



ServerAgent User Guide

July 20, 2007

© 2007 AlertSite. All rights reserved. AlertSite is a trademark of Boca Internet Technologies, Inc. This publication and features described herein are subject to change without notice. AlertSite assumes no responsibility for errors or omissions. All other products, services and company names mentioned herein may be trademarks of their respective owners.

Boca Internet Technologies, Inc
4611 Johnson Road, Suite 6
Telephone: (954) 312-0188 Fax: (954) 312-0186
www.alertsite.com



I. What is ServerAgent?	3
II. What are the current features?	3
III. What are the benefits?	3
IV. What platforms are supported?	4
V. What are the possible status codes from ServerAgent?	4
VI. Where can I download ServerAgent?	4
VII. How does it work?	4
VIII. How is ServerAgent installed?	4
IX. Configuring ServerAgent to monitor user defined scripts	6
X. How does ServerAgent communicate with AlertSite?	8
XI. How to confirm that ServerAgent is working?	9
XII. Monitoring a process & ServerAgent config file	11
XIII. Testing Connections & ServerAgent config file	11
XIV. Enabling Alerts	12
XV. ServerAgent screenshots	12
XVI. Troubleshooting	17
XVII. ServerAgent Metrics	18



I. What is ServerAgent?

ServerAgent is AlertSite's server monitoring agent. It can reside on a Windows or Unix server and collect system health statistics reporting them back to the AlertSite monitoring service on a 5 or 15 minute interval. Thresholds can be set for both warning and error conditions supporting instant notification through all AlertSite notification mechanisms.

http://www.alertsite.com/systems_monitoring.shtml

II. What are the current features?

ServerAgent will collect, report and alert on system health and connectivity:

- CPU load average (5 min. average)
- Disk utilization for all logical drives
- Memory use
- Monitor for the presence of processes
- User defined monitoring

Warning and error thresholds can be defined for any value ServerAgent is monitoring.

Notifications are sent when any monitored items breach an error threshold or the server has not reported in.

- In order for notification for a monitored item to be activated, the Notify and Enabled checkboxes for that item must be checked in the edit server screen.

Current status is reported in the AlertSite monitoring console and historical status and results can be reported in the Report Center.

Daily, weekly and monthly email summaries.

Most configuration can be managed remotely through the AlertSite console.

III. What are the benefits?

Track system resource utilization.

Capture data for capacity planning.

Fully integrated into AlertSite's notification system.

- Instant notification via email, pager, SMS and telephone.
- Flexible alerting and escalation policies.

When combined with AlertSite's website and web transaction monitoring, ServerAgent can help you quickly identify and resolve system problems.



IV. What platforms are supported?

Windows 2000 and above.
Unix – Linux, BSD, and Solaris.

V. What are the possible status codes from ServerAgent?

- 4050 – server not responding
- 4040 – error threshold exceeded
- 4030 – warning threshold exceeded

VI. Where can I download ServerAgent?

http://www.alertsite.com/download_sa.shtml

The windows version is currently available for download to anyone.

The Unix version is currently provided as a source code installation package. It is available from the Control Panel Download page for all registered customers. For information on a ServerAgent trial, please contact customercare@alertsite.com.

VII. How does it work?

- 1) you pre-register the device assigning it a name you like on our server and we assign a 32 id for it.
- 2) you take this id, install the client-side software, and start talking to us (sending the id).
- 3) on the server side we map the id to the device and record your data.

VIII. How is ServerAgent installed?

Installation instructions for Windows

Installation directory: C:\Program Files\Nemo

- 1) You need to "Add a new server" from the AlertSite Edit Server web page.
This will generate the 32 character Server ID you will need at the completion of installation.
Save this ID in a convenient place, you will need to enter it to complete installation.

