EPS Monitoring System

A crucial part of every System Administrator's job is to have a monitoring system able to provide exactly the state of the system, with features such as getting timely alerts of any server problems (software and hardware), getting servers performance data, and obtaining a detailed inventory of hardware and software.

Even though all of these requirements might be fulfilled by other tools, 'EPS MS' provides a complete and extremely easy to configure full solution.

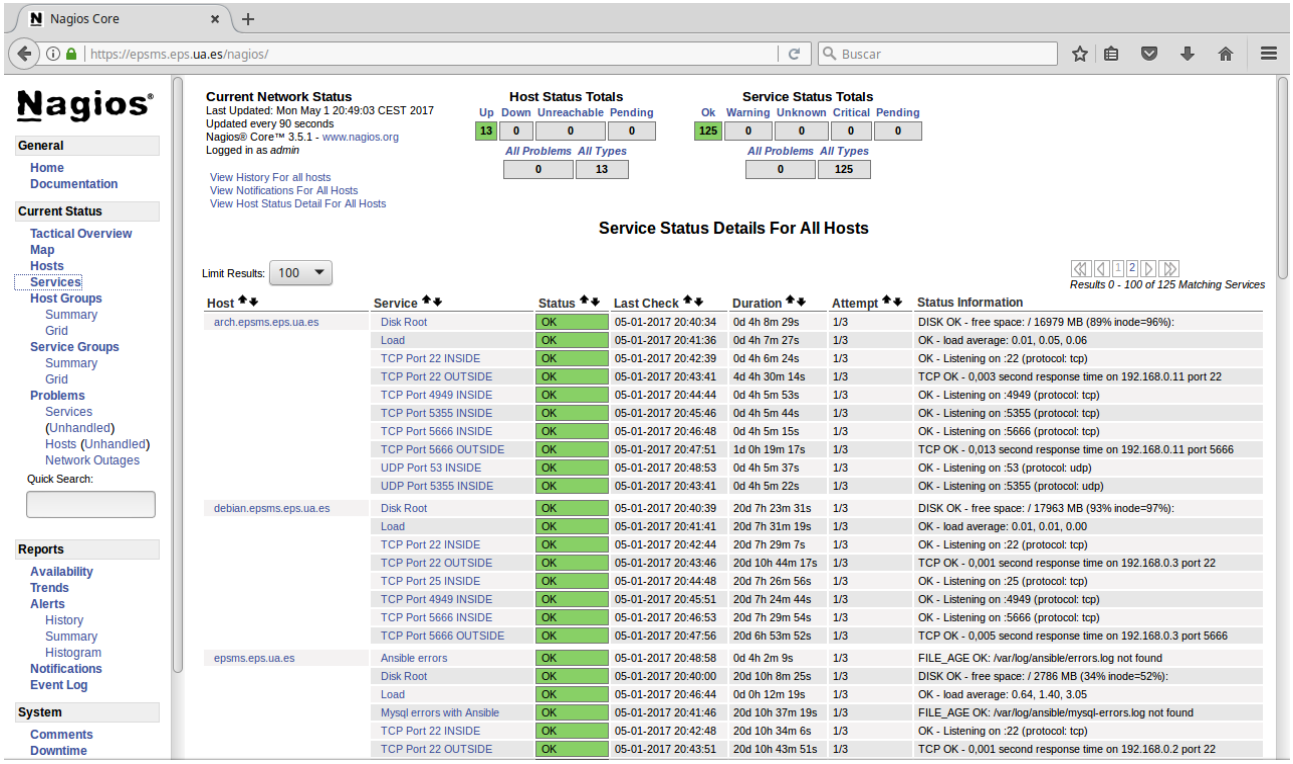
For those users that only need a subset of the provided features (for instance, alerts or performance) it is very likely they don't have the time and/or money to invest in a fully-fledged monitoring system. In this case, 'EPS MS' will complete their 'monitoring system'.

For the other sysadmins who don't have any monitoring system currently active, 'EPS MS' will be a perfect solution because at no cost, and with very little time required for installation and configuration, they will get a complete, automatic and free monitoring system.

Live Demo available at https://epsms.eps.ua.es (**user: 'epsms', password: 'epsms'**). Read only user 'epsms' to watch hardware/software/security information collected from a real network in real-time.

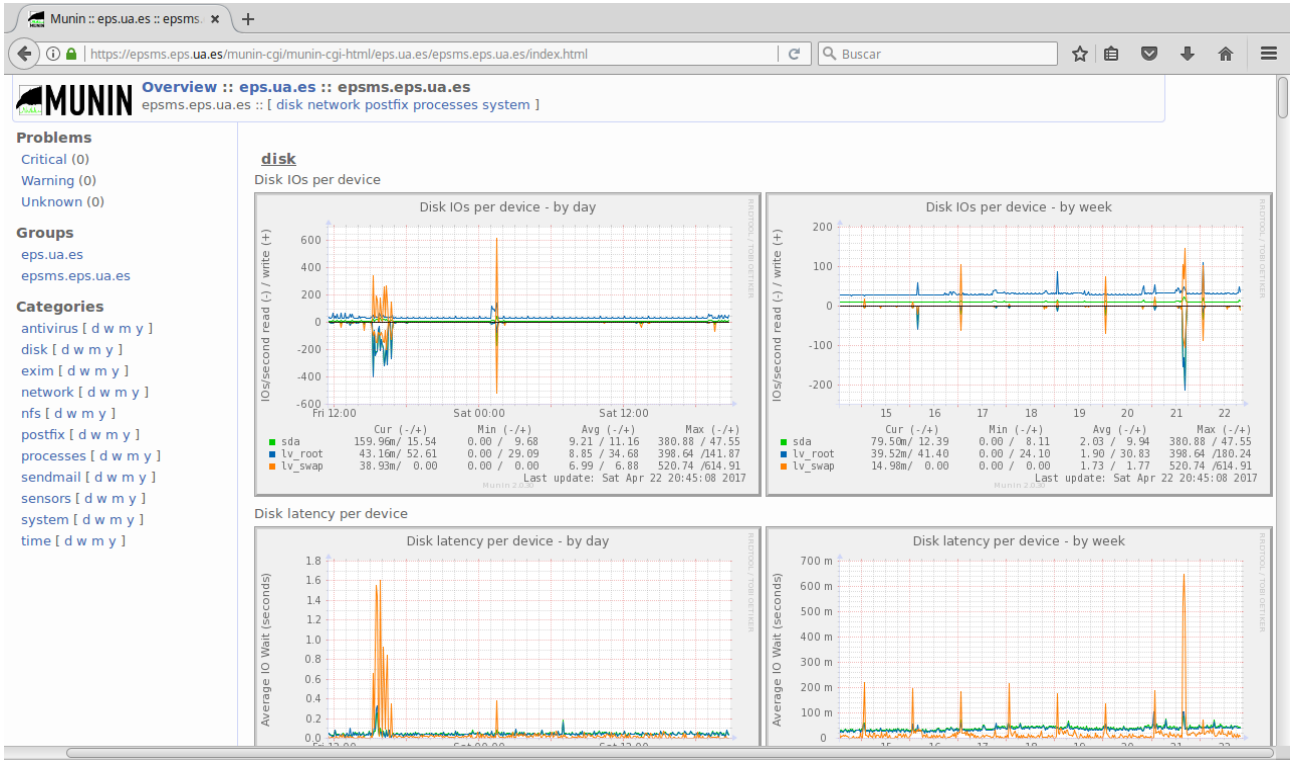
Basically, 'EPS MS' **provides**:

- Events & alerts monitoring system (**Nagios**) to analyze hosts and services status.



