AGM NETWORK CONSULTANCY

Zabbix for MSPs

AGM NETWORK CONSULTANCY

Zabbix Summit 2024

www.agm-nc.com | info@agm-nc.com | +44 3309 120130

My Journey to Zabbix

- 2008 – BEng Computer Networking
- 2012 – MSc Networks & Security
- 2014 – Managed 14 sites networks in the UK
  - Needed a centralized tool that would allow me to troubleshoot
  - Zabbix vs other tooling – Zabbix seemed the simplest to use, yet had a comprehensive feature set
  - Setup a basic server at one of the sites and used a VPN to access remote sites

My Journey to Zabbix

Starting Out with Zabbix

- 2016 – Lead Network Engineer
  - Supporting 80 Companies Networks
  - Break fix ethos – fix issues once they become apparent
  - Currently using another proprietary tool, but met our license limits and the company had no interest in investing more into monitoring
  - Some other options had nice graphs… but was heavy and a struggle to navigate functionality and feature set between their licensing tiers

My Journey to Zabbix
Starting Out with Zabbix

- 2020 – Started AGM Network Consultancy
  - Support over 30 sites networks
  - Started Using Zabbix Primarily for Network Devices
  - Started Using Remote Proxies to:
    - remove the reliance on VPN connectivity
    - allow sites to be independently monitored and templated
    - Offset the load from the Zabbix Server
- 2022 – Support Over 100 Sites Engineering & Energy
  - Needed a templateable solution
  - Looking to be able to take on up to 20 sites per month if necessary

What Were My Problems

- Reactive troubleshooting
- Lack of monitoring data prior to problems occurring
- Not able to pass on the tooling to lower-level technical staff

What Were My Wants

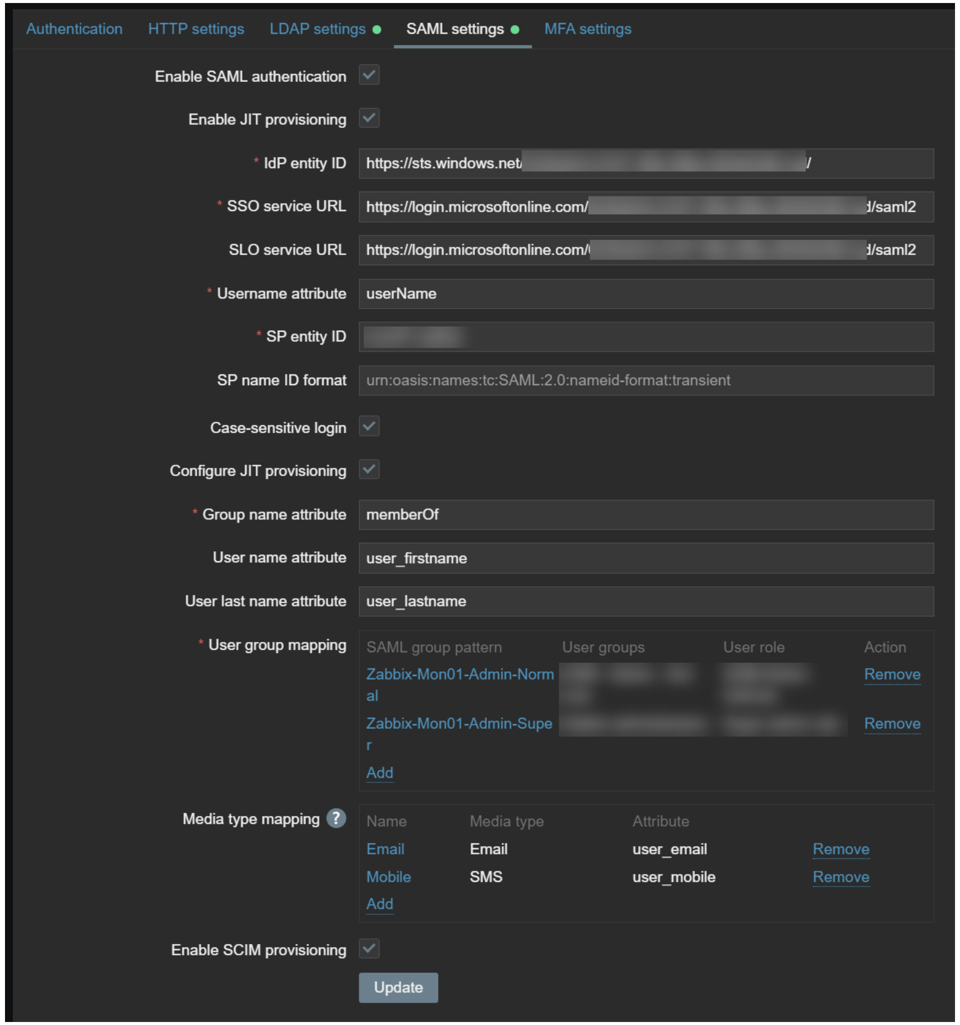
- Affordable Solution
- Customizable look, feel, monitoring intervals
- Monitoring… beyond SNMP!!! MODBUS, Certificates, Custom Items
- Scalable solution – increasing number of devices
- Scalable security: Local, LDAP… then SAML (Entra ID)
- Audit logging

The MSP World Alternatives

- RMM (Remote Monitoring & Management) Systems:
  - Vendor lock in
  - Limited User Interface constructions
  - Limited measurement intervals
  - Starting cost for my 100 network devices a minimum of £2,400 per year with not all of the functions I needed
  - burnt fingers over the past few years with customers tooling: SolarWinds, Pulse Secure etc.
- Zabbix
  - Had all of my needs covered, and the wants were in the pipeline: SAML, possibility of being multi-tenant
  - Clear view of future goals
  - OpenSource

Authentication

- Started with local authentication
- Now use Office 365 SAML falling back to LDAP
- Users added to specific Office 365 Groups are auto-provisioned
- Groups and Roles are assigned automatically according to the SAML Group Pattern
- Email & SMS details are populated for escalations



Enable SAML authentication	☑
Enable JIT provisioning	☑
* IdP entity ID	https://sts.windows.net/[redacted]/
* SSO service URL	https://login.microsoftonline.com/[redacted]/saml2
SLO service URL	https://login.microsoftonline.com/[redacted]/saml2
* Username attribute	userName
* SP entity ID	[redacted]
SP name ID format	urn:oasis:names:tc:SAML:2.0:nameid-format:transient
Case-sensitive login	☑
Configure JIT provisioning	☑
* Group name attribute	memberOf
User name attribute	user_firstname
User last name attribute	user_lastname

* User group mapping

SAML group pattern	User groups	User role	Action
Zabbix-Mon01-Admin-Normal	[redacted]	[redacted]	Remove
Zabbix-Mon01-Admin-Super	[redacted]	[redacted]	Remove
Add			

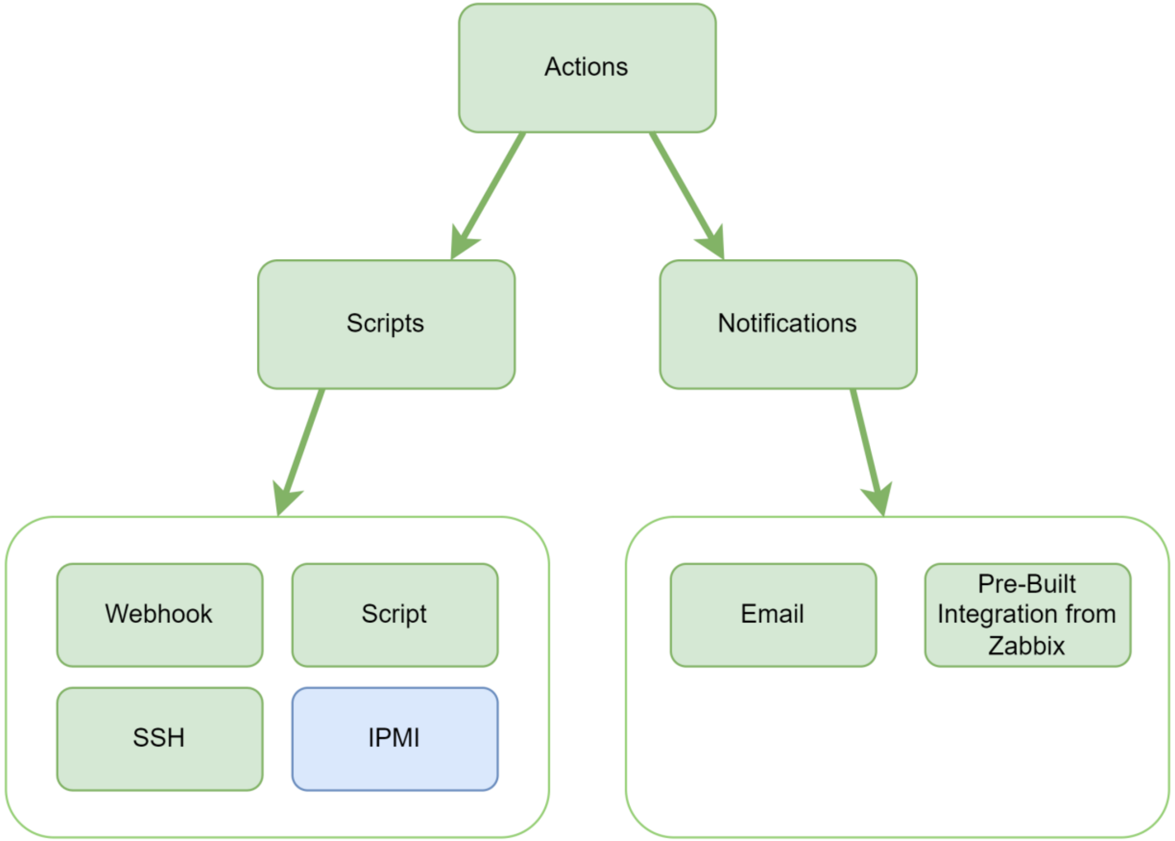
Media type mapping ?

