Seth Ayers

10/30/2017

IT 330 – 01

Homework 4   
AyersS\_HW4.docx

**Quiz 1:**

1. A(n) **Switch** is a device that connects network devices together and operates at the Data Link ayer of the OSI model.
2. A(n) **Router** is a network device that can forward packets across computer networks.
3. A(n) **Proxy Server** is a computer or an application program that intercepts a user request from the internal secure network and then processes that request on behalf of the user.
4. A device that can detect an attack as it occurs is known as a(n) **IDS (Intrusion detection system)**.

**Quiz 2:**

1. As a packet leaves a network, NAT removes the **Private IP address** from the sender’s packet and replaces it with an alias IP public address.
2. True or False: The DMZ functions as a separate network that rests outside the secure network perimeter. **TRUE**
3. Instead of just having networks and hosts, with **Subnetting**, networks can be divided into three parts: network, subnet, and host.
4. **Remote access** refers to any combination of hardware and software that enables remote users to access a local internal network.

**Quiz 3:**

1. C
2. B

4 D

6 B

7 A

8 D

9 D

10 C

12 C

13 D

18 B

20 C

**Part 2:**

**Project 1 (Case Project 7-2)**

|  |  |  |  |
| --- | --- | --- | --- |
| Firewall Product | 01-SSC-0802 SonicWALL SuperMassive E9800 | Cisco Meraki MX600 Large Branch / Campus Security Appliance | Palo Alto Networks PA-7080 Firewall |
| Price | $81, 300.00 | $22,065.00 | $300,000.00 |
| Protection Level | UTM Enabled | UTM Enabled | NA |
| Max Throughput | 40 Gbps | 2 Gbps | 200 Gbps |
| Firewall Type | Wired Firewall | Wired Firewall | Wired Firewall |
| Max Clients | 10,000 | 10,000 | NA |
| New Sessions per second | 280,000 | NA | 1,200,000 |
| Software Included? | No | No | No |
| Packet filtering | Stateful packet filtering | Stateful packet filtering | Stateful packet filtering |
| Rule-based/Application? | Rule Based | Rule based or Application-aware\* (Requires yearly license subscription, 3yr $22,000) | Rule based AND Application-aware\* (Requires yearly license subscription, 5yr $238,958.99) |
| Extra features | Prioritize important applications, throttle down unproductive applications, blocks unwanted application components, Mobile access (Phone), Caches frequently used website. | Web search filtering, Anti-virus engine and anti-phishing filtering, Geography based firewall, Application usage statistics, Robust remote administration,  Web caching | Automatically scales as new computing power becomes available, agentless integration with MS AD, blocks a range of known threats, Identifies unknown malware, Uses single-pass classification engine that analyzes all traffic. |
| Support | 1 year | \*Must buy license | \*Must buy license |

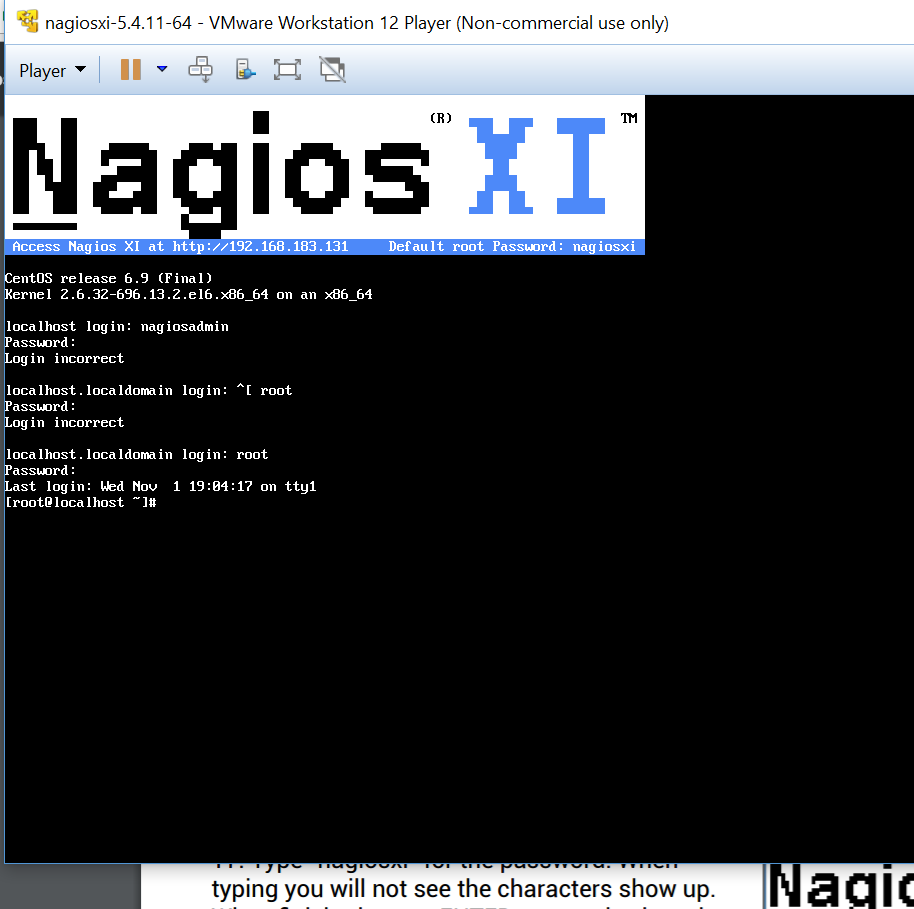
**Recommendations:**

The various listed firewall appliances are obviously intended to medium to large, or very large (Service providers) enterprises. Although the base hardware prices are listed, the licensing fees defiantly need to be taken into consideration (see the 7080’s fee for $230k +). Mostly, these servers share the same capabilities in preventing attacks on business networks, with a few exceptions of the 7080. The biggest difference is the ability to facilitate the intended userbase (clients), the number of session requests in a given second, and dedicated throughput with all security options enabled. Being said, particularly in these firewalls, the size and scope of the business needs to be taken into account.

