NETWORKWORLD
FROM IDG

THE CONNECTED ENTERPRISE

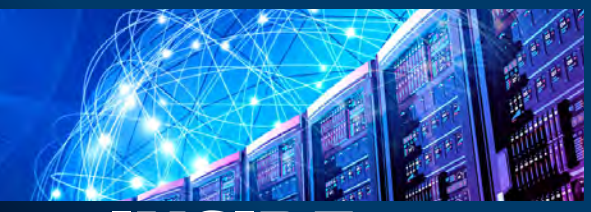
INSIDER EXCLUSIVE

4 REVIEW [FREE] OPEN-SOURCE MONITORING TOOLS

Which is right for you?

NetworkWorld.com

INSIDER EXCLUSIVE




INSIDE

JUST AS WITH COMMERCIAL, for-pay monitoring software, there are open-source options that have varying features, and the goal of an enterprise is to find the best fit for its environment. That's where this downloadable package of reviews can help.

It evaluates four popular free, open-source network-monitoring platforms—Icinga, Nagios, Observium and Zabbix—highlighting pros and cons and giving enough context that this bundle can serve as a guide for IT pros seeking advice.

Editor's NOTE

ICINGA | This open-source monitoring software can determine the availability of hosts and services from switches and routers and find network services such as HTTP, SMTP and SSH. The software runs on most Linux distros and comes with specific instructions for Ubuntu, Debian, Red Hat (including CentOS and Fedora) and SUSE/SLES.

Installation of Icinga Core is straightforward, but the Web install is less so. It offers a number of plugins—literally thousands of them—that check hosts and services, and there are third-party plugins as well.

NAGIOS CORE | Installing Nagios Core requires issuing about 20 commands, which isn't difficult, but a script could make it simpler.

The software has a Web interface that is essentially read-only, so it can't be used for tasks such as adding hosts or configuring alerts. But it does provide an overview of the network to give a sense of problems that can then be investigated more thoroughly via drilldowns.

A wealth of plugins monitor the hosts and services on the network, and the platform provides a network map and some on-screen reporting, but no apparent way to export the reports.

OBSERVIUM | Observium comes in two versions—Community and Pro—with Pro having additional features including automatic grouping, traffic accounting and restful API. Pro also has an optional subscription fee of about $284 per year that includes daily updates.

Observium's script makes installation easier, although manual installation allows for more granular setting of parameters for each component. Its Web-management interface shows a network map for spotting overall issues.

The software can manage a wide variety of devices, and that process can be enhanced with a host agent for Linux and some Unix devices.

ZABBIX | The Zabbix software monitors Linux and Windows environments from a Linux server, and provides detailed online installation instructions for Ubuntu, Red Hat, CentOS, Oracle Linux and Debian in particular, as well as for MySQL or PostgreSQL databases. The Web interface for Zabbix provides widgets for configuring discovery, general system, host status and the like. It supports multiple custom dashboards to break monitoring tasks into groups.

The software monitors hosts and items. A host is a device with its own IP address, and items are individual metrics of a host that an admin might want to monitor. A single host could have several items associated with it, providing the potential for a fine level of granularity. Adding to that granularity is Zabbix's support for monitoring agent JMX, IPMI, SSH, TELNET and all versions of SNMP.

It's possible to test drive Zabbix from a virtual appliance that runs on most virtualization platforms including KVM, Zen, VMware, VirtualBox, Hyper-V and Azure. ◆

SUSAN PERSHCKE *is a web and database developer with 15+ years of industry experience. You can reach her at susan@arcseven.com.*

Icinga

Enterprise-grade software that scales. **BY SUSAN PERSHCKE**

CONTINUING OUR QUEST for robust, enterprise-grade open-source network monitoring, we tested Icinga Core 2 (version 2.8.1) and the stand-alone Icinga Web 2 interface. Created in 2009 as a fork of the Nagios network monitoring tool, Icinga has come a long way.

We found Icinga to be a powerful monitoring tool with many great features. The Icinga Core install is straightforward, and basic monitoring is easy with either pre-configured templates or plugins. However, we discovered that the Web install is a bit more complicated and could stand to be streamlined.

Icinga runs on most of the popular Linux distros and the vendor provides detailed installation instructions for Ubuntu, Debian, Red Hat (including CentOS and Fedora) and SUSE/SLES. Icinga does not publish specific hardware requirements, but our installation ran well on a quad-core processor with 4 GB RAM, and this is probably a good starting point for a basic installation.

As with most monitoring applications, storage is an important variable that largely depends on the number of hosts and services monitored and how often information is written to the log. With too little storage, the logs can easily fill up and freeze the system.

We were able to quickly install Icinga on Ubuntu 16.04 LTS with just a few simple commands at the prompt. The first step was to download the necessary files to the local repository, and then install the actual Icinga application. Icinga can be used to monitor the availability of hosts and services from switches and routers as well as a variety of network services like HTTP, SMTP and SSH.

To comment on this story, visit Network World's Facebook page.

Plugins

One of Icinga's strengths is the availability of plugins that can be used for most monitoring tasks, and as part of the installation you need to install the basic monitoring plugins to check external services. There are literally thousands of plugins available, both directly from the Icinga Exchange and from third parties. For third-party plugins from unknown sources, it is a good security practice to examine the source code and compile it yourself or stick to known and trusted plugin authors.

