

# Enhancing ITA's Network Reliability with PRTG Network Monitoring

---

Presented By:

Sidrah Hashmi, Aysha Bilai, Al Nowshin Rahman



# ITA's Problem:

- Rapidly company growth
- Complaints:
  - laggy
  - unstable
  - hard to troubleshoot
- No centralized visibility
- Hard to determine what is online, down or configured



# Why PRTG?



## PRTG offers:

- Centralized monitoring
- Auto-discovery
- Topology maps
- Basic IP address management
- Alerts and notifications
- Easy to deploy and use

# PRTG Installation & Monitoring

---

## **PRTG Core Server:**

- Installed in Head Office Data Centre
- Monitors WAN links and remote branches
- Uses sensors to pull data from routers, switches, servers and firewalls

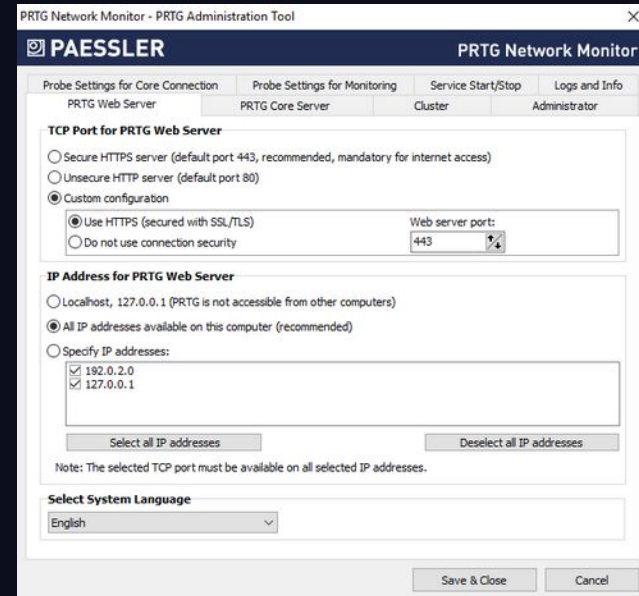
## **PRTG monitors using:**

- Sensors = individual checks (interface load, ping, CPU, VLAN traffic)
- Device groups
- Dashboards: real-time health status (green/yellow/red)

# IP Address Management

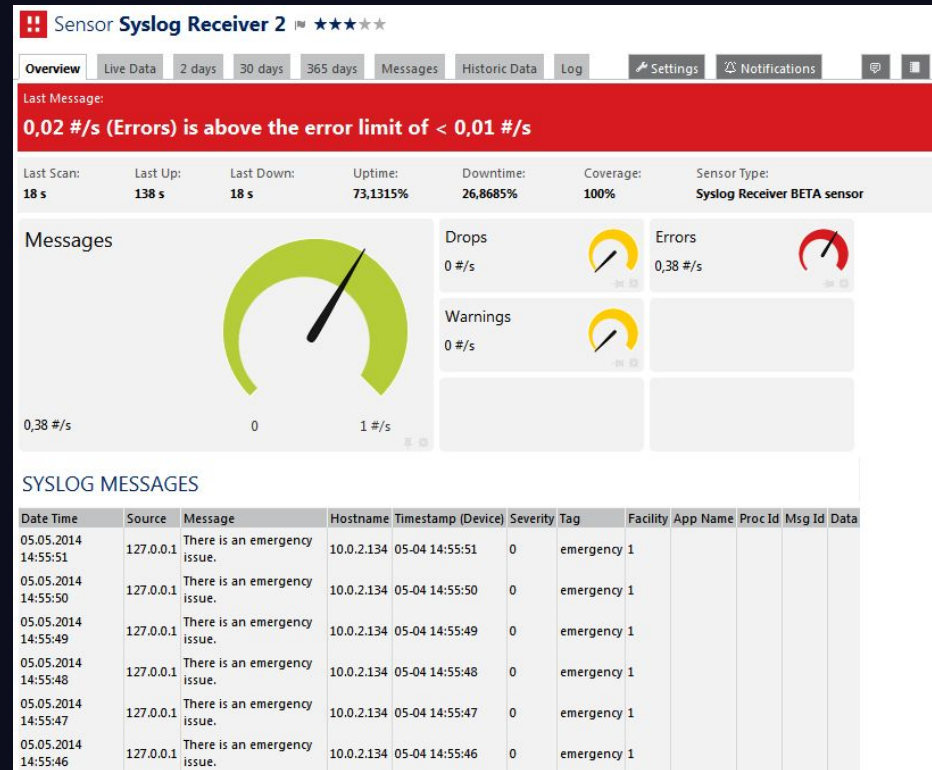
PRTG helps ITA with:

