

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.

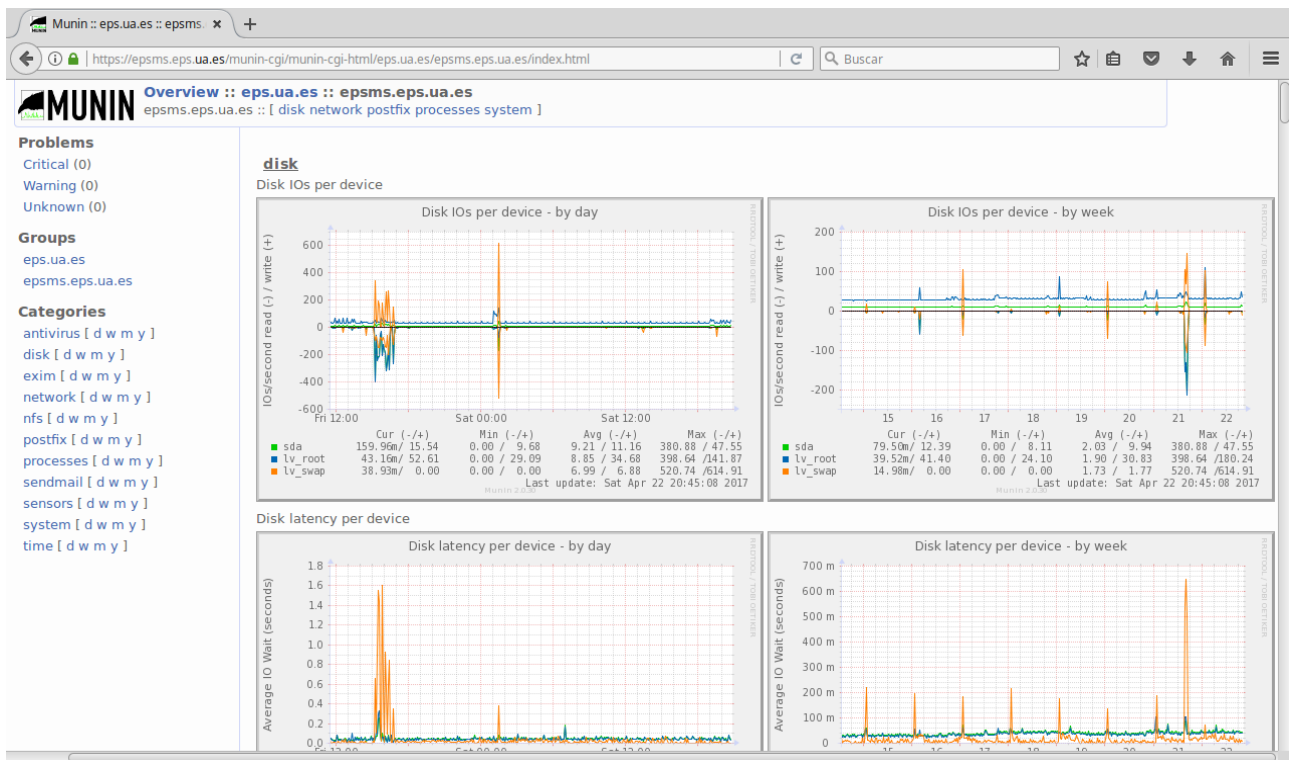
The screenshot displays the Nagios Core web interface. The top navigation bar includes the Nagios logo, a search bar, and various icons. The left sidebar contains a menu with categories like General, Current Status, Tactical Overview, Map, Hosts, Services, Host Groups, Service Groups, Problems, Reports, System, and Comments. The main content area is divided into several sections:

- Current Network Status:** Shows the last update time (Mon May 1 20:49:03 CEST 2017) and the number of hosts (13) and services (125) that are up, down, unreachable, or pending.
- Host Status Totals:** A table showing the status of all hosts. The table has columns for Up, Down, Unreachable, and Pending. The values are 13, 0, 0, and 0 respectively.
- Service Status Totals:** A table showing the status of all services. The table has columns for Ok, Warning, Unknown, Critical, and Pending. The values are 125, 0, 0, 0, and 0 respectively.
- Service Status Details For All Hosts:** A table showing the status of all services for all hosts. The table has columns for Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The table shows details for three hosts: arch.epsms.eps.ua.es, debian.epsms.eps.ua.es, and epsms.eps.ua.es.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
arch.epsms.eps.ua.es	Disk Root	OK	05-01-2017 20:40:34	0d 4h 8m 29s	1/3	DISK OK - free space: / 16979 MB (89% inode=96%):
	Load	OK	05-01-2017 20:41:36	0d 4h 7m 27s	1/3	OK - load average: 0.01, 0.05, 0.06
	TCP Port 22 INSIDE	OK	05-01-2017 20:42:39	0d 4h 6m 24s	1/3	OK - Listening on :22 (protocol: tcp)
	TCP Port 22 OUTSIDE	OK	05-01-2017 20:43:41	4d 4h 30m 14s	1/3	TCP OK - 0.003 second response time on 192.168.0.11 port 22
	TCP Port 4949 INSIDE	OK	05-01-2017 20:44:44	0d 4h 5m 53s	1/3	OK - Listening on :4949 (protocol: tcp)
	TCP Port 5355 INSIDE	OK	05-01-2017 20:45:46	0d 4h 5m 44s	1/3	OK - Listening on :5355 (protocol: tcp)
	TCP Port 5666 INSIDE	OK	05-01-2017 20:46:48	0d 4h 5m 15s	1/3	OK - Listening on :5666 (protocol: tcp)
	TCP Port 5666 OUTSIDE	OK	05-01-2017 20:47:51	1d 0h 19m 17s	1/3	TCP OK - 0.013 second response time on 192.168.0.11 port 5666
debian.epsms.eps.ua.es	UDP Port 53 INSIDE	OK	05-01-2017 20:48:53	0d 4h 5m 37s	1/3	OK - Listening on :53 (protocol: udp)