MAXIPHOTO / GETTY IMAGES

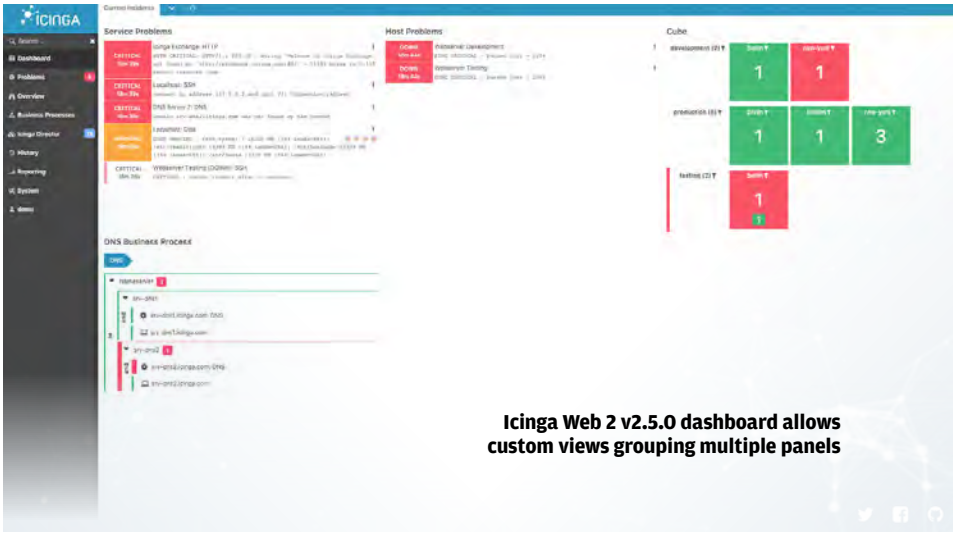
Granular monitoring capabilities

Icinga provides impressive granularity as to how hosts and services are monitored. For instance, you can create what Icinga calls a host object, which is essentially a rule or task, to monitor a server. For each server you can define what services to check, from a simple ping command to make sure the server is on and responding or checking to see if the HTTP or FTP services are running. Icinga provides flexibility in how often to check, with various warning levels defining how and who to alert when something needs attention.

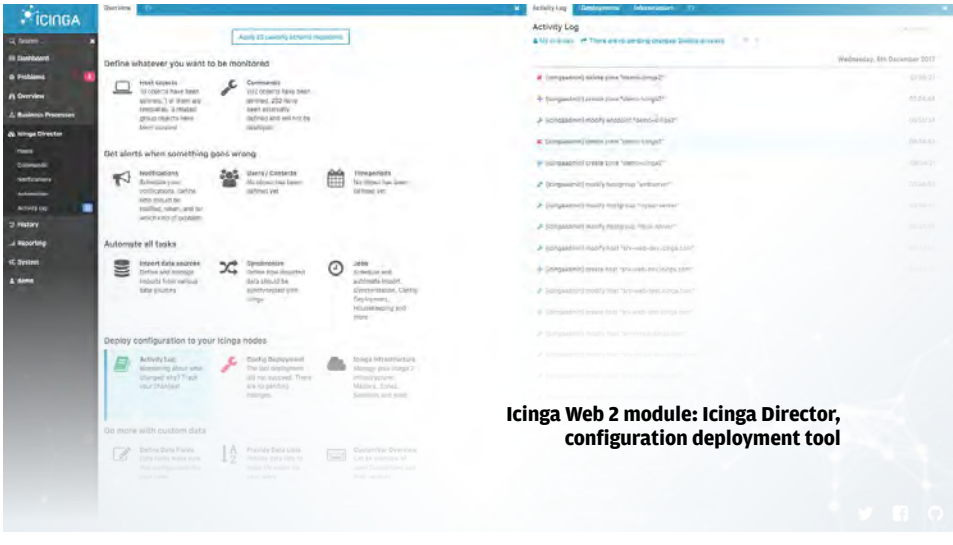
Icinga uses a series of configuration files to store information about how the infrastructure is monitored. In addition to the 10-plus default files, you can create your own custom files and include these as part of the overall Icinga configuration. While this approach might be a bit overwhelming for first-time users, we found that the concepts are fairly easy to grasp once you spend some time with the various files. Icinga provides templates that cover most scenarios, making it easier to customize its use in your environment.

Icinga utilizes different monitoring methods; the most common is the use of a pre-built or custom service-monitoring plugin. With the abundance of available plugins, you may never need to build your own, but Icinga provides instructions on how to accomplish this, if desired.

Plugins are available for monitoring hosts and services like Linux, Windows, databases, SMTP, Web services, hardware, mail servers and third-party applications like VMware and SAP. In cases where remote access may not be available, Icinga offers agent-based monitoring. One common method is an SNMP daemon



Icinga Web 2 v2.5.0 dashboard allows custom views grouping multiple panels



Icinga Web 2 module: Icinga Director, configuration deployment tool

that runs on the remote system. For those needing solid Windows support, Icinga can utilize the NSClient++ to run local scripts which provide detailed system information.

Configuration

If you need to make changes on a regular basis, Icinga may become a bit time-consuming to configure and manage from the command prompt. Conveniently, there are several Web interfaces that can be used, and we chose Icinga Web 2. This is a standalone application that communicates with Icinga Core. While the Icinga Core installation was very straightforward and literally took less than 10 minutes, we found the Web application to be a bit kludgy and took more than 30 minutes.