- 2) Download the ServerAgent Installation program - NemoInstaller.exe

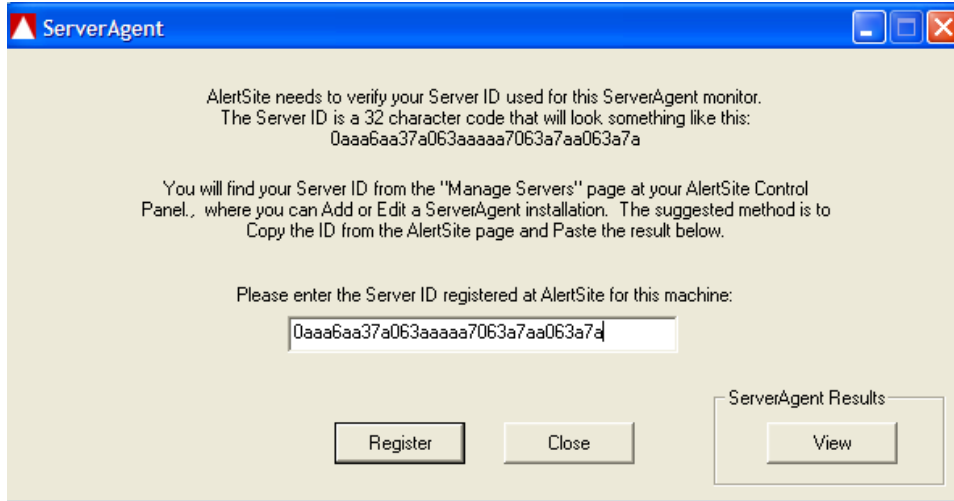
- 3) Run the downloaded installer

This will place the ServerAgent package in C:\Program Files\Nemo

- 4) Upon completion you will be asked to reboot your computer.



5) When the system restarts you will be presented a dialog box asking for the Server ID generated in step 1. Enter that value and select "Register".



This will add some additional fields to the Nemo.ini file.

You're done ! Shortly you should see information related to your new server displayed on the AlertSite web-site !

NOTE: The registration screen shown in step 5 can be started at any time by selecting "AlertSite / Register ServerAgent" from your Windows Start Menu.

Installation instructions for Unix

Installation directory: /usr/local/nemo

- 1) You need to "Add a new server" from the AlertSite Edit Server web page. This will generate the 32 character id you will need at the completion of installation.
- 2) Download the ServerAgent Installation package - nemo-1.7.85.tar.gz
- 3) Execute the following commands

```
tar -xvzf nemo-1.7.85.tar.gz
cd nemo-1.7.85
./configure
make
make install
```

The last step will place the ServerAgent package in /usr/local/nemo

Boca Internet Technologies, Inc
4611 Johnson Road, Suite 6
Telephone: (954) 312-0188 Fax: (954) 312-0186
www.alertsite.com



4) Go to `/usr/local/nemo/share` and edit `alertsite.rc`

The first line should read `"serverid="`

Place the 32 character id you generated in step 1 after the equal sign and save the file.

5) Go to `/usr/local/nemo/bin`.

execute `./nemo init`

This will add some additional fields to the `alertsite.rc`.

6) Now execute `./nemo` (no parameters this time)

You're done ! Shortly you should see information related to your new server displayed on the AlertSite web-site !

IX. Configuring ServerAgent to monitor user defined scripts

AlertSite's ServerAgent can monitor processes, CPU, and basic disk utilization natively. Many customers, however, want to integrate resource or environment specific monitoring with ServerAgent.

This is done by adding user defined monitoring scripts to ServerAgent.

Almost any executable script, cmd file or program that outputs a single integral value to standard out can be integrated into ServerAgent.

How it works

ServerAgent will scan for any user scripts at startup. It will attempt to run each script found on each monitoring pass (typically every minute).

It will read the first line of output generated by the script, expecting an integral value, and use that value to test for error/warning conditions configured in your AlertSite account.

Any other text produced by the script will be saved as additional information for your own use. For example, if you had a script that searched for error conditions in your system log files, you could add the actual error messages as output to the script after the numeric value used to indicate the error/warning condition.