	UDP Port 5355 INSIDE	OK	05-01-2017 20:43:41	0d 4h 5m 22s	1/3	OK - Listening on :5355 (protocol: udp)
	Disk Root	OK	05-01-2017 20:40:39	20d 7h 23m 31s	1/3	DISK OK - free space: / 17963 MB (93% inode=97%):
	Load	OK	05-01-2017 20:41:41	20d 7h 31m 19s	1/3	OK - load average: 0.01, 0.01, 0.00
	TCP Port 22 INSIDE	OK	05-01-2017 20:42:44	20d 7h 29m 7s	1/3	OK - Listening on :22 (protocol: tcp)
	TCP Port 22 OUTSIDE	OK	05-01-2017 20:43:46	20d 10h 44m 17s	1/3	TCP OK - 0.001 second response time on 192.168.0.3 port 22
	TCP Port 25 INSIDE	OK	05-01-2017 20:44:48	20d 7h 26m 56s	1/3	OK - Listening on :25 (protocol: tcp)
	TCP Port 4949 INSIDE	OK	05-01-2017 20:45:51	20d 7h 24m 44s	1/3	OK - Listening on :4949 (protocol: tcp)
epsms.eps.ua.es	TCP Port 5666 INSIDE	OK	05-01-2017 20:46:53	20d 7h 29m 54s	1/3	OK - Listening on :5666 (protocol: tcp)
	TCP Port 5666 OUTSIDE	OK	05-01-2017 20:47:56	20d 6h 53m 52s	1/3	TCP OK - 0.005 second response time on 192.168.0.3 port 5666
	Ansible errors	OK	05-01-2017 20:48:58	0d 4h 2m 9s	1/3	FILE_AGE OK: /var/log/ansible/errors.log not found
	Disk Root	OK	05-01-2017 20:40:00	20d 10h 8m 25s	1/3	DISK OK - free space: / 2786 MB (34% inode=52%):
	Load	OK	05-01-2017 20:46:44	0d 0h 12m 19s	1/3	OK - load average: 0.64, 1.40, 3.05
	Mysql errors with Ansible	OK	05-01-2017 20:41:46	20d 10h 37m 19s	1/3	FILE_AGE OK: /var/log/ansible/mysql-errors.log not found
	TCP Port 22 INSIDE	OK	05-01-2017 20:42:48	20d 10h 34m 6s	1/3	OK - Listening on :22 (protocol: tcp)
	TCP Port 22 OUTSIDE	OK	05-01-2017 20:43:51	20d 10h 43m 51s	1/3	TCP OK - 0.001 second response time on 192.168.0.2 port 22

Nagios

- A performance monitoring system ([Munin](#)) to analyze 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 #####
##
## 0. Help
## 1. Configure System
## 2. Configure Extra Variables
## 3. Prepare Host(s) to be Node(s)
## 4. Stop/Start/Restart System
## 5. Scan Network
## 6. Install Node(s)
## 7. Get Data from Node(s)
## 8. Get Data from Windows Nodes
## 9. Scan Vulnerabilities
## e. Check System Errors
## m. Check DB (SQL) Errors
## c. Clean System & DB Errors
## l. List Servers & Nodes
## s. View System Configuration
## x. View Executions List
## r. Log Running Executions (CTRL+C to exit)
## q. Quit Menu
##
#####
Select option: 
```

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.

inventory:servers [Inventor: x +]

