

MONITIS INTERNAL MONITORING AGENT: SECURITY AND PERFORMANCE

Monitis provides an internal server and network monitoring agent that can check the health of servers, networks and applications within and outside of the customer's firewalls, and deliver the monitoring results in real-time to the Monitis Main Server, to be further displayed via the web-based dashboard and to trigger warnings and critical alerts. This whitepaper provides brief overview around the architecture of Monitis agents and discusses their

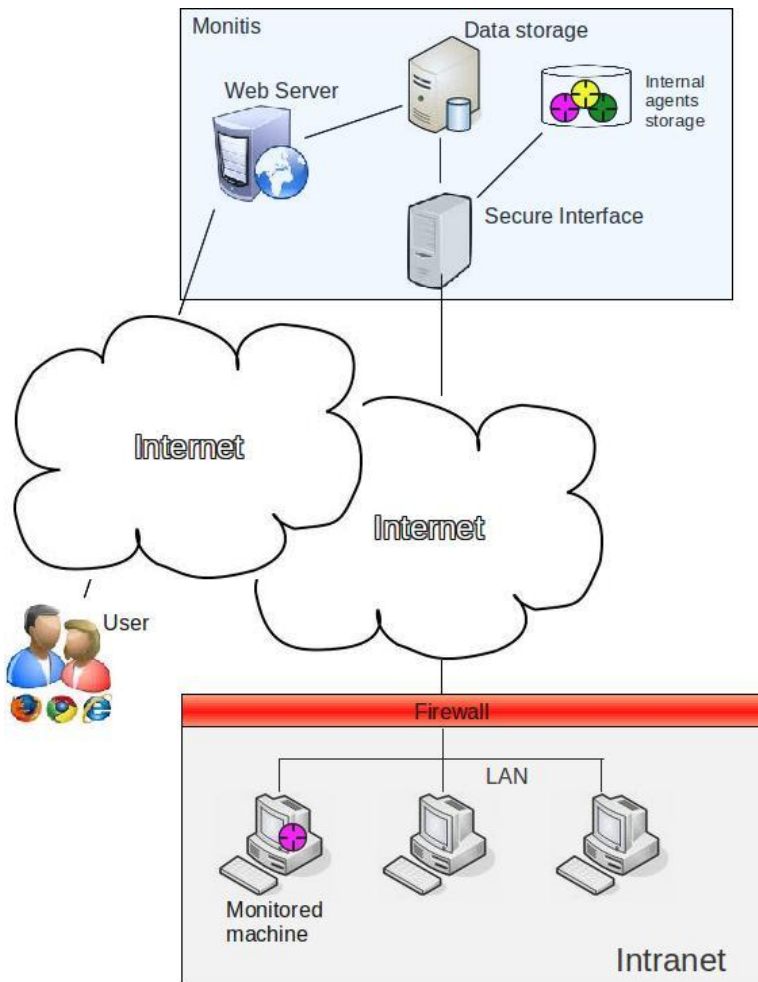
security, performance and bandwidth utilization.

Monitis provides downloadable agents for Windows, Linux and Solaris operating systems.

User may install just one agent within each local network and use it to monitor other servers agentlessly or/and may deploy an agent per each monitored host/machine. After deployment of the agents, users configure monitors for agents centrally from the Monitis dashboard. The agent will periodically run the user-configured checks and will transmit accumulated information to the Monitis Main Server using the HTTPs protocol. The usage of HTTPs is important as there is no need to open additional ports on the firewalls.

