Pandora FMS feature map

PANDORAFMS
ENTERPRISE

Version 2 | 版二
www.version-2.com

Network monitoring features	
Traffic monitoring	Through sFlow, NetFlow or JFlow method.
Supports IPv4 and IPv6	Supports IP versions IPv4 and IPv6.
Traffic information detail	The information shows a history with a minimum granularity of one minute and a history of several years. The graphics zoom in and keep the highest level of detail.
Communication link performance	Monitoring network interfaces, bandwidth, consumption, maximum occupancy, availability, errors, discards, packet losses, real speed, etc.
Map and network diagram creation	Presentations in active network diagrams. These network diagrams will be updated automatically with the new network nodes, identifying new elements.
Discovered equipment features	Brand, model and firmware are automatically specified.
Equipment usage	CPU, memory, disk and communication equipment buffer usage.
Compatibility with SNMP	Compatibility with the SNMP and ICMP standard for obtaining information from devices, for versions 1, 2, 2c and 3.
Use of physical and logical ports	Open and in-use physical and logical ports are shown for routers and switches.
Log and event collection	Log collection parallel to monitoring. No megabyte limit. Log collection via syslog (remote) and local agents (Linux and Windows).
Relationship between network devices at network and link level	If the information is available, Pandora FMS is able to show the relationships at network level and the link level between the different ports of the routers / switches and the connected equipment.

Detection of active devices to monitor	Scans and generates monitoring information of physical and virtual equipment, servers, workstations, routers, switches, firewalls, band-width administrators, load balancers, access point and printers.
Application server performance	Verifies OAS, JBoss, Tomcat, WebSphere, GlassFish services and equivalents.
Remote connection to network equipment	Allows remote connection to communications equipment centrally in the solution itself, through SSH or Telnet.
Distribution of intermediate probes for information collection	Allows the use of intermediate probes to be able to monitor the network in a distributed way.
Possibility of high frequency polling	Rates network monitoring times at intervals of minimum frequency up to five seconds.
Custom remote queries	Allows the tool administrator to define their own complex (multi-step) remote checks based on dialogue / response over a TCP port.
Self-increase of test retries in case of failure	Increases checking attempts intervals in case of failure.
Scheduled monitoring	Schedules check-ups on specific dates and times.
WMI remote queries	Checks Windows computers remotely, using a WMI interface to add your own WML statements.
SSH Remote Queries	Queries Linux and Unix computers remotely, using remote commands on SSH.
SNMP trap receiving	Collects traps and alert assignments to these values. Collects numerical and / or alphanumeric values to enrich the alerts with data obtained from traps: critical system temperature, name of the down interface, filesystem alert, critical-state memory / CPU, etc.

Packet loss	Monitors network interface packet loss.
Real-time geographic maps (GIS)	Show the exact position of each device (GPS) and, if it is updated, that movement is shown on the map. You can save a movement history of each element and see it on the map.

Integrated reports	
BAM monitoring	Monitors business processes in real time in a single console (dashboard).
Reports	Report scheduling allows filtering information in time periods, reporting equipment failures (falls), warnings, displaying descriptive problem statistics and simple or combined graphs (multiseries).
SLA Reports	Daily, weekly and monthly SLA reports, in addition to global reports (by time periods).
Availability reports	Indicate, in a given period, the total number of tests performed, the success and failure percentages in that time for each test performed.
Top-N type custom reports	The operator can define a set of data that the application shows according to applied filters.
Planned stops and exclusion	Excludes from all types of reports the periods defined as maintenance windows.
Report templates	End users can easily create reports from templates defined by the administrator.
Sending scheduled reports	The administrator can define report scheduled sending by email (in PDF).

Graphic views	They allow the operator to create their own graphic panels where to include monitoring data: graphics, status icons and real-time values. These screens can relate to each other.
Real-time data	Graphs and reports show real-time data at all times, not pre-calculated data.
Information availability	Pandora FMS is managed in real time from a web application for modern standard browsers (Edge, Firefox, Safari, Chrome).
Information display	Information is presented centrally in a single interface, using graphics, screens, dashboards and information lists in different views.

Alert System	
Alarm generation and sending	Alarm generation and sending are available as on-screen alerts and allow immediate sending by text message to mobile phones or email.
Alarm filtering and scaling	Filters the alarm sending by maximum number of repetitions, minimum number of repetitions and consecutive failure concurrency.
Event auto-validation	Recovered events will allow auto-validation when the problem that triggered them is solved.
Manual corrective actions	Allows performing manual actions on the events using the information available to launch diagnostic tools, open incidents, add notes or leave the event in work mode.
Alarm correlation	Establishes sets of logical rules (AND, OR, NOT) that allow to refine alarms based on the events collected in the monitored systems.