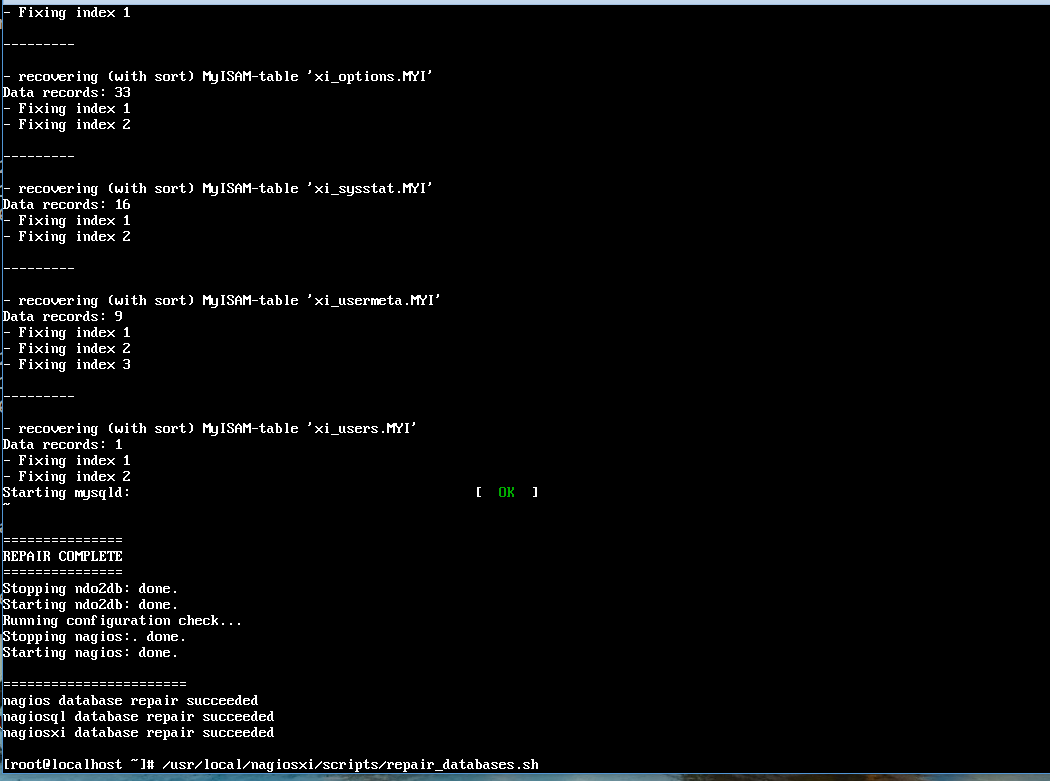
**Project 2:**

**(NAGIOS 11 VM):**

Nagios is an expansive network monitoring program that provide real time information on servers, devices, applications, infrastructure, and protocols. It also has third party support for add-ons for customizing for needs of the enterprise and the specific preferences of the administrators (Multiple API’s). Nagios also has reactive and proactive graphing abilities to clearly display impending trends or current metrics for admins to analyze. Finally, alerts can be customized to cater to the business’s needs; problems are detected and sent to IT staff via text or email.

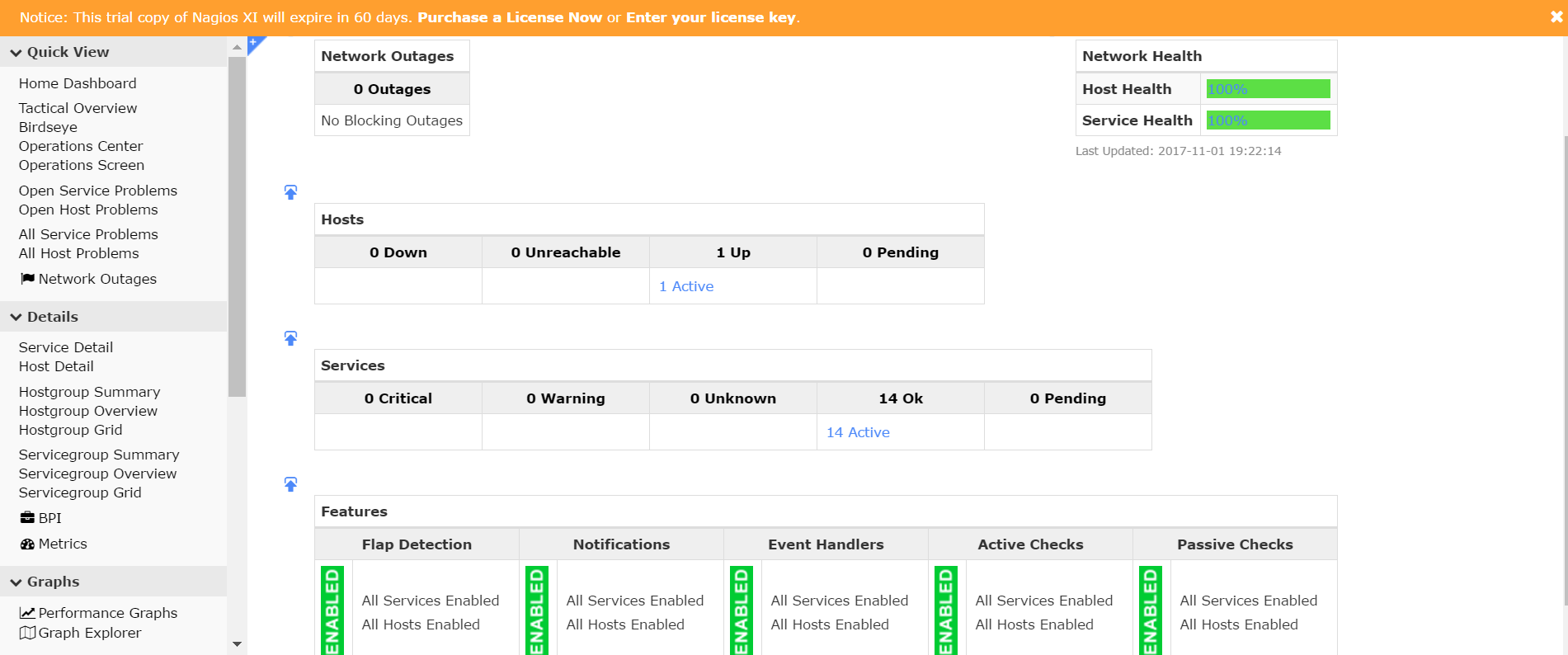


The Nagios 11 monitor is installed via a VM tool, in which a command line is presented after login. This is not the main GUI and is used for repairing and modifying Nagios 11. The actual monitoring software is accessed from any web browser by typing in the IP address of the VM. This IP can be found at the top of the VM or can be found by comparing the VM’s MAC address using the arp -a command/switch your host cmd.

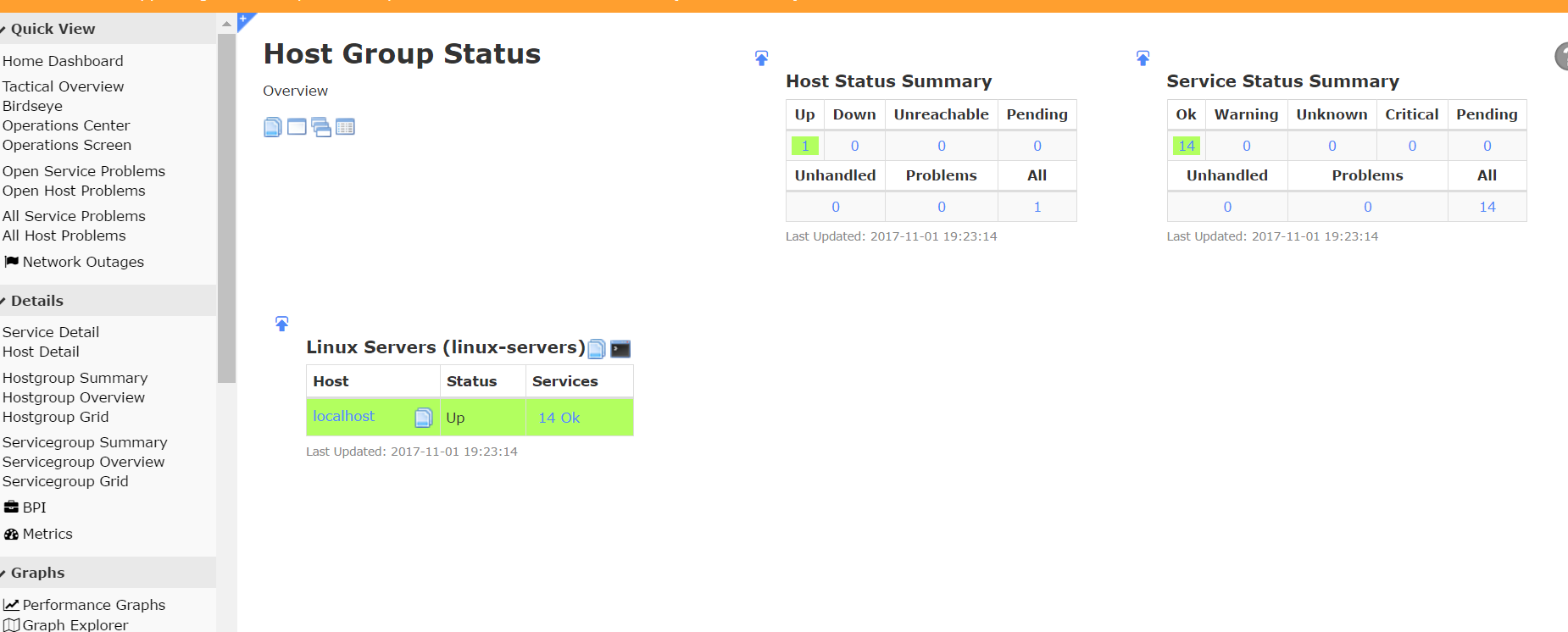


Interestingly, once I accessed the web GUI of Nagios, I immediately receive alerts for a database SQL issue that prevented Nagios to display graphs and charts for the metrics. The error, *“SQL Error [ndoutils] : Table './nagios/nagios\_servicestatus' is marked as crashed and should be repaired”,* was easily fixed by using the above command (/usr/local/nagiosxi/scripts/repair\_databases.sh), which scanned and fixed any issues with the database.