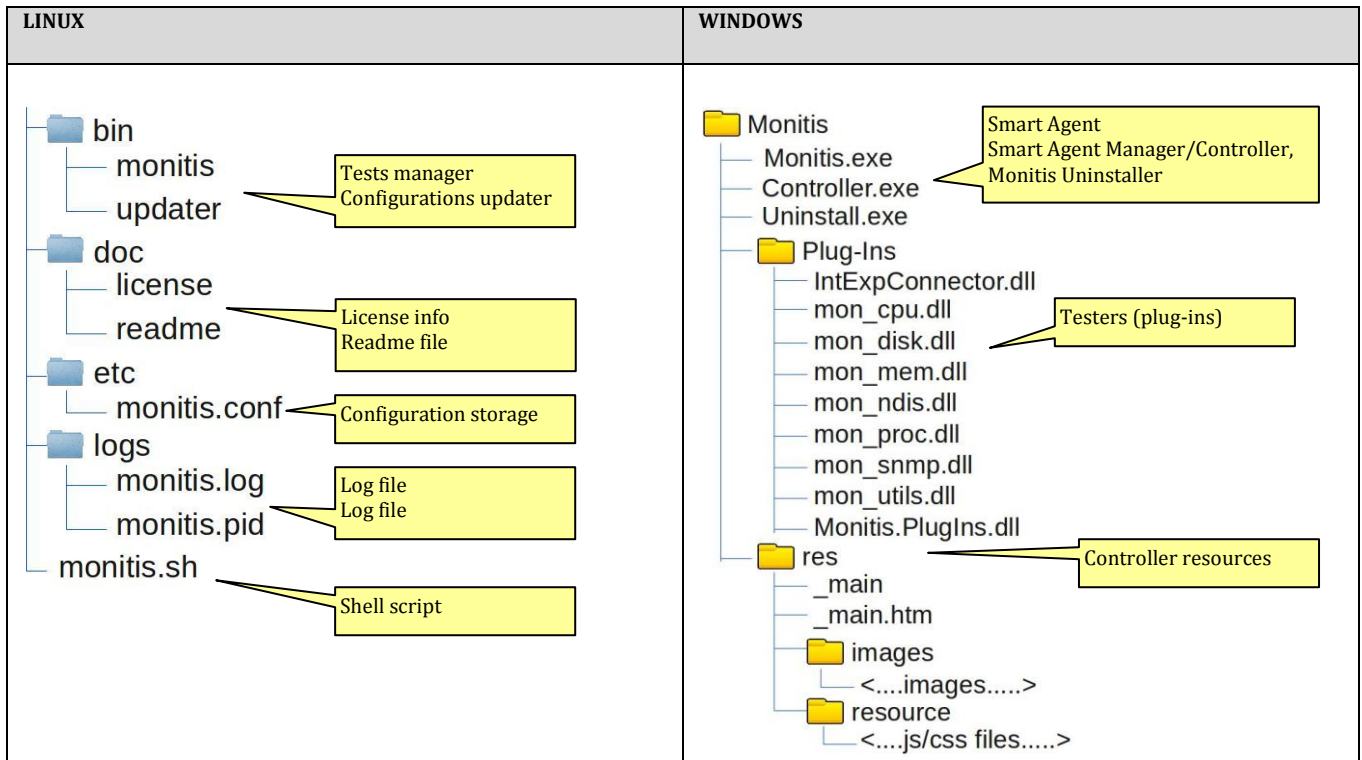
Agents are using the Monitis API which is well documented and publicly available. Advanced users (e.g. devops, people who both operate servers and also do program) can use the API to enhance and even build their own agents from scratch.

The global communication of the internal agent with the Main Server can be depicted as in the following diagram.



The agent may run as a daemon and execute each specific check module through internal threads. They were programmed in native C++ for low footprint.

After installation it should have the following files structure



The Linux version executable module (Tests manager) has only the command line interface as depicted below

```

monitis [-C configuration file] [-L log file] [-l lock file] [-D home directory] [-U user e-mail] [-A agent name]
[-V] [-h]
where:
-h, --help                Print detailed help screen
-V, --version             Print version information
-C, --conf-file=ADDRESS   Configuration file address ( default: /etc/monitis.conf )
-L, --log-file=ADDRESS    Log file address
-l, --lock-file=ADDRESS   Lock file address
-D, --home-dir=ADDRESS    Home directory address
-E, --user-email=E-MAIL   E-Mail address
-A, --agent-name=NAMA     Agent name
  
```

Depending on which testers are used, the Linux Internal agent may use some of the following libraries:

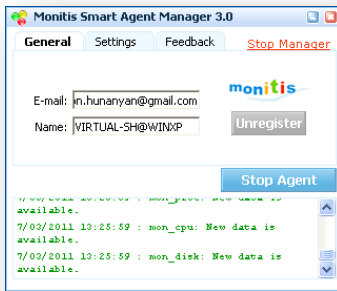
```
linux-gate.so, libpthread.so, libdl.so, libc.so, libz.so, libmysqlclient.so, libssl.so or libcrypto.0.9.8e, libsnmp.so
```

Of course, some of these are optional and can be skipped in case the corresponding test types will not be used. It is necessary to split the required and optional ones. For example libcrypto is required for the agent to start, but libmysqlclient is not.

