Using PRTG to Construct a Free Network Monitoring Environment (Postprint)

Authors: Zhang Zhiwei

Date: 2023-10-08T00:00:00+00:00

Abstract

Propelled by the wave of interconnectivity, both people' s work and daily life have become fully networked, necessitating a stable network environment for support, whether in domestic settings or organizational operations. Particularly for organizations, diverse business operations impose heightened demands on the stability and reliability of underlying network infrastructure. For network administrators in typical organizations, they must not only construct a network featuring reliable equipment and meticulous planning, but also possess the capability to monitor the network in order to comprehend fault conditions either prior to or during their occurrence. PRTG is a powerful network device monitoring software that enables network administrators to ascertain the real-time status of various devices within the internal network—including routers, firewalls, switches, servers, computers, and more—and to display such information through graphical and iconic representations, thereby facilitating comprehension. The ability to monitor equipment operation status in real-time and receive advance warnings proves critically important for network administrators in small and medium-sized organizations burdened with numerous responsibilities.

Full Text

Abstract

Driven by the wave of interconnectivity, people' s work and daily lives have become completely network-dependent. Whether for household use or daily operations within organizations, a stable network environment is essential for support. In particular, organizations demand higher stability and reliability from their underlying network infrastructure for various business operations. For network administrators in typical organizations, it is necessary not only to build a network with reliable equipment and careful planning but also to possess network monitoring capabilities to understand fault conditions before or as they occur.

PRTG is a powerful network device monitoring software that enables network administrators to understand the real-time status of various devices within the internal network, including routers, firewalls, switches, servers, and computers, presenting this information in graphical and icon-based formats for easy comprehension. For network administrators in small and medium-sized organizations burdened with numerous responsibilities, the ability to monitor equipment operation in real time and receive advance warnings is critically important.

Keywords: network device monitoring; PRTG; user interface; monitoring data
Classification Code: TN948.3
Document Code: A
Article ID: 1671-0134(2019)05-109-04
DOI: 10.19483/j.cnki.11-4653/n.2019.05.036

1.1 Introduction to PRTG

PRTG, fully named Paessler Router Traffic Grapher, is a powerful network monitoring application based on the Windows system, suitable for large, medium, and small networks. It can monitor virtually everything imaginable, including traffic, packets, applications, bandwidth, cloud services, databases, virtual environments, uptime, ports, IP addresses, hardware, security, Web services, disk usage, physical environments, and IoT devices. The software provides network administrators with real-time readings and periodic usage trends to optimize the efficiency, layout, and configuration of various network components such as routers, firewalls, and servers.

The software operates around the clock using Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), packet sniffers, NetFlow (as well as IPFIX, sFlow, and jFlow), and many other industry-standard monitoring protocols. It continuously records network usage parameters and system availability, storing this data in an internal database for analysis.

PRTG offers two network monitoring options: local PRTG and Paessler' s cloud-hosted PRTG. With local PRTG, the core server and local probe run within the local network; cloud-hosted PRTG operates the core server and hosted probe from the cloud. Both options use identical monitoring configurations and the same PRTG Web interface for viewing monitoring data.

To use PRTG locally, simply download it from the official website and install it on a Windows computer. To use cloud-hosted PRTG, create an account at https://my-prtg.com without needing to download any software.

1.2 PRTG Architecture

PRTG components are divided into three major categories: system components, user interfaces, and system administration programs.

(1) System Components: These consist of the core server and probes. The core server is the central component of PRTG, encompassing data storage, Web server, reporting engine, notification system, and more. It is configured as a long-running Windows service. Probes are the elements that actually perform monitoring in PRTG. PRTG includes local probes, remote probes, and cluster probes; cloud-hosted PRTG features hosted probes and remote probes. All monitoring data is collected to the central core server. Probes are also configured as long-running Windows services.

The core server executes the following processes: configuration management of monitored objects (such as servers, workstations, printers, switches, routers, virtual machines, etc.); management and configuration of connected probes; cluster management; database of monitoring results; notification management including mail servers for email delivery; report generator and scheduler; user account management; data purging (e.g., deleting data older than 365 days); and Web server and API server.

Probes perform actual monitoring through sensors created by PRTG on devices (such as computers, routers, servers, or firewalls), receive their configuration from the core server, run monitoring processes, and collect monitoring data to the core server.