Installing scripts

On Windows

- place the script in `c:\Program Files\Nemo\monitor\user`

(if the folder doesn't exist, create it)

- stop and restart the ServerAgent service using the services manager



On Unix

- place the script in /usr/local/nemo/bin/user
- kill and restart the ServerAgent process

Sample scripts

Sample Windows .cmd file that checks for the presence of a file.

```
----- testfile.cmd -----  
@ECHO OFF  
IF EXIST c:\tmp.txt (  
echo 1  
) ELSE (  
echo 0  
)  
-----
```

NOTE: If using a .bat or .cmd file and echo is used to generate output for ServerAgent, be sure to provide '@' character prior to echo keyword.

Sample Unix shell script that checks for the presence of a file.

```
----- chkfile.sh -----  
#!/bin/sh  
# returns "1" if a file exists  
  
if [ -e /tmp/somefile.txt ]  
then  
    echo "1"  
fi  
-----
```

Limiting User scripts with the Config file

Under normal conditions, the ServerAgent on your machine will run your user scripts approximately once per minute. Data is sent to AlertSite based on your ServerAgent plan, usually at 5 or 15 minute intervals. If, however, an error threshold is raised on your machine, that is transmitted immediately to AlertSite so you can be notified. After an error has been reported, no more data is sent to AlertSite until the next 5 or 15 minute interval.

There could be reasons why you want to limit how often a particular script runs on your machine, including:

1. It is very CPU intensive and you would like use it less often.
2. It monitors data that does not change very often, such as making sure a daily transaction occurred.
3. You want to make sure every transaction is captured by the AlertSite system for reporting purposes. In this case, you would want to run the script only on your particular 5 or 15 minute interval to make sure all the data is transmitted to AlertSite.



In all the above cases, you can add a line for "script_limits" into the ServerAgent configuration file (either Window's C:\Program Files\Nemo\Nemo.ini or Unix's /usr/local/nemo/share/alertsite.rc). This line can contain a list of scripts followed by a plus sign and the number of reporting intervals, each separated by semi-colon.

For example, consider that you have a 15 minute ServerAgent interval and want to limit "programA.bat" to run only on the actual 15 minute interval. You also have a "programB.bat" that you want to run once per hour (that is, every 4th interval). All other scripts will be run on the standard schedule. You can place the following line into your configuration file, and then restart the ServerAgent on your machine:

```
script_limits=programA.bat+1;programB.bat+4;
```

X.How does ServerAgent communicate with AlertSite?

The client software opens an outgoing socket to our server on port 4891.

Both the client side check-in packet and the server side response are (not encrypted) ascii packets. Here's a sample for one of our servers... As you can see we are not passing around any information that needs to be encrypted.

```
:: Incoming from client
Thu Apr 1 14:29:53 2004
<REPORT><Function>MONITOR</Function><ServerID>dbcae24c103443144d69b81a4d3c665a</ServerID><ClientVersion>1.0</ClientVersion><Hostname>GODZ</Hostname><Threshold>0</Threshold><CPU_USAGE><LOAD_AVERAGE>2</LOAD_AVERAGE></CPU_USAGE><DISK_INFO><DRIVE_C_USAGE>31</DRIVE_C_USAGE></DISK_INFO><PROCESS></PROCESS></REPORT>
```

```
:: outgoing from server
```

```
Thu Apr 1 14:29:54 2004 sending:
STATUS=0&VERSION=1.0&MINUTE=28&IPCTL=heat|oriole|bears|
spy030&INTERVAL=15&SEED=13&THRESHOLDS=0&
```