Monitis also provides a simpler way of controlling the agent by using shell script (monitis.sh) depicted below:

```
monitis.sh {conf|start|stop|restart|status|show|log}

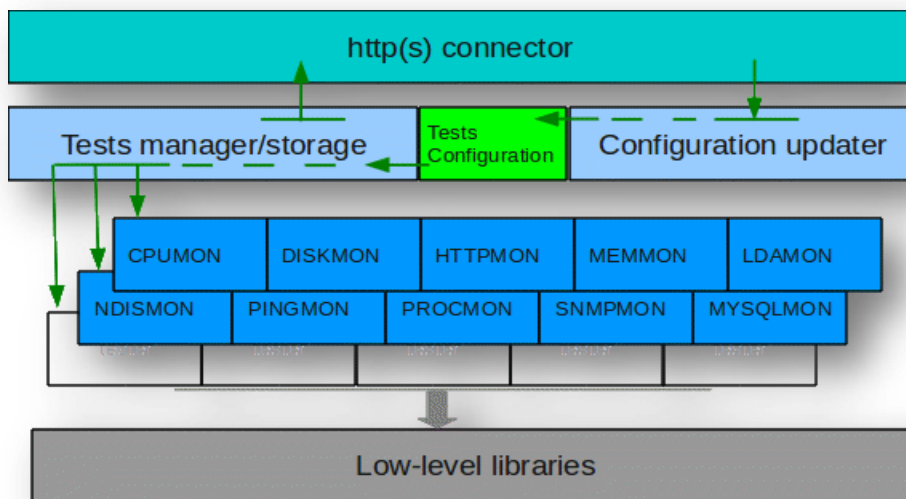
where:
conf      run configuration wizard
start     start monitis
stop      stop monitis
restart   stop if running and start again
status    show monitis current status
show      show main configuration
log       open log file with 'tail -f'. (default value: 100)
```



Monitis provides for Windows users a graphical interface. The Monitis Smart Agent Manager allows users to register/unregister an agent, start an agent as a Windows service or simple application, and provide the visual log. It also has the feedback functionality that allows users to send comments and feedback to Monitis.

INTERNAL AGENT ARCHITECTURE

The Monitis internal architecture is depicted in the following diagram



- HTTP(S) connector serves for communication with the Monitis Main Server.
- The Configuration Updater sends periodically the request to the main server for tests configuration changes and stores tests configuration internally.
- Test manager activates the chosen testers (from tests configuration) and collects testing data on the required interval (scheduled by the Main Server). The activated testers perform the necessary tests by using required resources/libraries and send back the test information. Below are descriptions for the existing testers:

TESTER	DESCRIPTION	USED RESOURCES	COMMENTS
CPUMON	Monitoring the CPU(s) load/utilization for user (applications level), kernel (system level), nice (applications with nice priority), idle (unutilized CPU(s) part), iowait (CPU(s) idle during I/O request)	/proc/stat	
DISKMON	Monitoring the free and used disk(s) space		
HTTPMON	Monitoring the applications/sites by using HTTP(S) connection	libssl.so library	Can be used for intranet and extranet services/sites monitoring from intranet.
MEMMON	Monitoring the free memory and swap sizes.	/proc/meminfo	Notice that for remote memory parameters uses "snmptable.so" library
LDAMON	Monitoring the average system load over a period of time (1, 5 and/or 15-minute periods)	/proc/loadavg	Linux only
MYSQLMON	Monitoring MySQL database health status	libmysqlclient.so library	
NDISMON	Monitoring network traffic by using NDIS possibility		
PINGMON	Monitoring for intranet and extranet hosts by using PING protocol		ICMPMON in Windows
PROCMON	Monitoring the chosen process CPU utilization, memory and swap sizes usage.	/proc/%ProcID%/stat /proc/%ProcID%/cpu	
SNMPMON	Monitoring host by using host-embedded SNMP engine.	libsnmp.so library	
OSINFMON	Monitoring Operating system structure		Windows only
EVENTLOGMON	Monitoring System Events log info		Windows only