In order to use Icinga Web, we first needed to install a database. Our options were PostgreSQL or MySQL, and we opted for the latter. Then we had to run through a series of additional commands and screen prompts to download, install and configure a variety of options, including the Apache Web server and PHP.

The last step was to create a token needed to launch the Icinga Web interface. With our newly minted token in hand, we finally were able to start our browser and were presented with a Web wizard. Although the wizard was easy to use, we found it to be too complex (more than 10 steps) and required us to go back to the prompt several times, once to set the time zone for the PHP configuration file and at least once to change database settings.

With installation and initial configuration complete, we were finally able to launch the Icinga Web interface. The initial screen you see is the 'dashboard,' which displays an overview of the infrastructure with any service and host-related warnings and errors listed.

In addition to the dashboard summary overview, Icinga provides multiple ways to sort and display infrastructure data. Data can be displayed by hosts, services and groups, with the ability to drill down to view details about a specific issue.

When viewing details about an error, you have the option to perform different tasks such as acknowledge the error, perform an immediate re-check, add notes, send custom notifications or schedule downtime or future re-checks.

While Icinga Web is both easy and fast to use, we wanted a way to create, edit or delete monitoring rules from the interface, finding that most of these tasks need to be completed using the configuration files. Icinga says there are tools in development for this, but none is currently available.

Reporting

Basic on-screen reporting is serviceable in Icinga Web, but for more robust reporting, it's best to use Icinga's separate reporting module. This works with JasperReports Server to provide powerful reporting capabilities. There are also additional reporting and graphing add-ons such as Graphite and PNP, as well as log tools like GrayLog and LogStash.

Icinga provides a comprehensive online user manual that is well-organized, easy to navigate by topic or searchable by keyword. For larger installations, Icinga provides the option of setting up a distributed monitoring environment, including high-availability clustering.

Icinga offers commercial support at four different levels, bronze, silver, gold and platinum. There is no published online pricing for it. ◆

PROS

Easy to install Core, solid documentations for multiple Linux distros, thousands of available pre-configured plugins, scales well

CONS

The Icinga Web 2 install is cumbersome with too many steps, offers no way to create and manage rules from Web interface

INSIDER EXCLUSIVE

Nagios Core

A wealth of plugins and a steep learning curve.

BY SUSAN PERSHCKE

THE FREE AND OPEN-SOURCE network-monitoring software Nagios Core has a long and strong reputation, providing the base for other monitoring suites—Icinga, Naemon and OP5 among them—and a history dating back to 2002 when it launched under the name NetSaint.

For this review we tested Nagios Core version 4.4.2 for Linux, which monitors common network services such as HTTP, SMTP, POP3, NNTP and PING.

There's a Windows port that's a plugin, but many users say it's unstable. The version we tested also tracks the usage of host resources such as processor load, memory and disk utilization.

To comment on this story, visit Network World's Facebook page.

Hardware requirements vary depending on the number and types of items being monitored, but generally speaking Nagios recommends a server configuration with two or four cores, 4-8 GB of RAM and adequate storage for the intended application.

Installation

Nagios provides a PDF with step-by-step installation instructions and although the instructions were not updated for the latest version, we were able to apply the installation commands to the version we tested. The only prerequisite is to first install Apache/PHP, and the instructions provided a simple command for this task.

After downloading the Nagios Core and Plugins tarballs, we created a Nagios user and user group before continuing the installation. The installation itself is not particularly complicated but requires issuing about 20 different commands plus manually updating a configuration file. In our view, this could have been greatly simplified by providing a script or an executable.

Web interface

With the install and basic configuration completed, we proceeded to launch the Web interface. On our initial login, we were presented with a dashboard overview with a naviga-

PETROVICH9 / GETTY IMAGES

tion menu to the left and a main screen on the right. We were notified that our version, 4.4.1, was out of date and that we should upgrade to 4.4.2, which we did using steps found in the user manual.

The home screen contains links to quick-start guides, videos, plugins and other resources. Newbies will find this helpful when starting a new installation. It should be noted that the Web interface is essentially read-only, as there is no mechanism for performing tasks like adding hosts or configuring alerts.