(2) User Interfaces: These include the Web interface, Desktop interface, and mobile app. The Ajax-based Web interface is used for configuring devices and sensors, viewing monitoring results, and managing system and user administration. The Desktop interface is a cross-platform PC application that can be downloaded and installed on local computers to connect to different PRTG core servers and view their data. The PRTG mobile app enables network monitoring on the go and is compatible with iOS and Android devices.

(3) System Administration Programs: These consist of PRTG administration tools on the core server system and PRTG administration tools on remote probe systems. The former is used to configure basic core server settings within PRTG, such as administrator login, Web server IP and port, probe connection settings, cluster mode, and system language. The latter is used to configure basic probe settings such as probe name, IP address, and server connection settings.

2. Deployment of PRTG

It is recommended to install and run the PRTG Core Server and Remote Probes on X64 architecture PCs or servers with the following minimum hardware configuration: dual-core CPU, 3GB RAM, and 250 GB disk space. The preferred operating systems are 64-bit Microsoft Windows 7 or Microsoft Windows Server

2008 R2 and above, with .NET Framework version 4.7.2 installed. Note: Windows Server 2012 Core mode and Minimal Server interface are not supported.

2.1 Enabling SNMP on the Core Server

PRTG requires SNMP to read core server data. SNMP is disabled by default in Windows systems and must be manually enabled. For example, on Windows Server 2008 R2, open the Control Panel, click on Programs, then click Turn Windows features on or off. This opens the Server Manager. Locate Features Summary, click Add Features, and check SNMP Services, including SNMP Service and SNMP WMI Provider, then click OK.

2.1.1 Configuring SNMP Options Open the Control Panel, click Administrative Tools, then Services. Double-click SNMP SERVICE. In the Security tab, add a community name (which must match the setting on monitored devices), selecting either read-only or read/write permissions. Under the option to accept SNMP packets from these hosts, add the IP addresses of devices to be monitored, then click OK.

2.1.2 Opening Firewall Port 161 Open the Control Panel, click Windows Firewall, then Advanced Settings. Look for SNMP Service (UDP In) in the inbound rules; if it doesn' t exist, create a new rule. Select UDP, port 161, and in the advanced configuration, check Domain, Public, and Private, then click OK to activate.

2.2 Enabling SNMP on Monitored Devices

Monitored devices must have SNMP enabled and necessary parameters configured for PRTG to automatically monitor traffic and generate traffic graphs. Using H3C switches as an example (other brands can refer to their respective commands):

```
<H3C>system-view
[H3C]snmp-agent
[H3C]snmp-agent local-engineid xxxxxxxxxxxxxxx (device engine ID)
[H3C]snmp-agent community read xxxxxx (community name, must match core server setting)
[H3C]snmp-agent sys-info version v1 v2c
[H3C]snmp-agent target-host trap address udp-domain xxxx.xxx.xxx.xxx (PRTG server address) p
```

After completing the above steps, download the 30-day trial version of PRTG with an included license from the official PRTG website. Run the installation, accepting all defaults until completion. A PRTG Network Monitor icon will be automatically created on the core server desktop. The default login username and password are both 'prtgadmin' . Upon first login, PRTG automatically creates the first probe; PRTG' s local probe runs on the same computer as the PRTG core server. Users can choose to automatically scan devices or manually add devices by providing IP addresses and other information. After adding

devices, right-click on the device name to access a context menu and run Auto-Discovery. PRTG can inspect and create sensors; if it finds useful sensors that are available but not yet created, it will generate a recommended sensor list for user selection to ensure no critical monitoring information is missed. Of course, network administrators familiar with their equipment can also choose to manually add sensors.

3. PRTG Functionality Implementation

Leveraging over 10,000 built-in sensors, PRTG employs technologies including Ping, SNMP, WMI, performance counters, HTTP, SSH, packet sniffing, NetFlow, sFlow, jFlow, PowerShell, push message receivers, and PRTG Cloud. It covers monitoring targets such as Windows, Linux/macOS, virtualized operating systems, storage and file servers, email servers, databases, cloud services, and more. It enables monitoring of device availability/uptime, bandwidth/traffic, network speed/performance, CPU usage, disk usage, memory usage, hardware parameters, and network infrastructure.

3.1 Sensor Types

Commonly used network monitoring sensors include:

Ping Sensor: Sends ICMP echo request pings from the computer running the probe to monitored devices to monitor availability. The default is 5 pings per scanning interval, displaying: ping time; minimum ping time when using multiple pings per interval; maximum ping time when using multiple pings per interval; and packet loss percentage when using multiple pings per interval.