Name	Media type	Attribute	
Email	Email	user_email	Remove
Mobile	SMS	user_mobile	Remove
Add			

Enable SCIM provisioning ☑

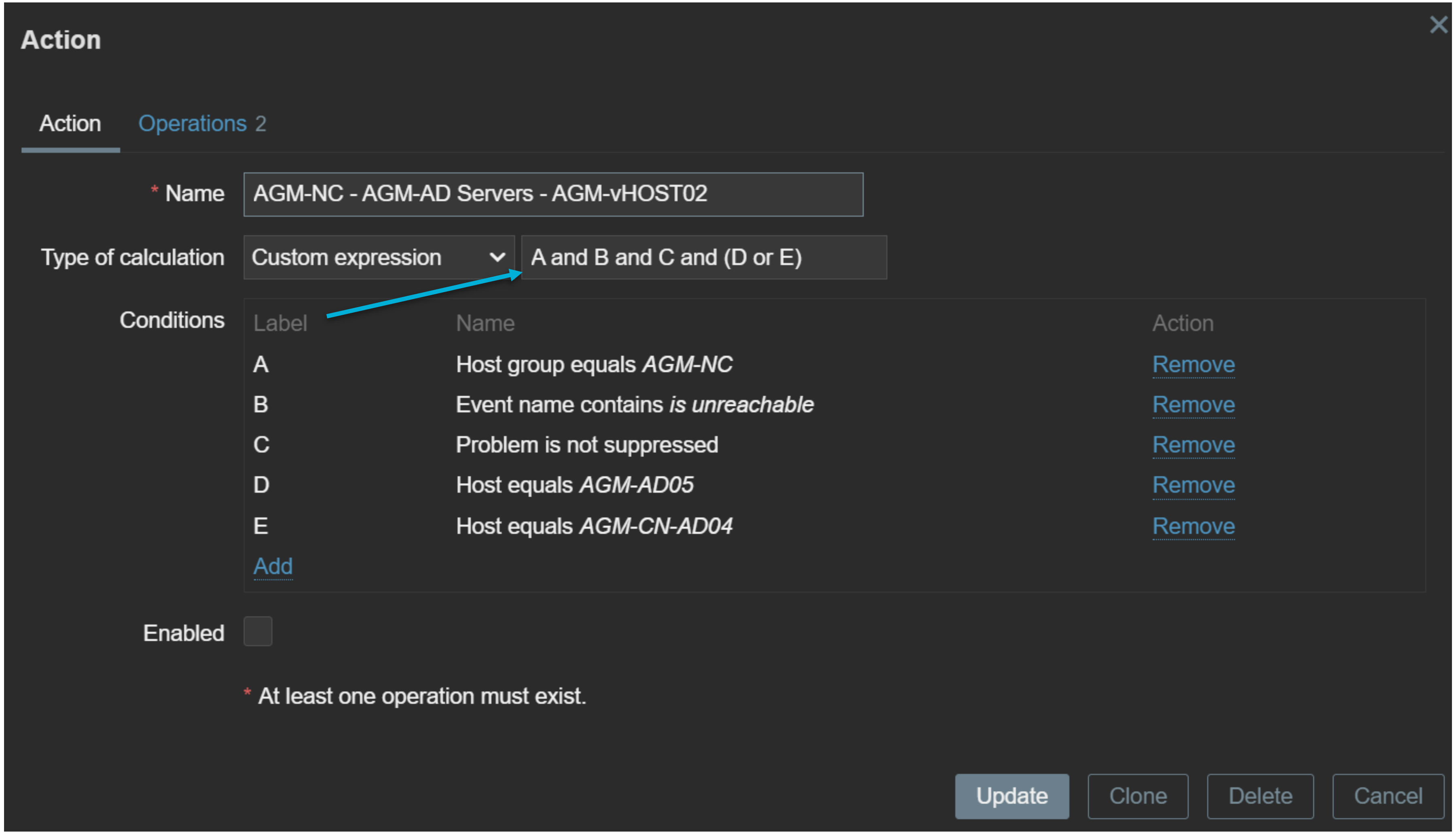
Actions
Doing Something

- Doing something after the problem state
- We mostly use Email, Teams Notifications, Webhooks and Scripts
- Webhooks and Scripts pretty much allow you to do what you want:
  - Reboot a remote device
  - Execute a command into another system



Actions

1 - Creating the Conditions



* Name: AGM-NC - AGM-AD Servers - AGM-vHOST02

Type of calculation: Custom expression | A and B and C and (D or E)

Conditions

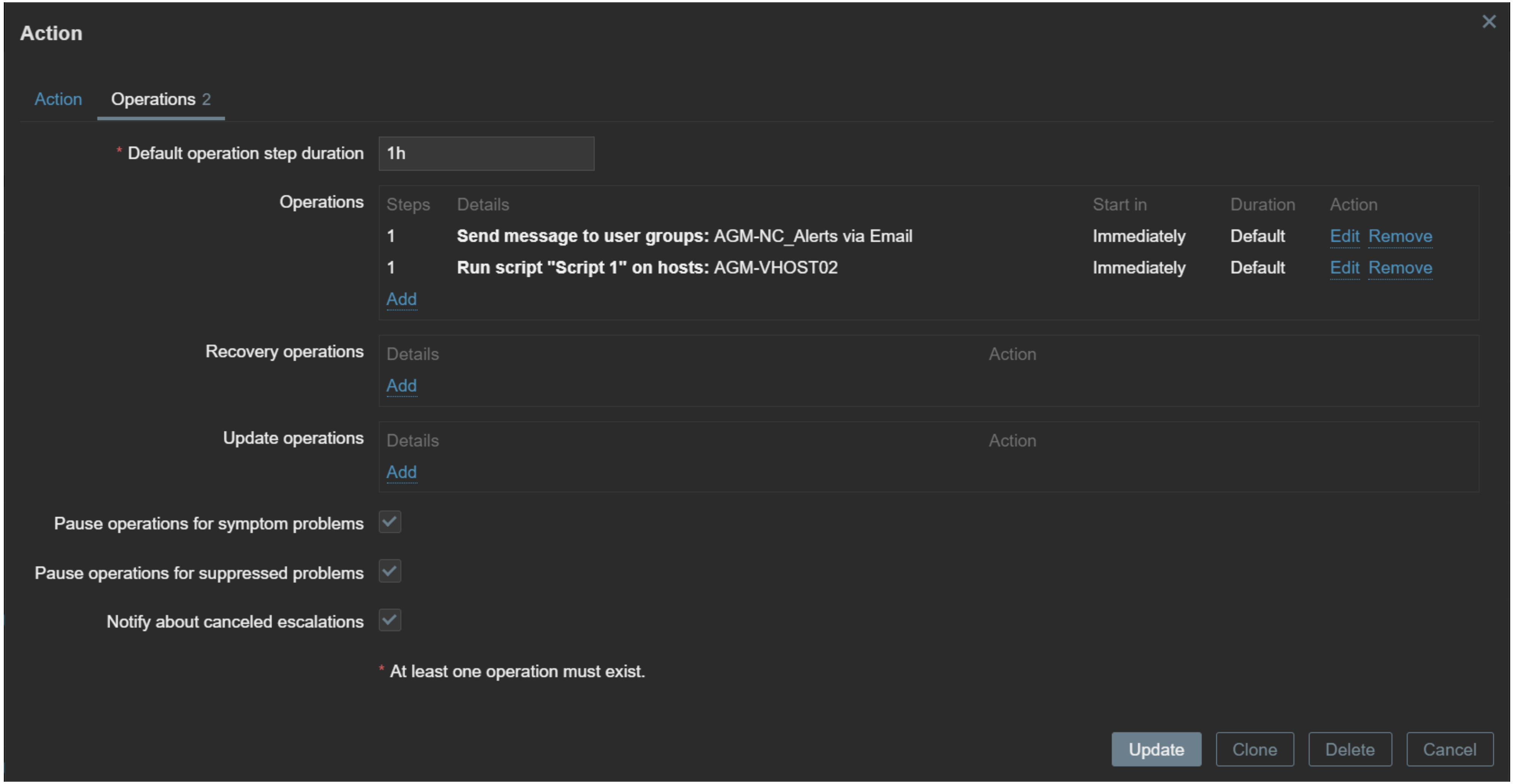
Label	Name	Action
A	Host group equals *AGM-NC*	Remove
B	Event name contains *is unreachable*	Remove
C	Problem is not suppressed	Remove
D	Host equals *AGM-AD05*	Remove
E	Host equals *AGM-CN-AD04*	Remove
Add		

Enabled □

* At least one operation must exist.