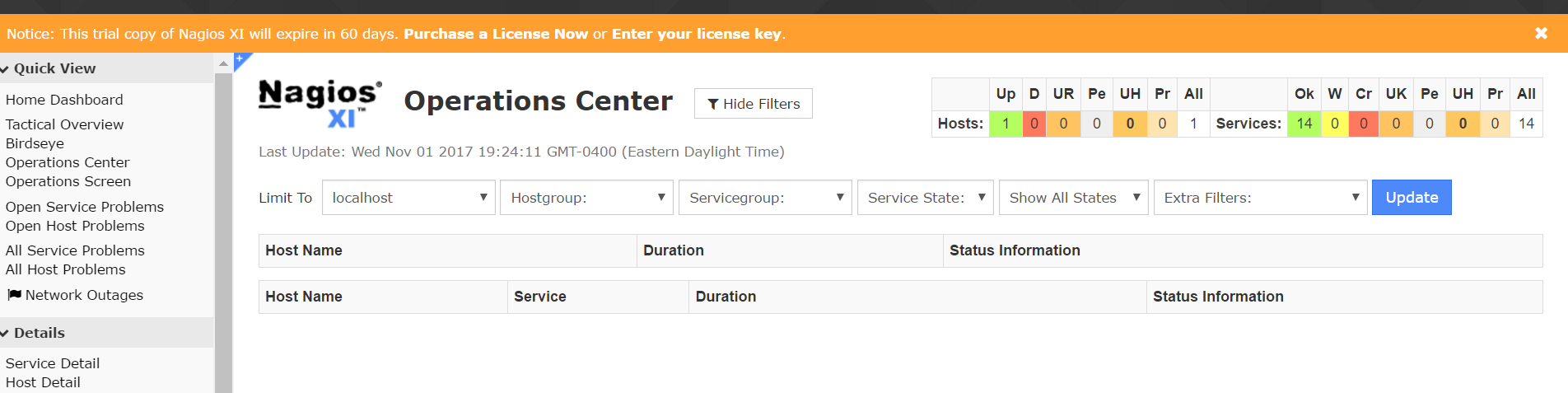
**Configuration settings:**



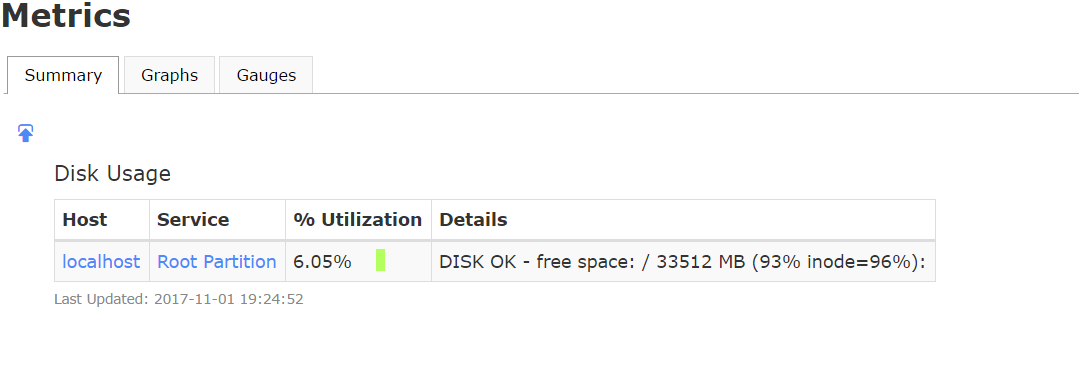
Nagios has an incredibly easy user interface for configuring passive checks, host monitoring, services, active checks, notifications, event handlers, and warning parameters.



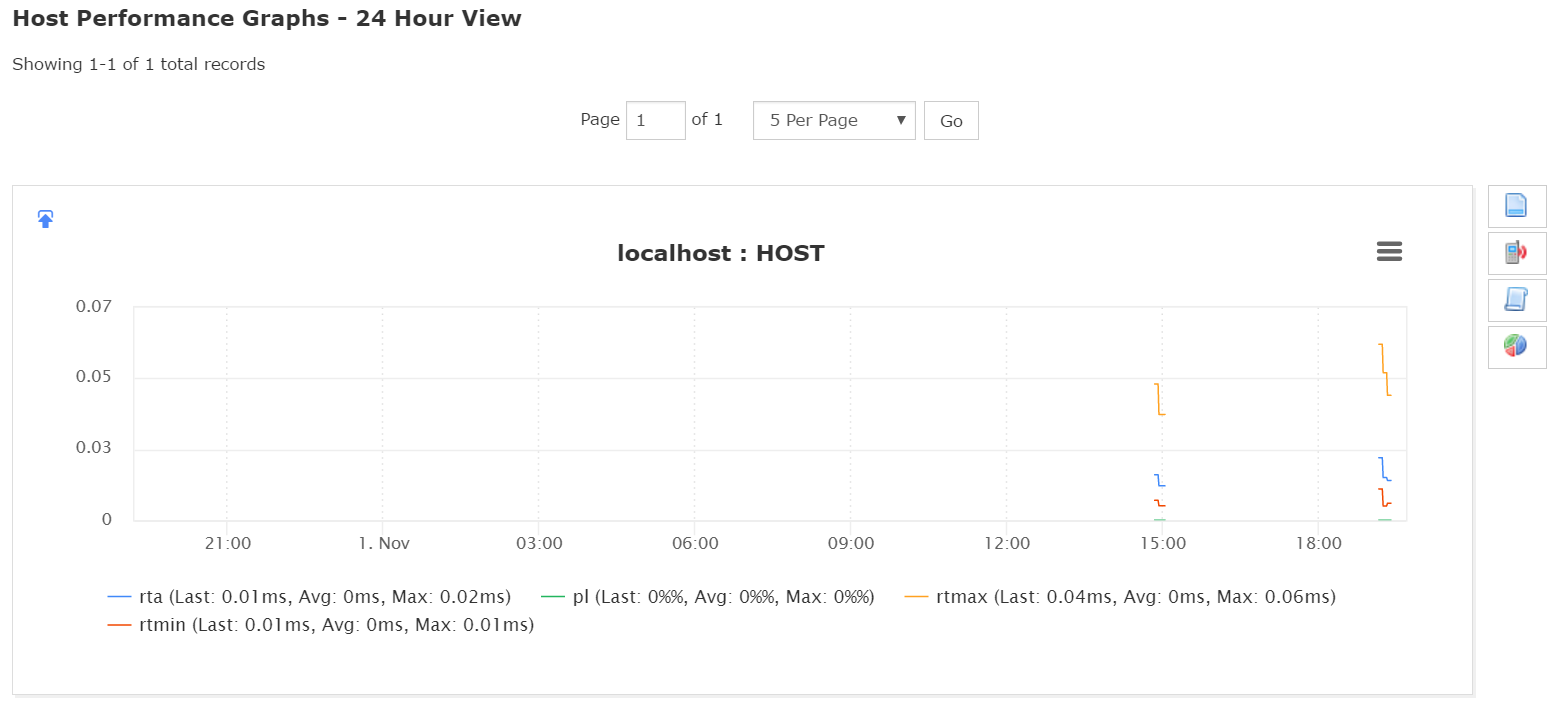
Host group status summaries, monitoring server status and services.