https://epsms.eps.ua.es/wiki/doku.php?id=inventory%3aservers

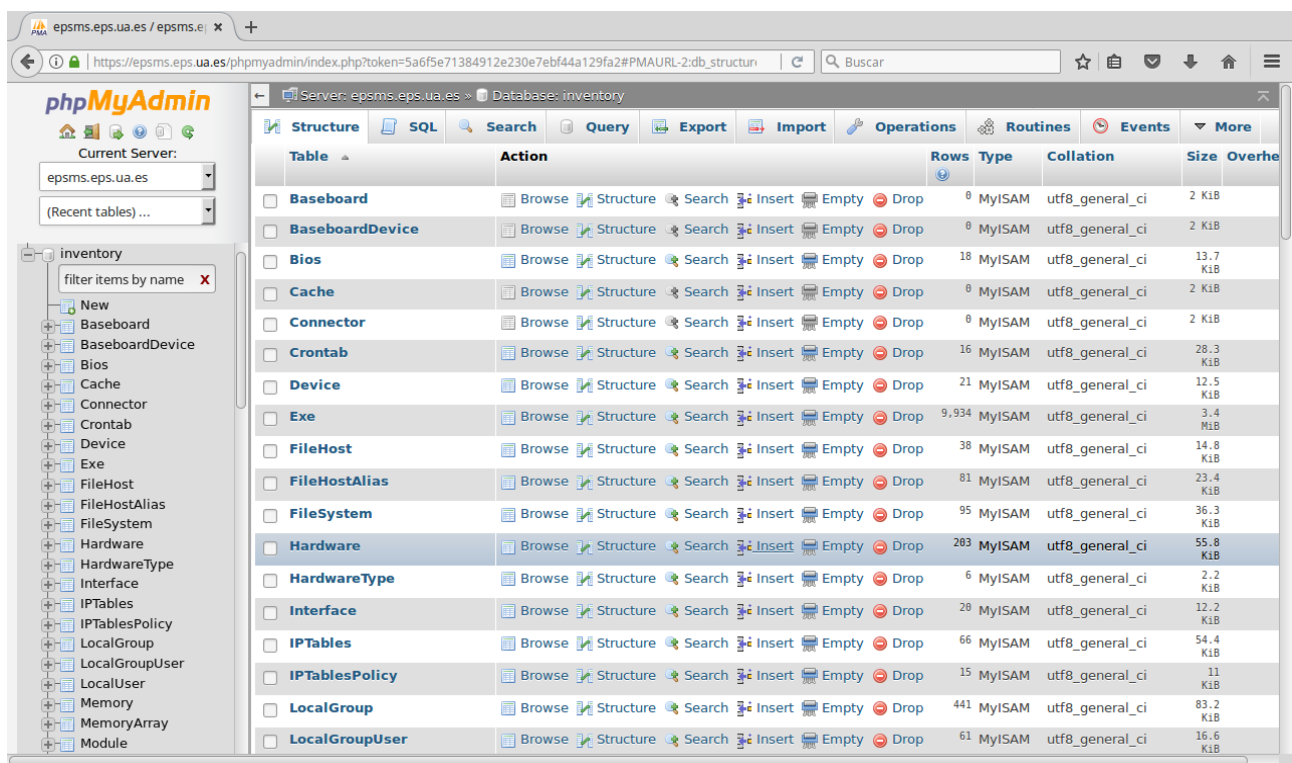
Buscar

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	+

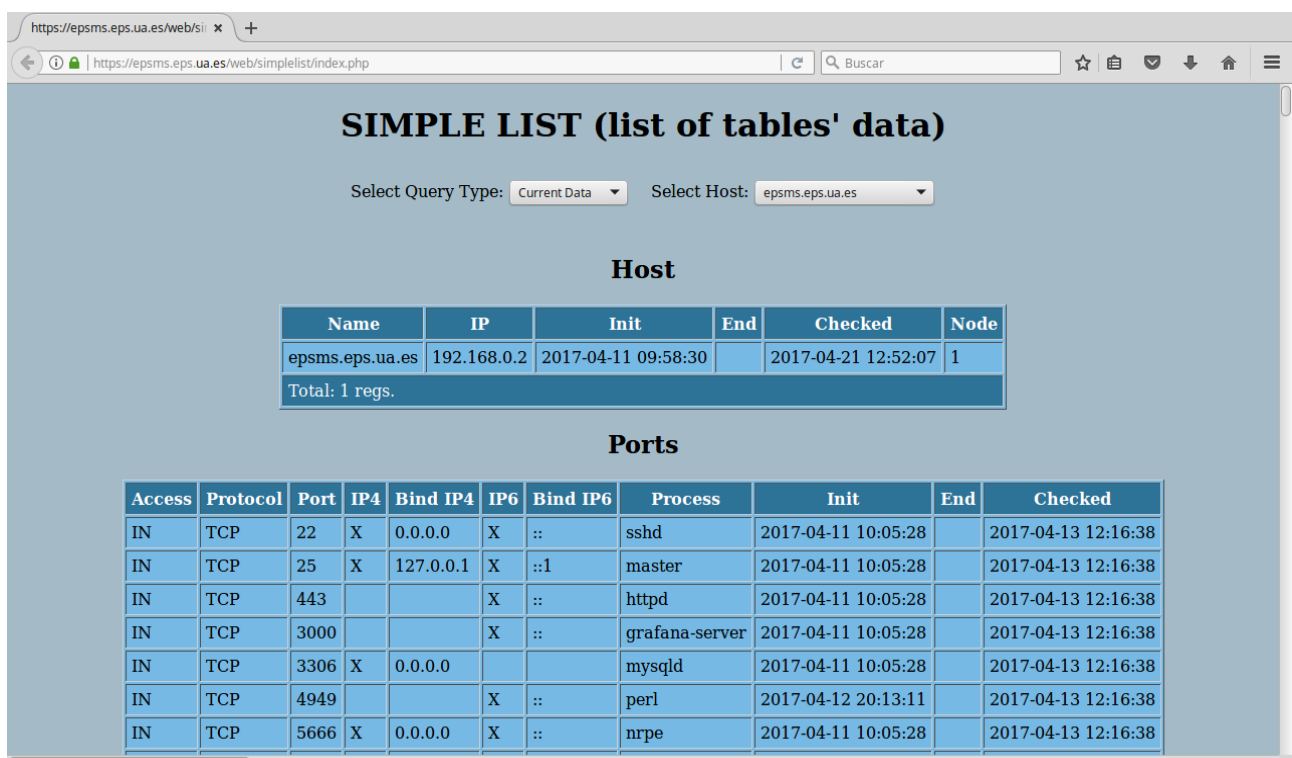
Dokuwiki

- 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)

<https://epsms.eps.ua.es/web/uj/>

UPDATES LIST (last events)

Select Time: Last day Select Host: All Hosts

Last Events (All Hosts)

Time	Host	Event
2017-04-21 16:46:51	win2008.epsms.eps.ua.es	New Openvas Scan (192.168.0.13): 2017-04-21 16:40:34 (CVSS 10.0 Severity High)
2017-04-21 16:40:19	ubuntu.epsms.eps.ua.es	New Openvas Scan (192.168.0.5): 2017-04-21 16:20:39 (CVSS 8.5 Severity High)
2017-04-21 16:20:23	solaris.epsms.eps.ua.es	New Openvas Scan (192.168.0.7): 2017-04-21 16:12:31 (CVSS 5.0 Severity Medium)
2017-04-21 16:12:21	openbsd.epsms.eps.ua.es	New Openvas Scan (192.168.0.12): 2017-04-21 16:05:30 (CVSS 8.5 Severity High)
2017-04-21 16:05:09	freebsd.epsms.eps.ua.es	New Openvas Scan (192.168.0.6): 2017-04-21 15:59:34 (CVSS 8.5 Severity High)
2017-04-21 15:59:24	fedora.epsms.eps.ua.es	New Openvas Scan (192.168.0.4): 2017-04-21 15:48:12 (CVSS 8.5 Severity High)
2017-04-21 15:48:02	epsms.eps.ua.es	New Openvas Scan (192.168.0.2): 2017-04-21 15:23:21 (CVSS 8.5 Severity High)
2017-04-21 15:23:11	debian.epsms.eps.ua.es	New Openvas Scan (192.168.0.3): 2017-04-21 15:11:52 (CVSS 8.5 Severity High)
2017-04-21 13:28:10	freebsd.epsms.eps.ua.es	New port (TCP/25): (IN) IP4/127.0.0.1 IP6/
2017-04-21 13:28:10	freebsd.epsms.eps.ua.es	Deleted port (TCP/5666): (IN) IP4/* IP6/*
2017-04-21 12:31:40	freebsd.epsms.eps.ua.es	New port (TCP/5666): (IN) IP4/* IP6/*
2017-04-21 12:31:40	freebsd.epsms.eps.ua.es	Deleted port (TCP/25): (IN) IP4/127.0.0.1 IP6/
2017-04-21 12:31:40	freebsd.epsms.eps.ua.es	Deleted port (TCP/5666): (IN) IP4/192.168.0.6 IP6/*

[illegible]

- The screenshot shows a web browser window with the address bar displaying 'https://epsms.eps.ua.es/web/rest/private/hardware'. The page has a title 'Hardware'. Below the title, there is a section 'Get Linux/Unix System information'. Under this section, it says 'GET /hardware/system'. The output is shown as 'Status: 200 OK' followed by a JSON array containing one object with various system properties. The browser interface includes back, forward, and search buttons, as well as a search bar with the text 'Buscar'.