Actions

2 – Operations: the doing



Action

* Default operation step duration: 1h

Operations

Steps	Details	Start in	Duration	Action
1	**Send message to user groups:** AGM-NC_Alerts via Email	Immediately	Default	Edit Remove
1	**Run script "Script 1" on hosts:** AGM-VHOST02	Immediately	Default	Edit Remove
Add				

Recovery operations

Details	Action
Add	

Update operations

Details	Action
Add	

Pause operations for symptom problems ☑

Pause operations for suppressed problems ☑

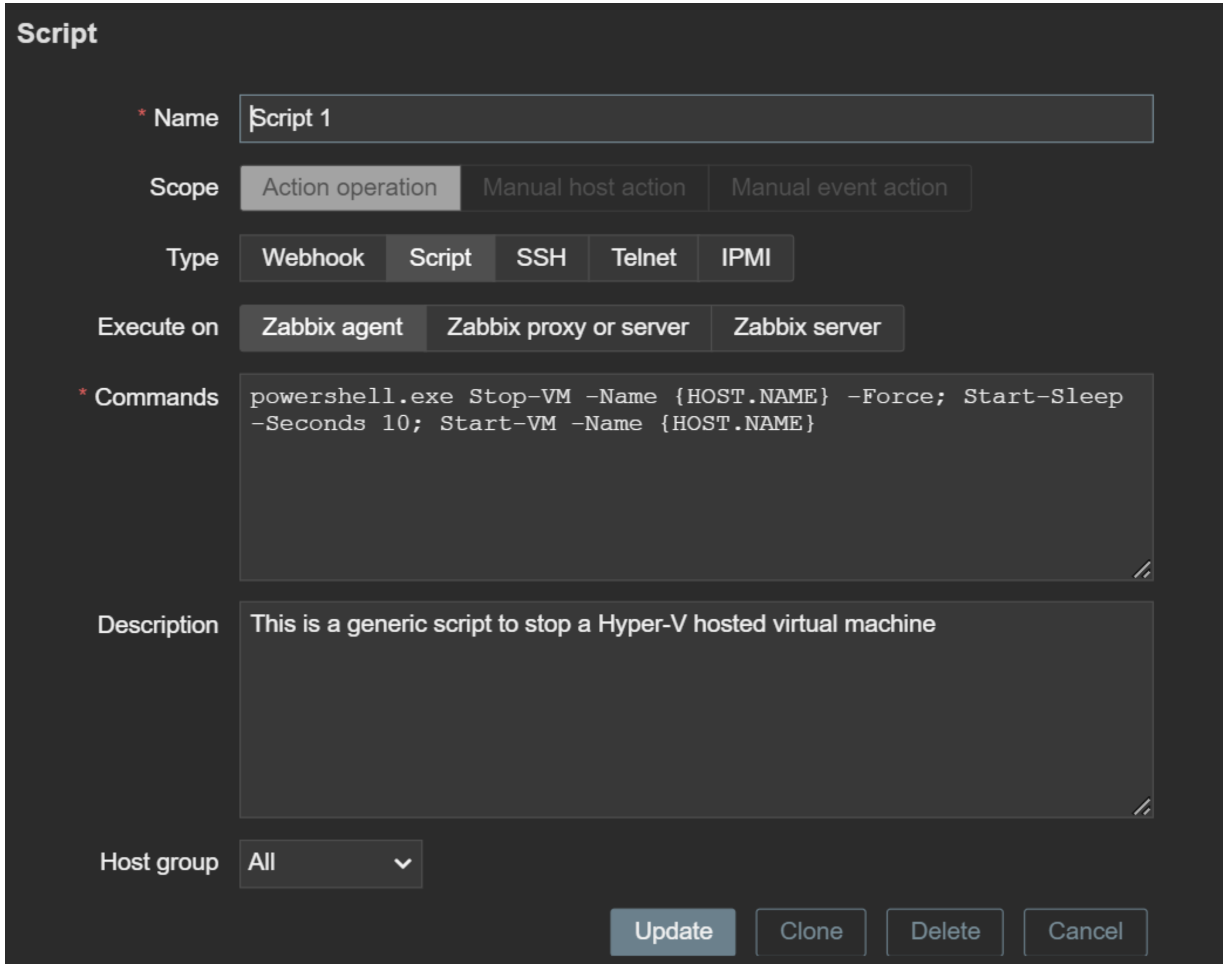
Notify about canceled escalations ☑

* At least one operation must exist.

Actions

3 – Operations: the script

- We started using scripts in Actions to automate the recovery of systems/services.
- The example to the right shows a (very) basic script to Force stop and start a Virtual Machine on a Hyper-V Hypervisor.



Script

* Name: Script 1

Scope: [✓ Action operation] Manual host action Manual event action

Type: Webhook [✓ Script] SSH Telnet IPMI

Execute on: [✓ Zabbix agent] Zabbix proxy or server Zabbix server

* Commands:

```
powershell.exe Stop-VM -Name {HOST.NAME} -Force; Start-Sleep
-Seconds 10; Start-VM -Name {HOST.NAME}
```

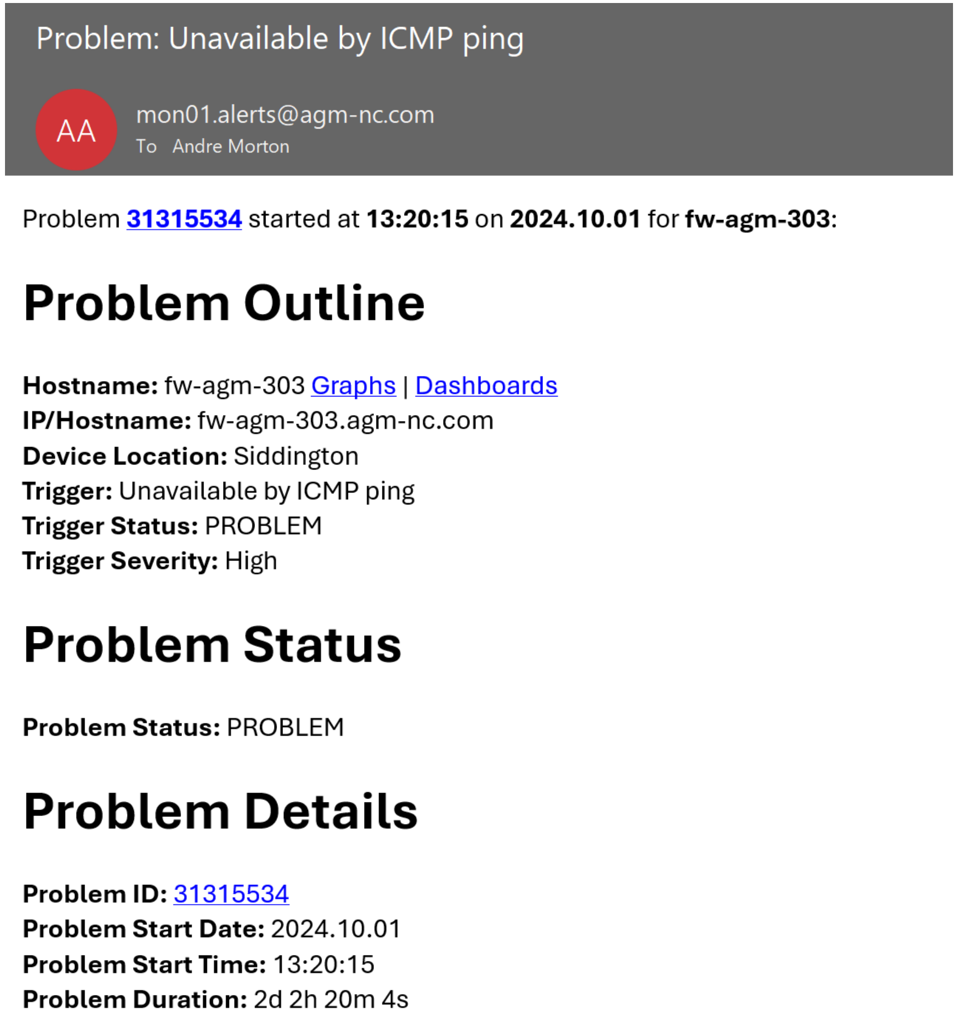
Description: This is a generic script to stop a Hyper-V hosted virtual machine

Host group: All

Actions

3 – Operations: the email notification

- Quick to create custom email notification templates
- Customisable per group / recipient
- Can jump straight into key information and data with a single click



Problem: Unavailable by ICMP ping

AA mon01.alerts@agm-nc.com
To Andre Morton

Problem 31315534 started at **13:20:15** on **2024.10.01** for **fw-agm-303**:

Problem Outline

Hostname: fw-agm-303 Graphs | Dashboards
IP/Hostname: fw-agm-303.agm-nc.com
Device Location: Siddington
Trigger: Unavailable by ICMP ping
Trigger Status: PROBLEM
Trigger Severity: High