Programmable alarm sending format	Alarm sending is user definable, so that it can be integrated with new platforms, such as Telegram, via API Rest
Sound warning console	Allows audible messages to be received by an operator, based on filters by origin and severity. This system is complementary to the others
Mobile application for receiving messages	Enables notice reception and their real-time checking for Android and iOS

Transactional WEB monitoring

Application and web server software	Scan and generate information on Java application (OAS-Oracle, JBoss-Redhat, WebLogic), IIS web servers and Apache monitoring.
Transactional monitoring and user experience	Verifies the proper operation of each step of an application from the user's point of view, being able to replicate each one, measuring success and total time.
Access via authentication	Checks application availability through user login and password.
Application traceability	Checks the availability of a request in the application following a navigation flow (trace); each independent request is monitored individually, in addition to the entire transaction.
Application availability	Scans application services to evaluate operation by URL and IP.
Transaction time breakdown	Breaks down in time periods each of the key transaction steps (server connection time, first iteration response time, application downloading time, etc).

Navigation with distributed probes	Remote web application monitoring is possible from different geographically distributed points, synchronized by a central manager.
Screenshots	Makes screenshots to use them as informs in case of failure and thus to analyze the problem as it looks like for a real user.

Database monitoring	
Commercial relational database engines supported	Supports Oracle, Sybase, Informix, DB2, Microsoft SQL Server, MySQL and PostgreSQL.
Commercial NoSQL database engines supported	Supports MongoDB, RavenDB, HBase and Cassandra engines.
Storage system monitoring	Hard disk physical storage, disk groups, tablespace -datafiles-.
Availability	Reports availability by opening and closing a connection and services at operating system level.
Transactions	Reports database locks, number of open sessions, number of open cursors.
Log relation of events and warning	Logs errors, warnings, user and session status, checks replication processes; updates data outside applications; generates and verifies backups.
CPU usage	Identify the database usage percentage on the server that contains it.
Cache usage	Shows cache usage by the database.
Total number of connections and their status	Shows connection real-time movement.

Job failures	Reports any errors in job execution.
Fragmentation	Identifies fragmentation level in data stores.
Backup errors	Generates manual and programmed alarms for failures in backup.
Custom SQL queries	Monitors the result of custom SQL (or equivalent) queries.

Monitoring Servers and Equipment

Agents	It has the local and remote agent feature, so that the equipment can be monitored in both ways, as appropriate.
Remote agent installation	Allows distributing and installing agents unattended from the administration console; Windows and Linux systems.
Automatic agent provision	Agents are configured when contacting for the first time the central server, and a configuration determined by a set of rules is applied.
Support to different platforms	In 32-bit and 64-bit architectures, information is obtained from Windows, Linux and Unix operating systems (Solaris, HP-UX, AIX), Mac OS X and BSD systems.
Server hardware operation	CPU, RAM, physical memory, virtual memory, cache and paging are monitored. Open processes, zombies, swap, access to the environment, etc.
Operation Information	Fans and internal temperature.
Storage	Availability, available space per partition and mounting points.

New storage system hot detection	Monitoring new mounting points automatically.
Network card	Availability and charging by network card.
Operating System and general configuration	Describes operating systems and equipment configuration.
Conditional monitoring	Allows monitoring based on whether certain criteria are met, evaluating it in each execution.
Local corrective actions	They run on agents, based on a given condition
Screen monitoring	Allows taking "screenshots" of the output of certain commands
Service and Process Watchdog	Allows restart in case of failure, and monitors it automatically (Windows).
Use of intermediate proxies to send information	If agents cannot contact the central server.
Local data collection in case of disconnection	The information will be stored locally if the network falls down, so that, when it can connect again with the central server, it sends the information for that period.
Execution of agents with users without privileges	So that they cannot access inside information.
Cluster monitoring	Valid for any manufacturer and any cluster model, A / P or A / A, and also for application or network clusters.
Remote Agent Configuration	Individually or collectively for configuration bulk changes.
Virtual environments	VMware, HypeErV, HPVM, RHEL VM, Nutanix, OpenNebula, IBM, HMC, LPAR, KVM and XenServer monitoring.

Environment monitoring	
UPS	Compatibility with the main manufacturers.
Air conditioning	History of use and air conditioning sensors, generation of reports and alarms.
Access control	Historical of access control to the computer center, generation of reports and alarms.
IoT / Sensors	Possibility of integration with different IoT systems through direct connection (SNMP) or Rest API.

Inventory	
Obtaining the inventory	Inventory is obtained both by remote network probes or agents.
Inventory systems	Network equipment (routers,switches), as well as Linux or Windows servers.
Network equipment remote configuration	Periodically collects remote configurations of network equipment and stores their different versions over time
Detection of inventory changes	Allows the operator to be notified in case of detecting changes from one inventory review to another.
Display of equipment configuration differences	Visually displays configuration changes on remote computers from which your configuration is collected as part of the inventory.
CPU	Collects information about CPUs.
VIdeo	Collects information about PC-installed video cards.
Hard drives	Collects information about computer-installed hard drives.