- Greenbone Security Assistant

Logged in as Observer **epsms** | Logout

Mon May 1 19:30:28 2017 UTC

Scan Management Asset Management SecInfo Management Configuration Extras Help

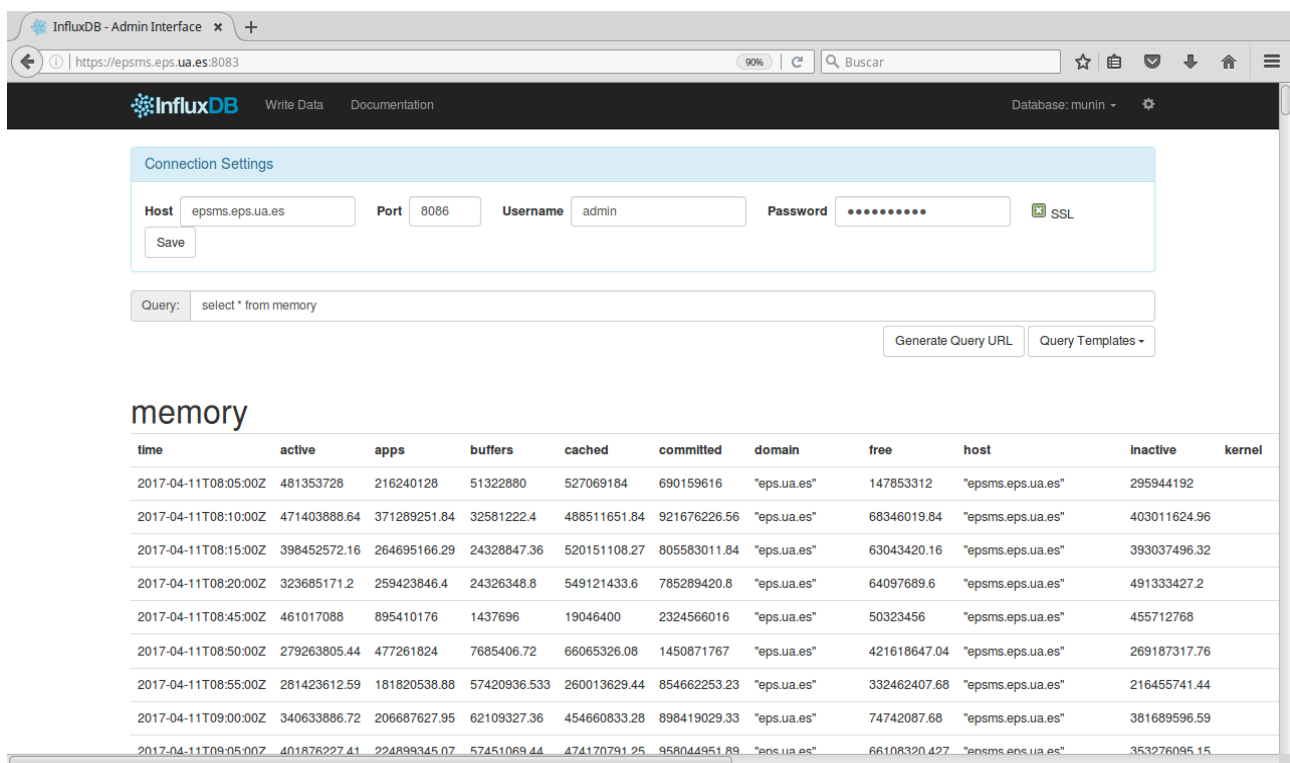
Tasks 1 - 15 of 24 (total: 24) vNo auto-refresh

Filter: apply_overrides=1 rows=15 permission=any owner=any first=1 sort=

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
arch.epsms.eps.ua.es	Done	1 (1)	Apr 25 2017	8.5 (High)		
arch.epsms.eps.ua.es	Done	1 (1)	May 1 2017	2.6 (Low)		
debian.epsms.eps.ua.es	Done	1 (1)	Apr 21 2017	8.5 (High)		
debian.epsms.eps.ua.es	Done	1 (1)	May 1 2017	8.5 (High)		
epsms.eps.ua.es	Done	1 (1)	Apr 21 2017	8.5 (High)		