Problem Status

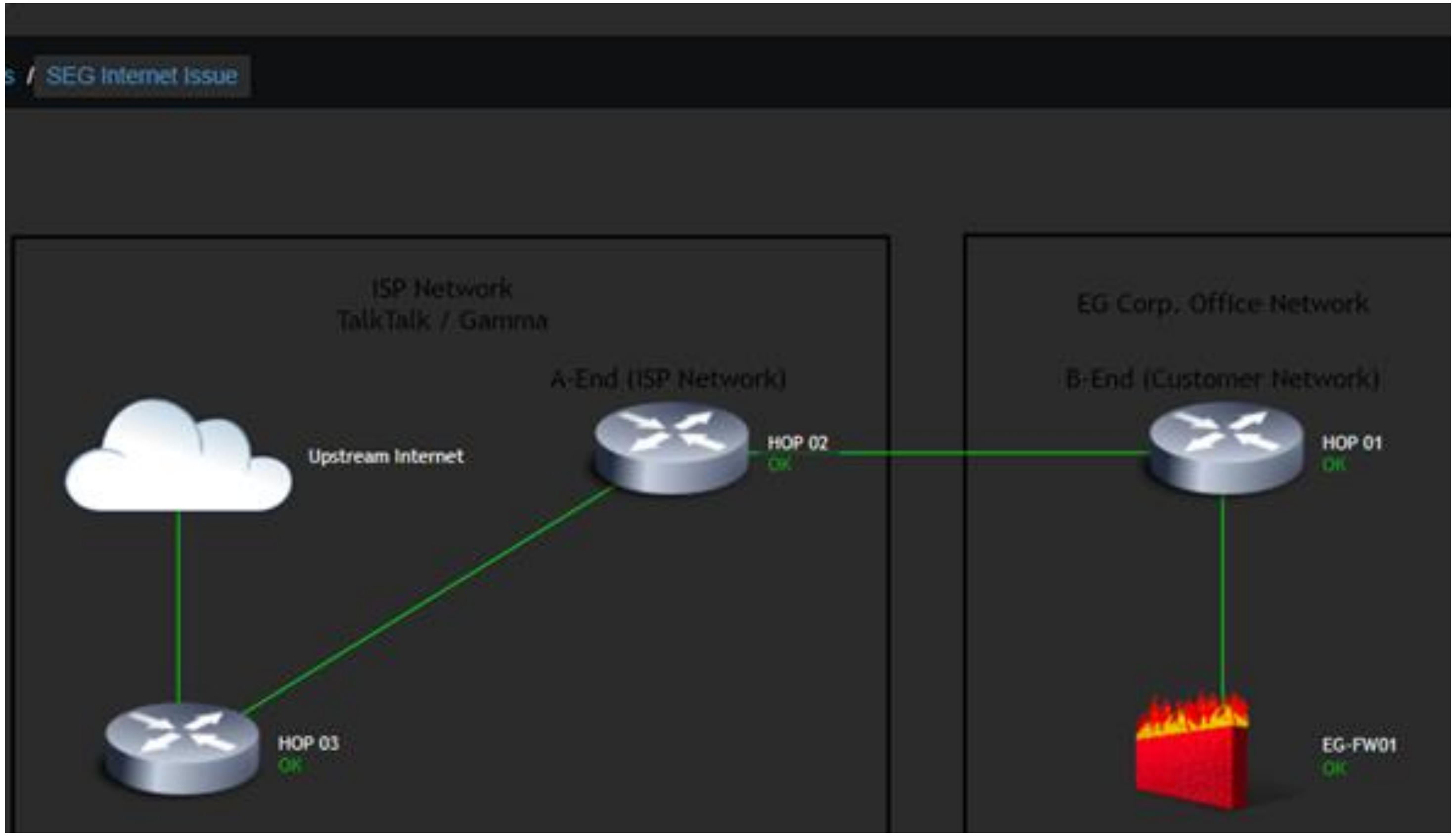
Problem Status: PROBLEM

Problem Details

Problem ID: 31315534
Problem Start Date: 2024.10.01
Problem Start Time: 13:20:15
Problem Duration: 2d 2h 20m 4s

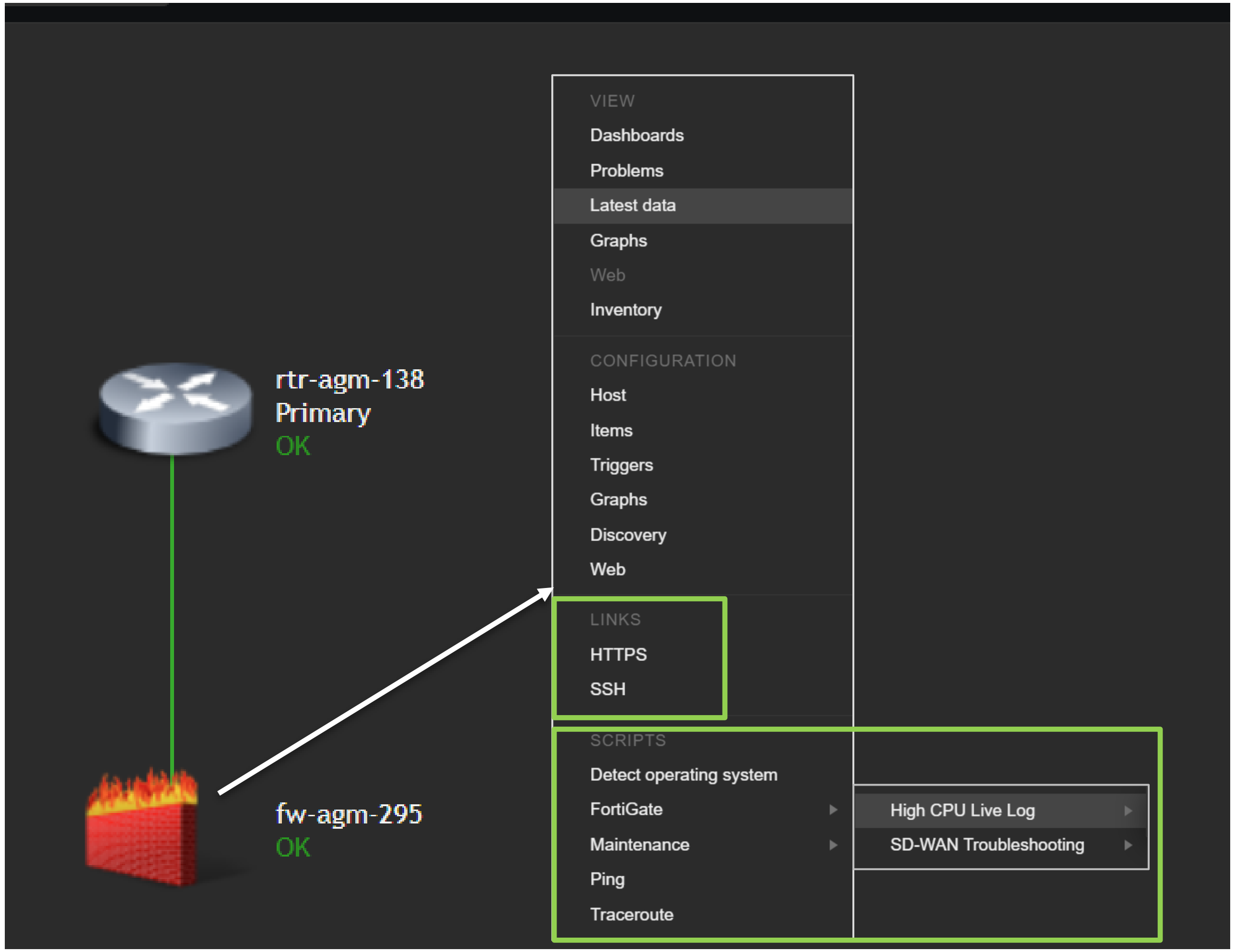
Creating Maps for Recurring Problems

- Quickly create a visual for problems
- Ability to drill down into graphs and historical data

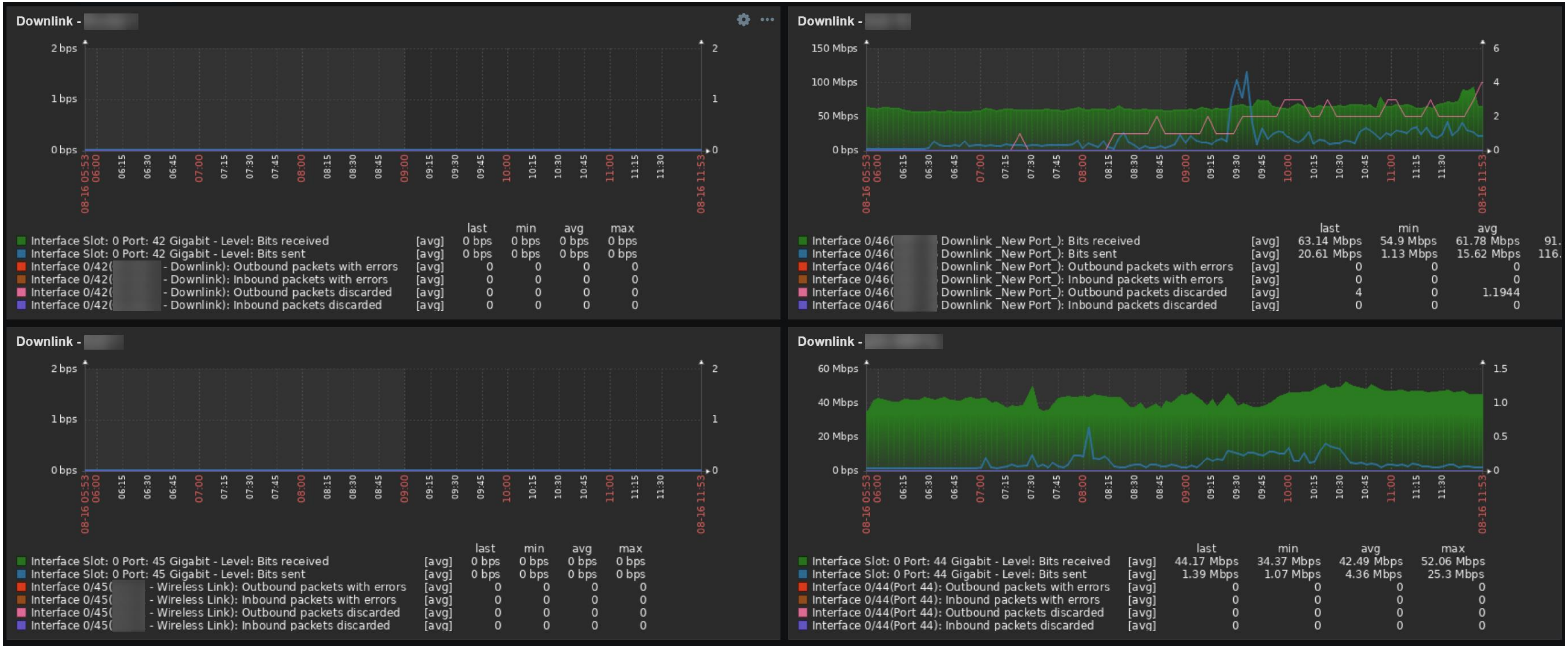


Maps - Interactive

- Interactive map objects
- Get straight to the information you want to interrogate
- Can add custom links & scripts



Dashboards – Key Link Status



Downlink - [redacted]

		last	min	avg	max
🟩 Interface Slot: 0 Port: 42 Gigabit - Level: Bits received	[avg]	0 bps	0 bps	0 bps	0 bps
🟦 Interface Slot: 0 Port: 42 Gigabit - Level: Bits sent	[avg]	0 bps	0 bps	0 bps	0 bps
🟥 Interface 0/42([redacted] - Downlink): Outbound packets with errors	[avg]	0	0	0	0
🟫 Interface 0/42([redacted] - Downlink): Inbound packets with errors	[avg]	0	0	0	0
🟪 Interface 0/42([redacted] - Downlink): Outbound packets discarded	[avg]	0	0	0	0
🟪 Interface 0/42([redacted] - Downlink): Inbound packets discarded	[avg]	0	0	0	0