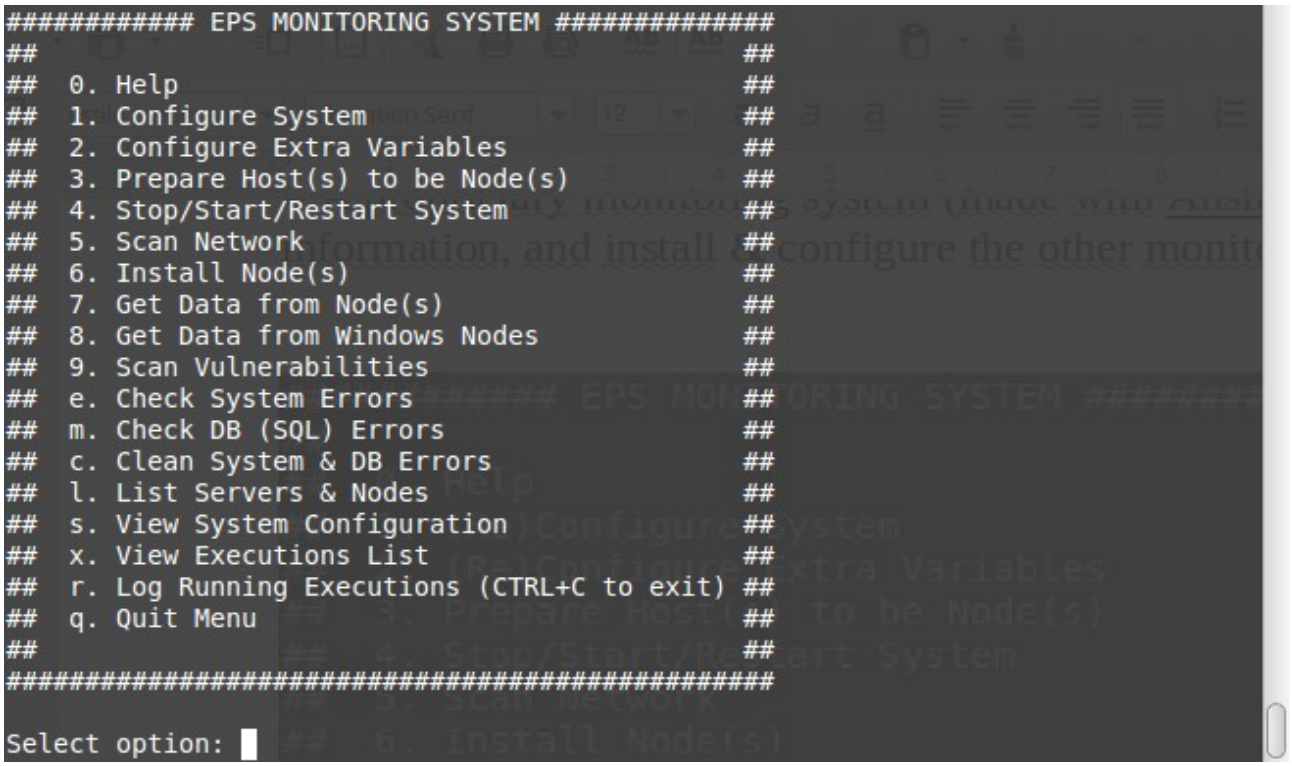
Nagios

● A performance monitoring system (**Munin**) to analize hosts performance graphically.



Munin

● A proprietary monitoring system (made with Ansible) to collect hardware, software and security information, and install & configure the other monitoring systems: Nagios, Munin, Openvas...



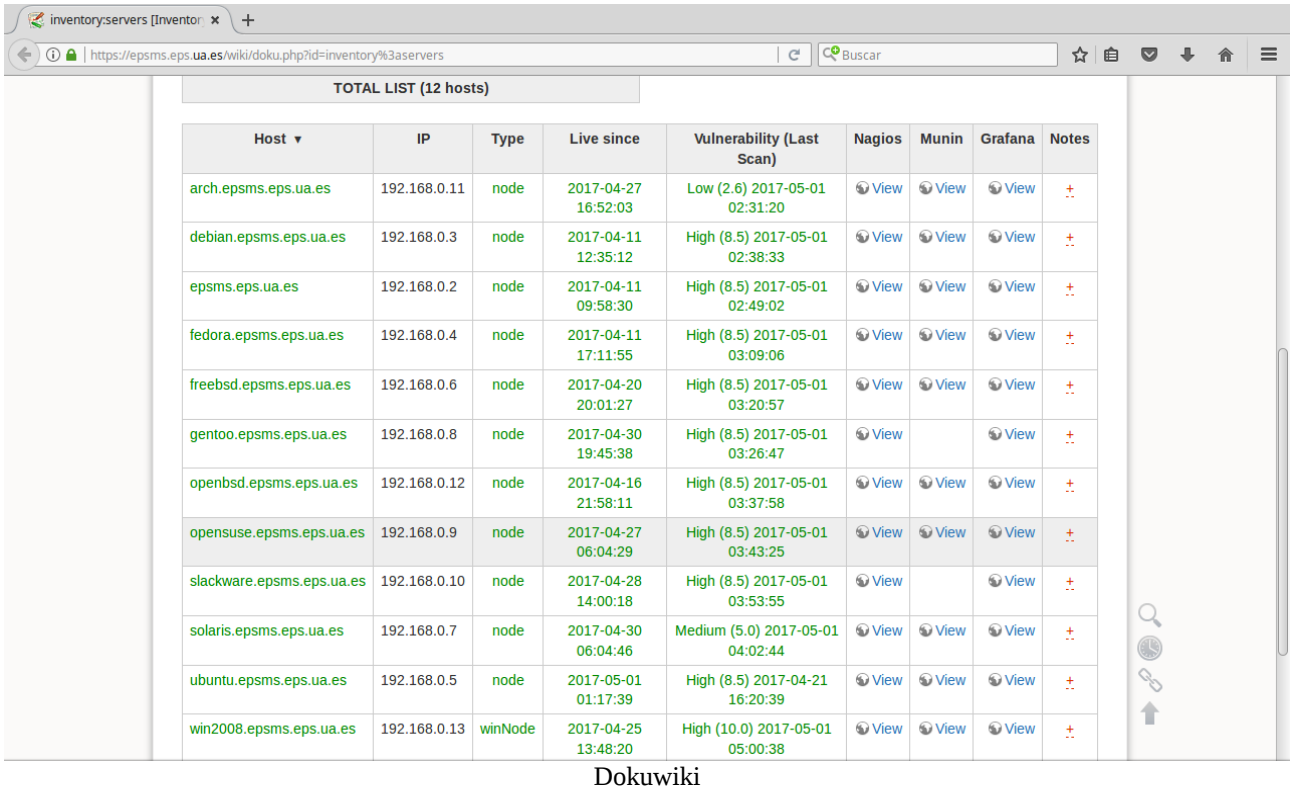
EPS Monitoring System

● A **Mysql** database to store collected information (current and historical).

```
[root@centos ansible]# mysql -h epsms.eps.ua.es -u admin -p inventory
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2985
Server version: 5.1.73-log Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select Port, Protocol, Process, IP4, BindIP4, BindIP6, Access, Init, End from ServerPort where Server='epsms.eps.ua.es' and Auto LIMIT 18;
+------+----------+---------------+------+-----------+---------+--------+---------------------+---------------------+
| Port | Protocol | Process       | IP4  | BindIP4   | BindIP6 | Access | Init                | End                 |
+------+----------+---------------+------+-----------+---------+--------+---------------------+---------------------+
|   22 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
|  443 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
| 3000 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
| 3306 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
| 8083 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
| 8086 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
| 8088 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 09:58:30 | NULL                |
|   22 | TCP      | sshd          |    1 | 0.0.0.0   | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
|   25 | TCP      | master        |    1 | 127.0.0.1 | ::1     | IN     | 2017-04-11 10:05:28 | NULL                |
| 3000 | TCP      | grafana-server |    0 |           | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
| 3306 | TCP      | mysqld        |    1 | 0.0.0.0   |         | IN     | 2017-04-11 10:05:28 | NULL                |
|  443 | TCP      | httpd         |    0 |           | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
| 4949 | TCP      | perl          |    0 |           | ::      | IN     | 2017-04-11 10:05:28 | 2017-04-12 16:09:46 |
| 5666 | TCP      | nrpe          |    1 | 0.0.0.0   | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
| 8083 | TCP      | influxd       |    0 |           | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
| 8086 | TCP      | influxd       |    0 |           | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
| 8088 | TCP      | influxd       |    0 |           | ::      | IN     | 2017-04-11 10:05:28 | NULL                |
| 5666 | TCP      |               |    0 |           |         | OUT    | 2017-04-11 12:35:13 | NULL                |
+------+----------+---------------+------+-----------+---------+--------+---------------------+---------------------+
18 rows in set (0.05 sec)

mysql>
```

Mysql

● A **Dokuwiki** server to show collected information.

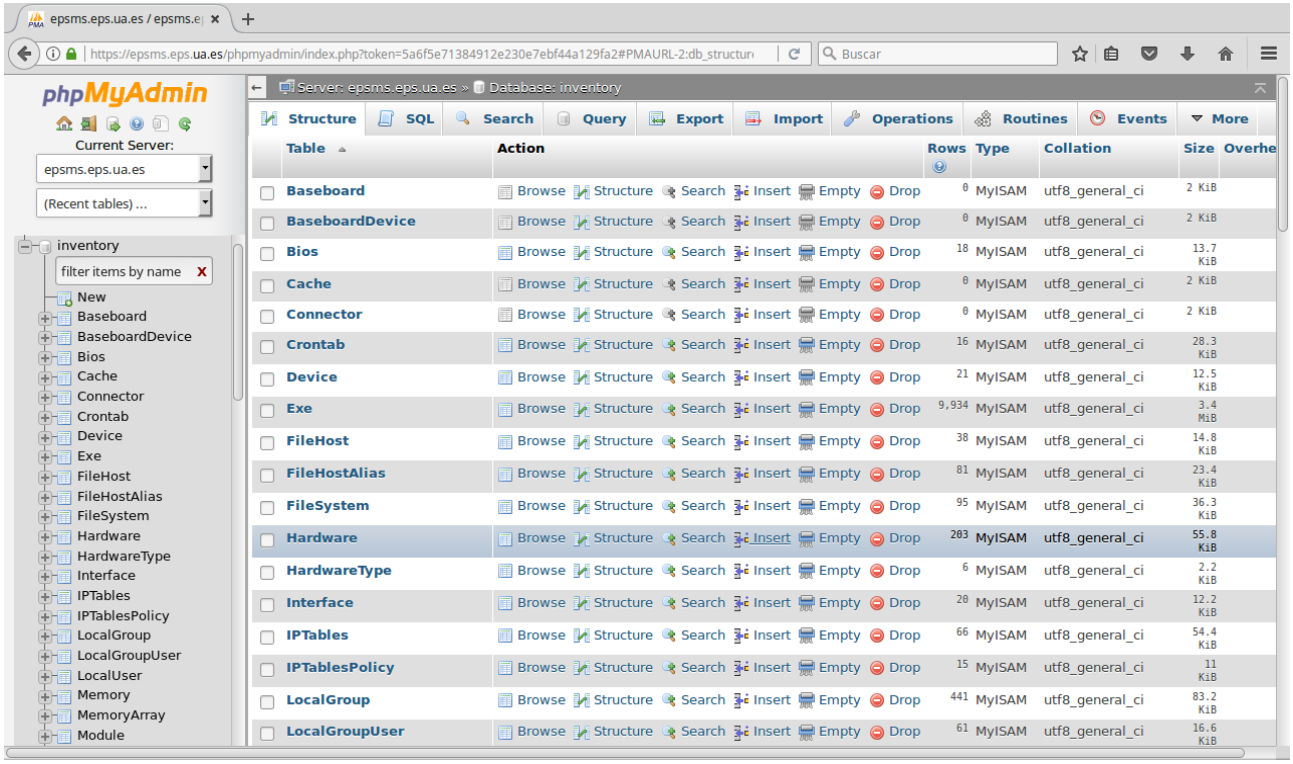


TOTAL LIST (12 hosts)

