HPSA Agent Characterization

Product	HP Server Automation (SA)
Functional Area	Managed Server Agent
Release	9.0

HPSA Agent Characterization

Quick Links

High-Level Agent Characterization Summary

SA 9.0 managed server agent functionality was exercised in the performance lab to validate resource demand and managed server impact for several sample use cases. Both Windows and Linux agents were examined in three different use cases: agent resource usage while idle, while installing the agent, and while audit feature was being run. In all tested cases, the agent generally exhibited low CPU usage and moderate memory usage. The SA agent exhibited low overhead on the test systems and minimal impact to the managed server.

Test Case Descriptions

Six test cases were examined for this study: agent installation, agent while idle, and agent during an audit job were executed on both Windows and Linux. In each case, a single virtual machine was used for the managed server under test. For Windows, a Windows Server 2003 virtual machine was used along with a recent agent. For Linux, a Red Hat AS4 32-bit virtual machine was used along with the same version of agent. Both agents were registered to an active SA core. For more information about the hardware and software set up in the test environment, see Appendix B.

Agent characterization during the initial agent installation and in the "Idle Agent" use case was selected because they are common use cases. The SA "Audit" use case was selected because that job type is representative of the most active agent workload. Other SA job types have a similar or lesser agent resource demand during run time compared to the Audit use case. Additionally, Windows and Linux represent two of the most common operating systems in most deployments and were selected to represent Windows-based operating systems and Unix-like operating systems. Other operating systems should have comparable results to those discussed below.

Agent Characterization during Installation

Agent installer resource demand was monitored for the initial agent installation process. The agent installer executable was placed on the target managed server and executed manually. The Agent Deployment Tool was not used. During the installation, normal registration with the core occurred. The agent was not installed before the test was run and as a part of the installation, the agent was not automatically started to capture the resource demand of the installer phase alone, but otherwise ran with default options. Once the installer completes and the agent is started, resource demand reflects the agent while idle test case. For more information about the monitoring methodology, see Appendix A.

Agent Characterization while Idle

Agent resource demand was monitored for twenty-four hours during which no jobs or tasks were run on the managed server. The agent was running normally and registered to a core. The SA core did continue to do its regular activity by periodically pinging the agent to verify it was still reachable, doing two hardware registrations, and one software registration. For more information about the monitoring methodology, see Appendix A.

Agent Characterization during Audit

Agent and overall system resource demand were monitored while an audit was run against the managed server. Windows and Linux audits were based on prior audit test cases for each platform. For Windows, the audit compared the C:\WINDOWS directory between a snapshot and the managed server. The Linux audit consisted of using the HP Live Network PCI (Payment Card Industry) audit against the managed server. Please refer to the HP Performance Center of Excellence studies on audit for more information about general audit performance. For further information about the monitoring methodology, see Appendix A.

Note that when similar processes are run either manually or through HPSA to accomplish a use case task, such as those run for audit, these processes are not considered apart of HPSA as they would be run even in the absence of automation. The data captured for the agent during audit reflects only those HPSA automation processes which add additional overhead to the use case.

Windows Agent Characterization

Results Summary

In two test cases, agent CPU resource usage was moderately low. Agent installation consumed moderate CPU cycles over a short window, but this is consistent with installation for any software. SA Agent installation had a lower resource requirement than the installation of a popular A/V agent. See the Agent Installation Results section below. Also of note, the "Idle Agent" test case used almost no CPU resources, and when it did, it was only during a brief interval every few hours. Memory usage was moderately low compared to other resident processes in all cases.

Agent Test Case	Elapsed Time (sec)	CPU Time Used (sec)	Avg. Private Memory (MB)
SA Agent Installation	15 seconds	10.41	13.3
AV Agent Installation[1]	45 seconds	26.6	25.7
Idle	24 hours	0.11	16.2
Audit	14 seconds	0.22	21.8

Agent Installation Results

The agent installation required some CPU time, moderate memory usage, and took little real time to execute. Higher CPU usage is expected as that is typical of software installation in general. Total CPU utilization of the managed server spikes a few times during the installation, but the overall CPU time required and elapsed installation time was low. A majority of this CPU demand is disk I/O as the required files are installed on the hard drive and is typical of software installation activity. Memory usage was comparable with the idle agent as well as the agent under load.

[1] As a comparison to the SA Agent Installation, a popular enterprise anti-virus client was run as an unattended install.

As a comparison, a popular enterprise anti-virus client was run as an unattended install. The anti-virus client took three times as long to install, required nearly two and a half times more CPU resources to execute, and required approximately twice as much memory to run.