THE BENCHMARK TEST

The simple benchmark test was fulfilled having a goal to checking how the Linux internal agents use the system resources. The sample test was done on a low-profile Desktop machine with the following parameters:

LINUX	WINDOWS
<ul style="list-style-type: none"> • CPU Intel Pentium Dual Core 2.4GHz • RAM 2048 MB • OS Linux-Ubuntu 11.04 (natty) • Kernel 2.6.35-25 • NET Ethernet 100Base-T (100Mbps) 	<ul style="list-style-type: none"> • CPU Intel Pentium Dual Core 2.4GHz • RAM 1024 MB • OS WinXP SP3 • NET Ethernet 100Base-T (100Mbps)

The following tests were set: average load (LDAMON), CPU utilization (CPUMON), free memory check (MEMMON) and monitoring for the Monitis internal agent process itself (PROCMON). In addition, the special test tools named "nethogs_0.7.0" (on Linux machine)

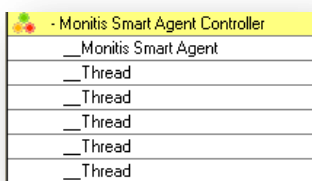
```
sudo nethogs -t -d5 | grep monitis
```

and "NetLimits_3.0" (on Windows machine) were used internally to test the bandwidth generated by the agent. Please notice that some other applications were active on the monitored machine too (Firefox browser, Skype messenger, Text editor, terminal, etc.)

On the Linux machine the Monitis agent runs as a daemon and calls the updater and testers as a LWP process (thread)

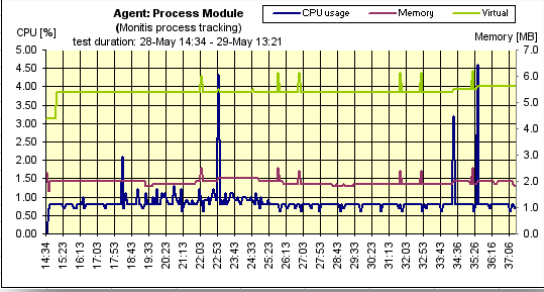
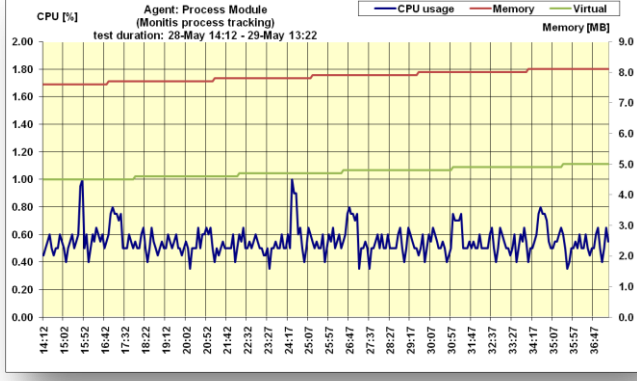
PID	PPID	LWP	C	PRI	NI	ADDR	SZ	WCHAN	TTY	TIME	CMD
3768	1	-	1	-	-	-	1115	-	?	00:00:11	monitis
-	-	3768	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3770	0	80	0	-	-	hrtime	-	00:00:00	-
-	-	3772	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3773	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3774	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3775	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3776	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3777	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3778	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3779	0	80	0	-	-	futex_	-	00:00:00	-
-	-	3780	1	80	0	-	-	futex_	-	00:00:11	-

On the Windows machine the Monitis agent is activated as a simple application and therefore the chosen testers run as Windows threads.