Downlink - [redacted]

		last	min	avg	
🟩 Interface 0/46([redacted] Downlink _New Port_): Bits received	[avg]	63.14 Mbps	54.9 Mbps	61.78 Mbps	91.
🟦 Interface 0/46([redacted] Downlink _New Port_): Bits sent	[avg]	20.61 Mbps	1.13 Mbps	15.62 Mbps	116.
🟥 Interface 0/46([redacted] Downlink _New Port_): Outbound packets with errors	[avg]	0	0	0	
🟫 Interface 0/46([redacted] Downlink _New Port_): Inbound packets with errors	[avg]	0	0	0	
🟪 Interface 0/46([redacted] Downlink _New Port_): Outbound packets discarded	[avg]	4	0	1.1944	
🟪 Interface 0/46([redacted] Downlink _New Port_): Inbound packets discarded	[avg]	0	0	0	

Downlink - [redacted]

		last	min	avg	max
🟩 Interface Slot: 0 Port: 45 Gigabit - Level: Bits received	[avg]	0 bps	0 bps	0 bps	0 bps
🟦 Interface Slot: 0 Port: 45 Gigabit - Level: Bits sent	[avg]	0 bps	0 bps	0 bps	0 bps
🟥 Interface 0/45([redacted] - Wireless Link): Outbound packets with errors	[avg]	0	0	0	0
🟫 Interface 0/45([redacted] - Wireless Link): Inbound packets with errors	[avg]	0	0	0	0
🟪 Interface 0/45([redacted] - Wireless Link): Outbound packets discarded	[avg]	0	0	0	0
🟪 Interface 0/45([redacted] - Wireless Link): Inbound packets discarded	[avg]	0	0	0	0

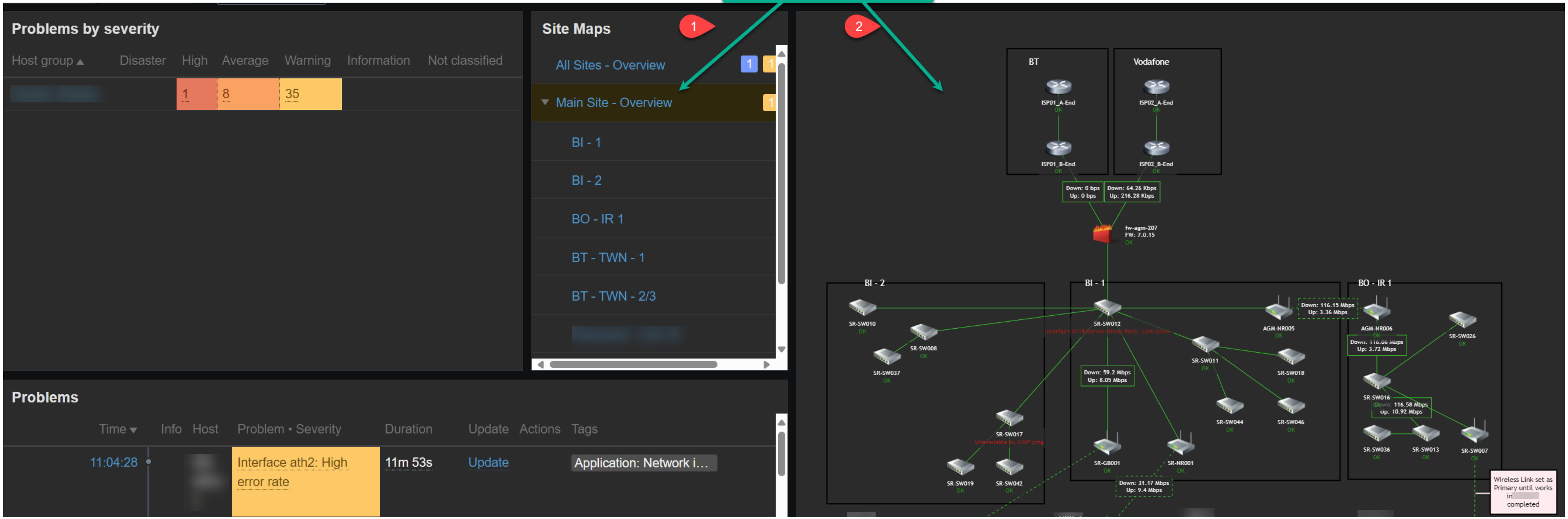
Downlink - [redacted]

		last	min	avg	max
🟩 Interface Slot: 0 Port: 44 Gigabit - Level: Bits received	[avg]	44.17 Mbps	34.37 Mbps	42.49 Mbps	52.06 Mbps
🟦 Interface Slot: 0 Port: 44 Gigabit - Level: Bits sent	[avg]	1.39 Mbps	1.07 Mbps	4.36 Mbps	25.3 Mbps
🟥 Interface 0/44(Port 44): Outbound packets with errors	[avg]	0	0	0	0
🟫 Interface 0/44(Port 44): Inbound packets with errors	[avg]	0	0	0	0
🟪 Interface 0/44(Port 44): Outbound packets discarded	[avg]	0	0	0	0
🟪 Interface 0/44(Port 44): Inbound packets discarded	[avg]	0	0	0	0

Dashboards – High Level Overview

High Level Overview & Drill-Down

Maps Menu selection updates Map Widget



Problems by severity

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
[redacted]		1	8	35		

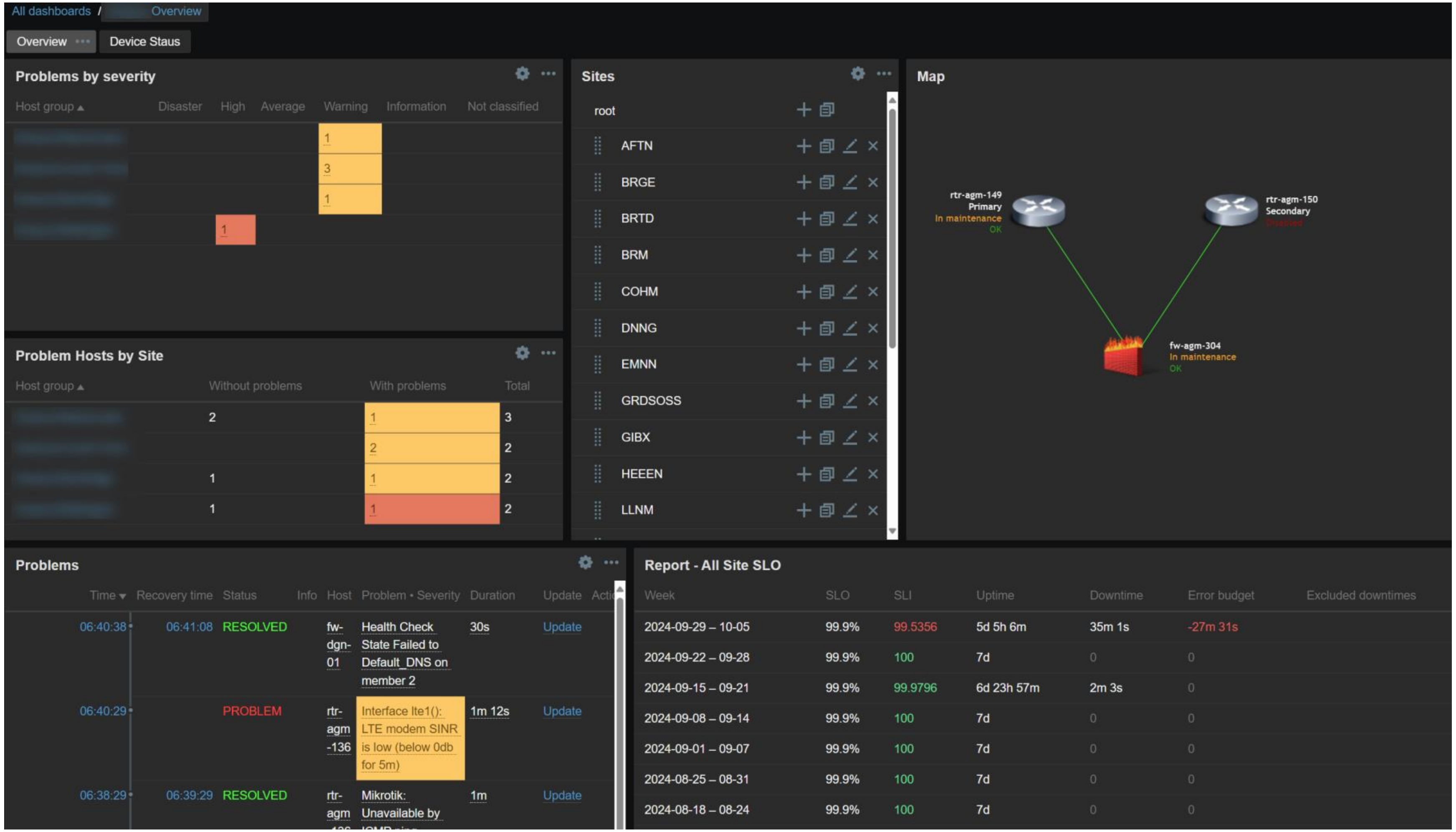
Site Maps

- All Sites - Overview 1 1
- Main Site - Overview 1
  - BI - 1
  - BI - 2
  - BO - IR 1
  - BT - TWN - 1
  - BT - TWN - 2/3
  - [redacted]

Problems

Time ▾	Info	Host	Problem • Severity	Duration	Update	Actions	Tags
11:04:28		[redacted]	Interface ath2: High error rate	11m 53s	Update		Application: Network i…

Dashboards – High Level Overview
Multi-Site Templated Layouts



All dashboards / [redacted] Overview

Overview ··· | Device Staus

Problems by severity

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
[redacted]				1		
[redacted]				3		
[redacted]				1		
[redacted]		1				

Problem Hosts by Site

Host group ▲	Without problems	With problems	Total
[redacted]	2	1	3
[redacted]		2	2
[redacted]	1	1	2
[redacted]	1	1	2