Idle Agent Results

Over the twenty four hours of monitoring, the idle agent used almost no CPU time and had moderate memory usage. The working set memory usage was very stable over time. Only the agent and agent watchdog processes were active during this time.

Agent during Audit Results

The entire audit job took an average of fourteen seconds to run. Not all of that time is spent on the managed server as the core also does work during the audit. During the audit window, the agent temporarily increases its memory footprint to handle the audit job and uses less than one second of CPU time for this use case.

During the audit, additional processes and scripts were executed outside of the agent and these consumed additional CPU time and memory in addition to the increased agent resource demands. These processes capture the data used in the audit. A large majority of these processes are the same processes that would be executed if a Windows audit of the same nature was written and executed by hand without automation software. Since they would be run even in the absence of SA automation, they are not considered a part of the HPSA agent.

The HPSA Agent adds a small amount of additional overhead to the task, but a significant percentage of the CPU and memory utilization is consumed by the spawned auditing processes, not by the HPSA agent. The HPSA agent only consumed a maximum of 11% of the total CPU resources during the audit execution time period.

Linux Agent Characterization

Results Summary

In two test cases, agent CPU resource usage was moderately low. Agent installation consumed moderate CPU cycles over a short window, but this is consistent with installation for any software. See the Agent Installation Results section below. Also of note, the “Idle Agent” test case used almost no CPU, and when it did use CPU resources, it was only every few hours. Memory usage was moderate compared to other resident processes in all cases.

Agent Test Case	Elapsed Time (sec)	CPU Time Used (sec)	Avg. Private Memory (MB)
SA Agent Installation	4 seconds	1.39	11.2
Idle	24 hours	0.20	9.8
Audit	48 seconds	4.50	15.4

Agent Installation Results

The agent installation required very little CPU time, moderate memory usage, and took very little real time to execute. Increased CPU usage is expected as that is typical of software installation in general. Total CPU utilization of the managed server varies during the installation, but the overall CPU time required and elapsed installation time were low. A majority of this CPU demand is disk I/O as the required files are installed on the hard drive and is typical of software

installation activity. As the CPU time and real time required was low, this is not a performance concern. Memory usage was lower than the idle agent as well as the agent under load.

Idle Agent Results

Over the twenty four hours of monitoring, the idle agent used almost no CPU time and had moderate memory usage. The memory usage was very stable over time. Only the agent and agent watchdog processes were active during this time.

Agent during Audit Results

The entire audit job took an average of forty-eight seconds to run. Not all of that time is spent on the managed server as the core also does work during the audit. During the audit window, the agent temporarily increases its memory footprint to handle the audit job and uses approximately five seconds of CPU time for this use case.

During the PCI audit several dozen processes and scripts were executed outside of the agent processes and these consumed additional CPU time and memory in addition to the increased agent resource demands. These processes capture the data used in the audit. A large majority of these processes are the same processes that would be executed if a PCI audit was written and executed by hand without automation software. Since they would be run even in the absence of automation, they are not considered a part of the HPSA agent. Examples of these spawned processes from this use case include:

```
find / -xdev -type f ( -perm -04000 -o -perm -02000 )
find / -xdev -nouser -o –nogroup
```

The HPSA agent adds a small amount of overhead to the task, but a significant percentage of the CPU and memory utilization is consumed by the spawned auditing processes, not the HPSA agent. The HPSA agent CPU utilization reaches a momentary maximum of 16% during the audit operation.

Conclusions

In general, the agent is fairly lightweight in terms of CPU and memory usage on both platforms. Installation does not take very long to complete, and it generally uses similar resources to The Idle and audit test cases. The SA Agent installation consumes lower CPU resources than does the Agent installation of a representative A/V Agent, and requires less real time to complete installation. The low amount of CPU time and real time required to complete the agent installation reduces the overall impact of the higher CPU usage the installer exhibits.

While only one agent at a time was tested for this study, previous studies have indicated that overall job performance is bound by the HPSA core when multiple managed servers were specified in a job. When a managed server is not actively being worked on or accessed by the core, its agent performance profile is not significantly different than while the agent is idle. Agent performance is not impacted by the number of other managed servers specified in an HPSA job.

The idle agent uses negligible CPU resources over a one day period and its memory utilization is moderate, but stable over time. The idle overhead for CPU even while doing software and hardware registration responses for the HPSA core is negligible.

Additional CPU resources are consumed by the agent during the "Audit" test case, but the CPU usage is still relatively low and the memory usage does not increase by a significant amount. During the Audit, other processes are invoked to complete the task. These processes are the same processes that would be executed if the task was scripted and executed manually without HP SA automation software.

