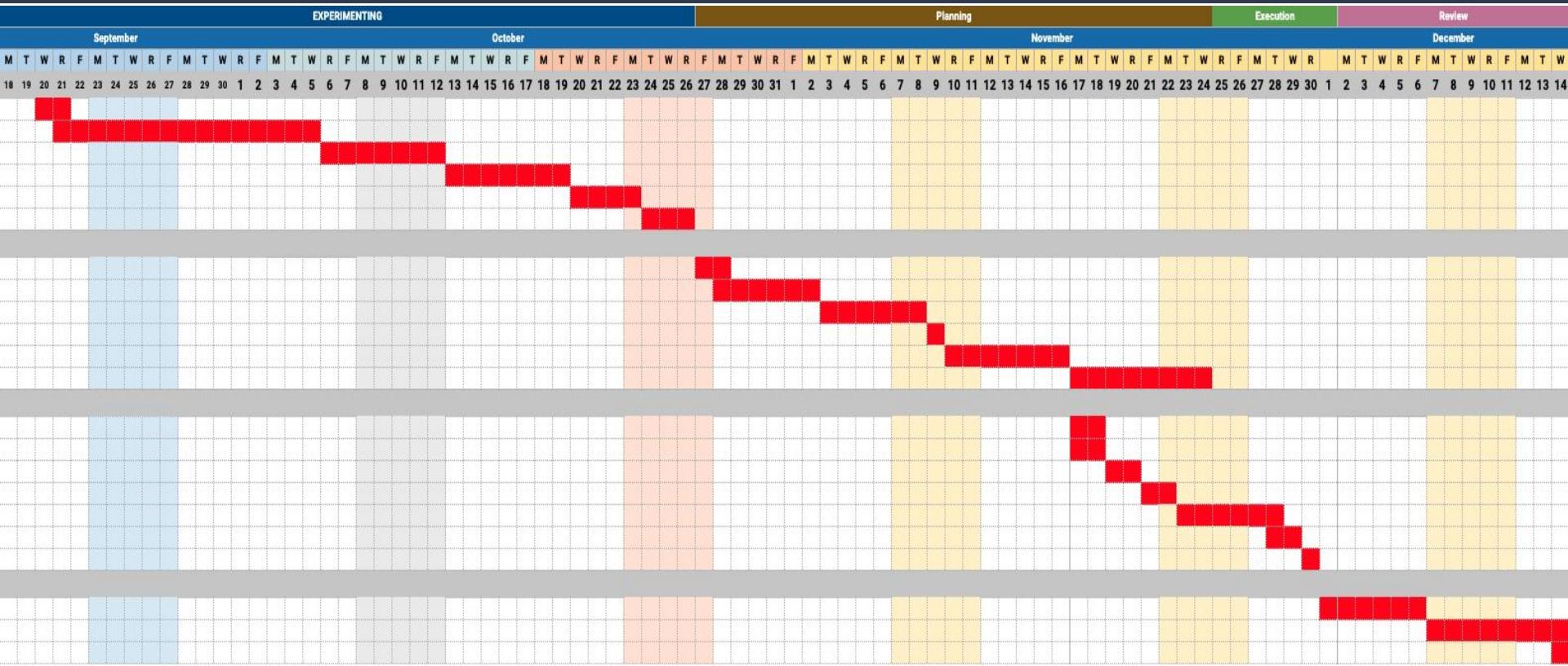
Phase	Activities
Phase 1: Planning and Initiation	Assess infrastructure; Set up Zabbix in Docker; Develop monitoring strategy
Phase 2: Fieldwork	Implement Zabbix on AWS WordPress site; Configure alerts and metrics; Optimize system
Phase 3: Reporting / Results	Report activities and findings; Evaluate system performance; Adjust and discuss scalability

Detailed Timeline

1 Project Conception and Initiation		Start	End	3 Project Conception and Initiation			
1.1	Virtualization	9/20/23	9/21/23	3.1	Set Up Docker Containers	11/17/23	11/18/23
1.2	Learn Kali Linux	9/21/23	10/5/23	3.2	Set up Bridged Virtual Machines	11/17/23	11/18/23
1.3	Networking Fundamentals	10/6/23	10/12/23	3.3	Configure Zabbix	11/19/23	11/20/23
1.4	Nmap	10/13/23	10/19/23	3.4	AWS Cloud Deployment	11/21/23	11/22/23
1.5	NetDevOps	10/20/23	10/23/23	3.5	Solution Updates	11/23/23	11/28/23
1.6	Docker	10/24/23	10/26/23	3.6	Testing	11/28/23	11/29/23
2 Project Definition and Planning		3.7		3.7	Presentation	11/30/23	11/30/23
2.1	Cyber Range Scope Requirements	10/27/23	10/28/23	4 Project Performance / Monitoring			
2.2	Research Docker Tools	10/28/23	11/2/23	4.1	Document Lessons Learned	11/30/23	12/6/23
2.3	Draft initial Architecture	11/3/23	11/8/23	4.2	Solution Enhancement	12/7/23	12/14/23
2.4	Request for Proposal Release	11/9/23	11/9/23	4.3	Project Performance	12/14/23	12/14/23
2.5	Draft Request for Proposal	11/10/23	11/16/23				
2.6	Final Request for Proposal	11/17/23	11/24/23				



Gantt Chart

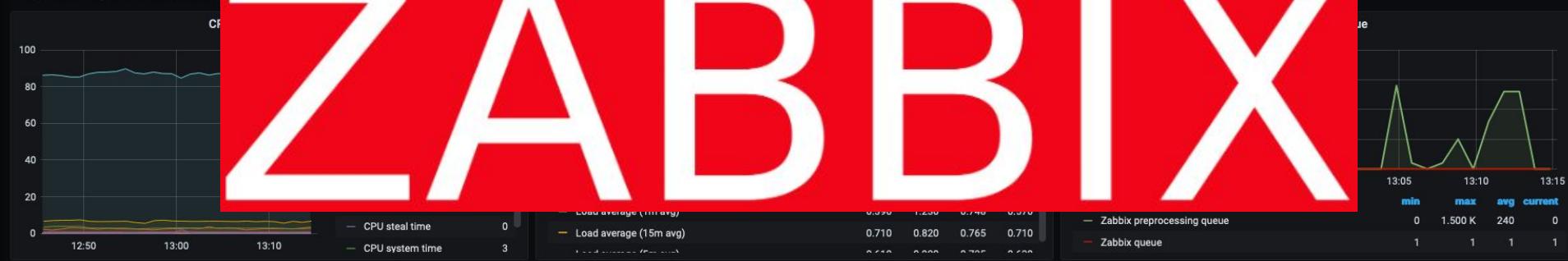


THANK YOU

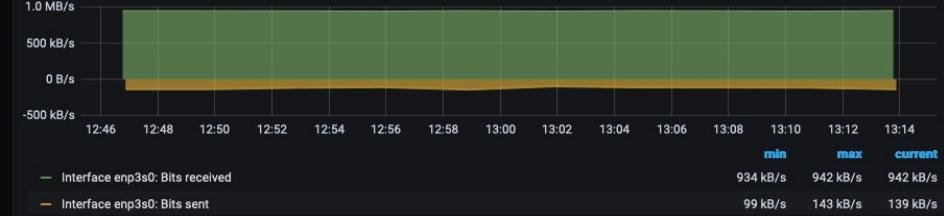
Busy Processes of Zabbix server



CPU/Memory/Disk/Network of Zabbix server



Network Adapters



Available memory



Free disk space