Sites

- root
- AFTN
- BRGE
- BRTD
- BRM
- COHM
- DNNG
- EMNN
- GRDSOSS
- GIBX
- HEEEN
- LLNM

Map

Problems

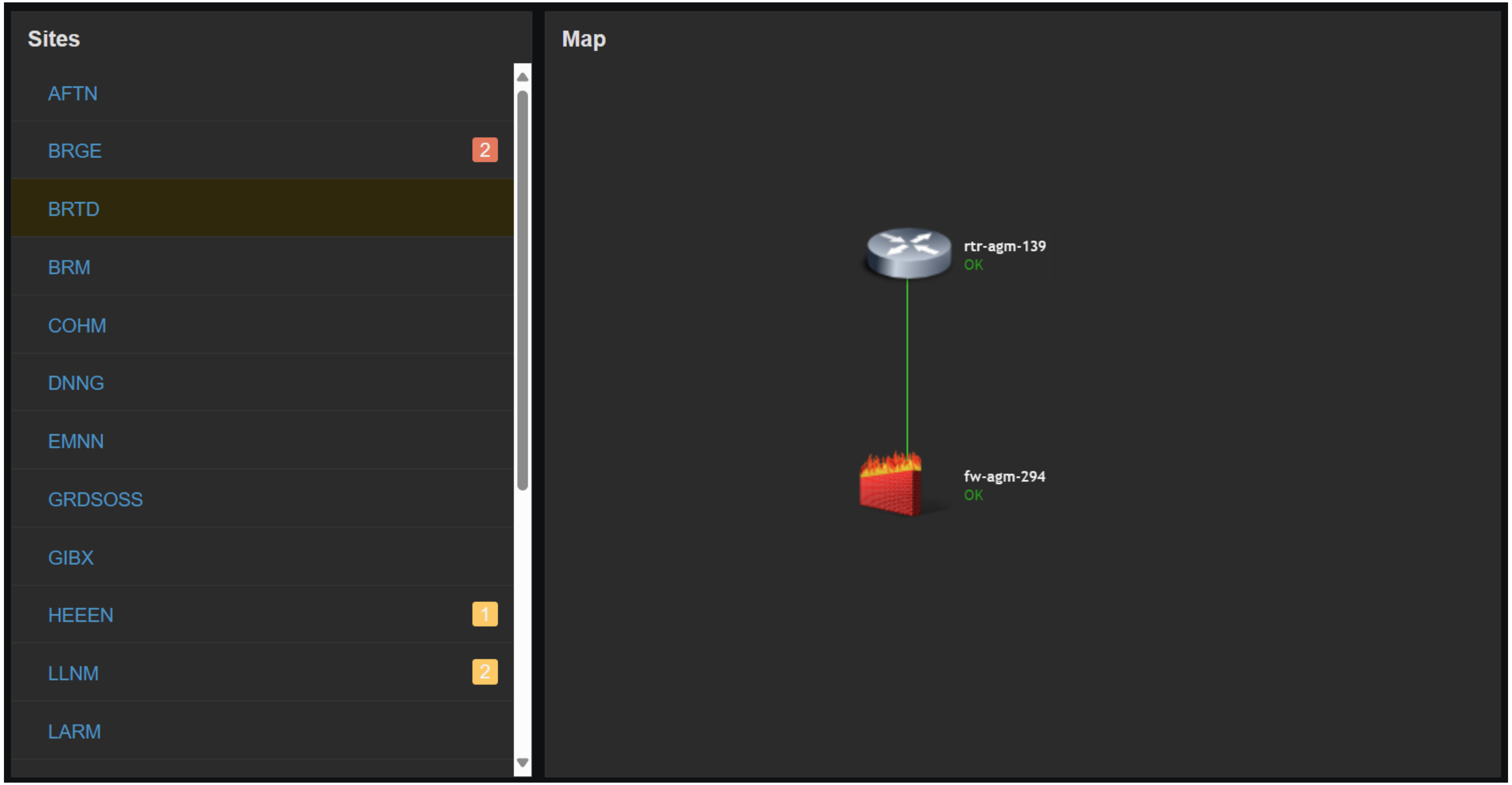
Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Acti
06:40:38	06:41:08	RESOLVED		fw-dgn-01	Health Check State Failed to Default_DNS on member 2	30s	Update	
06:40:29		PROBLEM		rtr-agm-136	Interface lte1(): LTE modem SINR is low (below 0db for 5m)	1m 12s	Update	
06:38:29	06:39:29	RESOLVED		rtr-agm	Mikrotik: Unavailable by	1m	Update	

Report - All Site SLO

Week	SLO	SLI	Uptime	Downtime	Error budget	Excluded downtimes
2024-09-29 – 10-05	99.9%	99.5356	5d 5h 6m	35m 1s	-27m 31s	
2024-09-22 – 09-28	99.9%	100	7d	0	0	
2024-09-15 – 09-21	99.9%	99.9796	6d 23h 57m	2m 3s	0	
2024-09-08 – 09-14	99.9%	100	7d	0	0	
2024-09-01 – 09-07	99.9%	100	7d	0	0	
2024-08-25 – 08-31	99.9%	100	7d	0	0	
2024-08-18 – 08-24	99.9%	100	7d	0	0	