HTTP Sensor: Monitors web servers using Hypertext Transfer Protocol (HTTP), displaying webpage load times. This is the simplest method for monitoring website accessibility.

HTTP Advanced Sensor: Monitors webpage source code using HTTP, supporting authentication, content checking, and other advanced parameters. It can display: load time; bytes received; download bandwidth (speed); and time to first byte.

SNMP Sensor: The most diverse sensor type in PRTG, fully utilizing SNMP' s simple network management capabilities to present collected traffic information, performance, load, disk space, and other device parameters in graphical or tabular formats. Companies such as Cisco, Dell, HP, and Lenovo provide specialized custom SNMP sensors for monitoring their own equipment.

Among these, the SNMP Traffic Sensor is the primary sensor for monitoring network infrastructure, commonly used for routers, firewalls, switches, and other network infrastructure. When adding this sensor, the monitored device' s IP address and community name (which must match the network device settings) are required. Each port on a device has a traffic sensor that can display: traffic

in/out; total traffic; errors in/out; discards in/out; unicast packets in/out; non-unicast packets in/out; multicast packets in/out; broadcast packets in/out; and unknown protocols. The actual channels displayed depend on the monitored device and sensor configuration.

3.2 Sensor Status Indicators

In the PRTG device tree, multiple sensors are typically created for each device to monitor different aspects. A simple color code system provides conspicuous visual indication of network events.

Sensor colors always reflect their current status. Additionally, sensor status display follows a hierarchical structure. Whenever sensor status is displayed (in the device tree or on geographical maps), the higher its position in the hierarchy, the greater its priority in status display. For example, if all sensors on a device are in normal status but one sensor reaches a down state, the overall device status will display as down (shown in red in tree view), because the down state has the highest priority in the hierarchy.

3.3 Alert and Notification Processing

PRTG allows login via PC or Android/iOS mobile apps to view device monitoring status. In addition to routine proactive inspections, PRTG can use notifications to send alerts to network administrators when defined conditions are detected (such as slow sensors, failures, or sensor channels exceeding thresholds). It supports defining unlimited notifications using one or multiple communication channels, including email, SMS, and push notifications to Android and iOS devices.

PRTG sends notifications to notification contacts configured by users, and each user account on PRTG can configure individual notification settings.

Sensor status or data can trigger notifications, and external alerts can be configured as needed. While sensors activate notification triggers, groups or devices can have higher-level notification triggers set in the hierarchy. Inheritance mechanisms can also be used to configure notification triggers for multiple sensors simultaneously. PRTG includes default notification triggers for the root group; if any sensor in the PRTG installation remains down for 10 minutes, the default notification trigger sends a standard notification email to the PRTG administrator. To complete notification setup, verify that the following four configurations are properly set:

(1) Check and configure notification delivery settings to confirm how and to which recipients PRTG will send messages; (2) Check and configure notification contacts for PRTG users to confirm message recipients; (3) Check and configure notification templates to confirm notification methods and content; (4) Check and configure notification triggers for monitoring targets to confirm when notification messages are sent.

A single sensor can monitor only one aspect of a network device—for example, traffic on one switch port, server CPU load, or available disk space requires three separate sensors. On average, each server requires approximately 15-20 sensors, while each switch can selectively monitor several key ports based on usage. For most organizations without dedicated network administrators, where staff handle multiple roles and cannot provide 24/7 monitoring, using the free version of PRTG to monitor only critical components of essential network infrastructure —such as main gateways, firewalls, switches, and servers—can fully satisfy daily network security management needs through reasonable prioritization, as the free version supports up to 100 sensors.

PRTG features an easy-to-use Web interface with rich visualization capabilities, including real-time charts, detailed report generation, and historical data trend display. It supports multiple protocols for data collection, enabling the gathering of data from nearly all components in the network. The software is both powerful and simple to use. PRTG offers several paid versions based on sensor license quantities. After the 30-day trial period expires, if no license is purchased, PRTG automatically reverts to a permanent free version supporting up to 100 sensors.

References

[1] Getting started with PRTG - Academy modules [EB/OL]. https://www.paessler.com/support/getting-started.
[2] PRTG How-to Guides - Step by step to start with PRTG [EB/OL]. https://www.paessler.com/support/how-to.
[3] PRTG Network Monitor User Manual [EB/OL]. https://www.paessler.com/manuals/prtg.

(Author' s affiliation: Xinhua News Agency Beijing Branch)

Note: Figure translations are in progress. See original paper for figures.