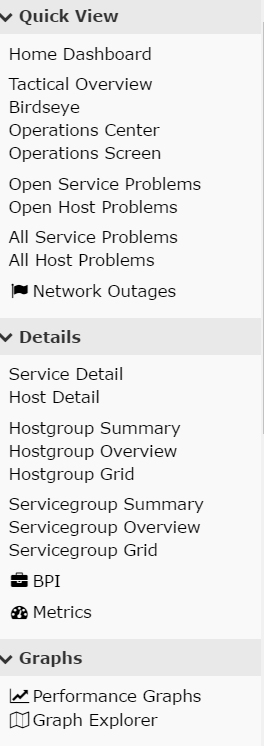
The Nagios operation center combines all running hosts and services to easily view the entirety of all network status. Uptime/Downtimes (upper right hand corner)



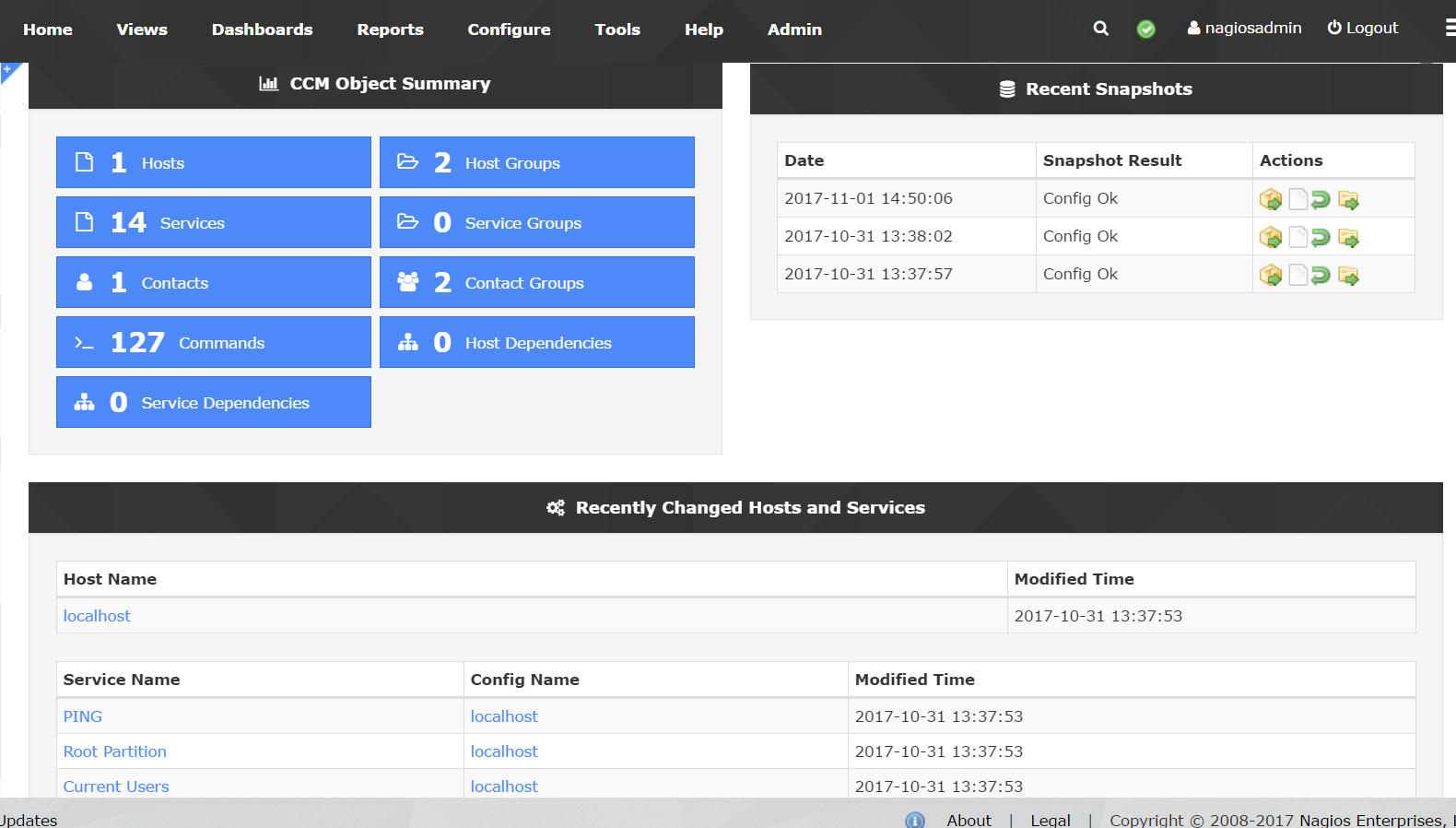
Metrics for monitoring disk utilization and exact details.



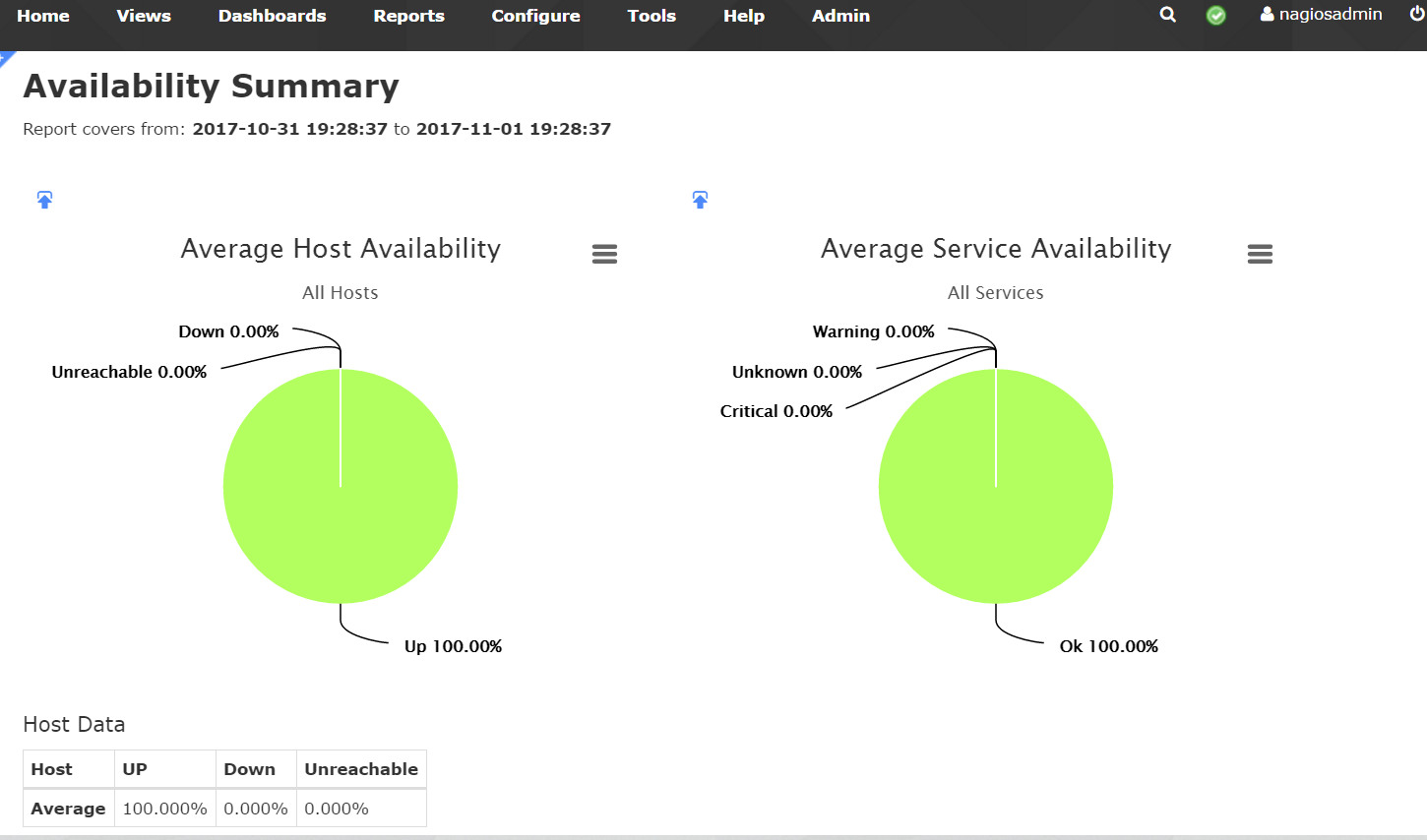
Host performance in the form of a graph. Options on the right allow for adjusting preferences in the graphical display or adjusting alerts.