epsms.eps.ua.es	Done	1 (1)	May 1 2017	8.5 (High)		
fedora.epsms.eps.ua.es	Done	1 (1)	Apr 21 2017	8.5 (High)		
fedora.epsms.eps.ua.es	Done	1 (1)	May 1 2017	8.5 (High)		
freebsd.epsms.eps.ua.es	Done	1 (1)	Apr 21 2017	8.5 (High)		
freebsd.epsms.eps.ua.es	Done	1 (1)	May 1 2017	8.5 (High)		
gentoo.epsms.eps.ua.es	Done	1 (1)	Apr 25 2017	8.5 (High)		
gentoo.epsms.eps.ua.es	Done	1 (1)	May 1 2017	8.5 (High)		
openbsd.epsms.eps.ua.es	Done	1 (1)	Apr 21 2017	8.5 (High)		
openbsd.epsms.eps.ua.es	Done	1 (1)	May 1 2017	8.5 (High)		
opensuse.epsms.eps.ua.es	Done	1 (1)	Apr 25 2017	8.5 (High)		

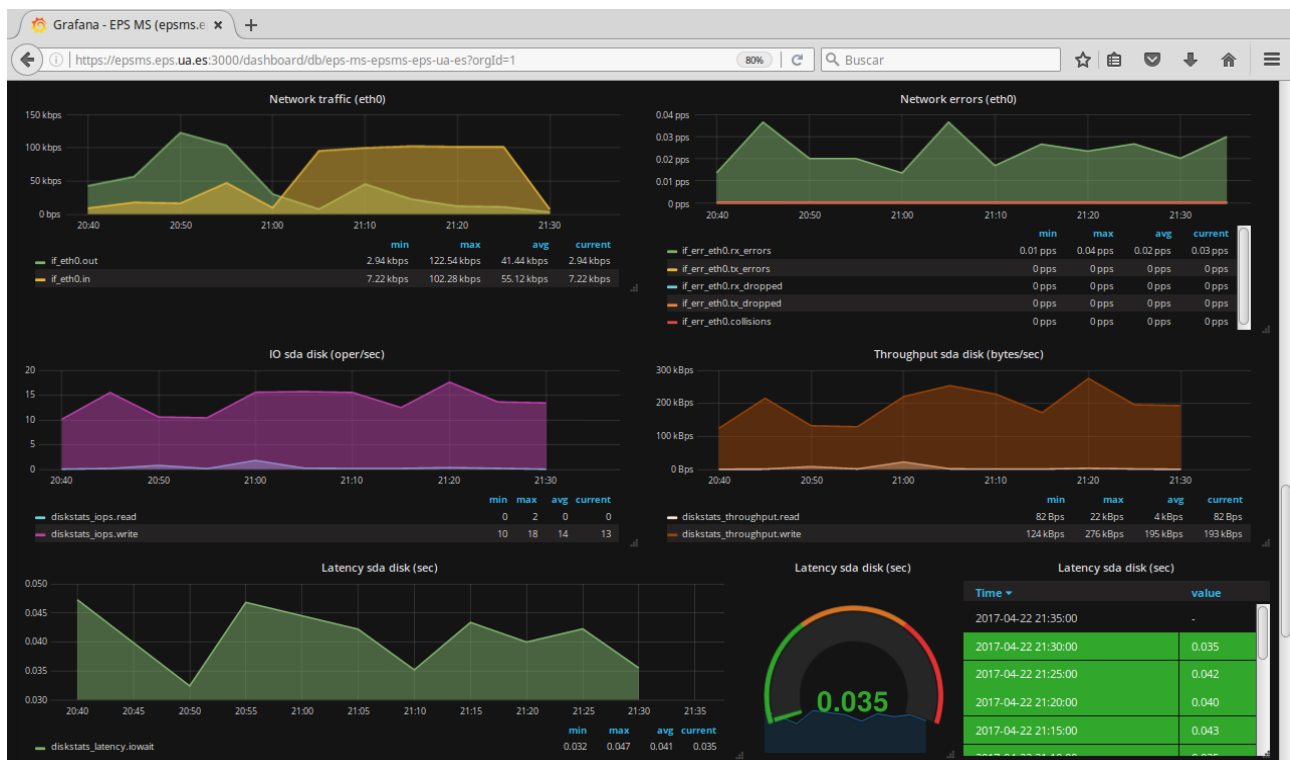
Openvas

- 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').