- Auto-discovery of IP ranges
- Tracking used/unused IPs
- Detecting duplicate IPs
- Seeing devices online/offline
- Preventing IP conflicts



# What is Syslog?

- Standard **system logging protocol**
- Used to **transfer log information** from network devices to a **central server**
- Uses a **specific message format** for consistency
- Helps track the **overall health** of network devices by simplifying log management



# How Syslog Works

- Devices **send event messages** using the syslog protocol
- Messages are sent to a **logging / syslog server**
- **Each message can include:**
  - **Timestamp**
  - **Device ID & IP address**
  - **Severity level**
  - **Event details**

## Syslog servers

### Syslog Listener

- Listens on the network to **receive syslog messages**

### Database/Storage

- Stores large volumes of log data
- Needs **fast read/write** for searching and reporting

# Monitoring & Alerts With Syslog

- Use **monitoring tools** to watch syslog messages  
Set up **alerts** for important events (e.g., email to admins)
- Can trigger **automated scripts** for certain events
- Helps **respond faster**, reduce damage, and **improve application availability** during peak hours

Sensors With Status Down									
Show Filters ▾									
Sensor ▾	Probe Group Device ▾	Status ▾	Last Value ▾	Message	Graph	Priority ▾	Fav. ▾	Perf. Impact ▾	<input type="checkbox"/>
!! Ping v2	Local Probe (Local Probe) » Linux / macOS / Unix » 10.0.0.14	Down		Error caused by lookup value 'Unre...	Response Time	★★★★★	<input type="checkbox"/>	<div><div></div><div></div><div></div><div></div><div></div></div>	<input type="checkbox"/>
!! DNS v2	Local Probe (Local Probe) » Network Infrastructure » DNS: 64.71.255.204	Down		Error 4 occurred: Domain name not...	Records Resc No data	★★★★☆	<input type="checkbox"/>	<div><div></div><div></div><div></div><div></div><div></div></div>	<input type="checkbox"/>
!! DNS v2	Local Probe (Local Probe) » Network Infrastructure » DNS: 64.71.255.198	Down		Error 4 occurred: Domain name not...	Records Resc No data	★★★★☆	<input type="checkbox"/>	<div><div></div><div></div><div></div><div></div><div></div></div>	<input type="checkbox"/>

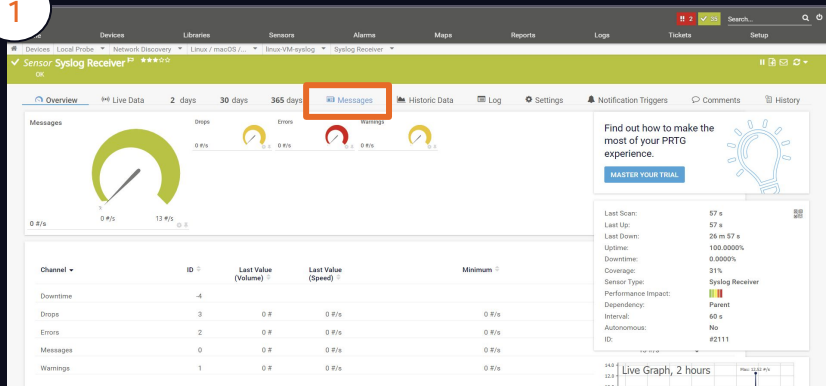


# Play demo vid

Setting up and sending a syslog message

# Filtering by severity, device, or keyword

1



2

## Syslog Messages

Select Range <span>Filter By Date</span>										
2025-08-06 01:31 <span>📅</span> — 2025-11-14 01:31 <span>📅</span>										
Filter <span>🔍</span>	Source	Message	Hostname	Severity	Tag	Facility	Appname	ProcId		
				Any <span>▼</span>		Any <span>▼</span>				
	Source	Message	Hostname	Timestamp (Device)	Severity	Tag	Facility	App Name	Proc Id	Msg Id
	2025-11-14 1:31:32 AM	172.20.225.136	PRTG TEST MESSAGE FROM Aysha-VM	Aysha	11-14 01:31:32	6	aysha	16		

# Centralized Logging

1

Elements of filters are: a parameter, and a value (comma separated) to match on a structured data value (RFC 5424)

**Fixed Include Filter** *This sensor runs on a specific device, so the sensor filters incoming syslogs for the source IP address of this device and shows matching messages only. If you want to see all messages that are sent to a probe system, create this sensor on the probe device.*