Side bar display for easy access to different capabilities that Nagios provides.



Overview object summary for groups, hosts, relevant contacts, services, and changes. Also provides snapshots of past host statuses and an audit of changes that have been made.



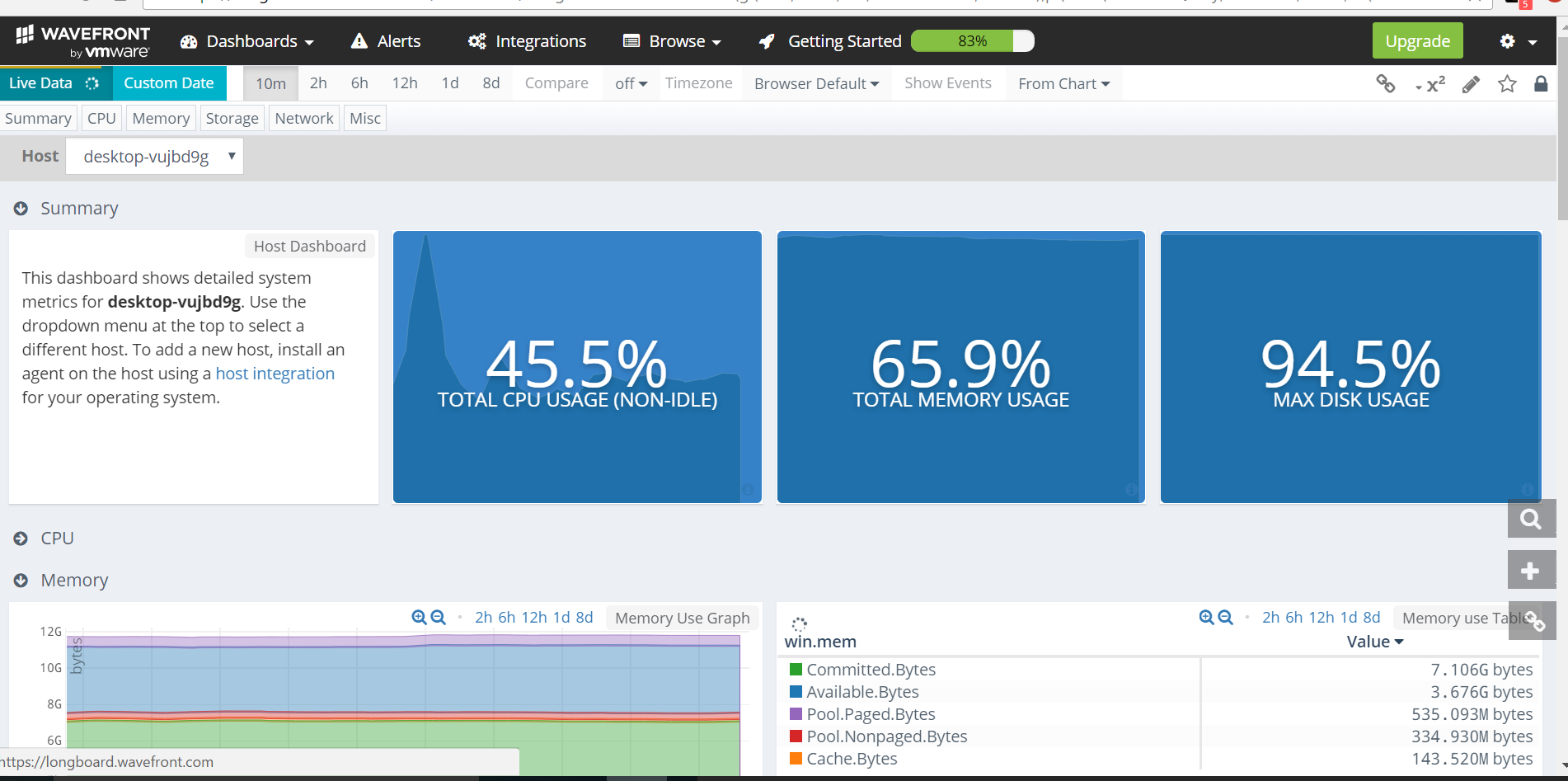
Finally, graphical visualization of all or single hosts/services. Uptime/downtime and warnings, critical issues, and unknown problems.