This is a "typical" handshake with a Windows client. The Unix client differs slightly. (after reboot) , the client sends along some configuration information which we record in our db. here's an example of that packet.

```
Tue Feb 17 20:07:18 2004
<REPORT><Function>CONFIGURATION</Function><ClientVersion>1.0</ClientVersion><ServerID>dbcae24c103443144d69b81a4d3c665a</ServerID><Hostname>GODZ</Hostname><Threshold>0</Threshold><GENERIC_INFO><Computer_Name>GODZ</Computer_Name><Hostname>GODZ</Hostname><Version>Windows
2000/XP</Version></GENERIC_INFO><NETWORK_INFO><Ip_Address>192.168.0.8</Ip_Address></NETWORK_INFO><PROCESSOR_INFO><Number_Processors>1</Number_Processors><Processor_Type>586</Processor_Type><Processor_Level>15</Processor_Level><MHZ>1992</MHZ><Identifier>x86
Family 15 Model 2 Stepping 4</Identifier><Processor_Name_String>
Intel(R) Pentium(R) 4 CPU
2.00GHz</Processor_Name_String><Update_Status>0</Update_Status><Vendor_Identifier>GenuineIntel</Vendor_Identifier></PROCESSOR_INFO></REPORT>
```



XI. How to confirm that ServerAgent is working?

After the final step of the installation process for Windows, where the server ID is entered and the send request button is pressed, a SUCCESSFUL message will be returned if the agent was able to communicate back to the AlertSite service. **Within a few minutes status icons should appear in the status console for that monitored server.**

Log files

ServerAgent currently keeps a 7 day rolling history of log files.

Naming convention Nemo.YYYYMMDD.

Location:

- Windows: c:\Program Files\Nemo\logs
- Unix: /usr/local/nemo/bin/logs/

A **successfully** functioning ServerAgent will have entries in the logfile that show each monitoring module that was loaded and successful communication with one of the AlertSite monitoring servers.

*** this section is ServerAgent starting up and loading each necessary module ***

```
04/01/2004 10:31:49 entering monitor collection loop
04/01/2004 10:31:49 Attempting load of C:\PROGRA~1\Nemo\monitor\CpuUsage.dll
04/01/2004 10:31:50 Setting up CpuUsage.dll
04/01/2004 10:31:50 Attempting load of C:\PROGRA~1\Nemo\monitor/DiskUsage.dll
04/01/2004 10:31:50 Setting up DiskUsage.dll
04/01/2004 10:31:50 Attempting load of C:\PROGRA~1\Nemo\monitor/TaskUsage.dll
04/01/2004 10:31:50 Setting up TaskUsage.dll
04/01/2004 10:31:50 entering config collection loop
04/01/2004 10:31:50 Attempting load of C:\PROGRA~1\Nemo\config/GenericConfig.dll
04/01/2004 10:31:50 Setting up GenericConfig.dll
04/01/2004 10:31:50 Attempting load of C:\PROGRA~1\Nemo\config/NetworkConfig.dll
04/01/2004 10:31:50 Setting up NetworkConfig.dll
04/01/2004 10:31:50 Attempting load of C:\PROGRA~1\Nemo\config/ProcessorConfig.dll
04/01/2004 10:31:50 Setting up ProcessorConfig.dll
04/01/2004 10:32:50 No serverid specified
04/01/2004 10:33:29 Going to server for id
04/01/2004 10:33:29 Header
POST /cgi-bin/Nemo HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
```

*** this section is the initial connect to AlertSite ***

```
04/01/2004 10:33:29 Connecting to the server... www.alertsite.com : 80
04/01/2004 10:33:31 Socket: 360 - Sending packet...(POST /cgi-bin/Nemo HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 157
```

*** the request to Add the server ***

```
XML=%3cREQUEST%3e%3cServerID%3ef9de5e20760da06ca8f74f16378101cd%3cServerID%3e%3cHostname%3eT
ODD%3c/Hostname%3e%3cThreshold%3e0%3c/Threshold%3e%3c/REQUEST%3e)
```



04/01/2004 10:33:31 Reading response...
04/01/2004 10:33:32 Got 207 chars:'HTTP/1.1 200 OK
Date: Thu, 01 Apr 2004 15:31:22 GMT
Server: Apache/1.3.29 Ben-SSL/1.53 (Unix) PHP/4.3.4
Connection: close
Content-Type: text/html