Dashboards – High Level Overview

Multi-Site Templated Layouts



Sites

AFTN	
BRGE	2
BRTD	
BRM	
COHM	
DNNG	
EMNN	
GRDSOSS	
GIBX	
HEEEN	1
LLNM	2
LARM	

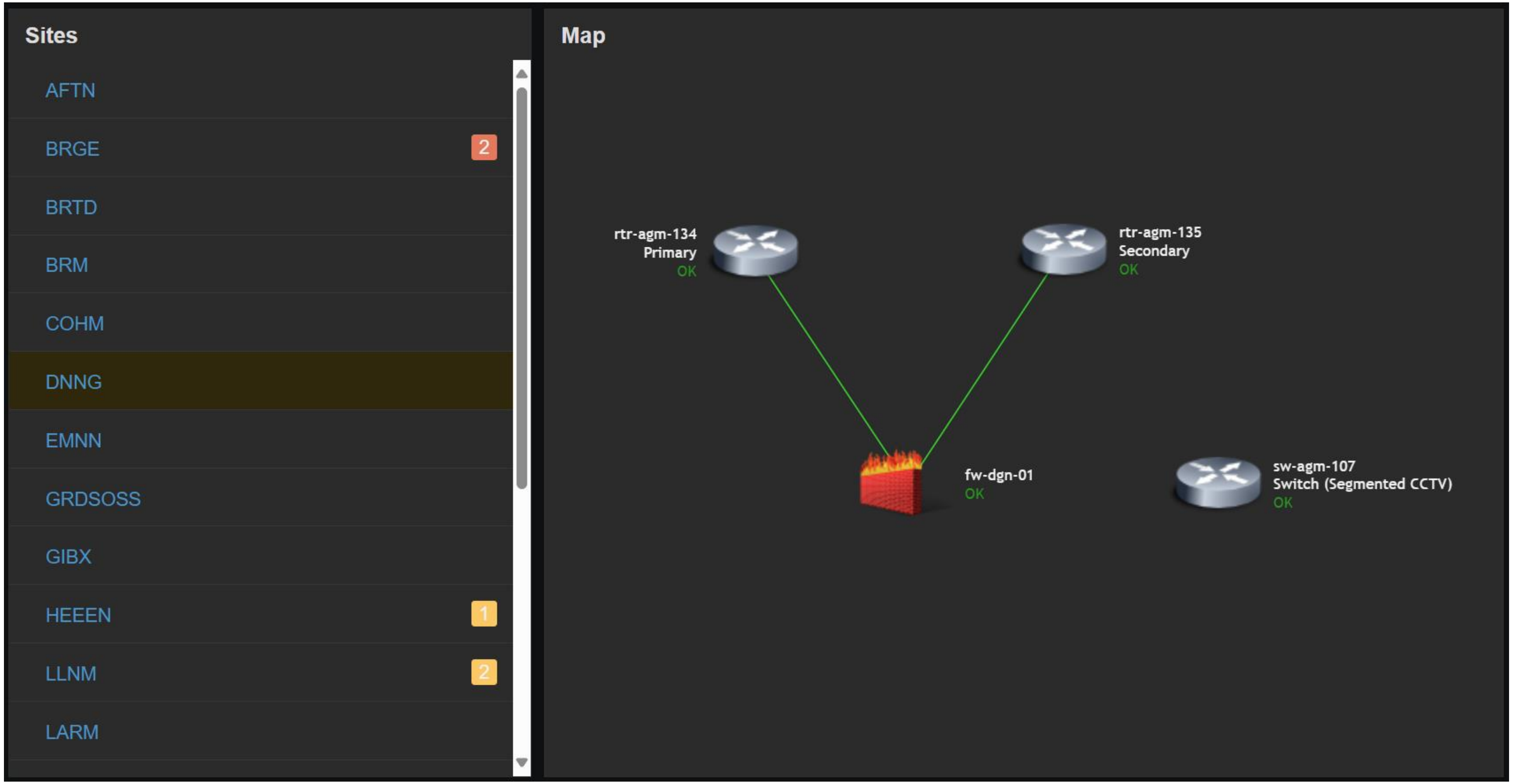
Map

rtr-agm-139
OK

fw-agm-294
OK

Dashboards – High Level Overview

Multi-Site Templated Layouts

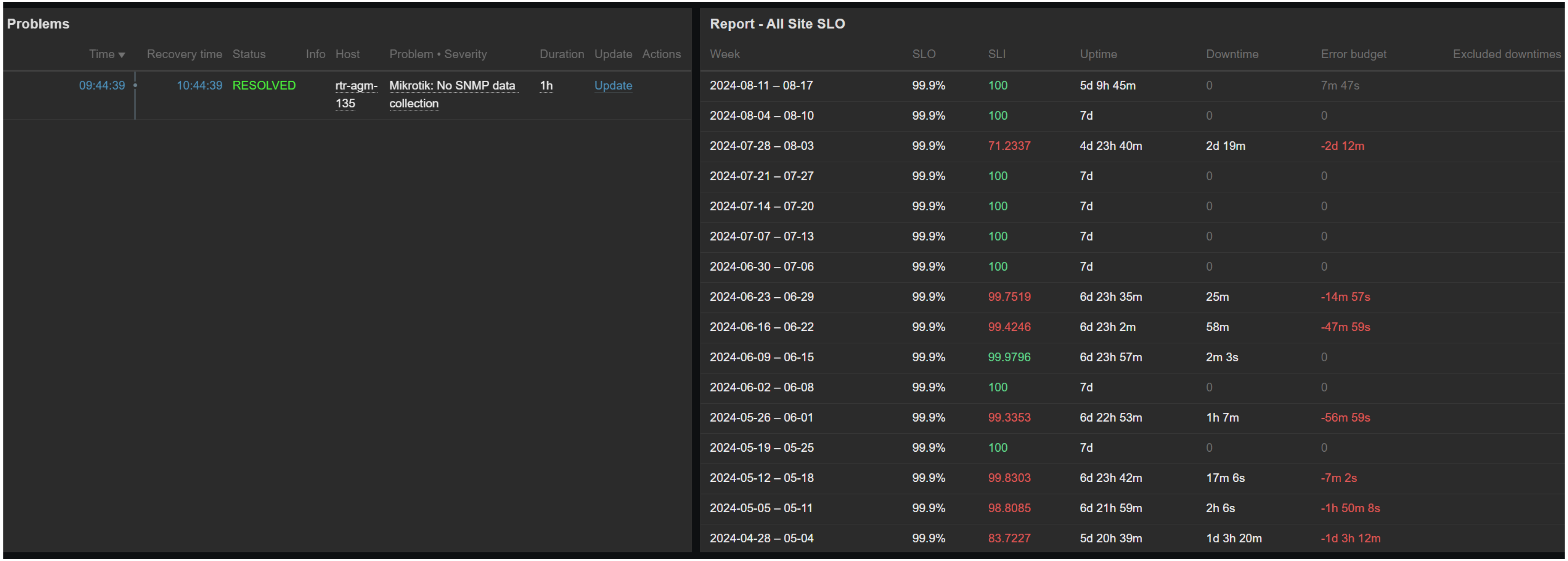


Sites

AFTN	
BRGE	2
BRTD	
BRM	
COHM	
DNNG	
EMNN	
GRDSOSS	
GIBX	
HEEEN	1
LLNM	2
LARM	

Map

Dashboards – High Level Overview
Multi-Site Templated Layouts



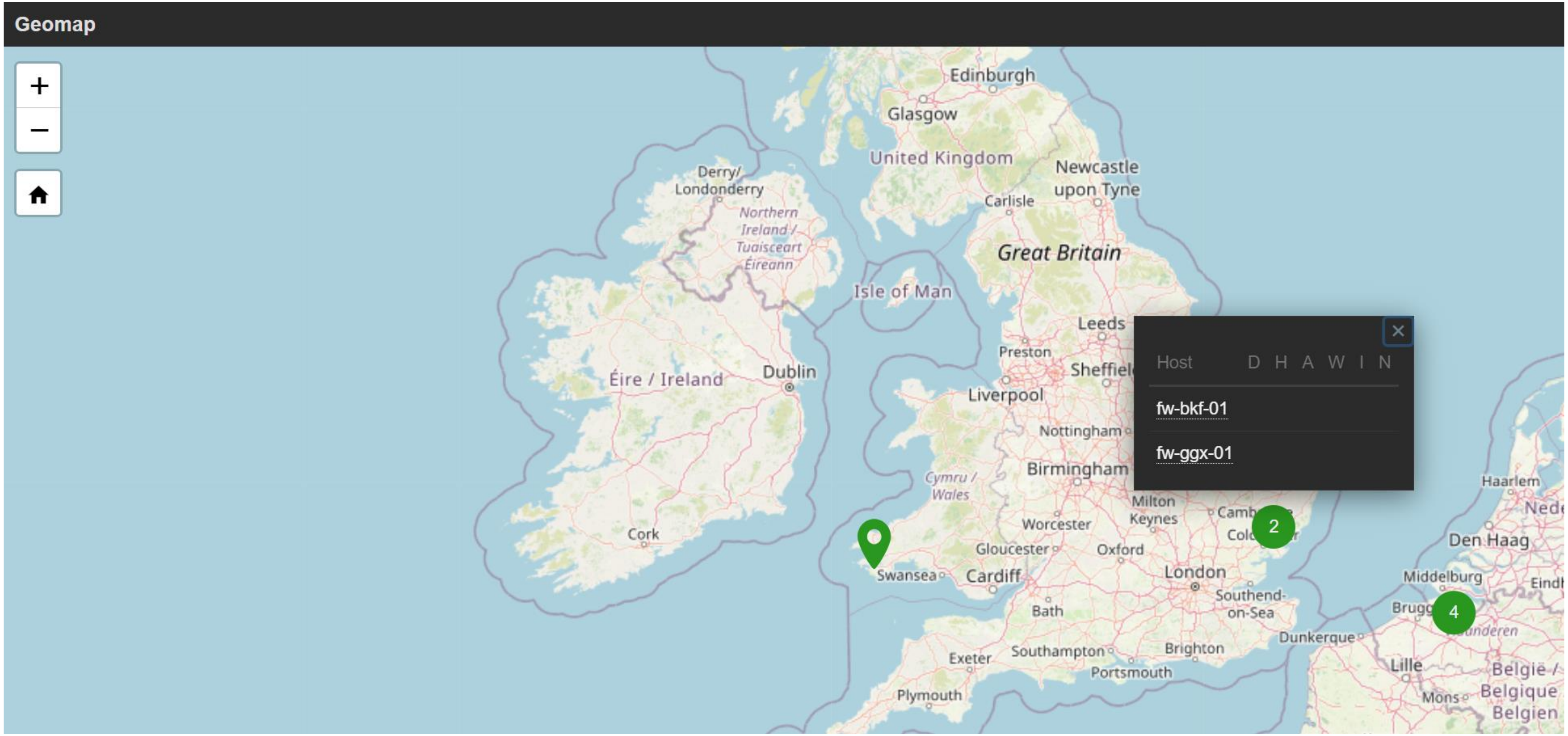
Problems

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Update	Actions
09:44:39	10:44:39	RESOLVED		rtr-agm-135	Mikrotik: No SNMP data collection	1h	Update	

Report - All Site SLO

Week	SLO	SLI	Uptime	Downtime	Error budget	Excluded downtimes
2024-08-11 – 08-17	99.9%	100	5d 9h 45m	0	7m 47s	
2024-08-04 – 08-10	99.9%	100	7d	0	0	
2024-07-28 – 08-03	99.9%	71.2337	4d 23h 40m	2d 19m	-2d 12m	
2024-07-21 – 07-27	99.9%	100	7d	0	0	
2024-07-14 – 07-20	99.9%	100	7d	0	0	
2024-07-07 – 07-13	99.9%	100	7d	0	0	
2024-06-30 – 07-06	99.9%	100	7d	0	0	
2024-06-23 – 06-29	99.9%	99.7519	6d 23h 35m	25m	-14m 57s	
2024-06-16 – 06-22	99.9%	99.4246	6d 23h 2m	58m	-47m 59s	
2024-06-09 – 06-15	99.9%	99.9796	6d 23h 57m	2m 3s	0	
2024-06-02 – 06-08	99.9%	100	7d	0	0	
2024-05-26 – 06-01	99.9%	99.3353	6d 22h 53m	1h 7m	-56m 59s	
2024-05-19 – 05-25	99.9%	100	7d	0	0	
2024-05-12 – 05-18	99.9%	99.8303	6d 23h 42m	17m 6s	-7m 2s	
2024-05-05 – 05-11	99.9%	98.8085	6d 21h 59m	2h 6s	-1h 50m 8s	
2024-04-28 – 05-04	99.9%	83.7227	5d 20h 39m	1d 3h 20m	-1d 3h 12m	