**Wavefront (Standalone, Windows):**

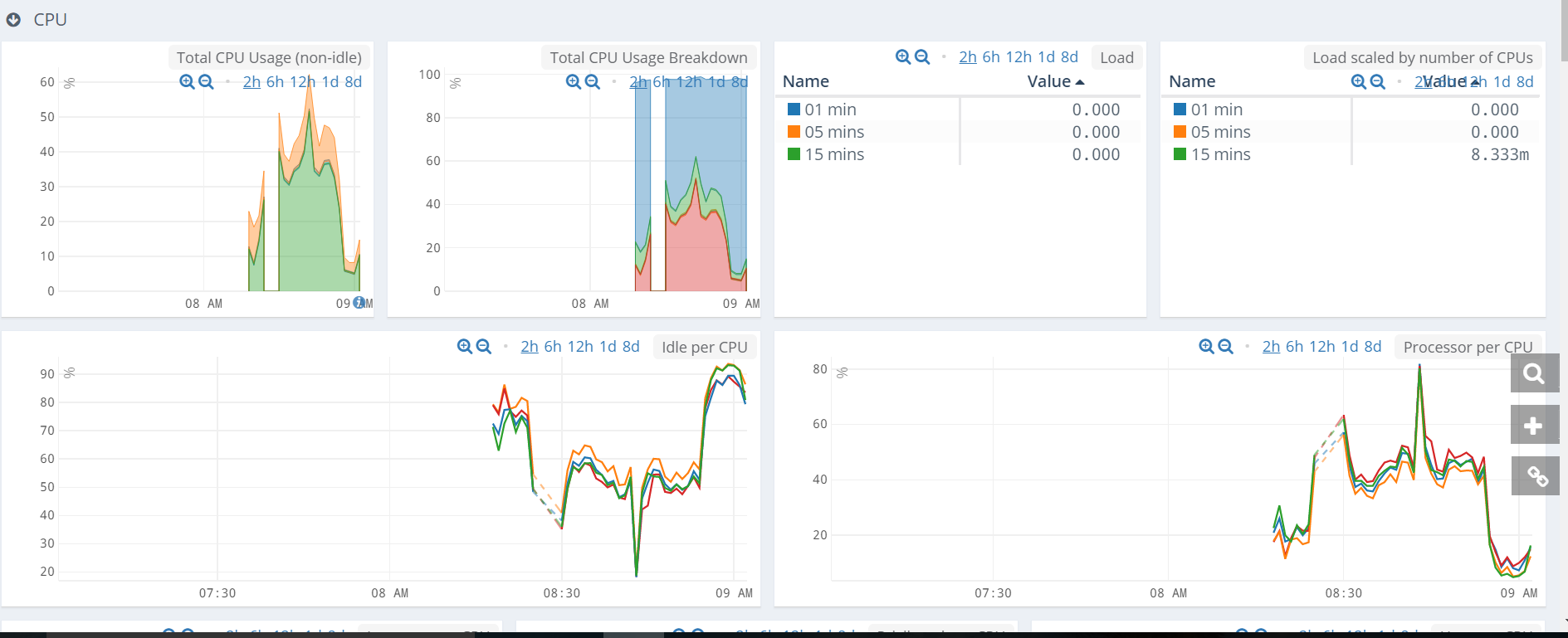
Wavefront is a networking monitoring software as a service program provided by VMware that is almost entirely web based with very few install processes. I was required to download a proxy server and set it up so that the program would have a host to monitor. The set-up process was streamlined, including a wizard that provided clear steps in getting the server running and configuring Wavefront. Wavefront provides a huge array of information, real time, with graphs all displayed on the main summary page. The main dashboard displays one host summary at a time if the option to create charts specific to the needs of the administrators. Graphs show the following:

* Total CPU usage
* Total Memory Usage
* Max Disk Usage
* Total CPU Usage (Non-Idle)
* Total CPU Usage Breakdown
* Load
* Load scaled by number of CPU’s
* Idle per CPU
* Processor per CPU
* Interrupt per CPU
* Privileged per CPU
* User per CPU
* Memory Use Graph
* Swap Memory Graph
* Disk Free vs. Disk Used
* Bytes Sent/Received
* Error Packets Sent/Received
* Discarded Packets Sent/Received
* TCP Connections
* UDP Traffic

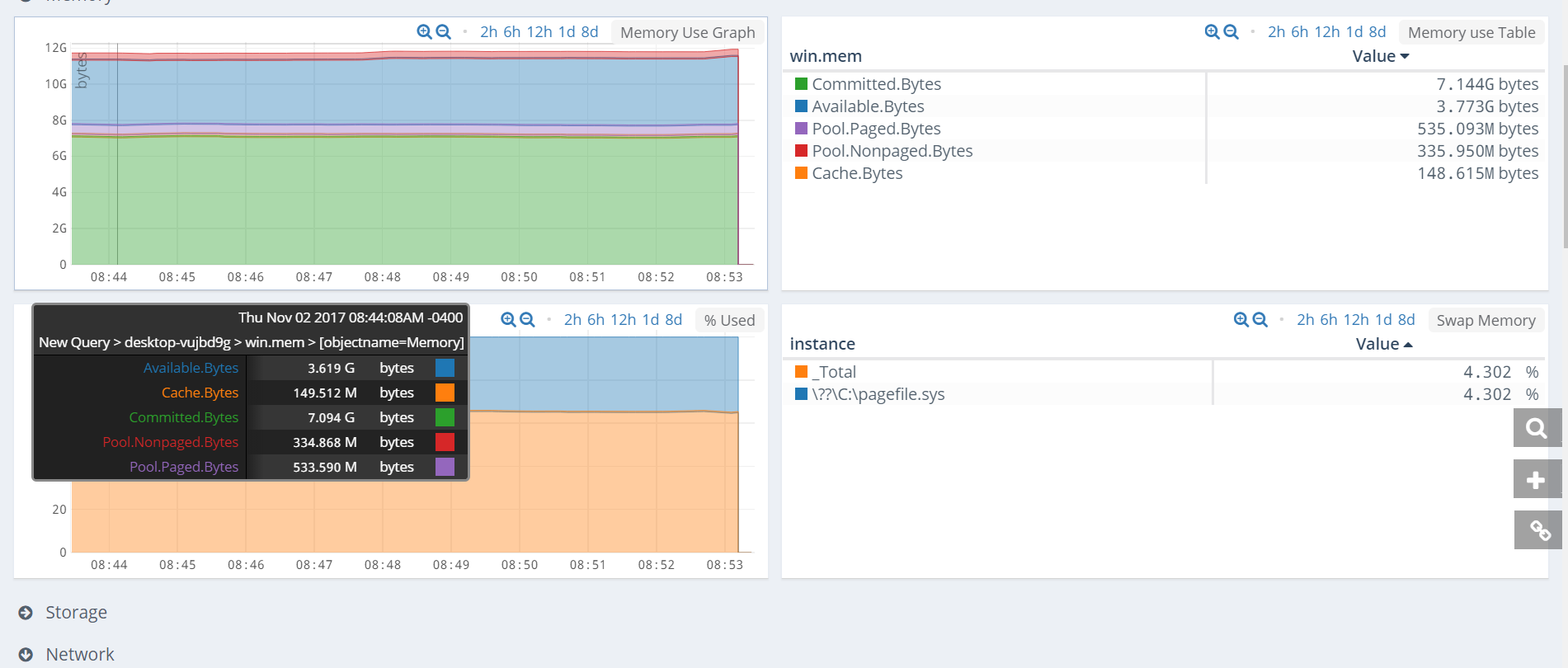
These graphs can be time adjusted with the option to compare snapshots of different states. Alerts, integration control, and dashboard settings can also be set.



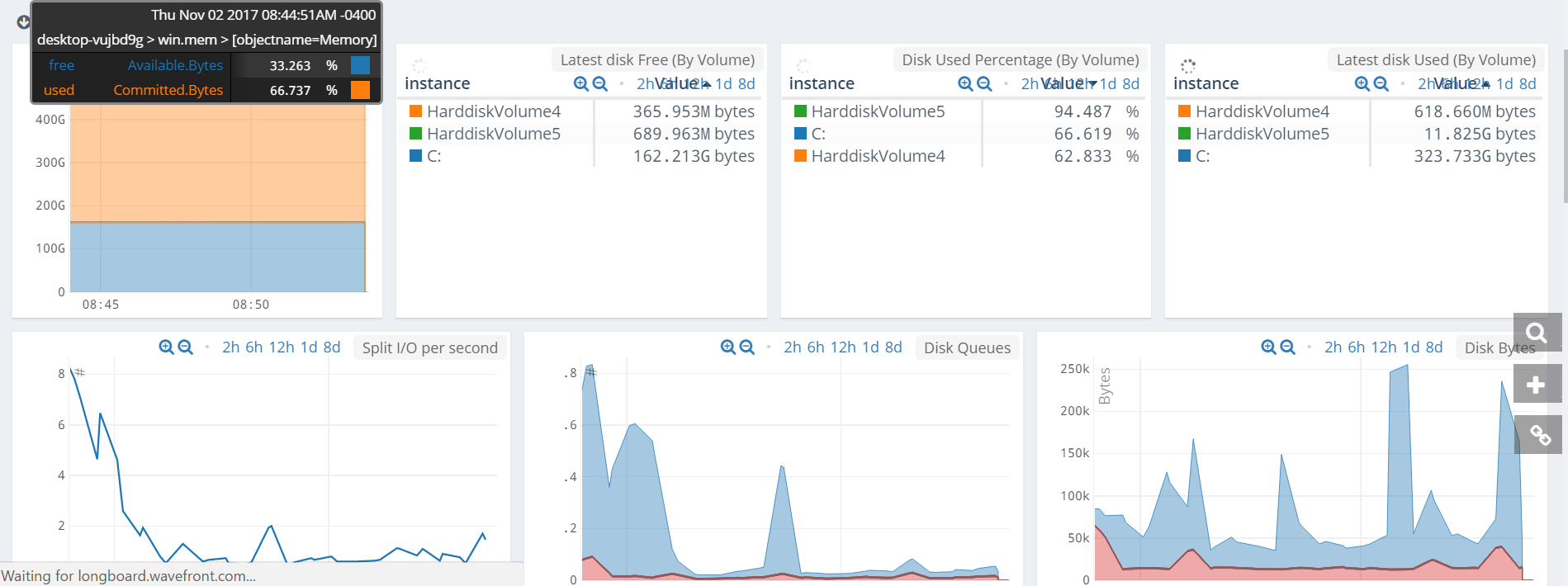
Main dashboard page showing the overview of the entire host.