STATUS=0&IP=cowboy.alertsite.com&SEED=14&INTERVAL=15&

04/01/2004 10:33:50 Connecting to the server... cowboy.alertsite.com : 4891
04/01/2004 10:33:52 Socket: 360 - Sending
packet...(XML=%3cREPORT%3e%3cFunction%3eCONFIGURATION%3c/Function%3e%3cClientVersion%3e1.0%3c/ClientVersion%3e%3cServerID%3ef9de5e20760da06ca8f74f16378101cd%3c/ServerID%3e%3cHostname%3eTODD%3c/Hostname%3e%3cThreshold%3e0%3c/Threshold%3e%3cGENERIC%5fINFO%3e%3cComputer%5fName%3eTODD%3c/Computer%5fName%3e%3cHostname%3eTODD%3c/Hostname%3e%3cVersion%3eWindows+2000/XP%3c/Version%3e%3c/GENERIC%5fINFO%3e%3cNETWORK%5fINFO%3e%3cIp%5fAddress%3e192.168.0.7%3c/Ip%5fAddress%3e%3c/NETWORK%5fINFO%3e%3cPROCESSOR%5fINFO%3e%3cNumber%5fProcessors%3e1%3c/Number%5fProcessors%3e%3cProcessor%5fType%3e586%3c/Processor%5fType%3e%3cProcessor%5fLevel%3e15%3c/Processor%5fLevel%3e%3cMHz%3e1594%3c/MHz%3e%3cIdentifier%3ex86+Family+15+Model+1+Stepping+2%3c/Identifier%3e%3cProcessor%5fName%5fString%3e+++++Intel%28R%29+Pentium%28R%29+4+CPU+1.60GHz%3c/Processor%5fName%5fString%3e%3cUpdate%5fStatus%3e0%3c/Update%5fStatus%3e%3cVendor%5fIdentifier%3eGenuineIntel%3c/Vendor%5fIdentifier%3e%3c/PROCESSOR%5fINFO%3e%3c/REPORT%3e

04/01/2004 10:33:52 Reading response...
04/01/2004 10:33:53 Got 79 chars:'STATUS=3&VERSION=1.0&MINUTE=30&IPCTL=heat|oriole|bears|spy030&INTERVAL=&SEED=&

04/01/2004 10:33:54 Result buffer:
<REPORT><Function>MONITOR</Function><ServerID>f9de5e20760da06ca8f74f16378101cd</ServerID><ClientVersion>1.0</ClientVersion><Hostname>TODD</Hostname><Threshold>0</Threshold><CPU_USAGE><LOAD_AVERAGE>0</LOAD_AVERAGE></CPU_USAGE><DISK_INFO><DRIVE_C_USAGE>82</DRIVE_C_USAGE></DISK_INFO><PROCESS></PROCESS></REPORT>

04/01/2004 10:33:54 Connecting to the server... cowboy.alertsite.com : 4891
04/01/2004 10:33:55 Socket: 712 - Sending
packet...(XML=%3cREPORT%3e%3cFunction%3eMONITOR%3c/Function%3e%3cServerID%3ef9de5e20760da06ca8f74f16378101cd%3c/ServerID%3e%3cClientVersion%3e1.0%3c/ClientVersion%3e%3cHostname%3eTODD%3c/Hostname%3e%3cThreshold%3e0%3c/Threshold%3e%3cCPU%5fUSAGE%3e%3cLOAD%5fAVERAGE%3e0%3c/LOAD%5fAVERAGE%3e%3c/CPU%5fUSAGE%3e%3cDISK%5fINFO%3e%3cDRIVE%5fC%5fUSAGE%3e82%3c/DRIVE%5fC%5fUSAGE%3e%3c/DISK%5fINFO%3e%3cPROCESS%3e%3c/PROCESS%3e%3c/REPORT%3e