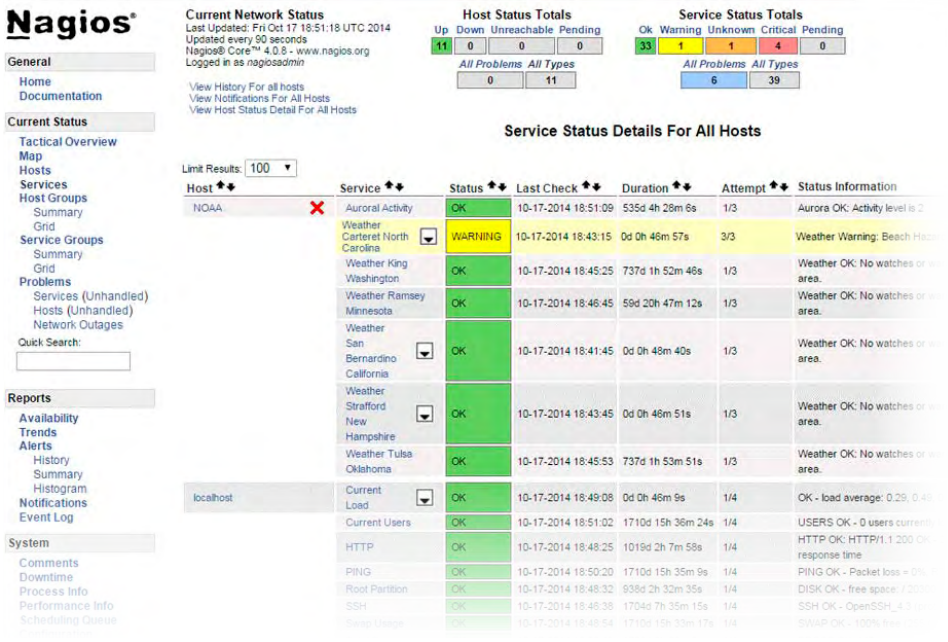
The Web interface provides a big-picture, tactical-overview status screen that allows administrators to identify problems at a glance. From there, you can drill down to view details about a specific problem and take certain alert actions like acknowledging the error message and scheduling downtime.

Overall, the Web interface is easy to navigate, but feels a bit dated and could benefit from more modern and larger fonts along with some updated graphics. However, as with most things Nagios, there are downloadable third-party-themed plugins available that allow you to apply a different look and feel.

The infrastructure is generally organized with hosts and services in mind, allowing administrators to view the infrastructure from both a host and/or a service perspective. Both hosts and services can be organized into groups, which makes it easier to manage larger network infrastructures.

Configuration

Nagios is principally configured using a number of configuration files, the main ones being the log, services, hosts and commands files.



Nagios provides comprehensive monitoring of mission-critical infrastructure components.

Each file has examples of how to configure the various parameters, and the user manual has additional configuration details. While this approach certainly has its supporters, we would have liked to see some of these configuration abilities added to the Web user interface. This would be particularly helpful when monitoring larger and heterogeneous infrastructures.

Many public services such as HTTP, FTP and SMTP can be monitored without deploying an agent to the host or relying on SNMP, but other services such as CPU and memory usage, information about system users, service state and running processes require an agent to be installed on the host. There are agents available for most hosts such as Windows servers, Linux/Unix servers, printers, routers and switches. In addition to installing the agent you will need to update various configuration files in order to start monitoring.

Lots of plugins

The Nagios Exchange website offers a large selection of plugins for various monitoring/management scenarios. In fact, one of the strengths of Nagios is the availability of an impressive number of plugins which are compiled executables or scripts that check the status of a host or service. Nagios uses the information from plugins to determine the current status of hosts and services on your network. The plugins act as an abstraction layer between the monitoring logic present in the Nagios daemon and the actual services and hosts that are being monitored. The upside of this architecture is that you can monitor just about anything you can think

of. The downside is that Nagios has no idea what is being monitored. Its job is to track changes in the state of what is being monitored. Only the plugins themselves know exactly what they're monitoring and how to perform the actual checks.

The Nagios Exchange currently has almost 6,000 projects in over 400 different categories. While the majority of the projects are plugins, there is also a solid collection of documentation items, extensions and other add-ons. After a quick review of the available add-ons, we're pretty confident there is a plugin available for what most administrators will ever need, although the source code for these should be properly vetted prior to use.

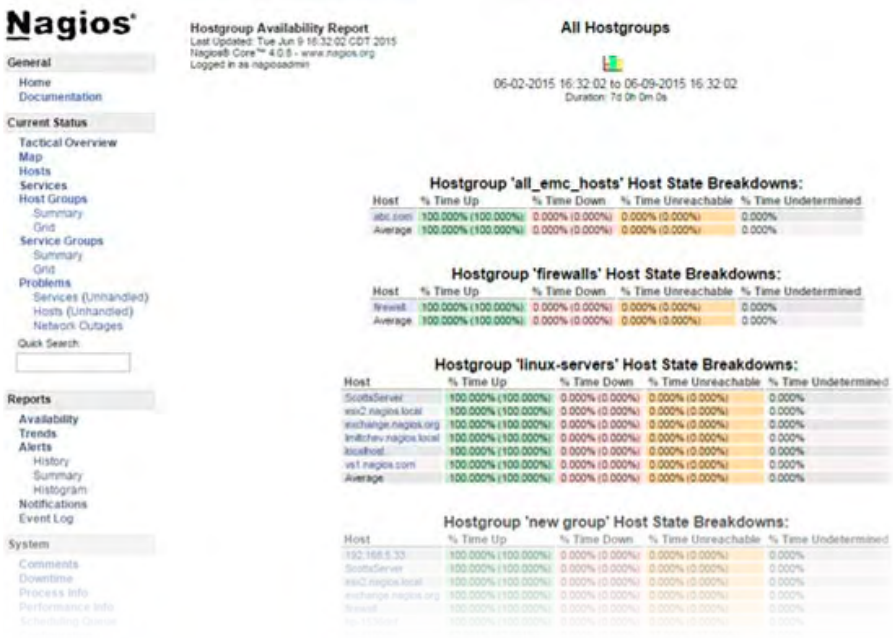
In addition to the Web monitoring features, Nagios includes a network map and some on-screen reporting capabilities. These include service and host summaries as well as alert history and the event log. One minor but smart feature is the ability to add comments related to hosts and services. Notification alerts can be delivered via email or SMS, and there is a system for notification escalation where individuals and groups can be notified based on the severity of a problem. We did not, however, find a way to export any of the on-screen reports to PDF or any other format.