**Include Filter** <sup>ⓘ</sup> severity[0-6]

**Exclude Filter** <sup>ⓘ</sup>




**Warning Filter** <sup>ⓘ</sup> severity[4]

**Error Filter** <sup>ⓘ</sup> severity[0-3]

Save

2

## Notification Triggers

Type ^	Rule	Actions
State Trigger	When sensor state is <u>Down</u> for at least <u>60</u> seconds, perform @ <u>Email and push notification to admin</u>	 
	When sensor state is <u>Down</u> for at least <u>300</u> seconds, perform  <u>Ticket Notification</u> and repeat every <u>5</u> minutes	
	When sensor state is no longer <u>Down</u> , perform <u>no notification</u>	

# Configuration Management in PRTG

Many branches → lots of repeated device types

- Linux servers, firewalls, switches at each site

Goal: **same monitoring config everywhere, minimal manual work**

PRTG tools we can use:

- Device templates → standard monitoring pack we can re-use
- Groups & tags → organize devices, share common settings
- SSH / custom script sensors → optionally watch for config changes

1

The screenshot shows the PRTG Network Manager interface. A context menu is open for a device named 'linux-VM-syslog'. The menu options include: Scan Now, Details..., Edit, Add Sensor..., Auto-Discovery, Create Device Template... (highlighted with an orange rectangle), Recommend Now, Sort Alphabetically, Delete..., Clone..., Move, Pause, Priority/Favorite, Historic Data, Device Tools, Find Duplicates..., Send Link by Email, and Add Ticket. The device's status bar at the bottom shows 'Syslog Receiver 0.08 #/s' and an 'Add Sensor' button.

2

The screenshot shows the 'Create Device Template for linux-VM-syslog' dialog box. It includes a note about sensors that cannot be saved in a device template. The 'Enter Template Name' section shows 'Linux Standard' as the template name. The 'Exclude Sensors' section lists two sensors: 'Ping v2' (checked) and 'HTTP' (unchecked). The 'OK' button is highlighted in blue.

Create Device Template for linux-VM-syslog

Note: There are sensors that you cannot save in a device template. For a list of these sensors, see the [PRTG Manual: Create Device Template](#).

Enter Template Name

Template Name ⓘ

Linux Standard

You can exclude sensors from the device template. Enable the checkbox in front of a sensor that you want to exclude.

Note: Sensors that you cannot save in a device template do not appear in this list.

Note: Sensors that dynamically scan for available monitoring items when you add the sensor to a device do not appear in this list. PRTG automatically includes these sensors in the device template if they support the device template functionality. You cannot exclude these sensors from the device template.

Exclude Sensors

Sensors

☐ ☒ Ping v2

☐ ☒ HTTP

Cancel OK

The background features a series of thin, flowing, light blue lines that create a sense of motion and depth against a dark blue gradient. The lines are most concentrated in the center and bottom, radiating outwards towards the top and sides.

**Play video**












Overview 2 days 30 days 365 days Alarms

!! 6 W 1 ✓ 34 ? 1 (of 42) S M L XL ⚙️

- 15 msec
- 10.0.0.199
  - ✓ Ping v2 5 msec Add Sensor
- 10.0.0.235 Paused by dependency
  - !! Ping v2 Add Sensor
- 10.0.0.237
  - ✓ Ping v2 111 msec Add Sensor
- 10.0.0.4 Paused by dependency
  - !! Ping v2 Add Sensor
- 10.0.0.50
  - ✓ Ping v2 5 msec Add Sensor
- 10.0.0.74 Paused by dependency
  - !! Ping v2 Add Sensor
- linux-VM-syslog
  - ✓ Syslog Receiver 0.08 #/s ✓ Ping v2 1 msec !! HTTP Add Sensor
- Linux branch 2
  - ✓ Ping v2 4 msec W HTTP (Please ... ? Syslog Receiver Add Sensor
- Printers