04/01/2004 10:33:55 Reading response...
04/01/2004 10:33:56 Got 79 chars:'STATUS=3&VERSION=1.0&MINUTE=30&IPCTL=heat|oriole|bears|spy030&INTERVAL=&SEED=&

Here are a sample of some **errors** from a customer's logfile:



```
04/01/2004 00:08:08 Connecting to the server... bears.alertsite.com : 4891
04/01/2004 00:08:09 ERROR: Connection refused
04/01/2004 00:09:07 Connecting to the server... bears.alertsite.com : 4891
04/01/2004 00:09:08 ERROR: Connection refused
04/01/2004 00:10:07 Connecting to the server... bears.alertsite.com : 4891
04/01/2004 00:10:08 ERROR: Connection refused
```

XII. Monitoring a process & ServerAgent config file

To configure ServerAgent to monitor that a process is up and running:

On Windows:

1) Edit the .ini file and add a line like the one below where proc1 is the name of the process as seen in task manager.

```
processes=proc1;proc2;proc3
```

ini file location c:\Program Files\Nemo\Nemo.ini

2) Start and stop the ServerAgent service using service manager.

On Unix:

1) Edit the .rc file and add a line like the one below where proc1 is the name of the process as viewed by ps.

```
processes=proc1;proc2;proc3
```

rc file location /usr/local/nemo/share/alertsite.rc

2) Start and stop ServerAgent.

XIII. Testing Connections & ServerAgent config file

To configure ServerAgent to monitor that a port connection can be made, you can edit the configuration file (Windows c:\Program Files\Nemo\Nemo.ini; Unix /usr/local/nemo/share/alertsite.rc) and add or change the value of "connect" in this format: "host name or ip address 'colon' port number 'semicolon'. For example, the following line would test connections to www.alertsite.com using port 80 and IP address 123.45.67.890 using port 1900:

```
connect=www.alertsite.com:80;123.45.67.890:1900;
```

- 1) Stop ServerAgent
- 2) Edit the connect statement
- 3) Start ServerAgent



XIV. Enabling Alerts

The Notify and Enabled checkboxes for the monitored items must be checked in order to receive alerts for any monitored item. These are found in the when editing any of the monitored servers.

XV. ServerAgent screenshots

The screenshot shows the AlertSite Network Monitoring Console interface. The main content area displays several tables of monitored items:

Site Name	IP Address / Port	Type	Monitor Interval	Monitor	Last Status	Last Checked	Last RespTime (secs)	Errors Last 24 Hrs (cnt/hh:mm)
BankOfAmerica	171.161.161.173	Secure Web Site	60	Enabled	0	2005-04-06 18:51:10	3.2273	
SLA Monitor	65.243.218.11	Secure Web Site	5	Enabled	0	2005-04-06 19:10:07	4.4870	
web server	216.131.127.206	Web Site	5	Enabled	0	2005-04-06 19:08:05	2.8316	

Transaction Name	Monitor Interval	Monitor	Last Status	Last Checked	Last RespTime (secs)	Errors Last 24 Hrs (cnt/hh:mm)
Browse AlertSite	60	Enabled	0	2005-04-06 18:48:03	0.9593	

Server Name	Cpu	Disk	Reporting Interval	Monitor	Last Status	Last Checked	Errors Last 24 Hrs (cnt/hh:mm)
Server1	▲	▲	15	Enabled	0	2005-04-06 19:09:00	1/19:39

Below the server table, there is a section for Security Devices:

Security Devices

No Security Devices found Use the [Security Devices](#) panel to add new Security Devices

The server named "Server1" currently has ServerAgent running on it.