Documentation and support

Nagios provides a useful online HTML user manual, which we found to be well-organized and easy to navigate. Nagios also has an online support forum and an online library for those who require support beyond what the user manual provides.

Nagios offers support for all of its products, including Core. However, some organizations may opt to go with Nagios XI, a commercial version of Nagios that offers quite a few additional features over the Core Edition. The cost of Nagios XI starts at $1,995 and includes email support for the first 12 months. An annual support plan for Nagios Core costs $2,495, which includes up to 10 annual support tickets with next-business-day response.

Although Nagios continues to support its free and open-source Core version, it is clear they would prefer you buy the commercial version. This is a common approach, and for some organizations that seek greater accountability and service response times, the commercial version might be preferable. It includes many of the missing features noted here, including the ability to configure from the Web interface using wizards, advanced reporting and customizable dashboards. However, for those who are willing to put in a bit of effort, we think the Core version is more than adequate for many tasks. It has a plugin for pretty much every scenario, good documentation and since it is available free and open source, the price is certainly right. ◆



Reporting ensures SLAs are being met and provide a historical record of critical information.

PROS
Lots of available plugins, good online documentation

CONS
Installation has too many steps; Web interface is a bit dated, lacks configurability; custom configuration can take a while to learn

Observium

Doesn't run on Windows but has a great user interface.

BY SUSAN PERSHCKE

OPEN-SOURCE network-monitoring tools continue to gain in popularity, and Observium came up on our radar as an enterprise-grade offering. Deployed worldwide by large organizations like eBay, PayPal, Twitter and the US Department of Energy, Observium is capable of handling tens of thousands of devices. The client list is impressive, but our test reveals what's really under the hood.

Observium runs on Linux but can monitor Windows and many other device types. The vendor recommends running Observium on Ubuntu/Debian, but it will also work on distros such as Red Hat/CentOS.

Since Apache and MySQL are prerequisites for Observium, your server needs to meet the hardware requirements to run them. In our test, a quad-core processor with 2GB of RAM and adequate storage provided enough horsepower to run our medium-size test environment.

Observium is currently in version 17.9 and available both in a Community and Professional edition. The Pro version is available as an annual subscription for about $284 per year and receives real-time daily updates, whereas updates to the Community version are available for download about every six months. The subscription license is valid for a single production installation and two testing or development installations. There is no difference between the two versions as to capacity and capabilities, but the Pro version has a few additional features—automatic grouping, traffic accounting and restful API.

To comment on this story, visit Network World's Facebook page.

Installing Observium

Observium can be installed in manual mode or by using an automated script. The manual mode is a more granular approach, which requires downloading and installing each component (Apache, MySQL etc.) separately. We used the automated script, which provides the option of installing the Community Edition or the Pro Edition. We opted for Community and the installation wizard presented a very short prompt sequence where we were asked to create both a MySQL and an Observium user. The install downloads the needed files on the fly, and at the end you have an option to create an Observium agent on the server, which we opted to do. The whole process took about 15 minutes. While the installation is

PIKEPICTURE / GETTY IMAGES

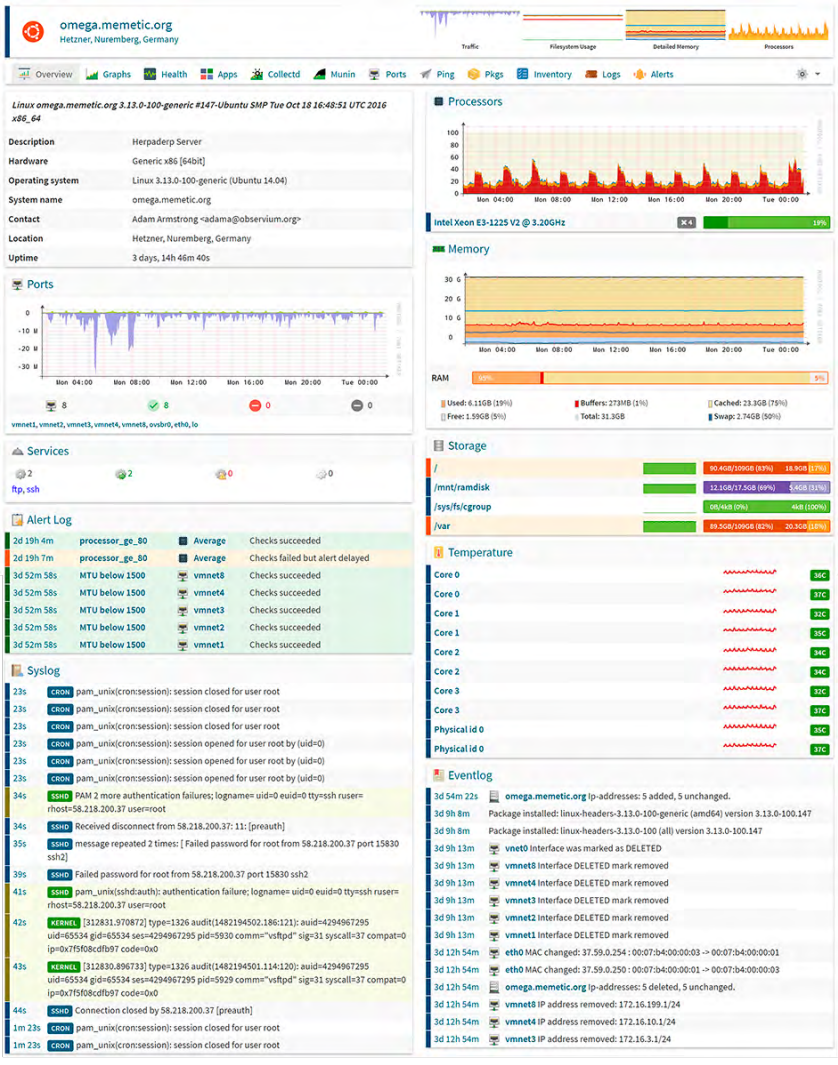
easy to complete, we would have also liked to see an appliance version that could be run as a virtual machine for testing purposes.