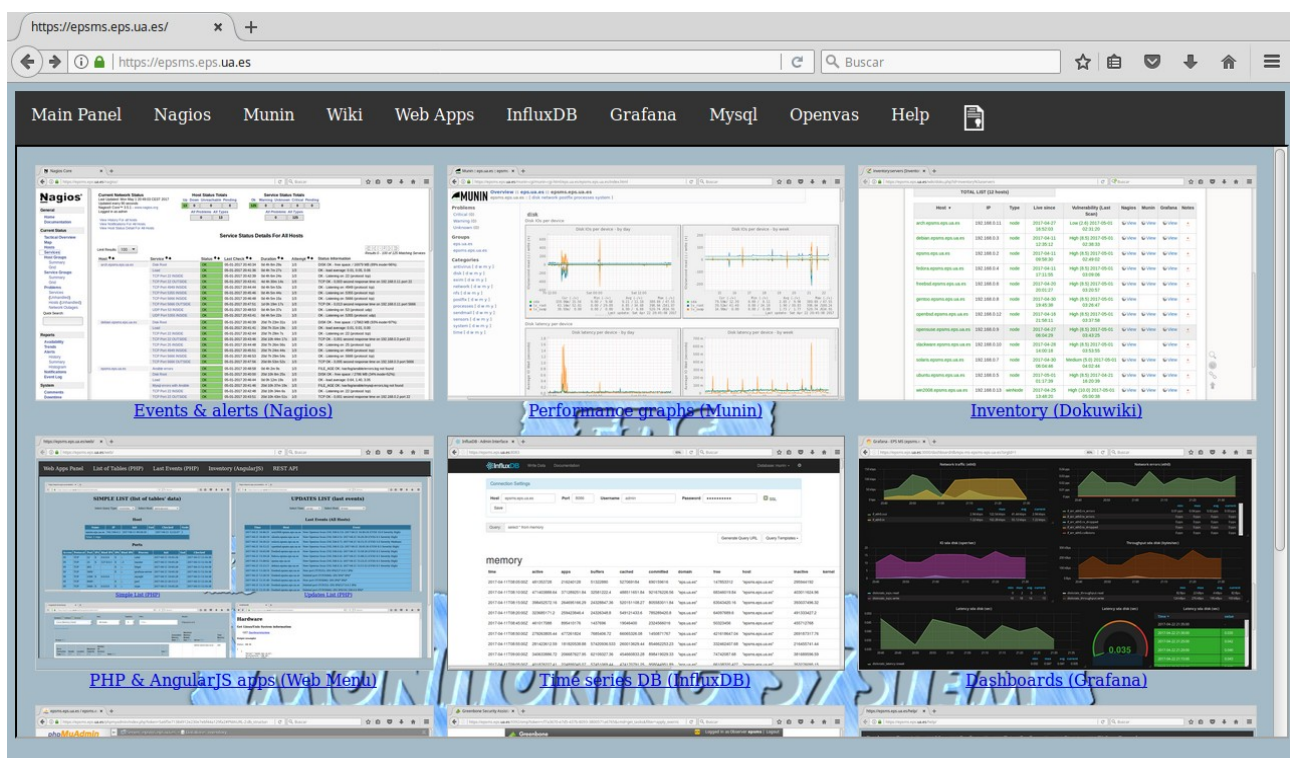
2. Execute '**install.py**' script to install 'EPS MS'.

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:

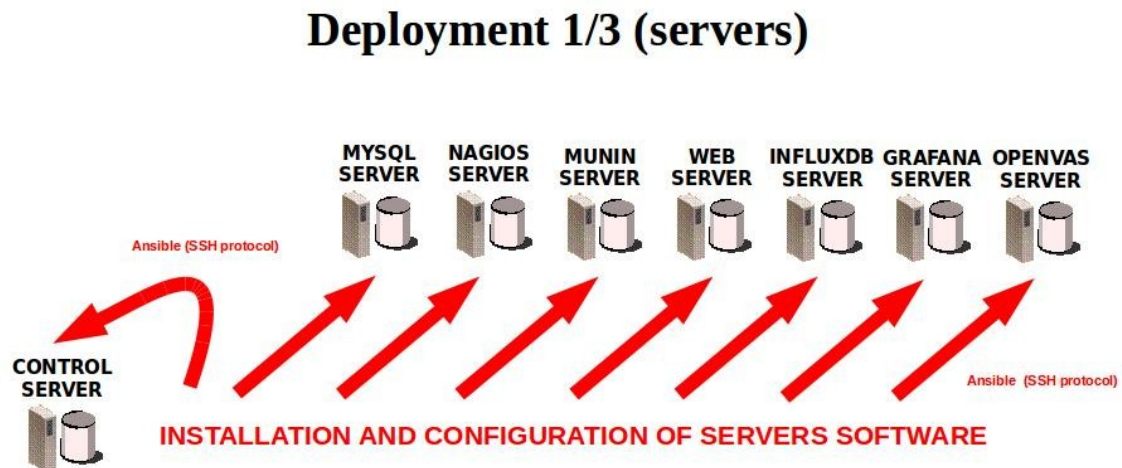
- User to connect to Linux/Unix hosts (connection by SSH without password, using public keys and sudo)
- User/password to connect to Windows hosts (connection by WMI 'Windows Management Instrumentation')
- IP addresses of Nagios, Munin, Mysql, Web (Dokuwiki, PhpMyAdmin and web Apps), Grafana and Openvas 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:

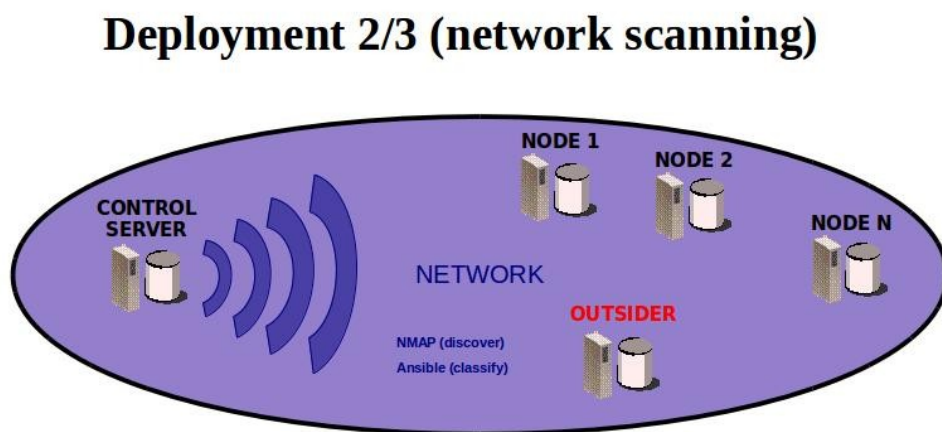


But, **how does it work** inside? These are the steps 'EPS MS' performs after configuration:

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



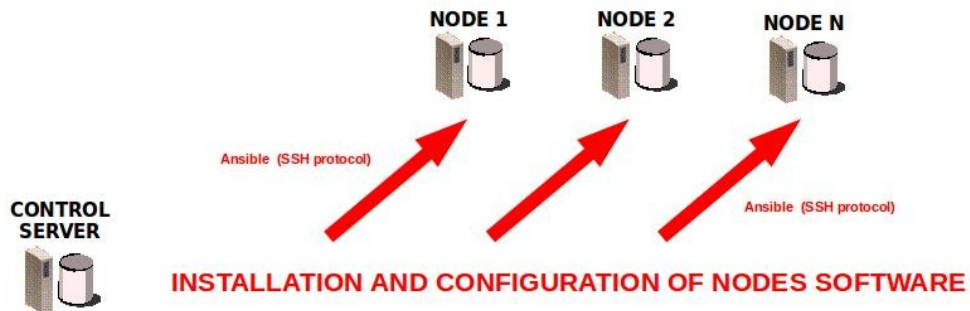
(A.2) Infrastructure deployment: **Network scanning** to discover '**nodes**' (hosts accessed by 'EPS MS') and '**outsiders**' (hosts not accessed).