Clicking on CPU status icon displays:

The screenshot shows a Mozilla browser window titled "Server Status - Mozilla". The page header includes the AlertSite logo and the text "The Web Site Monitoring Company" with a "Back to AlertSite" button. A "Close Window" link is visible in the top right. The main content area displays the following information:

Category	Cpu
Reporting Location	Dallas, Texas
Last Check-In	2004-03-19 15:44:44

Item	Current Value	Monitored Value	Status
LOAD_AVERAGE	2		0

Clicking on Disk displays:

The screenshot shows a Mozilla browser window titled "Server Status - Mozilla". The page header includes the AlertSite logo and the text "The Web Site Monitoring Company" with a "Back to AlertSite" button. A "Close Window" link is visible in the top right. The main content area displays the following information:

Category	Disk
Reporting Location	Dallas, Texas
Last Check-In	2004-03-19 15:44:44

Item	Current Value	Monitored Value	Status
DRIVE_C_USAGE	30		0



Clicking on Process yields:

Category	Process		
Reporting Location	Dallas, Texas		
Last Check-In	2004-03-24 14:38:32		
Item	Current Value	Monitored Value	Status
act.exe	1		0
ppcgrpno3.exe	1	1/1	0
PPCGRPov8.exe	1	1/1	0
PPCPro2002.exe	1	1/1	0
PPCPro2002no.ex	1	1/1	0



ServerAgent configuration screen.

Edit Server AlertSite
2005-04-06 19:10:52

Control Panel | Console | Sites | Transactions | Servers | Security | Notifiers | Groups | Reports | Account | Logoff | Back Delete Submit Help

Site Name: Site Plan:

Monitoring is: Notify on Error?:

IP Address:

TCP Traceroute on network error: Use Ping to verify network errors:

Reporting Interval: Device ID:

Enabled	Notify	Name	Compare	Warning Value	Threshold Value	Last Value	Last Status	Last Reported
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CPU_USAGE->LOAD_AVERAGE	>	<input type="text" value="90"/>	<input type="text" value="95"/>	8		2005-04-06 19:09:00
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	DISK_INFO->DRIVE_C_USAGE	>	<input type="text" value="25"/>	<input type="text" value="35"/>	31		2005-04-06 19:09:00

Control Panel | Console | Sites | Transactions | Servers | Security | Notifiers | Groups | Reports | Account | Logoff | Back

3290
Done



Current ServerAgent Report:

AlertSite Reports - Mozilla Firefox

Site Name: DB-moose From: 2005-02-02 00:02
 Report Type: Detail Report Thru: 2005-02-02 10:42

Status Summary

Status	Count	Description
0	129	Site responded normally to all tests

Results Summary

	OK	Warning	Errors	Server Unreachable	Total Tests
Cpu Usage: Bufferram	129	0	0	0	129
Cpu Usage: High	129	0	0	0	129
Cpu Usage: Load 15 Min	129	0	0	0	129
Cpu Usage: Load 1 Min	129	0	0	0	129
Cpu Usage: Load 5 Min	129	0	0	0	129
Cpu Usage: Procs	129	0	0	0	129
Cpu Usage: Ram	129	0	0	0	129
Cpu Usage: Sharedram	129	0	0	0	129
Cpu Usage: Swap	129	0	0	0	129
Cpu Usage: Uptime	129	0	0	0	129
Disk Info: Drive Root Blocks	129	0	0	0	129
Inode Info: Drive Root Inodes	129	0	0	0	129
Process: Cron	129	0	0	0	129
Process: Mysqld	129	0	0	0	129
Process: Ntpd	129	0	0	0	129
Process: Sendmail	129	0	0	0	129
User: Repdb In.Sh	129	0	0	0	129
User: Repmon.Sh	129	0	0	0	129
User: Repmon Out.Sh	129	0	0	0	129

Performance Results for - Cpu Usage: Bufferram

Done www.alertsite.com



XVI. Troubleshooting

Verify connectivity to the assigned monitoring server.