After completing the install, it was time to launch the Web management interface. This is accessed using the IP address of the server and upon successful login we were presented with an overview screen, dominated by a map and a list of recent events as reported by devices. The map is helpful when monitoring geographically dispersed devices.

Adding devices for Observium to monitor

With the server up and running and the basic configuration in place, we added more devices. Observium can connect to pretty much any networked device that supports any version of the SNMP protocol (v1, v2c and v3). Currently over 400 OS types are supported, including servers, storage and wireless devices, and network infrastructure. We started with a small collection Linux and Windows devices, which were easily added using a combination of CLI scripts or the Web interface. In addition to using SNMP, Observium also provides an agent that can be deployed on Linux devices as well as some UNIX devices, but not Windows. There are also ways to gather data using a few other methods such as syslog, rancid and collectd. These require additional configurations both within Observium and on the devices themselves. Observium also has an auto-discovery feature that, when launched, probes the network for devices configured to use any preset SNMP community.

Once the devices have been added, Observium starts polling information. On the overview page, you can easily view the number of devices



Observium: Linux device details

and the status of each, whether up, down, disabled etc. Observium makes it easy to perform a quick device health check or a conduct a more thorough, deep-dive into details for each device. Observium makes extensive use of graphs to display a host of parameters, ranging from memory utilization and CPU loads to network traffic and the number of users logged into each device. In the past we've experienced issues with the graphs being slow to load, but using PHP 7.0 as recommended seemed to resolve most of them.

With six different user levels, we found Observium to have more than adequate flexibility, allowing users to view device information and perform configuration tasks. For instance, a normal user account can be configured to have just a read-only view of data from a preset group of devices, whereas the administra-

tor account can have access to both viewing all data and performing all configuration tasks such as editing devices and setting alerts.

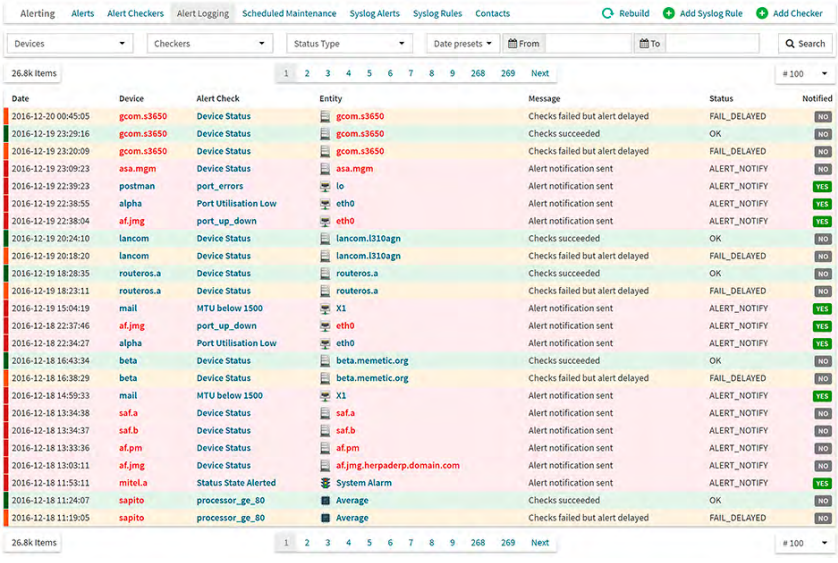
Creating alerts in Observium

Observium does not have any predefined alerts per se, but the user manual provides examples of how to build a variety of common alerts. For instance, by using the examples, we were able to quickly create an alert to warn us if the disk space exceeded 85% of capacity. Another alert notified us if the processor utilization went over 80%. We found the process to create alerts to be very intuitive and offered enough granularity to either create a network-wide rule or one that only applies to a certain set of devices, such as all Linux servers.

The online user manual is very good and provides enough detail for completing most tasks without getting too deep into the weeds. There is a comprehensive reference guide with a large number of metrics and attributes that can be used to build rules. Our only complaint is that it would be nice to have a downloadable PDF version of the user manual.

Observium provides support at a rate of about $284 for a two-hour minimum, with the ability to purchase larger blocks of time at a discount. Paid installation support is available along with the option to have custom features created.