NETWORK SCANNING TO DISCOVER NODES (EPSMS ACCESS) AND OUTSIDERS (NO ACCESS)

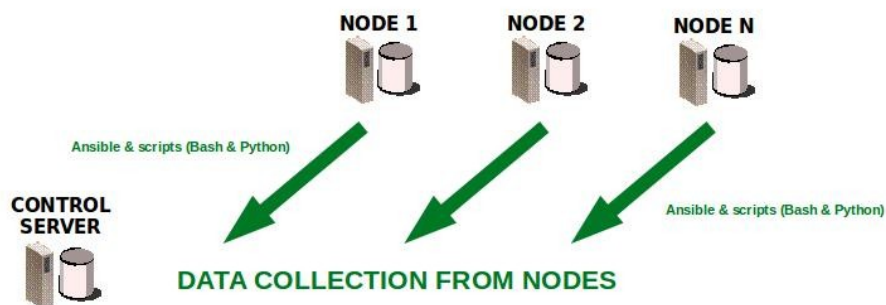
(A.3) Nodes deployment: **Installation and configuration of software in the nodes**

Deployment 3/3 (nodes)



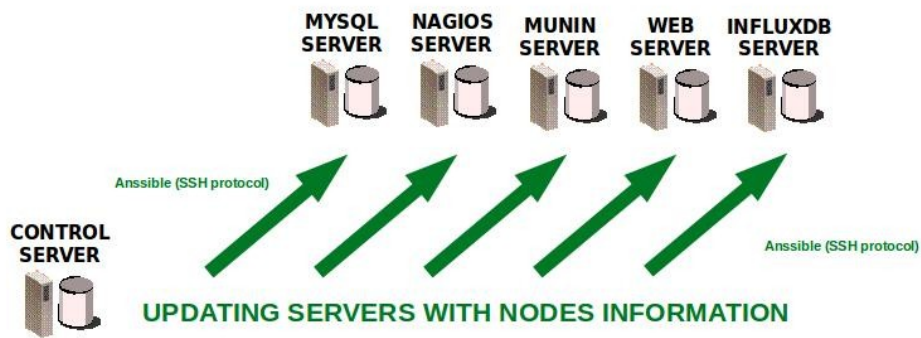
(B.1) Data collection: **Getting information from nodes**

Data Collection 1/2 (nodes information)



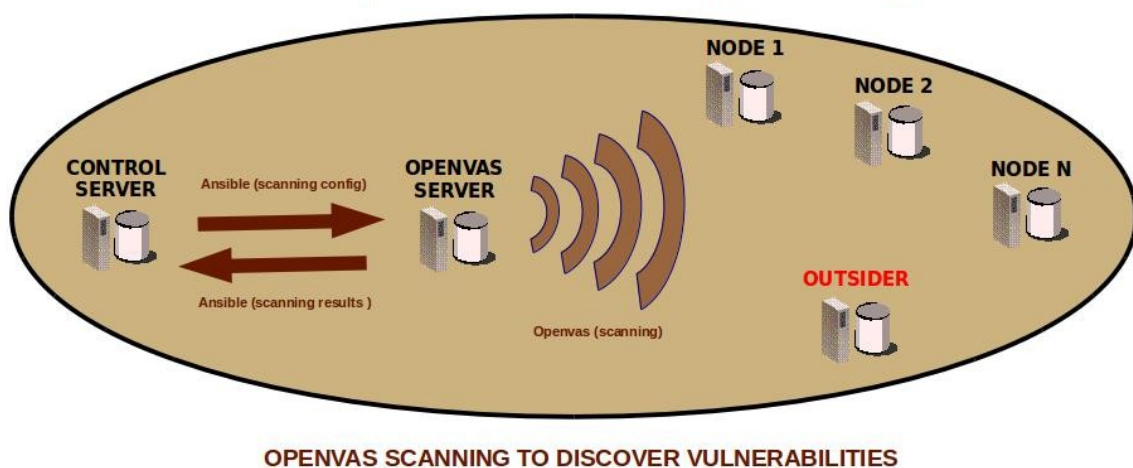
(B.2) Data collection: **Updating servers with information obtained from the nodes**

Data Collection 2/2 (updating servers)



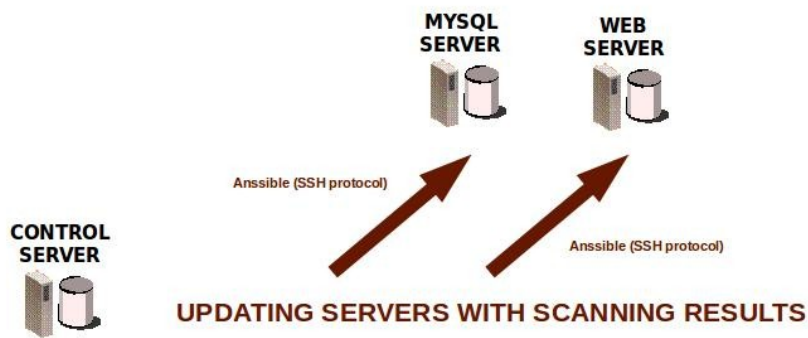
(C.1) Security Assessment: **Vulnerabilities scanning** of nodes and outsiders (with Openvas)

Security Assessment 1/2 (scanning)



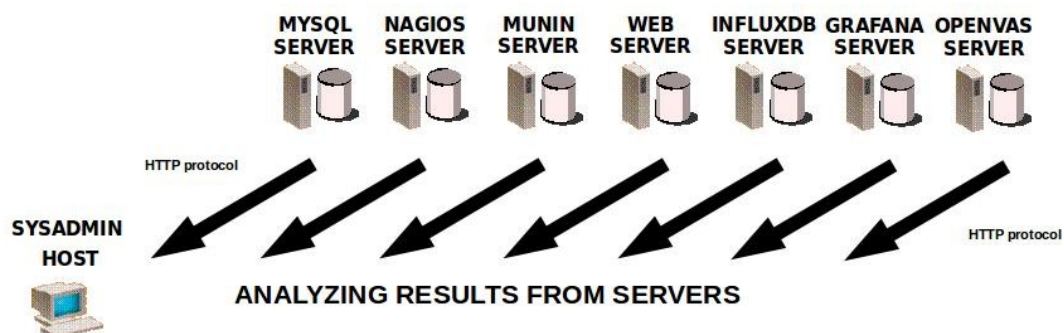
(C.2) Security assesment: **Updating servers with scanning results**

Security Assesment 2/2 (updating servers)

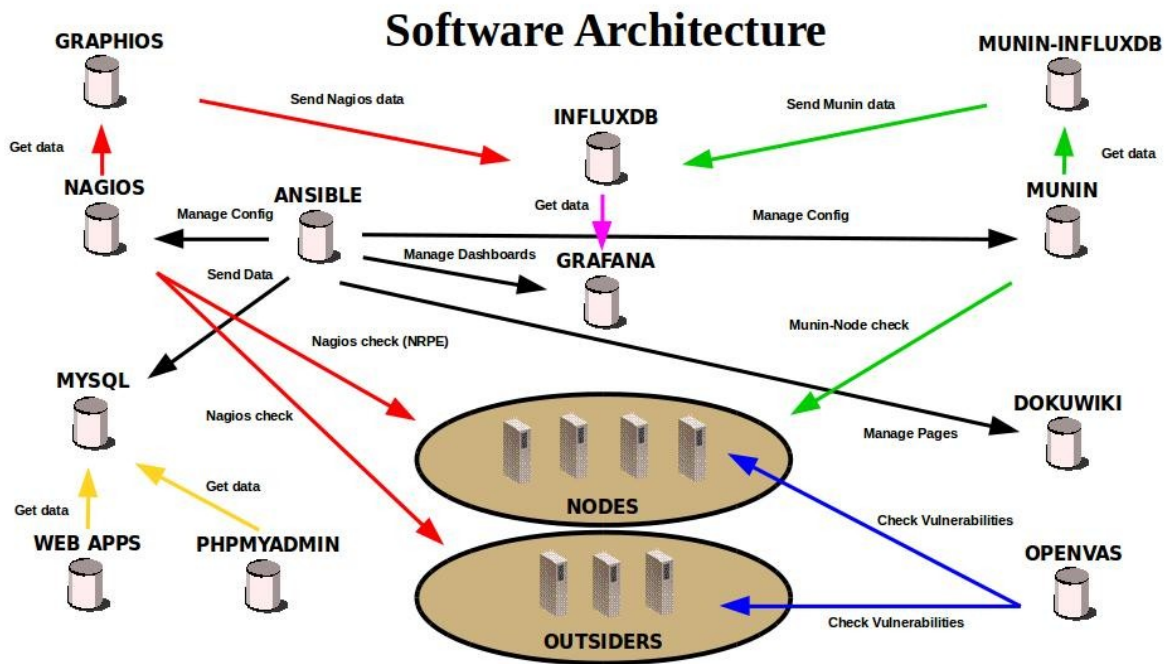


(D) **Analyzing results** stored in servers

Results Analysis



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

	<hr/> <p>Devices: Name, Model, Scheduler, Size, Vendor, Partitions For Every Partition: Name, Size</p> <hr/> <p>Network Interfaces: Name, Address, DNS Name, Network, NetMask, MAC, Type, Module, Active</p> <hr/> <p>Cache Memory: Handle, Socket Designation, Level, Enabled, Mode, Location, Installed Size, Maximum Size</p> <hr/> <p>Connectors: Handle, Internal Reference Designator, Internal Connector Type, External Reference Designator, External Connector Type, Port Type</p>