Host ▾	IP	Type	Live since	Vulnerability (Last Scan)	Nagios	Munin	Grafana	Notes
arch.epsms.eps.ua.es	192.168.0.11	node	2017-04-27 16:52:03	Low (2.6) 2017-05-01 02:31:20	View	View	View	+
debian.epsms.eps.ua.es	192.168.0.3	node	2017-04-11 12:35:12	High (8.5) 2017-05-01 02:38:33	View	View	View	+
epsms.eps.ua.es	192.168.0.2	node	2017-04-11 09:58:30	High (8.5) 2017-05-01 02:49:02	View	View	View	+
fedora.epsms.eps.ua.es	192.168.0.4	node	2017-04-11 17:11:55	High (8.5) 2017-05-01 03:09:06	View	View	View	+
freebsd.epsms.eps.ua.es	192.168.0.6	node	2017-04-20 20:01:27	High (8.5) 2017-05-01 03:20:57	View	View	View	+
gentoo.epsms.eps.ua.es	192.168.0.8	node	2017-04-30 19:45:38	High (8.5) 2017-05-01 03:26:47	View		View	+
openbsd.epsms.eps.ua.es	192.168.0.12	node	2017-04-16 21:58:11	High (8.5) 2017-05-01 03:37:58	View	View	View	+
opensuse.epsms.eps.ua.es	192.168.0.9	node	2017-04-27 06:04:29	High (8.5) 2017-05-01 03:43:25	View	View	View	+
slackware.epsms.eps.ua.es	192.168.0.10	node	2017-04-28 14:00:18	High (8.5) 2017-05-01 03:53:55	View		View	+
solaris.epsms.eps.ua.es	192.168.0.7	node	2017-04-30 06:04:46	Medium (5.0) 2017-05-01 04:02:44	View	View	View	+
ubuntu.epsms.eps.ua.es	192.168.0.5	node	2017-05-01 01:17:39	High (8.5) 2017-04-21 16:20:39	View	View	View	+
win2008.epsms.eps.ua.es	192.168.0.13	winNode	2017-04-25 13:48:20	High (10.0) 2017-05-01 05:00:38	View	View	View	+

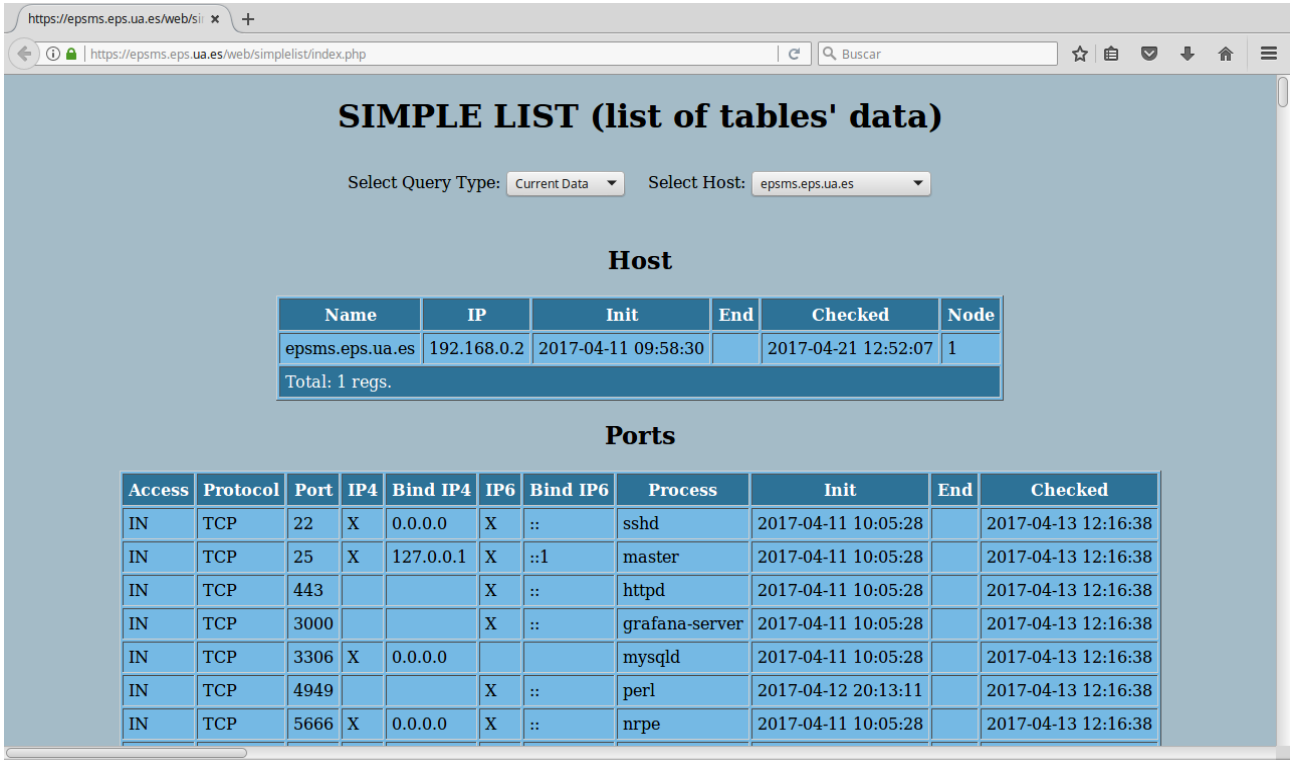
Dokuwiki

● A **PhpMyAdmin** server to manage graphically data stored in Mysql database.