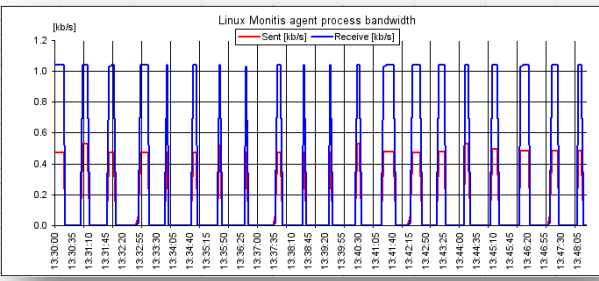
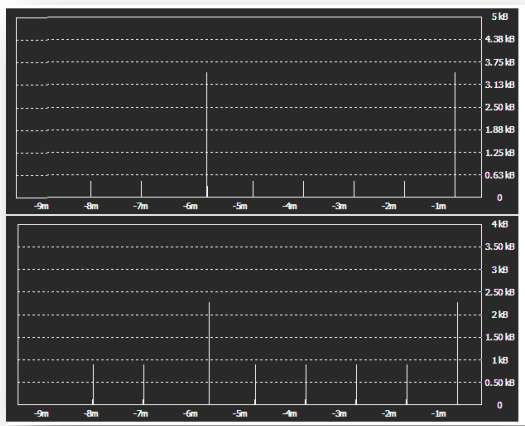
INTERNAL AGENT RESOURCES UTILIZATION

Generally speaking, the Monitis internal agent uses negligible resources on the monitored machine.

LINUX	WINDOWS
 <p>The internal Linux agent produces less than 0.8% of CPU load; occupying about 1.4MB RAM and 4 MB Virtual memory.</p>	 <p>The internal Windows agent produces less than 0.1% of CPU load; occupying about 8MB RAM and 5MB Virtual memory.</p>

INTERNAL AGENT BANDWIDTH UTILIZATION

Generally, the internal agent uses internet connection quite economically – it is predefined that the internal agent requests the main server for current tests configuration every 1 minute and sends the accumulated test information every 5 minutes.

LINUX	WINDOWS
 <p>The “nethogs” Linux tool measures the bandwidth of any process in real time. The simple calculation of average bandwidth shows that the received average bandwidth is near 0.25 kb/s and the sent bandwidth near 0.15 kb/s.</p> <p>The average amount of received/sent data is about 112KB/hour and 67 KB/hour correspondingly.</p>	 <p>The “NetLimits” Windows tool provides the network tracking per processes only (not bandwidth). So, the amount of measured sent data is about 96 KB/hour and receives about 92 KB/hour. Therefore, the necessary bandwidth is near 0.22 kb/s for download and 0.2 kb/s for upload.</p>

THE INTERNAL AGENT'S SECURITY

The Monitis agent provides standard security by using the following:

- Encrypted HTTPs protocol used for the connection with main server.
- Client initiated encrypted HTTP also eliminated altering firewalls, thus reducing risk for possible attacks.
- Heartbeat checks performed to ensure that agents are alive and connected with the Main Server.
- The tests configuration and necessary parameters are kept on the main server and sent periodically to the client by using an encrypted channel. The client stores the current configuration internally in the memory (not in the file).
- Monitis warrants that the internal client does nothing other than testing and therefore cannot cause unpredictable damage of a system.
- Monitis performs daily and weekly backups, including backups to storage outside of the Main Server's data center.

SUMMARY

Thus, it can be assured that the internal agent

- produces very low network traffic
- low CPU footprint
- utilizes tiny RAM and Virtual memory
- doesn't compromise a system's security

ABOUT MONITIS

Monitis believes that the Cloud is the biggest thing to happen in IT management since IT management. Having seen this vision early, Monitis is now the global leader in developing this market. It is the first affordable network and systems monitoring solution based 100% in the Cloud. Besides Monitis' enthusiastic and loyal user base of 70,000 customers from small businesses to Fortune 500 companies to government agencies and educational institutions, Monitis has won rave reviews from the technology analyst community, such as "Most Innovative Start-Up" from The 451 Group, a listing in OnDemand 100, a ranking by Morgan Stanley, KPMG, and AlwaysOn, of 100 top private companies globally.

Monitis was founded in 2005 by a team of seasoned IT developers fed-up and tired of the limits of software-based tools, while inspired by the promise of the Cloud. Headquartered in San Jose, CA, Monitis's team of IT professionals has extensive experience running enterprise-grade IT businesses, as well as starting and selling several IT start-ups. Monitis employs a global workforce and enjoys a robust average month-on-month revenue growth of over 10%.

For more information, contact:

Monitis Inc.
Sales & Marketing Department
sales@monitis.com
<http://www.monitis.com>
US & Canada Toll Free: +1-800-657-7949