Since our last review of Observium in 2015, we note it has matured quite a bit. One of our main complaints then was its inability to add devices by IP address. This has been corrected and makes life a whole lot easier for administrators who live by IPs as much as host names. There is still no way to export reports and data from the Web interface, but the on-screen reporting is very good. As the name indicates, Observium is an observational tool and a good one at that. It has an easy-to-use interface that allows for both quick at-a-glance overviews with the ability to drill down for more detail. Although we were not able to test with tens of thousands of devices, Observium scales well with only modest hardware requirements, although we note there is no built-in clustering capability. ◆



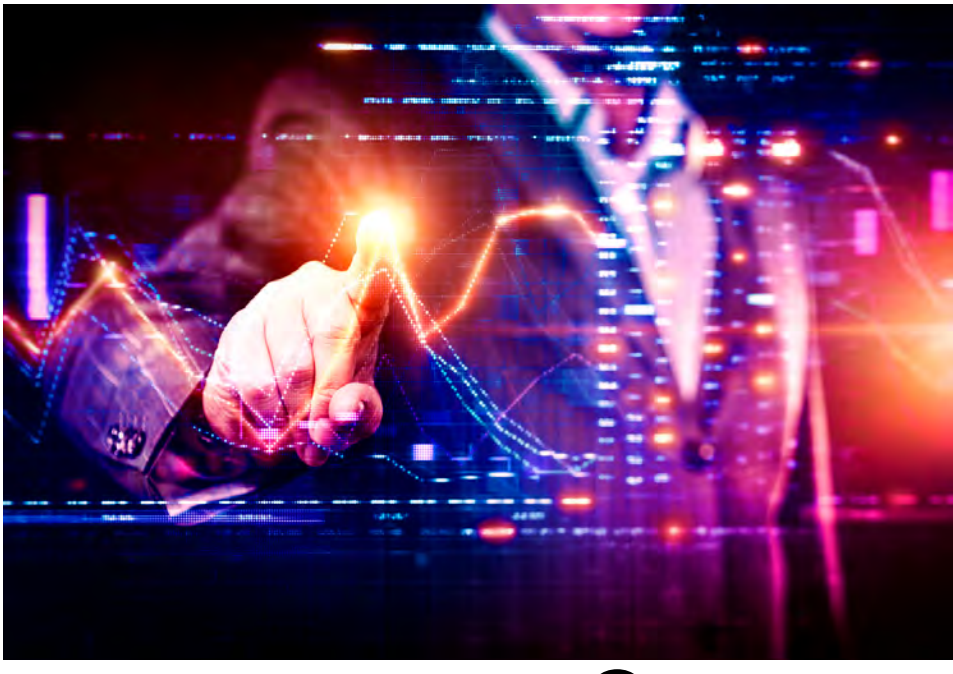
Observium: Alert logging

PROS

Easy to install and use with a great interface layout, low cost

CONS

Relies mostly on SNMP protocol monitoring, does not run on Windows, has no data export or clustering capability



Zabbix

A granular tool that requires lots of manual configuration. **BY SUSAN PERSHCKE**

WE TOOK A LOOK at open-source Zabbix network-monitoring software version 3.4.9 and found it to be a solid, straightforward offering that's easy to install, provides the configurability and granularity that enterprises demand and delivers fast discovery.

On the other hand, some customers might prefer less manual configuration and more pre-set options, and Zabbix is limited in the types of reports that can be exported.

To comment on this story, visit Network World's Facebook page.

Zabbix, which claims a user base of more than 300,000 installations, can monitor both Linux and Windows environments, but the Zabbix software itself runs only on Linux.

If you want to test drive Zabbix without committing to the entire installation and configuration process, Zabbix offers a pre-configured appliance for most popular virtualization platforms, including KVM, Zen, VMware, VirtualBox, Hyper-V, and Azure.

Installation

Zabbix provides an interactive online form that creates the proper installation steps based on your choice of Linux distribution (Ubuntu, Red Hat, CentOS, Oracle Linux and Debian) and database (MySQL or PostgreSQL). We selected Ubuntu and MySQL and then followed the installation steps: download and install the server software, install and configure the MySQL database, install the PHP frontend.

After completing these steps, which took less than 15 minutes, we launched the Zabbix Web interface from our browser. With proper configuration, the Web interface can be viewed in most browsers and from any location. Once logged in, we were presented with a ready-to-configure dashboard, consisting of a collection of default widgets for items like discovery, problem notification, general system and host status.

You can customize the dashboard by adding and removing widgets as needed. You can also drag and drop, resize, remove and rename widgets to suit your environment. We found the dashboard functionality to be very flexible, enabling us to quickly create multiple custom dashboards and easily switch between them.

Hosts and items

Zabbix network monitoring centers around hosts and items. To get started, we added a mix of Linux and

DA-KUK / GETTYIMAGES

Windows servers. You only need a name and IP address to add a new host. We customized each by adding items, which are single metrics you wish to monitor—anything from CPU load and memory usage to Web page load time and database status.

You can create multiple items for each host, which provides impressive granularity. With our mix of hosts and a few monitoring items applied for each, we then added triggers that would alert us to any problems. Triggers can be set with thresholds for notification, ranging from informational to hair-on-fire emergencies. Triggers display on the dashboard and can also be configured to send emails, SMS or IM messages when there is a problem.

Zabbix also allows custom scripts to be run when certain criteria are met. Based on the type of host you create, Zabbix can apply either pre-defined or custom templates. Templates that use pre-configured items and triggers speed up the configuration process. For our Zabbix main server, more than 80 items and 50 triggers were automatically added when we applied two built-in templates.