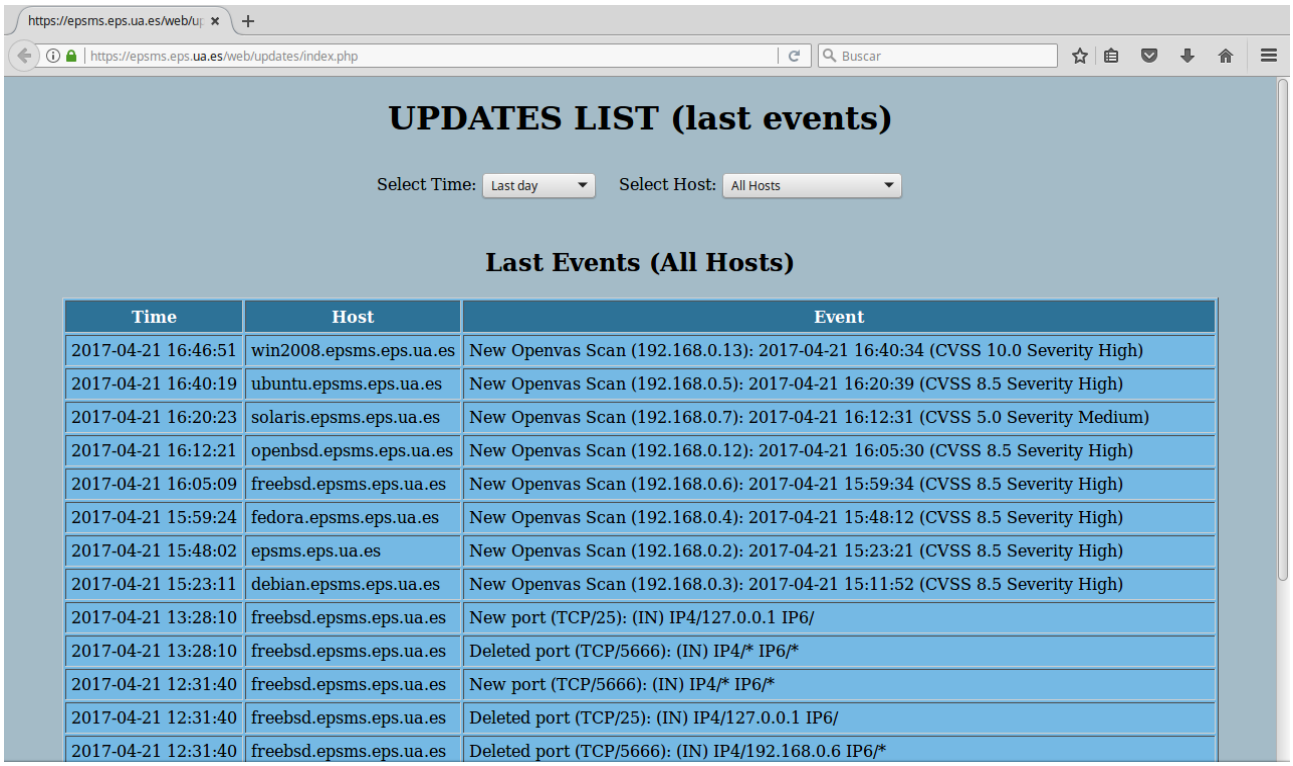


PhpMyAdmin

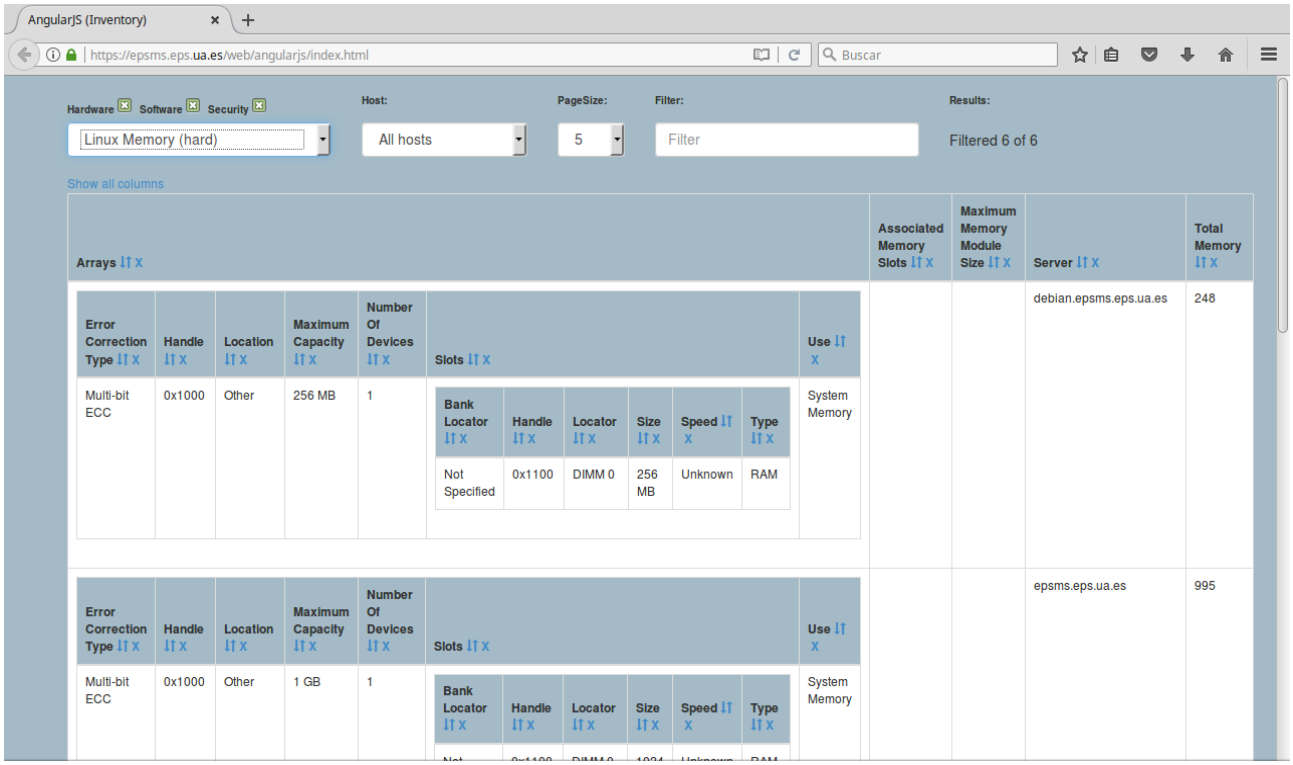
● A **Web application** (made with **PHP** and **Angularjs**) to analyze information in a customized way.



Simple List (PHP)

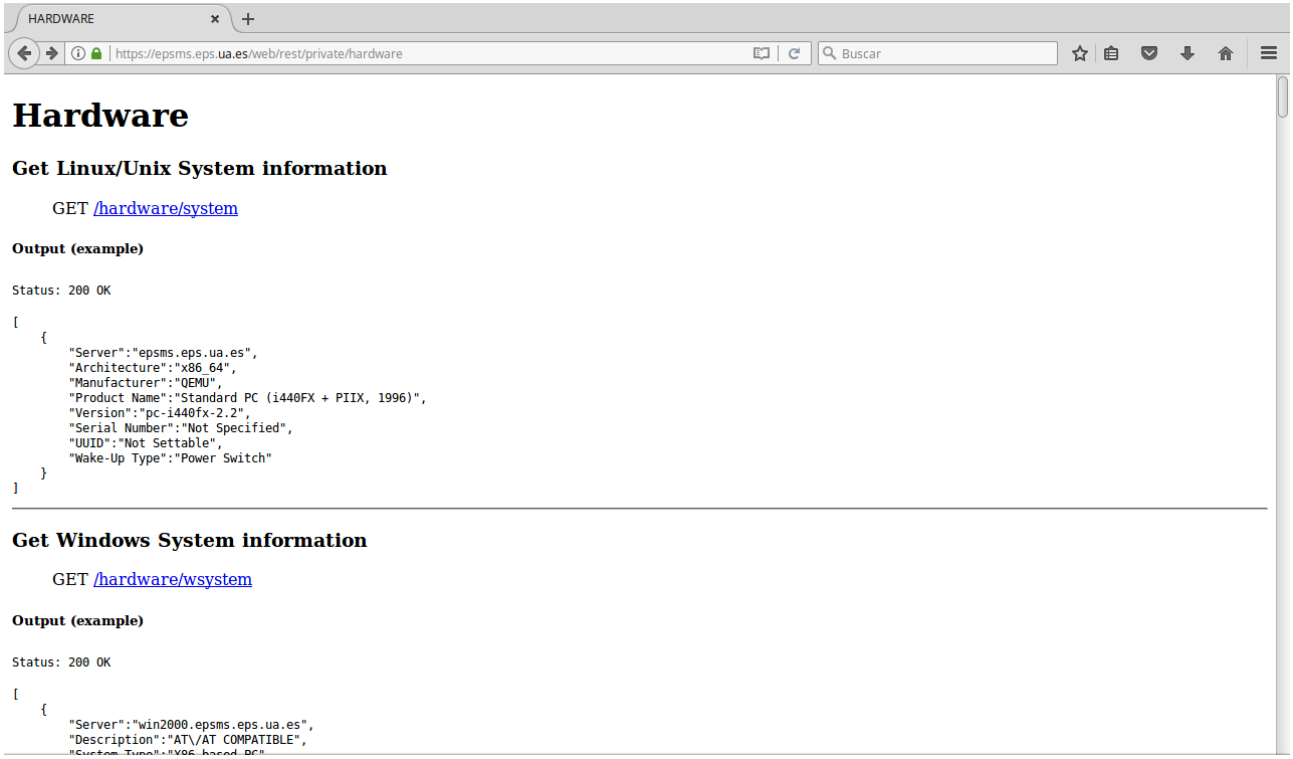


Updates List (PHP)

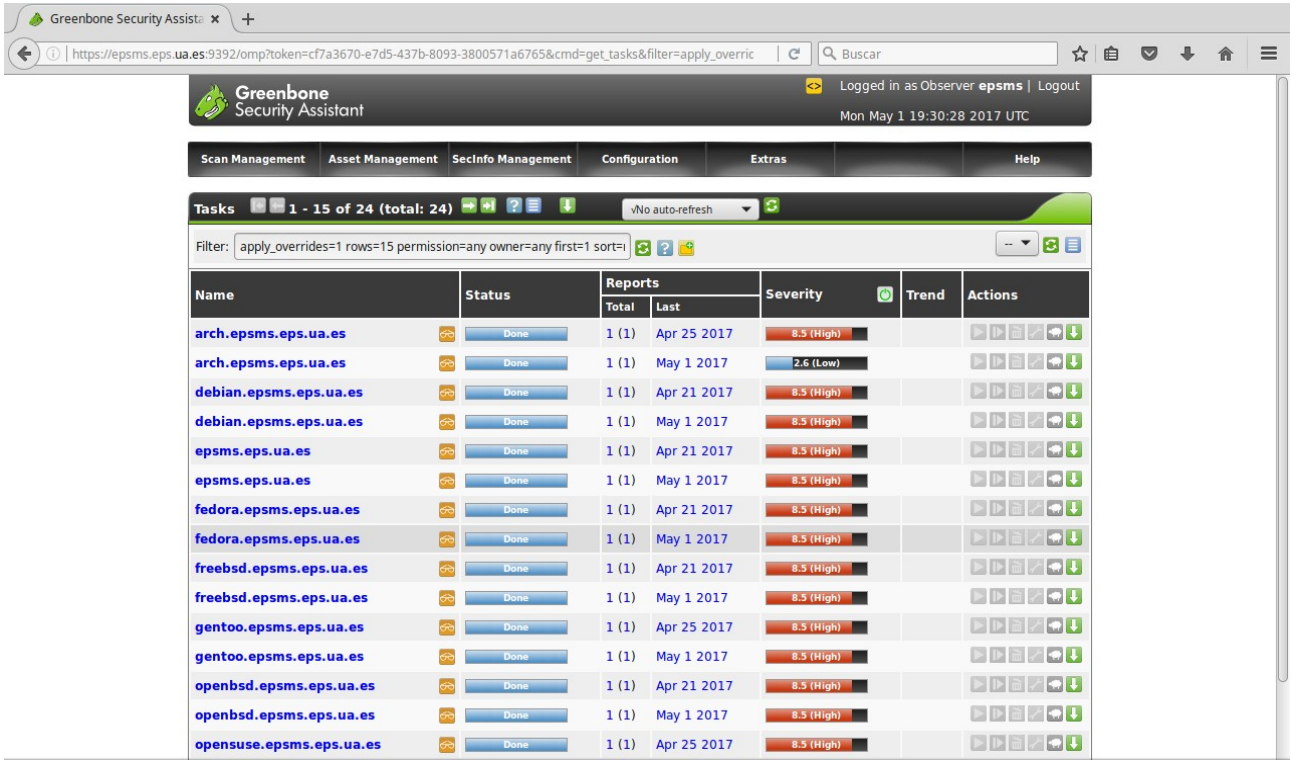


Inventory (angularjs)

