

Enigma NMS from NETSAS



PRODUCT REVIEW PRODUCT REVIEW PRODUCT

Enigma NMS brings a refreshingly new approach to monitoring enterprise networks because it scales easily to thousands of devices. However, it doesn't come with the high price tag normally associated with such solutions. Other key differentiators include a pricing per device model and not per monitored interface; also, all available features are provided within the core product, thus avoiding the costs and complexity of the modular alternatives.

Enigma NMS runs on CentOS so it can be deployed as a physical or virtual appliance, with high availability, if that is required. For lab testing we chose the former and used a dual Xeon 5500 rack server for our hardware platform. Installation starts with CentOS and we were impressed with the documentation which provides clear instructions for the entire process. Loading Enigma NMS on top of the base OS only takes a few minutes and then it's over to the intuitive web interface.

Automated network discovery can be fine-tuned with details of subnets to be scanned or excluded and SNMP community strings. We found the discovery process was lightning fast as Enigma NMS spotted all our Windows servers, workstations, printers, switches and routers in only a few seconds. Enigma NMS discovers MAC addresses so it can spot just about anything connected to the network such as iPhones, PCs and so on. It stores details of all discovered devices for a minimum of four weeks so it's easy enough to

check back to see if any unauthorised devices have been used.

The discovery works out logical network configurations allowing it to provide a greater visibility into the network's inner workings. It can pick up high level information such as QoS classes and policies, VLANs across VTP and MSTP domains, IP routing information, and even MPLS Traffic Engineering tunnels.

Its polling engine keeps track of all the monitored devices and polls the network every minute. It can store details on over 200,000 interfaces for up to one year without rolling over. For system monitoring, you can keep a close eye on details such as CPU, memory, network interfaces and hard disks and if required, tie these in with thresholds linked to an extensive alerting system.

A dashboard provides a complete overview of monitored devices which includes system and interface performance graphs. It can be easily customised with a wide range of filters and the polling engine will alert you if devices aren't responding. If a critical device such as a switch fails to respond, you can use dependencies to stop alert floods occurring for associated systems.

For server monitoring, Enigma NMS is capable of providing a wealth of information. For our Windows test servers, we could see CPU and memory utilisation, file systems, installed software and running processes

along with free and used hard disk space.

Most thresholds are configured out of the box with typical values and this feature speeds up deployment immensely. As a result, Enigma NMS can start reporting on device status immediately and with minimal intervention. The portal can also be branded with company logos, making Enigma NMS highly suited to service providers.

It has a sharp focus on WAN and MAN services with its Carriage Management and Billing feature. Administrators understand how easily costs for these can spiral out of control and Enigma NMS monitors all connections, ranging from ADSL to fibre MANs. It links these with bandwidth availability and tariff objects allowing it to determine whether SLAs are being maintained and reporting swiftly on outages.

Enigma NMS provides total visibility on enterprise networks. It allows support staff to quickly identify, analyse and remedy incidents as they occur. Its swift deployment, centralised management and very affordable price structure adds up and it comes highly recommended. **NC**

Product: Enigma NMS
Supplier: NETSAS Pty Ltd
Sales: sales@netsas.com.au
Web site: netsas.com.au