# Performance Monitoring in PRTG

## Historical Reports and Trends

 Overview	 2 days	 30 days	 365 days	 Alarms	 Log	 Management	 Settings	 Notification Triggers	 Comments	 History
Date Time	User	Message								
2025-11-14 7:54:58 PM	PRTG System Administrator	Subnode Created. Change Trigger ID:4/On Notification: Ticket Notification (ID: 302)								
2025-11-14 7:54:42 PM	PRTG System Administrator	Subnode Edited. Threshold Trigger ID:3/Off Notification: Networking Assignment (ID: 2088)								
2025-11-14 7:54:34 PM	PRTG System Administrator	Subnode Created. Threshold Trigger ID:3/Channel: Primary Threshold Trigger ID:3/Condition: above Threshold Trigger ID:3/Value: 0 Threshold Trigger ID:3/Latency: 60 Threshold Trigger ID:3/On Notification: no notification (ID: -1) Threshold Trigger ID:3/Off Notification: no notification (ID: -1)								
2025-11-14 7:53:52 PM	PRTG System Administrator	Subnode Created. Speed Trigger ID:2/Channel: Traffic In Speed Trigger ID:2/Condition: above Speed Trigger ID:2/Value: 10 Speed Trigger ID:2/Scale: Mbit Speed Trigger ID:2/Time: minute Speed Trigger ID:2/Latency: 10 Speed Trigger ID:2/On Notification: Networking Assignment (ID: 2088) Speed Trigger ID:2/Off Notification: Networking Assignment (ID: 2088)								
2025-11-14 7:53:36 PM	PRTG System Administrator	Subnode Edited. State Trigger ID:1/On Notification: Networking Assignment (ID: 2088) State Trigger ID:1/Off Notification: Networking Assignment (ID: 2088) State Trigger ID:1/Excitation Notification: Networking Assignment (ID: 2088)								
2025-11-14 2:25:05 PM	PRTG System Administrator	Created. 25.4.112.1189								

1 to 6 of 6

- Monitors CPU, RAM, Disk, and Bandwidth
- Real-time and historical tracking
- Detects overloaded or failing devices
- Key for diagnosing ITA's "laggy" performance issues

## Historical Reports and Trends

- Stores long-term Graphs
- Useful for capacity planning
- Shows recurring problem times

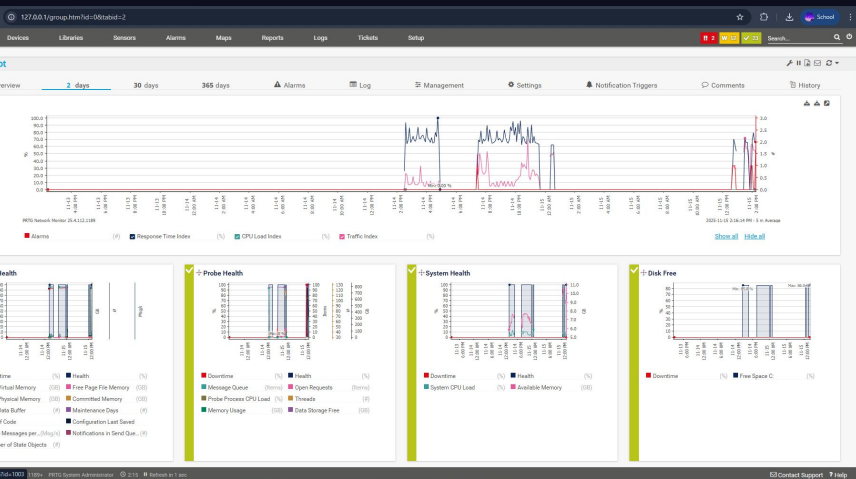


# Monitoring CPU and Memory Health

## CPU Monitoring

- Shows real-time processor usage
- Detects overloaded servers/routers
- CPU spikes = slow apps and lags