- A Rest API to access data (used by angularjs application)

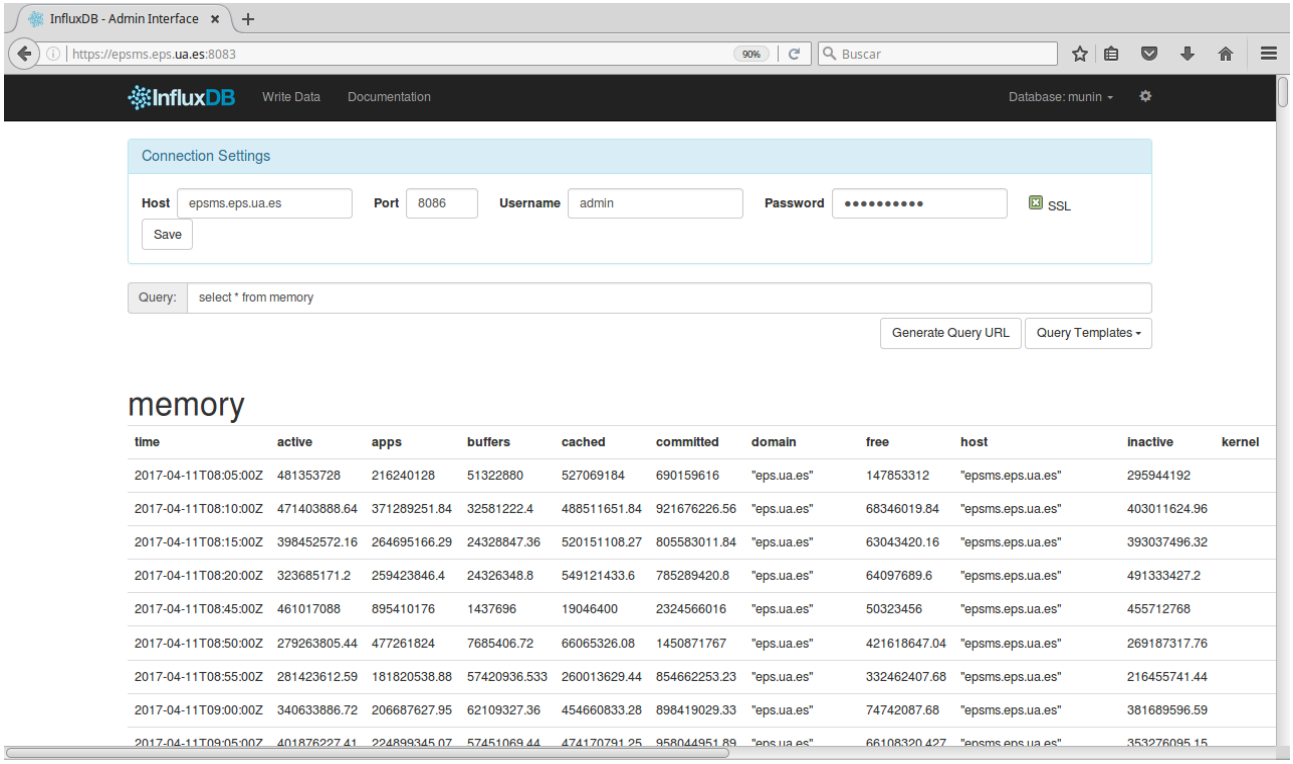


- A security monitoring system (**Openvas**) to scan hosts vulnerabilities.



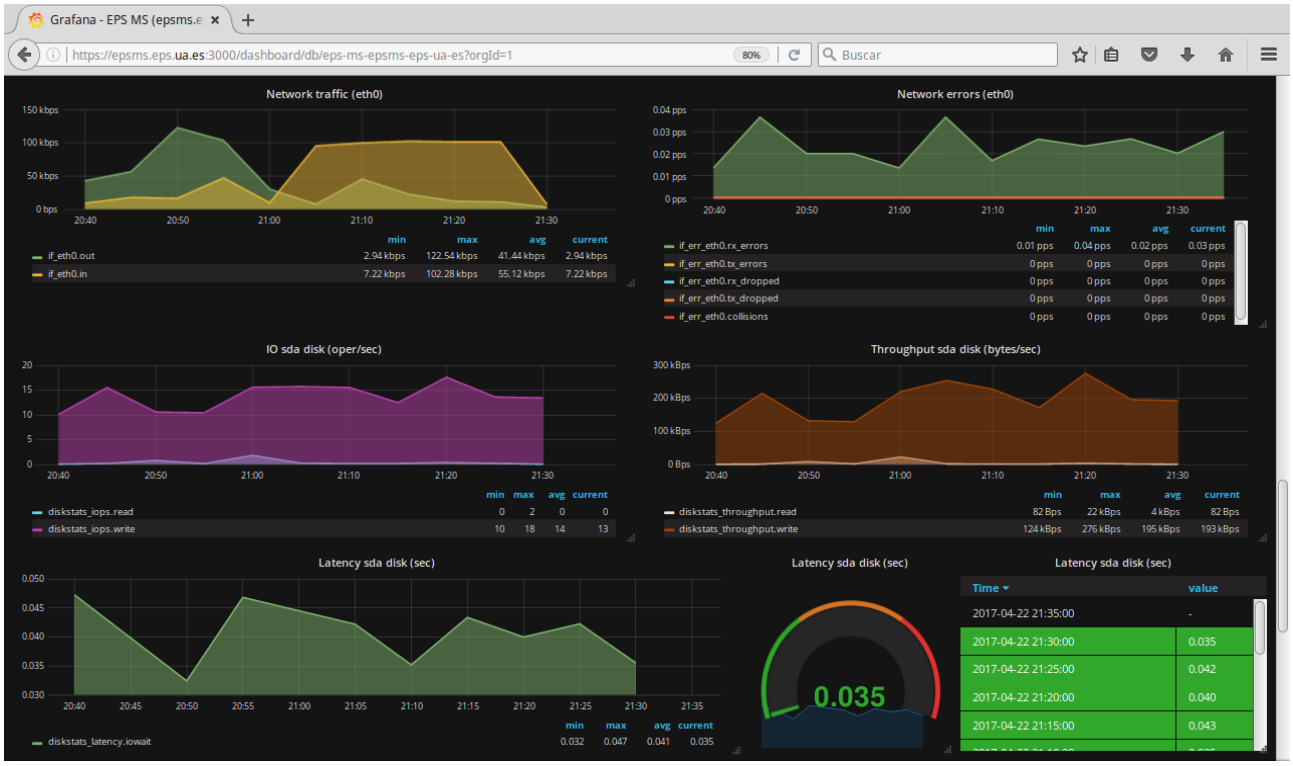
Openvas

● An **InfluxDB** database to store time-series data from munin and nagios.



InfluxDB

● A full-featured interactive dashboard (**Grafana**) to analyze influxdb information.



Grafana

OK, I want to try this software. But, how much time is required? Just a few minutes. These are the steps to **install and configure**:

1. Download **'epsms.tgz'** file of **install** directory and decompress it on a CentOS 6 host (this will be our 'Control Server').