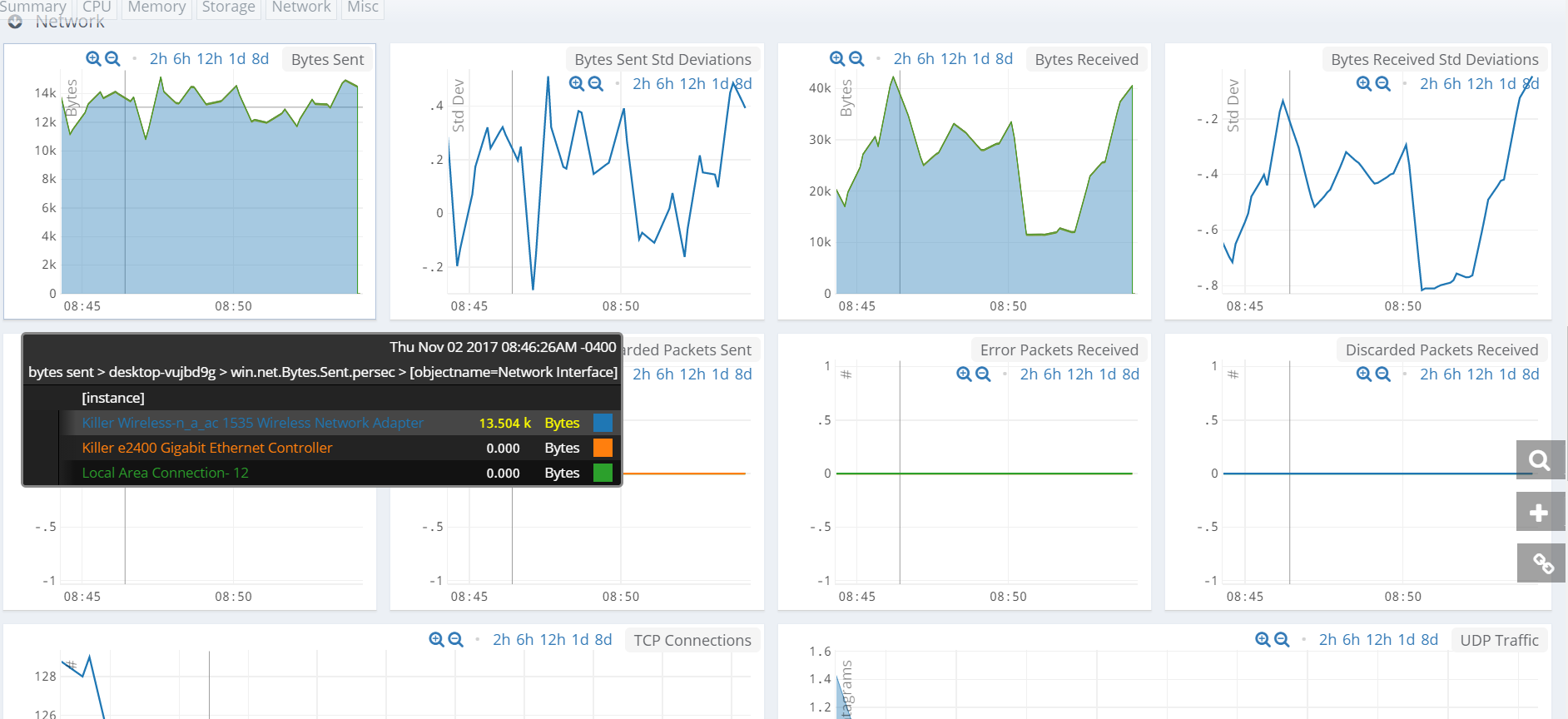
Host CPU Section of the dashboard.



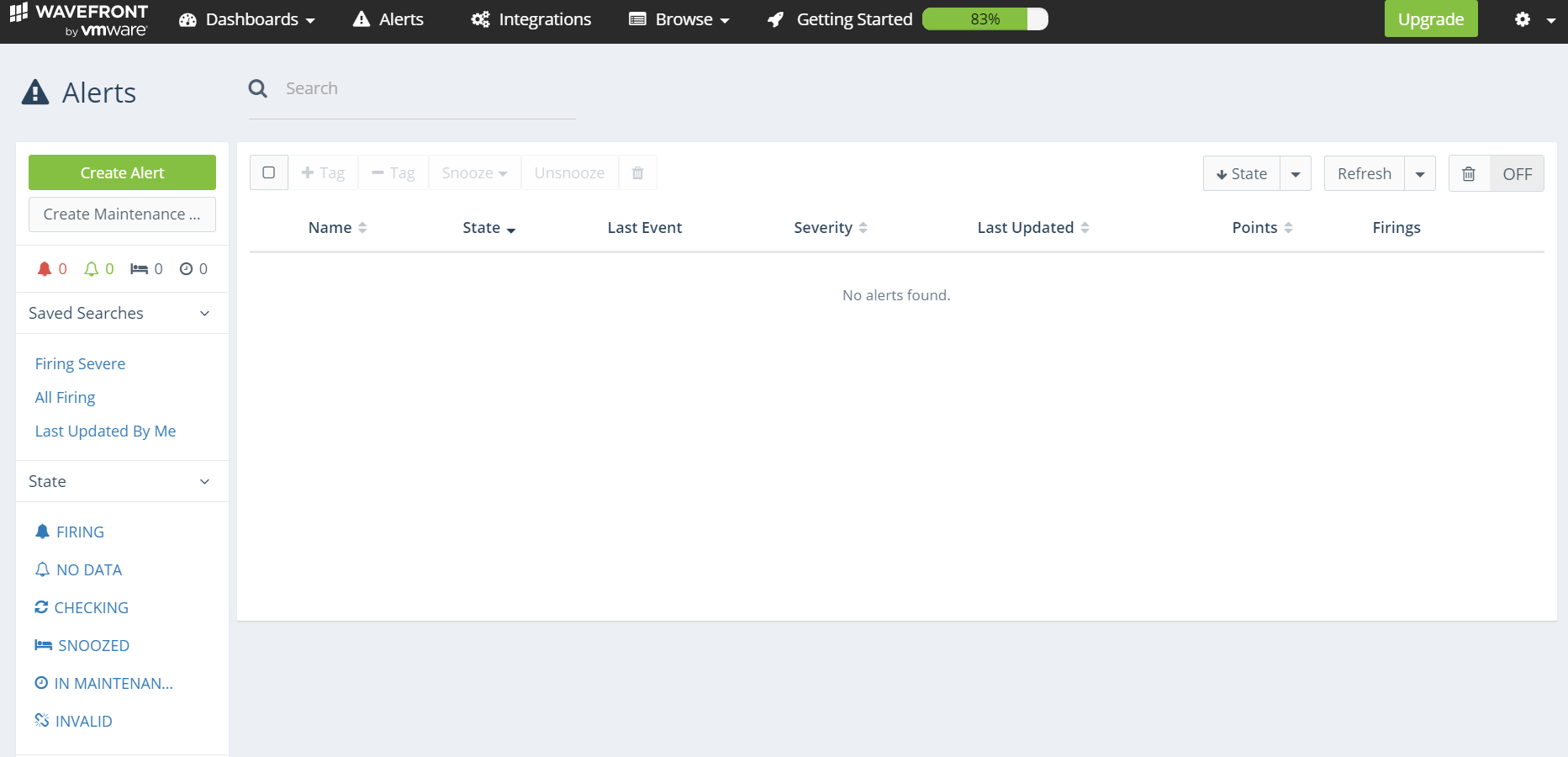
Host Memory section of the dashboard.