Partitions	Collects information about each of the partitions on each computer.
NIC	Collects information about installed network cards and drivers.
Patches	Collects information about computer-installed patches.
Software	Collects information about computer-installed software.
Processes	Collects information computer-running processes.
RAM	Collects information about computer-installed memory modules.
Users	Collects the number of administrator users or guests on each computer.

IP addressing management	
Automatic discovery	The tool has IP detection in a subnet, checking the response of each IP, resolving hostname and operating system.
IP Administration (IPAM)	The tool can configure, enable and disable each IP manually, add events in the IP, comments for each IP, reserve IPs and monitor dynamically the use of network IPs by network, subnet and supernet.
Customizing IP views	The tool can filter and view different IP groups.
Integrated IP with Microsoft DHCP Server management	The IPAM system can be integrated with the Microsoft server through local real-time data collection to refresh and update the status of IPs, including your reservation, lease and each IP lease time.

Subnet calculator compatible with IPv4 and IPV6	It allows the following data: network (address and bit mask), network mask, network wildcard, network address, broadcast address, first valid IP, last valid IP and network IP number.

Remote control

Computer Remote Desktop	Integrated into the software, without calling a third tool. Integrated in the interface. Compatible with Windows, Linux and Mac systems.
Remote shell	Integrated in the tool Interactive access by shell to Linux and Windows computers.
Copy of bidirectional files	Integrated in the main console of the tool, it allows the user to access the remote filesystem to download, delete and upload files from the PC.
Process and service control	Allows starting, stopping and restarting remote processes and services of the managed machine.

Issue manage ment

Creating manual tickets from an event or alert	Creates an issue associated with an event on an active problem to closely monitor the issue.
Creation / Update of automatic tickets	Creates tickets as an automatic response to a problem detected by monitoring.
Custom work workflow	Defines a life cycle for each ticket based on the creator, dates, criticality, work group, etc. This life cycle incorporates flow change notifications by email, automatic scaling and issue closure validation through external users.

Training and support	
Official training	Training in a standard way technicians on minimum indicated bases. Said training includes all usage levels and tool implementation.
Official certifications	Accreditation, by means of an official certification, certifying the knowledge of the technicians.
Online training platform	To make training easier, it has an online eLearning platform to learn about the tool and certifications.

Permission system and profiles	
Multitenant	With the same solution you can give service to different clients or groups without seeing each other.
Profiling system according to groups and accesses	Different users of the same group can perform different functions.
Internal audit	It reflects what operations each user has performed and when, including failed access attempts.
Password Policy	Allows forcing a policy of password change, with passwords of minimum length, special characters and history of old passwords.
Password Recovery System	A solution is provided so that the user can recover a forgotten password.
Authentication	It has its own system of users, profiles and roles, and supports Active Directory, LDAP and SAML.
Dual authentication system	Via Google Auth or equivalent, uses a mobile or external hardware device to perform a double authentication to enter the system.

Architecture	
Problem scaling system and root cause analysis	Allows analyzing the information based on the service as a whole, by grouping information. This makes the analysis of the problem root cause easier.
Automatic provisioning system	Distributes the load in case of new node registrations on the corresponding servers, or by load or custom rules.
Long-term data storage	It is able to keep all data history at full resolution for at least three years.
Communication via standard ports	Communication between the different components of the architecture is done through official ports, listed by the IANA.
Isolated environment monitoring	A system is provided by which an isolated network can be monitored through a component that does not have direct connectivity to the central monitoring infrastructure.
Backup	Includes an integrated backup system
Policies	Creates monitoring, correlation and inventory policies. These policies can be applied by specific groups or users, so that similar machine sets can be managed easily, quickly and evenly.
Single console	A single console is available, regardless of the final scaling of the implementation. The same user will work for all the tool features (network, applications, logs, reports) without logging in to different screens.
Horizontal scalability	There is an unlimited chance of growth by adding new servers.
High availability	HA is integrated in the solution. All system components support high availability without requiring external elements.

Distributed elements	Allows each element of the architecture to be in physical locations (different servers).
API/CLI	Provides REST API and command line tools to manage the solution.
Open SQL Database	The data model of the entire platform is open and documented, in order to use external queries to retrieve data.
Rebranding	Allows total product rebranding, hiding the name of the manufacturer, the name of the product and changing colors and icons by the administrator.
Licensing	It is licensed based on the total number of devices, regardless of the total number of metrics collected on each device.

Version 2 | 版一
www.version-2.com
Hong Kong | Taiwan | Singapore | Macau | Mainland China

Hong Kong & Macau
Tel : (852) 2893 8860
Email : sales@version-2.com.hk

Taiwan
Tel : (886) 02 7722 6899
Email : sales@version-2.com.tw

Singapore & Malaysia
Tel : (65) 6296 4268
Email : sales@version-2.com.sg