If ServerAgent cannot connect to its assigned monitoring server and is displaying error messages in the logfiles that look like this:

```
04/01/2004 00:08:08 Connecting to the server... bears.alertsite.com : 4891
04/01/2004 00:08:09 ERROR: Connection refused
```

The first thing to check is that the server they are installing ServerAgent on does have outbound connectivity to the appropriate AlertSite monitoring location. To verify that there is appropriate connectivity:

```
c> telnet bears.alertsite.com 4891
```

A connection should be established and upon hitting enter the "connection to host lost message" should be displayed.

Debugging:

ServerAgent can be configured to add debugging information to your log files for network problems. You can edit the configuration file (Windows c:\Program Files\Nemo\Nemo.ini; Unix /usr/local/nemo/share/alertsite.rc) and change the value of "debug" to 42 for network debugging.

- 4) Stop ServerAgent
- 5) Update the debug flag (debug=42)
- 6) Start ServerAgent

Any time ServerAgent cannot talk to AlertSite, it will perform a "ping" and a "traceroute" for the particular monitoring server and include that information in the log file. Please note that this requires the following commands to be included in the program path of the ServerAgent:

- Unix – "ping" and "traceroute"
- Windows – "ping" and "tracert"

This debugging is intended to only be included for a short time. It can take a long time to perform a traceroute with network errors and it is recommended that the debug flag be set back to its previous value as soon as possible.



XVII. ServerAgent Metrics

The ServerAgent program tracks different default values depending on the operating system where it is running. The ServerAgent also can track user specific metrics when you opt to measure certain processes (PROCESS) and/or user scripts (USER).

Unix

(Not all metrics are available on all Unix operating systems)

<i>Metric Name (Unix)</i>	<i>Description</i>
CONNECT: <i>host:port</i>	1 if successful, 0 if failed
CPU_USAGE: BUFFERRAM	Memory used by buffers
CPU_USAGE: LOAD_1_MIN	Active tasks averaged over prior 1 minute X 100
CPU_USAGE: LOAD_5_MIN	Active tasks averaged over prior 5 minutes X 100
CPU_USAGE: LOAD_15_MIN	Active tasks averaged over prior 15 minutes X 100
CPU_USAGE: NOTIFY_ON_REBOOT	Date and time when rebooting, otherwise 0
CPU_USAGE: PROCS	# of running processes
CPU_USAGE: RAM	% used main memory size
CPU_USAGE: SHAREDGRAM	Amount of shared memory
CPU_USAGE: SWAP	% used swap space
CPU_USAGE: UPTIME	Seconds since last reboot
CPU_USAGE: SWAP	% used swap space
DISK_INFO: DRIVE_ <i>name</i> _BLOCKS	% used disk blocks for drive <i>name</i>
DISK_INFO: DRIVE_ <i>name</i> _INODES	% used index nodes for drive <i>name</i>
PROCESS: <i>taskname</i>	Number of times process <i>taskname</i> is running now
USER: <i>userprogram</i>	Results of your <i>userprogram</i>

Windows

<i>Metric Name (Windows)</i>	<i>Description</i>
CONNECT: <i>host:port</i>	1 if successful, 0 if failed
CPU_USAGE: LOAD_AVERAGE	% cpu usage
CPU_USAGE: NOTIFY_ON_REBOOT	Date and time when rebooting, otherwise 0
CPU_USAGE: MEMORY_LOAD	Special value, provided by operating system, between 0 and 100 that gives a general idea of current memory utilization, in which 0 indicates no memory use and 100 indicates full memory use



<i>Metric Name (Windows)</i>	<i>Description</i>
CPU_USAGE: PHYSICAL_MEMORY_USAGE	% used of total physical memory
CPU_USAGE: PAGING_MEMORY_USAGE	% used of the paging file on disk
CPU_USAGE: PROCS	# of running processes
CPU_USAGE: VIRTUAL_MEMORY_USAGE	% used of the virtual address memory
DISK_INFO: DRIVE_ <i>letter</i> _USAGE	% used for fixed disk <i>letter</i>
PROCESS: <i>taskname</i>	Number of times process <i>taskname</i> is running now
USER: <i>userprogram</i>	Results of your <i>userprogram</i>