Hardware (Windows)	<p>System: Description, System Type, PC System Type, Manufacturer, Model, Infrared Supported, Wake-Up Type</p> <hr/> <p>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</p> <hr/> <p>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</p> <hr/> <p>BIOS: Name, Caption, Software Element ID, Software Element State, Target Operating System, Version, Build Number, Code Set, Current Language, Identification Code, Language Edition, Manufacturer, Primary BIOS, Characteristics For Every Characteristic: Char Code, Description</p> <hr/> <p>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</p> <hr/> <p>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</p> <hr/> <p>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</p>

	<p>Order, DNS Enabled for WINS Resolution, DNS Domain Search Order, IGMP Level, MAC Address, WINS Enable LMHosts Lookup, WINS Primary Server, WINS Secondary Server</p> <hr/> <p>Connectors: Tag, Connector Type, External Reference Designator, Internal Reference Designator, Port Type</p> <hr/> <p>Buses: Device ID, Caption, Bus Type, Bus Num, Availability, Config Manager Error Code</p>
Software (Linux/Unix)	<p>IP: Name, IP</p> <hr/> <p>Distribution: Distribution, Version</p> <hr/> <p>Kernel: Kernel</p> <hr/> <p>Modules: Name, File Name, Author, Description, License, Version, Version Magic, Source Version</p> <hr/> <p>Domain: Domain</p> <hr/> <p>DNS Resolver: Domain, NameServer 1, NameServer 2, NameServer 3, Options For Every Option: Option</p> <hr/> <p>'/etc/hosts' File: Rules</p> <hr/> <p>Routes: Destination, Gateway, Mask, Flags, Interfaces</p> <hr/> <p>Swap Memory: Swap</p> <hr/> <p>Virtualization: Virtualization Role, Virtualization Type</p> <hr/> <p>FileSystems: Name, Type, Mount, Options, Size</p>
Software (Windows)	<p>IP: Name, IP</p> <hr/> <p>Domain: Domain</p> <hr/> <p>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</p> <hr/> <p>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</p>

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