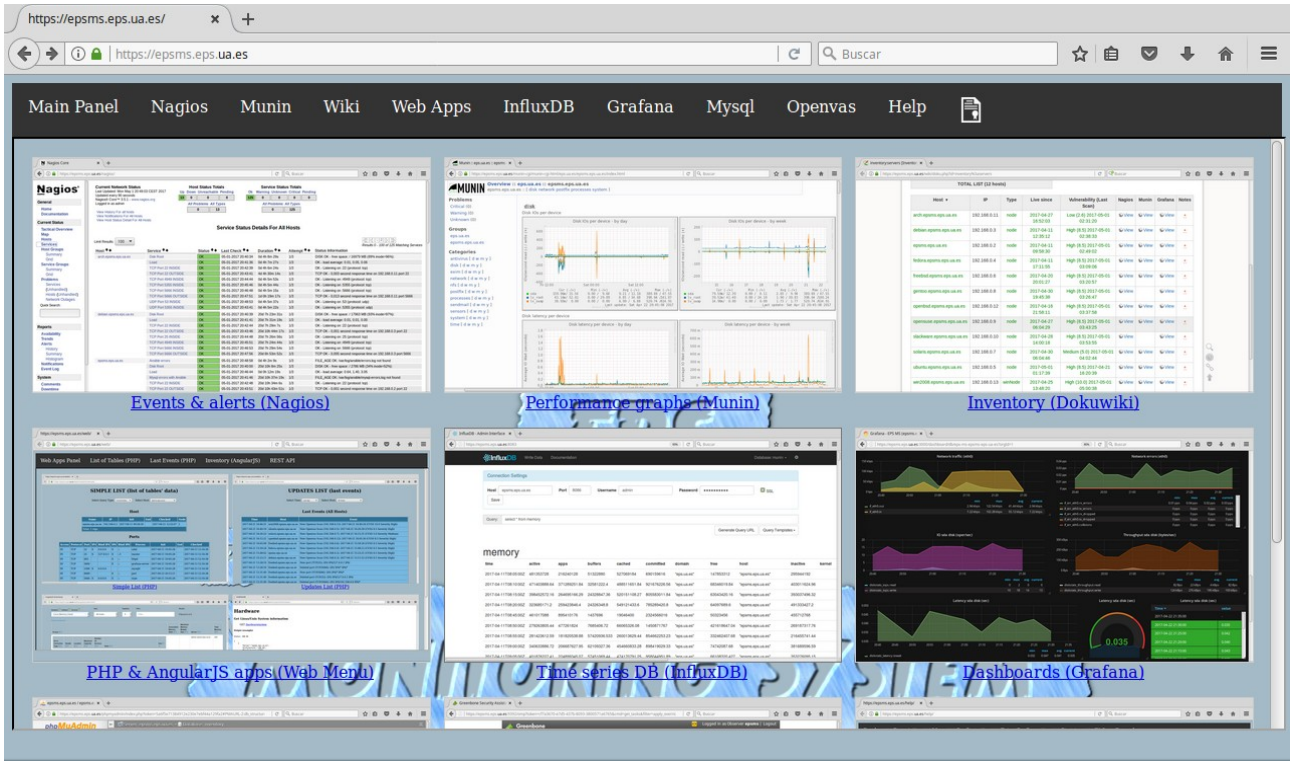
2. **Execute 'install.py'** script to install 'EPS MS'.

3. **Execute '/etc/ansible/menu.py'** in order to show the 'Control Menu'.

4. Select **option '1'** in 'Control Menu' to deploy 'EPS MS' infrastructure. This option will ask some questions about configuration such as:

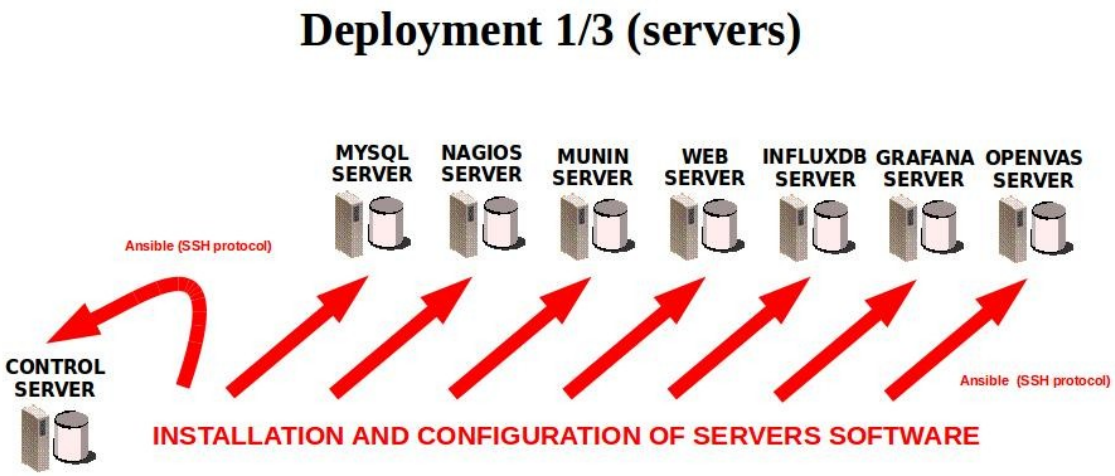
- User to connect to Linux/Unix hosts (connection by SSH without password, using public keys and sudo)
- User/password to connect to Windows hosts (connection by WMI 'Windows Management Instrumentation')
- IP addresses of Nagios, Munin, Mysql, Web (Dokuwiki, PhpMyAdmin and web Apps), Grafana and Openvas servers to install software (they have to be CentOS 6)
- Networks to monitor, collecting information of hosts inside them
- Admin password of Servers: Nagios, Munin, Mysql, Web (Dokuwiki, PhpMyAdmin and web Apps), Grafana and Openvas
- IP addresses of administrators hosts (access permission to servers)
- Frequencies to check servers (server's software installation and a correct configuration) and hosts (client's software installation, correct configuration and data collecting of hardware, software and security information from them)

5. After infrastructure's deployment, 'EPS MS' starts **collecting information** from hosts indefinitely. Results can be analyzed from 'https://hostnameWebServer' with links to Nagios, Munin, Wiki, Mysql (phpMyAdmin), web (PHP & AngularJS) Apps, InfluxDB, Grafana , Openvas and Help:

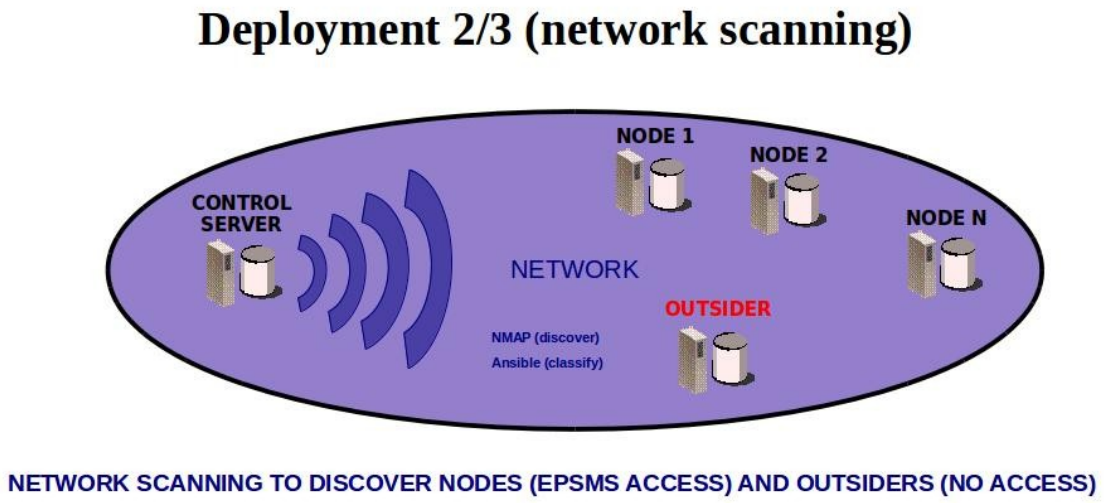


But, **how does it work** inside? These are the steps 'EPS MS' performs after configuration:

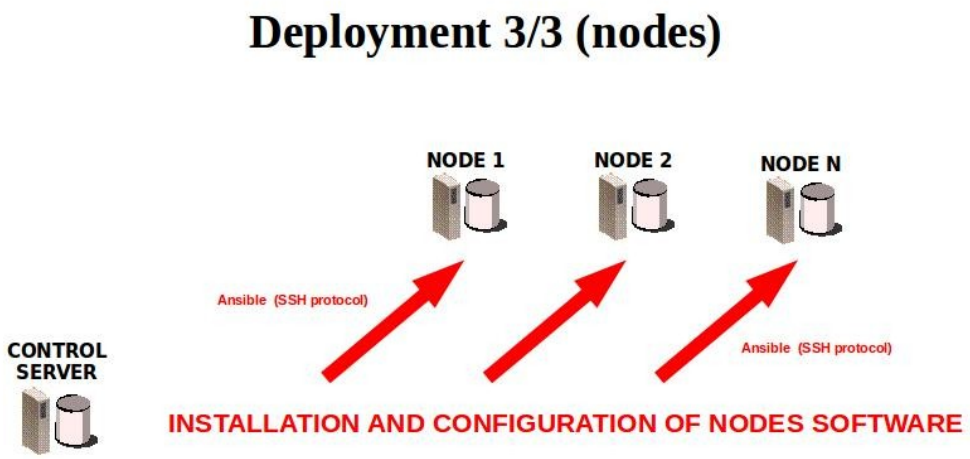
(A.1) Infrastructure deployment: **Installation and configuration of servers software**



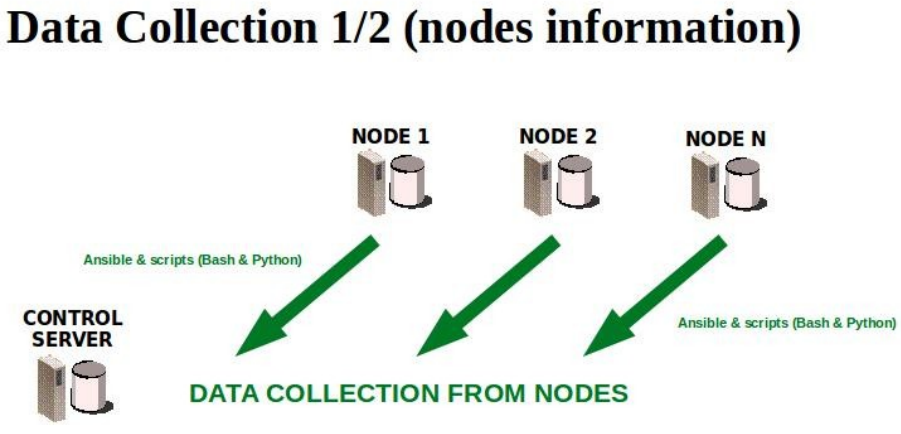
(A.2) Infrastructure deployment: **Network scanning** to discover '**nodes**' (hosts accessed by 'EPS MS') and '**outsiders**' (hosts not accessed).