Zabbix has a discovery feature which uses an IP range to scan the network for assets matching a set of criteria. For example, you can search for items running only SNMP or items with the Zabbix agent installed. A broader discovery rule allows you to ping every IP address within a range to locate hosts. We entered the subnet for one of our networks and Zabbix located all nodes (about 50) on the network in less than 10 minutes.

Granularity

While very basic monitoring can be accomplished using just a simple ICMP_PING, Zabbix supports more granular monitoring with agents like

Zabbix provides users with several built-in simple graphing functions, along with the ability to create more complex, customized graphs.

Zabbix web monitoring checks performance and availability of multiple web resources and generates graphs, alerts and notifications.

JMX, IPMI, SSH, TELNET, all versions of SNMP and other external checks, such as database monitors. Zabbix also has its own agent, available for most common Linux/UNIX distros and Windows. The Zabbix agent runs as a daemon process on Linux and as a service on Windows.

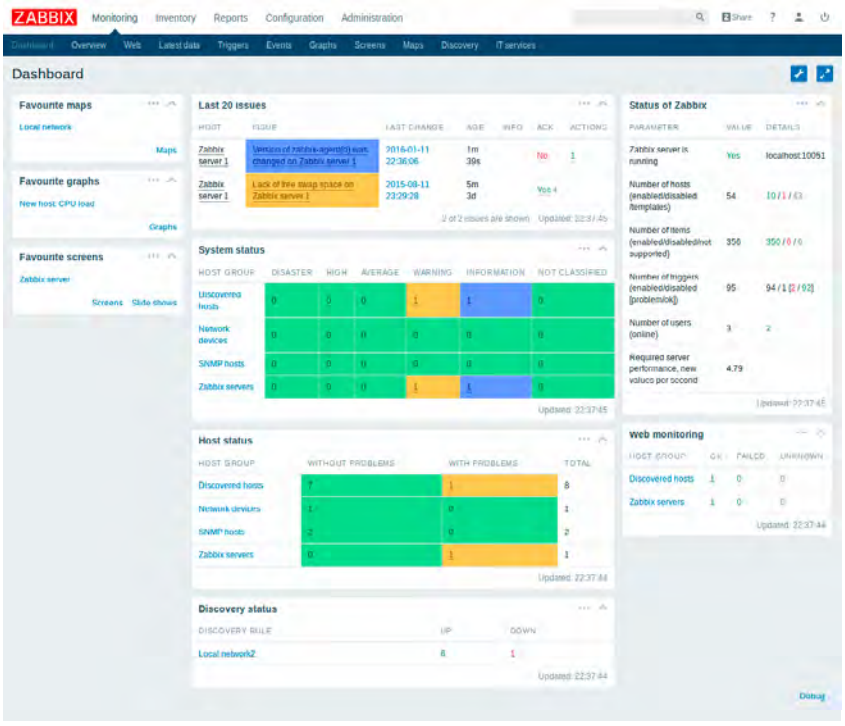
The Zabbix agent can be configured for either passive or active checks. Passive checks respond to server requests whereas active checks gather information and send it to the Zabbix server at preset intervals. Agents are set up using a configuration file with a sample provided to get you started. Our Zabbix test server already had the agent installed, and we installed the agent on one of our Windows servers. We found the agent footprint to be pretty small on both platforms, using less than 10 MB in our test case.

Zabbix on-screen reporting is very solid, and you can view your infrastructure from pretty much any conceivable angle, using dashboards, graphs, summaries and maps, all customizable to accommodate most scenarios. However, Zabbix comes up a bit short when it comes to export capabilities. Some items can be exported to CSV, but it would be helpful to also have some PDF export options for documentation or submitting reports to management.

Zabbix provides a comprehensive online manual, available for recent versions of the software, in multiple languages, with the ability to export to PDF or ODT for offline use.

The software is free, but Zabbix asks that those using it commercially for profit purchase some level of support to further development of platform. There is a basic plan (four instances, up to two days for a response) or an enterprise plan (unlimited instances, 24/7 support and four-hour guaranteed response). Support pricing depends on the number of servers and the complexity of the network.

While phone support is available, Zabbix manages most support issues through the Zabbix Support System, an online support-management portal.



Zabbix Dashboard provides details about the monitored environment. The dashboard can be filtered by host group, trigger severity, problem status and other parameters. Users can customize the dashboard, reallocate widgets with drag-and-drop, add and remove favorites.

PROS

Easy to install, fast discovery, custom dashboards, excellent granularity

CONS

Some rules complicated to configure, export reporting features limited to CSV, no Windows server version available

Zabbix has a cloud version in the works, but it was not available at the time of the review. It will be hosted by Zabbix at 16 data centers worldwide and is expected to provide access to the latest software, up and down scalability and secure backups, and it will eliminate the need for hardware.

At its core, Zabbix is very straightforward to install and operate with basic configurations. However, when getting into some of the details, it was easy to get a bit lost in the configuration jungle. When setting up a host, only a few fields are mandatory, but there are multiple sub-tabs with literally hundreds of available fields. We appreciate the granularity, but it might make sense to have pre-built basic, intermediate and advanced configuration choices for some of the features.

Minor complaints notwithstanding, we found Zabbix to be a solid enterprise-grade monitoring platform. ◆