Dashboards – High Level Overview
Multi-Site Templated Layouts

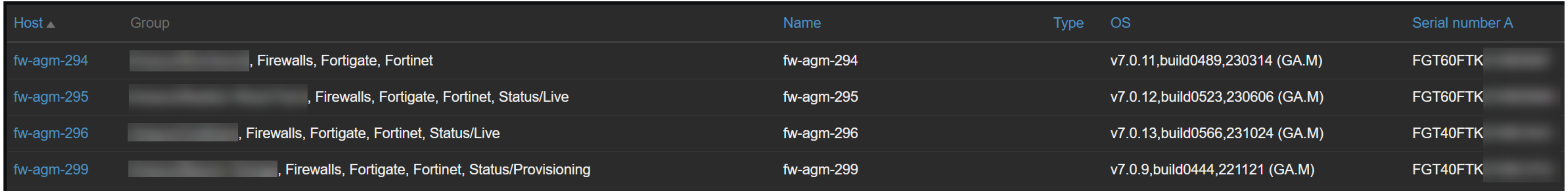


Geomap

Host	D	H	A	W	I	N
fw-bkf-01						
fw-ggx-01						

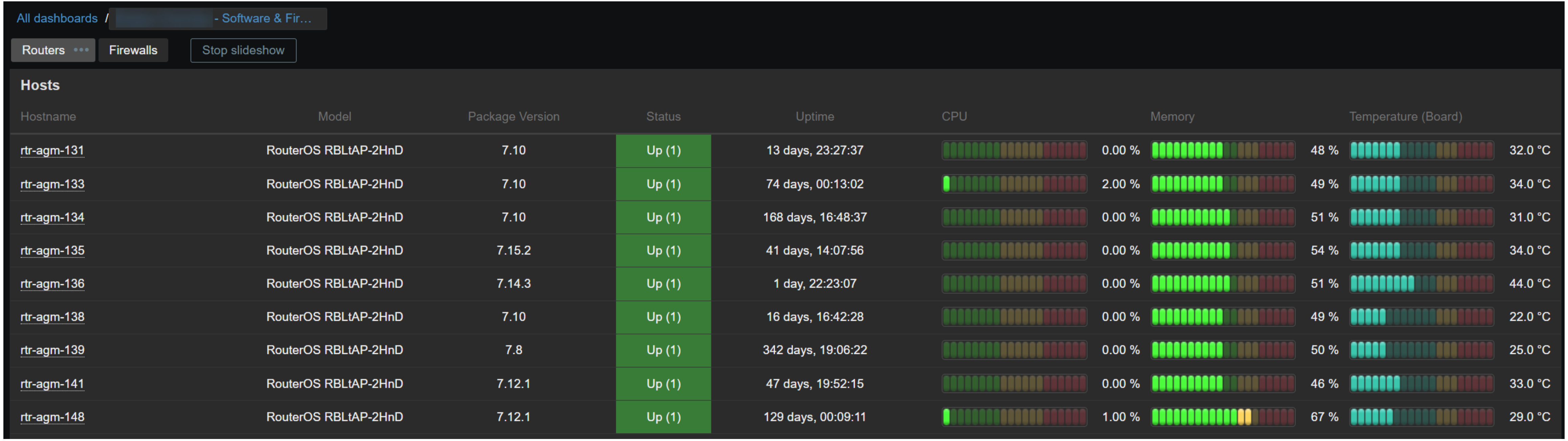
Inventory Views

Zabbix in-built Invetory



Host ▲	Group	Name	Type	OS	Serial number A
fw-agm-294	[redacted], Firewalls, Fortigate, Fortinet	fw-agm-294		v7.0.11,build0489,230314 (GA.M)	FGT60FTK[redacted]
fw-agm-295	[redacted], Firewalls, Fortigate, Fortinet, Status/Live	fw-agm-295		v7.0.12,build0523,230606 (GA.M)	FGT60FTK[redacted]
fw-agm-296	[redacted], Firewalls, Fortigate, Fortinet, Status/Live	fw-agm-296		v7.0.13,build0566,231024 (GA.M)	FGT40FTK[redacted]
fw-agm-299	[redacted], Firewalls, Fortigate, Fortinet, Status/Provisioning	fw-agm-299		v7.0.9,build0444,221121 (GA.M)	FGT40FTK[redacted]

Custom Dashboard for Inventory

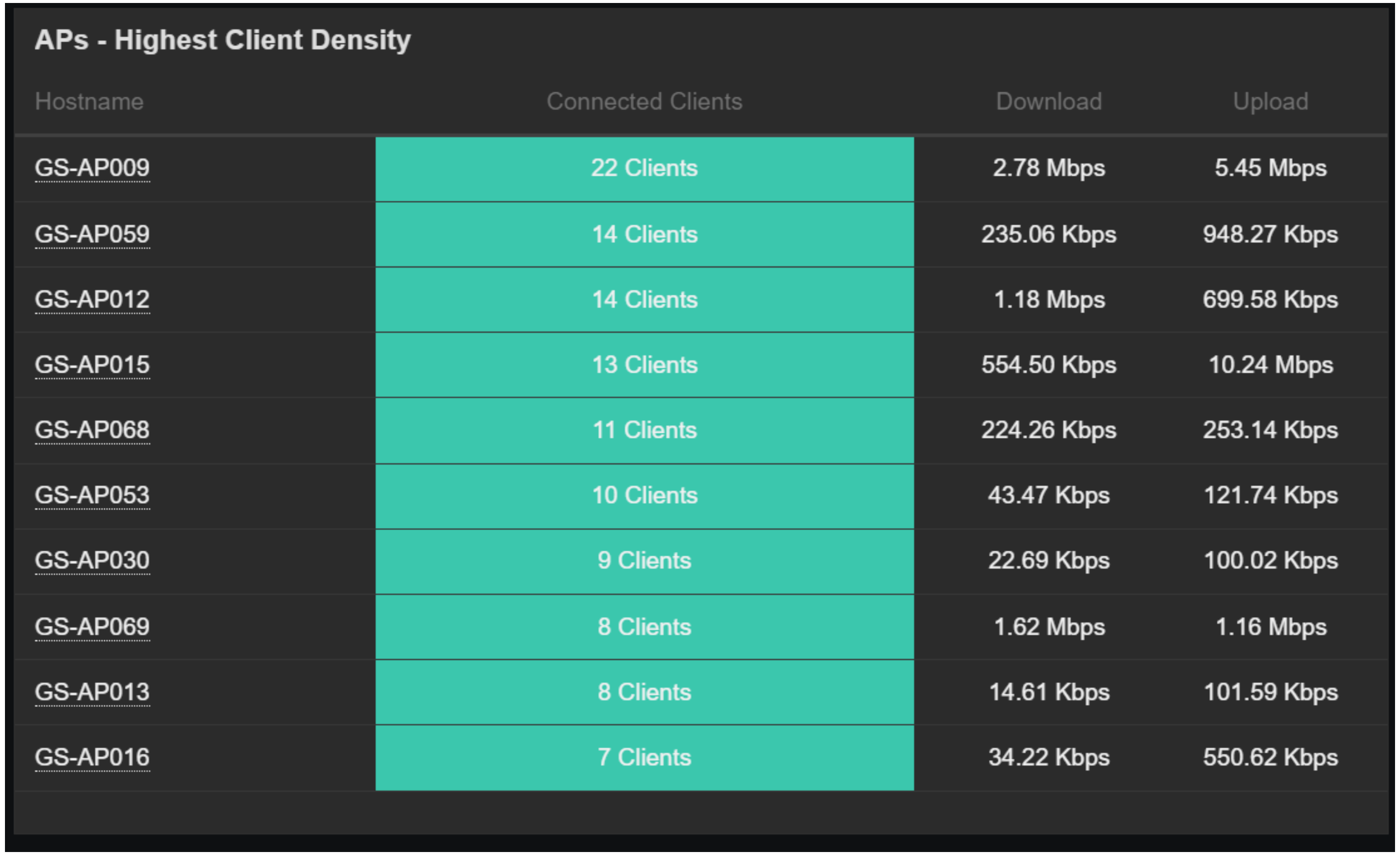


Hosts

Hostname	Model	Package Version	Status	Uptime	CPU	Memory	Temperature (Board)
rtr-agm-131	RouterOS RBLtAP-2HnD	7.10	Up (1)	13 days, 23:27:37	0.00 %	48 %	32.0 °C
rtr-agm-133	RouterOS RBLtAP-2HnD	7.10	Up (1)	74 days, 00:13:02	2.00 %	49 %	34.0 °C
rtr-agm-134	RouterOS RBLtAP-2HnD	7.10	Up (1)	168 days, 16:48:37	0.00 %	51 %	31.0 °C
rtr-agm-135	RouterOS RBLtAP-2HnD	7.15.2	Up (1)	41 days, 14:07:56	0.00 %	54 %	34.0 °C
rtr-agm-136	RouterOS RBLtAP-2HnD	7.14.3	Up (1)	1 day, 22:23:07	0.00 %	51 %	44.0 °C
rtr-agm-138	RouterOS RBLtAP-2HnD	7.10	Up (1)	16 days, 16:42:28	0.00 %	49 %	22.0 °C
rtr-agm-139	RouterOS RBLtAP-2HnD	7.8	Up (1)	342 days, 19:06:22	0.00 %	50 %	25.0 °C
rtr-agm-141	RouterOS RBLtAP-2HnD	7.12.1	Up (1)	47 days, 19:52:15	0.00 %	46 %	33.0 °C
rtr-agm-148	RouterOS RBLtAP-2HnD	7.12.1	Up (1)	129 days, 00:09:11	1.00 %	67 %	29.0 °C

Dashboards – Targeting Problems

- Example Dashboard Created to troubleshoot Wireless Access Point issues
- Firmware shows false high-density in vendor UI whilst SNMP data is accurate.



APs - Highest Client Density

Hostname	Connected Clients	Download	Upload
GS-AP009	22 Clients	2.78 Mbps	5.45 Mbps
GS-AP059	14 Clients	235.06 Kbps	948.27 Kbps
GS-AP012	14 Clients	1.18 Mbps	699.58 Kbps
GS-AP015	13 Clients	554.50 Kbps	10.24 Mbps
GS-AP068	11 Clients	224.26 Kbps	253.14 Kbps
GS-AP053	10 Clients	43.47 Kbps	121.74 Kbps
GS-AP030	9 Clients	22.69 Kbps	100.02 Kbps
GS-AP069	8 Clients	1.62 Mbps	1.16 Mbps
GS-AP013	8 Clients	14.61 Kbps	101.59 Kbps
GS-AP016	7 Clients	34.22 Kbps	550.62 Kbps

Premier Place
Cutler Street
Petticoat Tower
Brunswick House
Whitechapel High Street
Powell Way
Aldgate East Station
Aldgate East
Naylor Building East
Wynfrid House
Colefax Building
123 Cutlers Exchange
70 St Mary Axe
Houndsditch Post Office
Gravel Lane
Beaufort House
Calcutta House
Travelodge London City
Goulston Street
Old Castle Street
Tyne Street
Gardiner's Corner
Central Tower
59-63 Central House
White Church Lane
Hult International Business School
Coke Street
Weyhill Road
Commercial Road
New Drum Street
Stoney Lane
138 St Botolph Building
St Botolph Street
Capita
Houndsditch
Sari Garden
City Bouldering
Aldgate
Aldgate Square
2 Aldgate Tower
7 Aldgate Place
Blockhouse Gym
Buckle Street
Altitude
Henriques Street
Wells Lawrence House
Bury Street
31 Bury House
Mitre Street
Climb
The Aldgate School
Little Somerset Street
Braham Street
Braham Street Park
Braham Street Data Centre
BT
Camperdown Street
Alie Street
Leman Street
Canter Way
Piazza Walk
12 x 3
Chaucer Gardens
Cassia House
Gower's Walk
Back Church Lane
Harry Gosling Primary School
Fairclough Street
No1 Fitness
Fly

THANK YOU

Contact Us

Office Location

2 Leman Street,
London, E1 8FA

Website

www.agm-nc.com
info@agm-nc.com

phone

+44 3309 120130