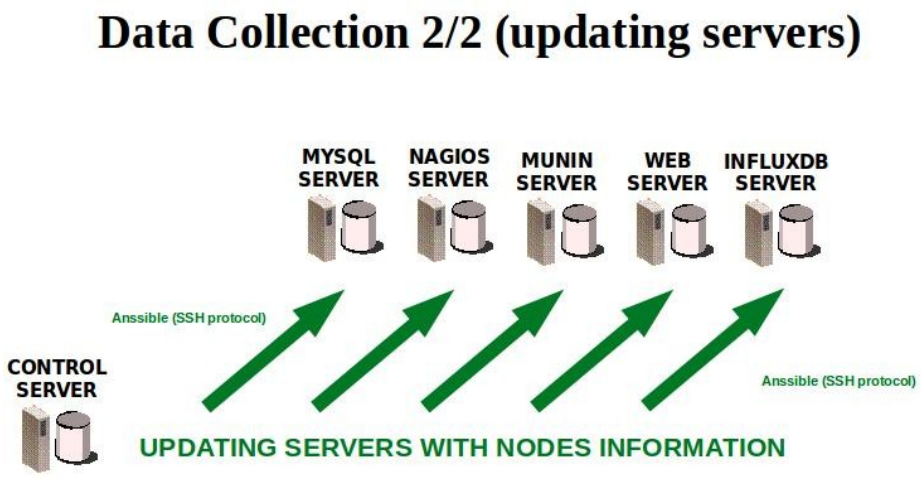
(A.3) Nodes deployment: **Installation and configuration of software in the nodes**



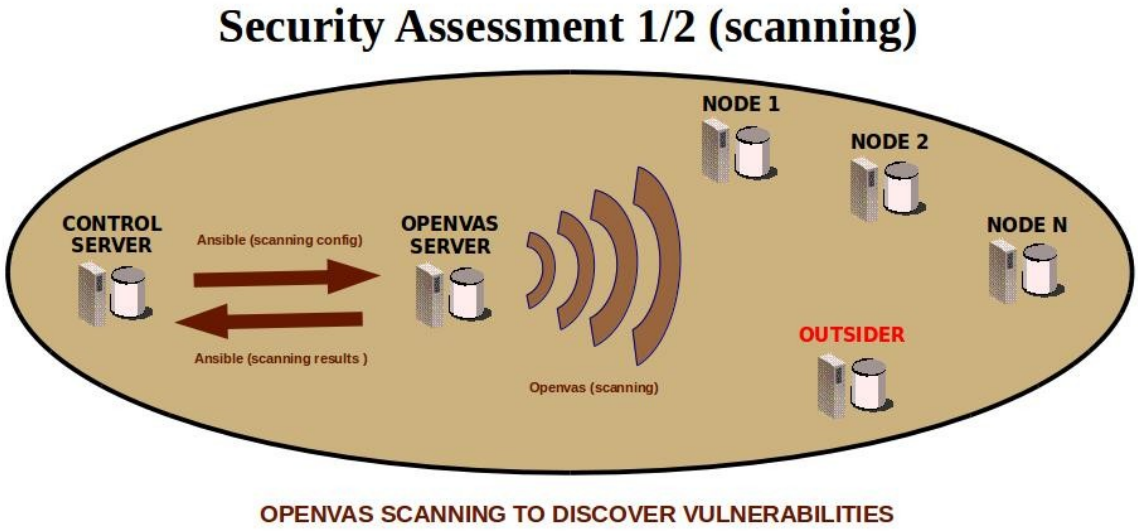
(B.1) Data collection: **Getting information from nodes**



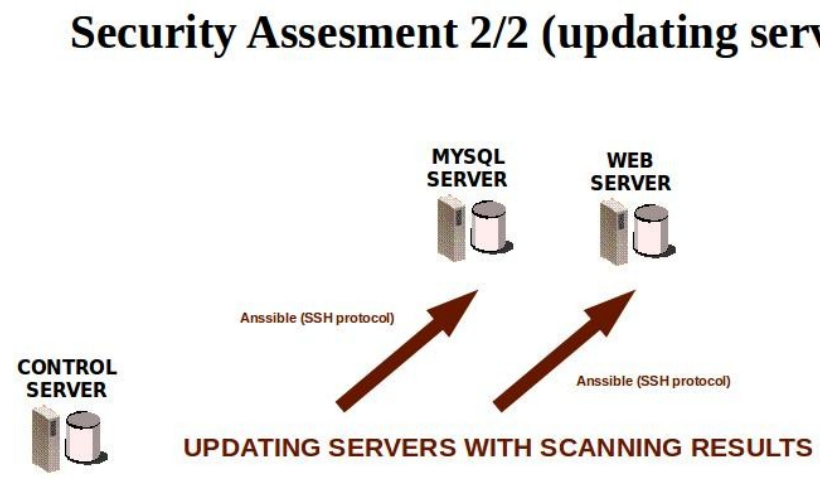
(B.2) Data collection: **Updating servers with information obtained from the nodes**



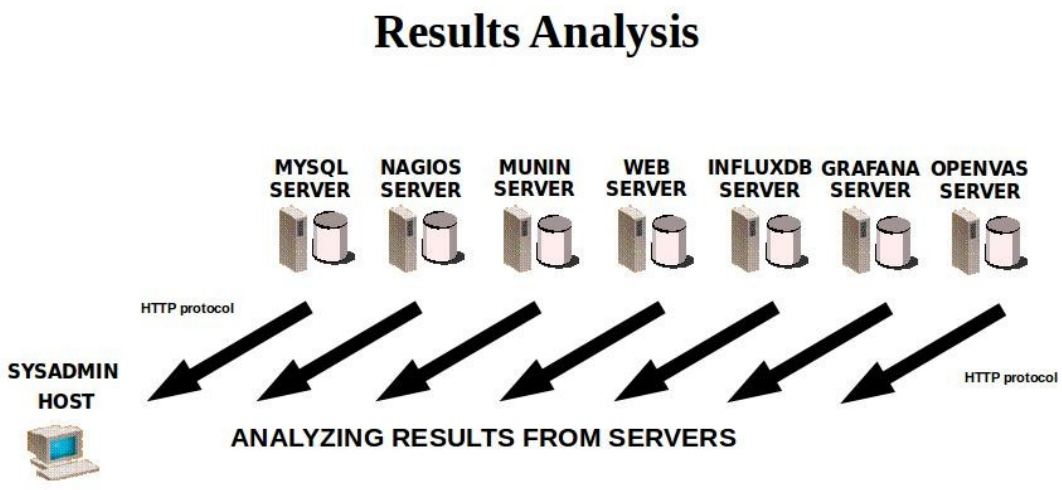
(C.1) Security Assessment: **Vulnerabilities scanning** of nodes and outsiders (with Openvas)



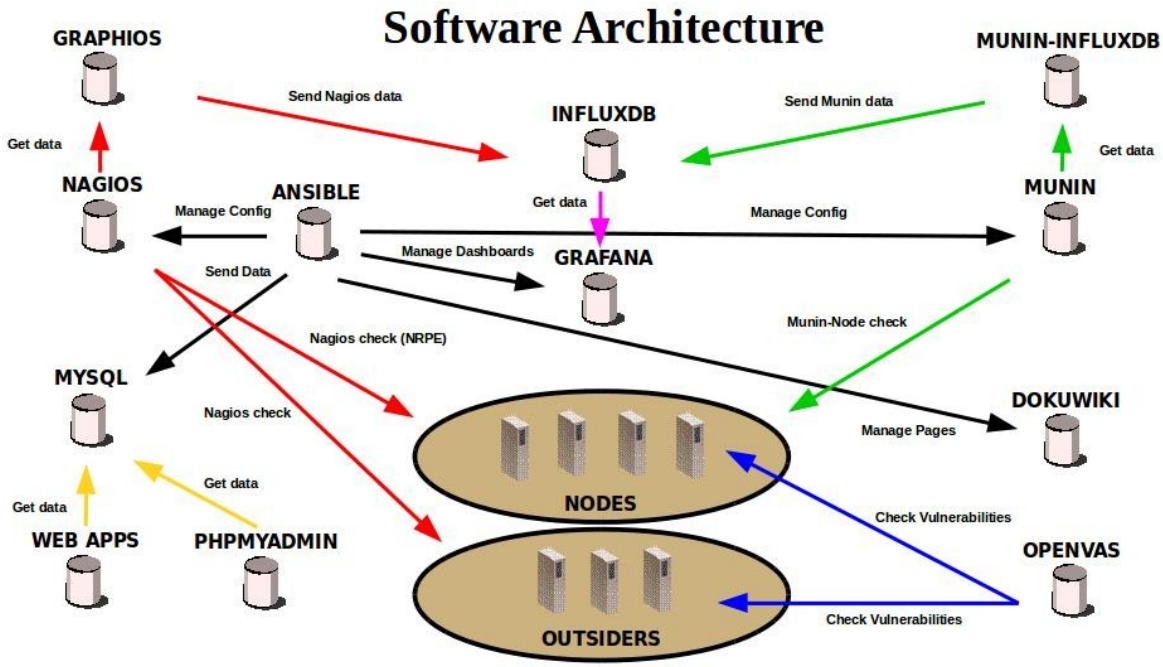
(C.2) Security assesment: **Updating servers with scanning results**



(D) **Analyzing results** stored in servers



Software Architecture



What kind of **information** will be obtained?