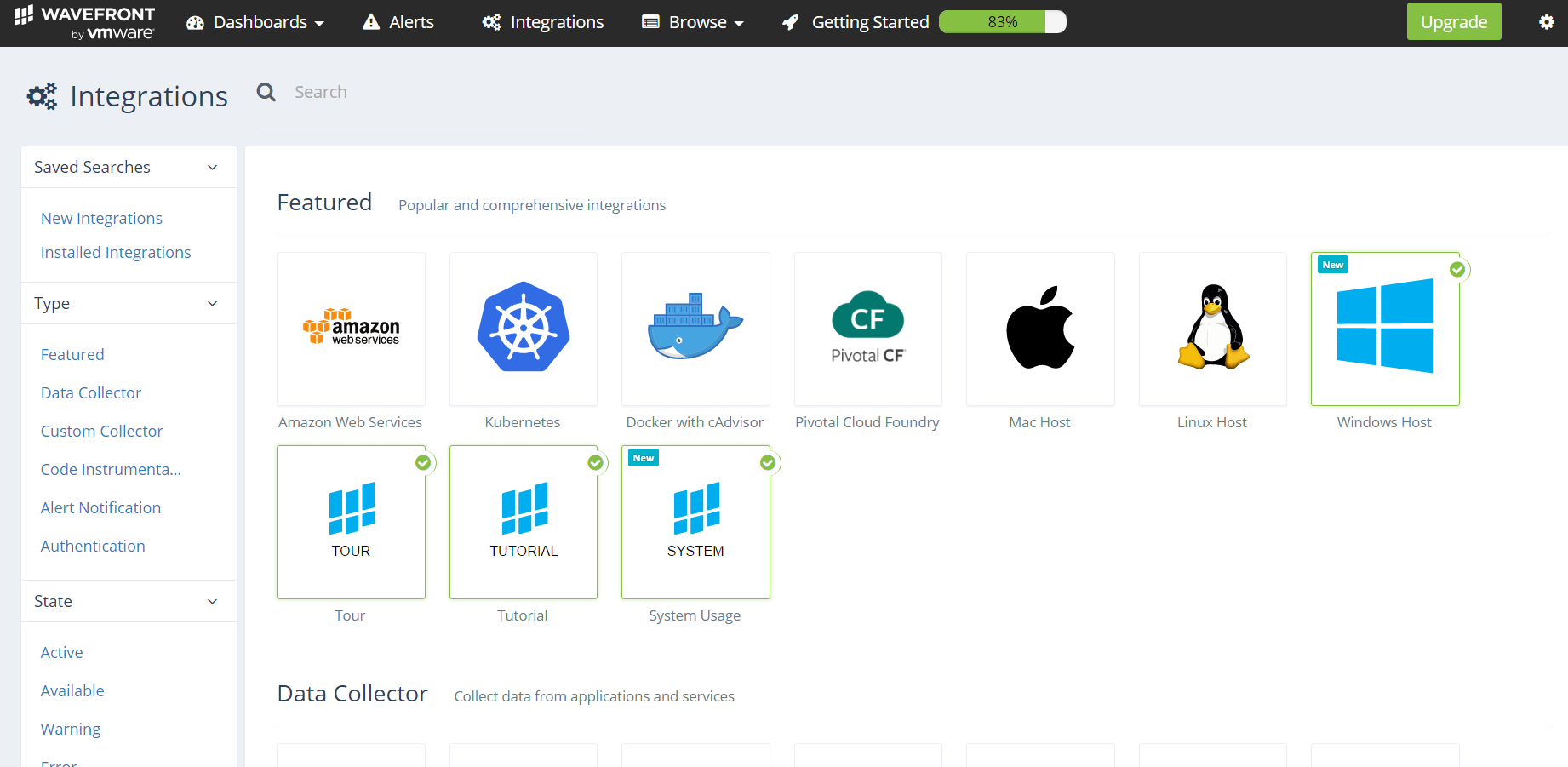
Host Storage portion of the Dashboard.



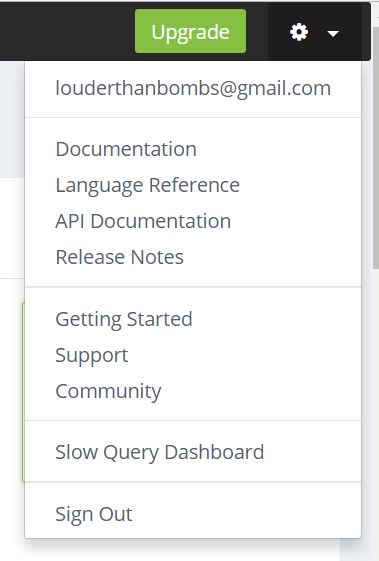
Network section of the Dashboard.



The alert options under “Alerts” tab.



Adding or removing integrations. Notice that Wavefront supports Linux, PCF, AWS, and Mac host in addition to Windows Host.



Account options tab.

**Comparison chart and final thoughts:**

|  |  |  |
| --- | --- | --- |
| **Feature** | **Nagios XI** | **Wavefront** |
| **Add and remove devices** | **Yes** | **Yes** |
| **Multi-OS** | **No** | **Yes** |
| **CPU monitoring** | **Yes** | **Yes** |
| **Custom Charts and Graphs** | **Yes** | **Yes** |
| **Uptime analysis** | **Yes** | **No** |
| **Alerts** | **Yes** | **Yes** |
| **Install required** | **Yes (Requires standalone VM)** | **No (SaaS)** |
| **Support** | **Yes** | **Yes** |
| **Graphical GUI** | **Yes** | **Yes** |
| **Cost** | **Standard $1,995**  **Enterprise $3,495** | **Interested parties must call for pricing\*** |

Overall, both Nagios XI and Wavefront are excellent choices for network monitoring. Both provide real-time, comprehensive access to network and device information. Ultimately, I feel that Nagios XI is better suited for enterprise level network infrastructure, given its ability to combine all servers and devices into one large scope, while Wavefront would be better for smaller infrastructure. That’s not to say that Wavefront isn’t capable, it’s GUI just has some limitations in displaying full scope. Also, pricing isn’t readily available for Wavefront (requiring a phone call), while Nagios is upfront about its costs. That is an extremely important factor when capital is constrained to budgets.

Being said, If I was buying monitoring software for enterprise level networks, I would prefer Nagios. However, If I was acquiring for a smaller network infrastructure, I would prefer Wavefront, unclear price points aside.