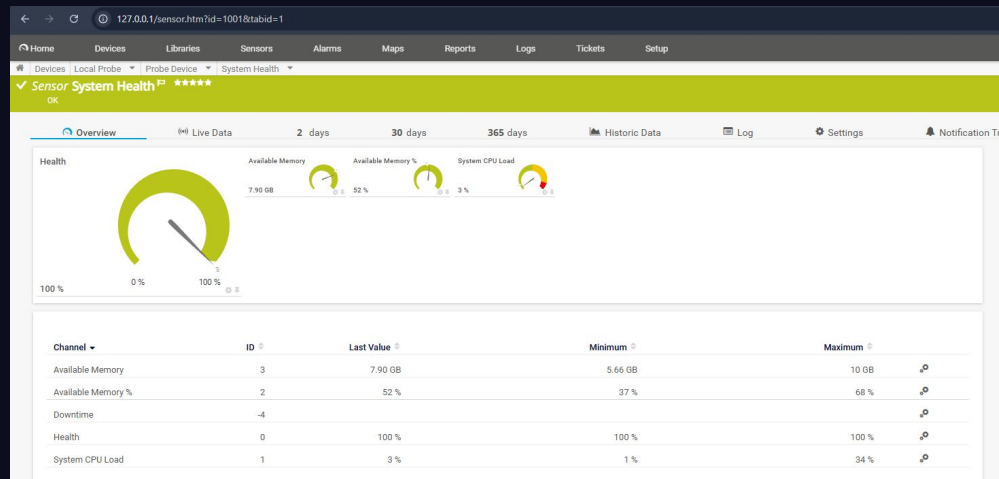
## CPU Monitoring



## Memory Monitoring

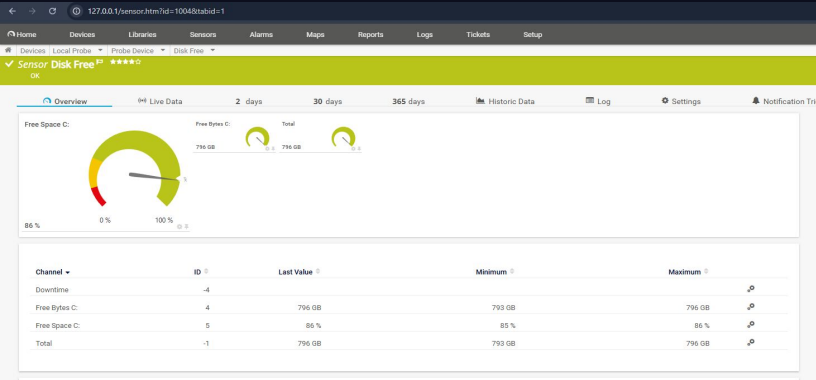
- Tracks RAM usage
- High memory means there's freezing and slowness
- Helps detect stressed equipment

## Memory Monitoring



# Storage and Network Traffic Monitoring

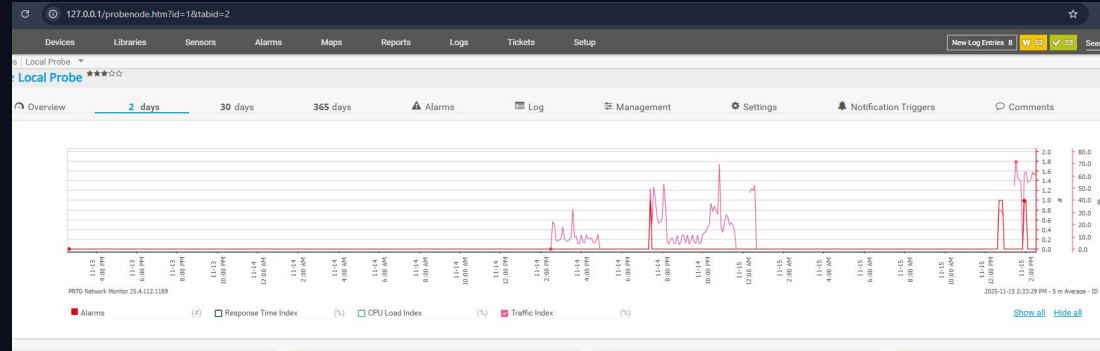
## Disk Space



## Disk Monitoring

- Monitors free disk space
- If disks are full there are service failures
- Important for servers storing logs, apps, backups

## Traffic Index



## Bandwidth Monitoring

- Measures WAN/LAN traffic
- Detects congestion on branch links
- Helps explain slow connections

# Alert and Threshold Triggers


## Alerts and Thresholds →

- Thresholds for CPU, RAM, Disk, Traffic
- Sends email, SMS, push alerts
- Notifies IT before users complain



## Live Alert Example →

- Alert triggers automatically
- Sensor turns yellow/red
- Incident is logged

 Disk Free	Warning	86 % (Free Space C:) is below the warning limit of 90 % in Free Space C:
<small>  Threshold Trigger ID:2/Channel: Total   Threshold Trigger ID:2/Condition: above   Threshold Trigger ID:2/Value: 90   Threshold Trigger ID:2/Latency: 60   Threshold Trigger ID:2/On Notification: no notification (ID: -1)   Threshold Trigger ID:2/Off Notification: no notification (ID: -1)</small>		

2025-11-15 4:29:27 PM  Probe Device

WMI Free Disk Space (Multi Disk)

 Disk Free

Subnode Created

The background features a series of smooth, flowing, light blue lines that create a sense of motion and depth against a dark blue gradient. The lines are most concentrated in the center and fade out towards the edges.

**Play video**

# Conclusion and Recommendation

- PRTG centralized monitoring and logging for all ITA devices
- Maps and dashboards allow IT to quickly identify network issues
- Alerts and notifications reduce downtime and speed up incident response
- Templates, device groups, and IPAM support standardized configurations and up-to-date inventories
- Helps ITA's "laggy, unstable" network providing visibility, proactive alerts, and trend analysis
- Recommendation: implement PRTG to improve network reliability, reduce outages, and support future growth.