Hardware (Linux/Unix)	**System:** Architecture, Manufacturer, Product Name, Version, Serial Number, UUID, Wake-Up Type **Processor:** Processor Type, Processor Count, Cores per Processor, Threads per Core, Total Virtual CPUs, Sockets **For Every Socket:** Designation, Type, Family, Vendor, Signature, ID, Version, Voltage, External Clock, Maximum Speed, Current Speed, Status, L1 Cache Handle, L3 Cache Handle, L3 Cache Handle, Serial Number **Memory:** Total Memory, Maximum Memory Module Size, Number of Arrays, Number of Slots, Arrays **For Every Array:** Handle, Location, Use, Error Correction Type, Maximum Capacity, Number of Devices, Slots **For Every Slot:** Handle, Locator, Array, Bank Locator, Size, Speed, Type **BIOS:** Vendor, Release Date, Version, ROM Size, Runtime Size, Characteristics **For Every Characteristic:** Characteristic, Value **Baseboard:** Handle, Manufacturer, Product Name, Version, Serial Number, Devices **For Every Device:** Handle, Type, Description, Enabled **Chassis:** Manufacturer, Type, Version, Serial Number

	Devices: Name, Model, Scheduler, Size, Vendor, Partitions **For Every Partition:** Name, Size **Network Interfaces:** Name, Address, DNS Name, Network, NetMask, MAC, Type, Module, Active **Cache Memory:** Handle, Socket Designation, Level, Enabled, Mode, Location, Installed Size, Maximum Size **Connectors:** Handle, Internal Reference Designator, Internal Connector Type, External Reference Designator, External Connector Type, Port Type
Hardware (Windows)	**System:** Description, System Type, PC System Type, Manufacturer, Model, Infrared Supported, Wake-Up Type **Processor:** Number of Processors, Number of Logical Processors, Sockets **For Every Socket:** Device ID, Name, Caption, Config Manager Error Code, CPU Status, Current Clock Speed, Data Width, Family, L2 Cache Size, L2 Cache Speed, L3 Cache Size, L3 Cache Speed, Manufacturer, Maximum Clock Speed, Number of Cores, Number of Logical Processors, Processor ID, Processor Type **Memory:** Total Physical Memory, Arrays **For Every Array:** Tag, Caption, Hot Swappable, Location, Maximum Capacity, Memory of Devices, Memory Error Correction, Memory Use, Slots **For Every Slot:** Tag, Caption, Capacity, Data Width, Total Width, Device Locator, Form Factor, Hot Swappable, Manufacturer, Memory Type, Position in Row, Speed **BIOS:** Name, Caption, Software Element ID, Software Element State, Target Operating System, Version, Buid Number, Code Set, Current Language, Identification Code, Language Edition, Manufacturer, Primary BIOS, Characteristics **For Every Characteristic:** Char Code, Description **Baseboard:** Tag, Caption, Manufacturer, Product, Model, Version, Serial Number, Hosting Board, Hot Swappable, Powered On, Devices **For Every Device:** Tag, Caption, Description, Device Type, Manufacturer, Model, Version, Serial Number, Enabled, Hot Swappable, Powered On **Devices:** Device ID, Caption, Disk Index, Interface Type, Model ,Size, Availability, Total Heads, Total Cylinders, Tracks per Cylinder, Total Tracks, Sectors per Track, Total Sectors, Bytes per Sector, Default Block Size, Media Type, Partition ID, Config Manager Error Code, Serial Number, SCSI Bus, SCSI Port, SCSI Target ID, SCSI Logical Unit, Partitions **For Every Partition:** Device ID, Caption, Disk Index, Partition Index, Partition Type, Size, Block Size, Number of Blocks, Access, Availability, Bootable, Boot Partition, Primary Partition **Network Interfaces:** Device ID, Name, Adapter Type, Manufacturer, MAC Address, Availability, Config Manager Error Code, Adapter Index, Net Connection ID, Net Connection Status, Service Name, Settings **For Every Setting:** Net Index, Description, IP Address, IP Subnet, Default IP Gateway, Default TOS, Default TTL, DHCP Enabled, DHCP Server, DNS Domain, DNS Domain Suffix Search

	Order, DNS Enabled for WINS Resolution, DNS Domain Search Order, IGMP Level, MAC Address, WINS Enable LMHosts Lookup, WINS Primary Server, WINS Secondary Server **Connectors:** Tag, Connector Type, External Reference Designator, Internal Reference Designator, Port Type **Buses:** Device ID, Caption, Bus Type, Bus Num, Availability, Config Manager Error Code
Software (Linux/Unix)	**IP:** Name, IP **Distribution:** Distribution, Version **Kernel:** Kernel **Modules:** Name, File Name, Author, Description, License, Version, Version Magic, Source Version **Domain:** Domain **DNS Resolver:** Domain, NameServer 1, NameServer 2, NameServer 3, Options For Every Option: Option **'/etc/hosts' File:** Rules **Routes:** Destination, Gateway, Mask, Flags, Interfaces **Swap Memory:** Swap **Virtualization:** Virtualization Role, Virtualization Type **FileSystems:** Name, Type, Mount, Options, Size
Software (Windows)	**IP:** Name, IP **Domain:** Domain **Operating System:** OS Name, OS Description, Boot Device, Service Pack Version, OS Architecture, OS Type, Product Type, Version, Serial Number, Country, Language, PAE Enabled, Manufacturer, Current Time Zone, Encryption Level, Number of Licensed Users, Operating System SKU, Organization, Registered User, Maximum Number of Processes, System Device, System Drive, Windows Directory, System Directory, Total Visible Memory Size, Total Swap Space Size, Total Virtual Memory Size, Distributed **Logical Devices:** Device ID, Caption, Drive Type, File System, Size, Access, Availability, Compressed, Config Manager Error Code, Supports Disk Quotas, Quotas Disabled, Supports File Based Compression, Volume Name, Volume Serial Number, Partitions **For Every Partition:** Partition Device ID

Security (Linux/Unix)	**Servers:** Name, IP, Node **TCP/UDP Ports (inside Scan):** Protocol, Port, IP4, Bind IP4, IP6, Bind IP6, Process **TCP Ports (outside scan):** Protocol, Port **Packages:** Name, Version, Size **Executables:** Name, Package, File Size, File User, File Group, File Permissions, Signature **Executables (with no package):** Name, File Size, File User, File Group, File Permissions **Executables (setUID):** Name, Package, File Size, File User, File Group, File Permissions **Executables (setGID):** Name, Package, File Size, File User, File Group, File Permissions **Users:** Name, UID, GID, Password Type, Last Change, Description, Home, Shell **Groups:** Name, GID, Users **For Every User:** User **Sudo:** Defaults, User Alias, Cmnd Alias, Runas Alias, Rules Alias **For Every Default:** Rule **For Every User Alias:** Rule **For Every Cmnd Alias:** Rule **For Every Runas Alias:** Rule **For Every Rules Alias:** Rule **Crontab:** User, Minute, Hour, Day, Month, DayWeek, Command **IPTables:** IPTable, Chain, Policy, Rules **For Every Rule:** Rule **TCP Wrappers:** Type, Service, Hosts **For Every Host:** Host **PAM Access:** Modules, Rules **For Every Module:** Module **For Every Rule:** Rule **Openvas:** IP, Start Scan, CVSS, Total High, Total Medium, Total Low, Total Log, Total False Positive
Security (Windows)	**Servers:** Name, IP, Node **TCP/UDP Ports (inside Scan):** Protocol, Port, IP4, Bind IP4, IP6, Bind IP6, Process **TCP Ports (outside scan):** Protocol, Port

	Users: Domain, Name, System Account, Caption, Account Type, Disabled, Full Name, Local Account, Lockout, Password Changeable, Password Expires, Password RequiredSID, SID Type **Groups:** Name, GID, Users **For Every User:** User **Drivers:** Name, Caption, Error Control, Path Name, Service Type, Start Mode, State, Tag ID **Services:** Name, Caption, Error Control, Path Name, Process ID, Start Mode, State, Tag ID **Shares:** Name, Caption, Path Share, Type Share **Openvas:** IP, Start Scan, CVSS, Total High, Total Medium, Total Low, Total Log, Total False Positive