Audit is an agent-intensive use case. Its results are representative of the upper limit for agent resource demand. Other HPSA use cases such as patching, software install, and application configuration will cause agent demand less than or at most equal to the audit resource demand results. The other HPSA tasks will also cause additional managed server load beyond what the HPSA agent uses, but the same load would be experienced if these tasks were executed without HPSA automation. The agent overhead is a small portion of the overall resource demand for audit and, by extension, other HPSA use cases.

Appendix A: Monitoring Methodology

The agent consists of two running processes on Windows and Linux. One process is a watchdog and is the parent of the actual agent process. These two processes were monitored together as the "agent" process.

Windows

On Windows, Windows PerfMon logging was used to measure resource demand of the processes of interest and of the system overall. CPU usage, virtual memory usage, and working set memory usage were all monitored. For the running agent, there are two executables which serve as the watchdog (watchdog.exe) and agent itself (python.exe). For the agent installation case, there are many scripts run outside of the installer binary, so PerfMon was used to find the idle resource usage of the managed server and then found the difference between the installer activity and the idle system. In general, logging occurred at one second intervals.

Linux

On Linux, the HP OpenView Performance Agent (OVPA) was used to measure resource demand of the processes of interest. CPU usage, virtual memory usage, and resident memory usage were all monitored. For the running agent, there are two Python processes which serve as the watchdog and agent itself. These were placed in an OVPA application definition and used in the idle agent and audit test cases. For the agent installation case, there are many scripts run outside of the installer binary, so OVPA was used to find the idle resource usage of the managed server and then found the difference between the installer activity and the idle system.

Due to the limitations of process monitoring, data was captured in one second intervals and this data was aggregated into fifteen second intervals in the extracted output, so for the shorter test cases, the granularity of the data collection was low.

Notes on Specific Test Cases

For agent installation, the monitoring tools on the managed server captured server resource demand before, during, and after the installation. Agent installation resource demand was calculated by finding the difference between the installation activity and the test system's normal background resource demand.

During the idle agent test, the combined total activity of both the agent processes on Windows and Linux was captured. Larger data collection intervals were used over the 24 hour period.

The two agent processes were monitored separately from the system resource usage. Audit job effect on the overall system was determined by noting the difference between the idle state of the managed server before and after the job and the activity of the system during the audit itself.

Note that when similar processes are run either manually or through HPSA to accomplish a use case task, such as those run for audit, these processes are not considered apart of HPSA as they would be run even in the absence of automation. The data captured for the agent during audit reflects only those HPSA automation processes which add additional overhead to the use case.

Appendix B: System Under Test

SA Core

Server Role	Database (Truth)
Hardware Specs	Local Disk: 2x 72GB 10K SAS RAID-1 (Linux boot) SAN Attach: 4Gbps single path FC, MSA2012 Array Memory: 16GB OS: RHEL AS 4 64-bit CPU: 2x Quad-Core 2.66 GHz Intel Xeon 5355 Model: HP BL460cG1
Network Config	Network: 1 Gbps LAN
Software Specs	Oracle 10.2.0.2.0 Standard Edition
HPSA Version	SA 9.0 – Build 40.0.1492.0
Server Role	Infrastructure services Media Repository Storage "Slice" scalable services
Hardware Specs	Local Disk: 2x 72GB 10K SAS RAID-1 (Linux boot) SAN Attach: 4Gbps single path FC, MSA2012 Array Memory: 16GB OS: RHEL AS 4 64-bit CPU: 2x Quad-Core 2.66 GHz Intel Xeon 5355 Model: HP BL460cG1
Network Config	Network: 1 Gbps LAN
HPSA Version	SA 9.0 – Build 40.0.1492.0
Server Role	"Slice" scalable services
Hardware Specs	Local Disk: 2x 72GB 10K SAS RAID-1 (Linux boot) SAN Attach: 4Gbps single path FC, MSA2012 Array Memory: 16GB OS: RHEL AS 4 64-bit CPU: 2x Quad-Core 2.66 GHz Intel Xeon 5355 Model: HP BL460cG1
Network Config	Network: 1 Gbps LAN
HPSA Version	SA 9.0 – Build 40.0.1492.0

Managed Servers

Server Types	HP Blade servers hosting VMware VMs
Hardware Specs	Local Disk: 2x 72GB 10K SAS RAID-1 (ESX boot) SAN Attach: 4Gbps single path FC, MSA2012 Array (VM images) Memory: 32GB OS: VMware ESX Server 3.5.2 CPU: 2x Quad-Core 2.66 GHz Intel Xeon 5355 Model: HP BL460cG1
Windows VM Specs	Windows 2003 Standard Edition, 32-bit 1x Virtual CPU 4 GB Virtual Memory 5 GB disk space
Linux VM Specs	Red Hat AS 4, 32-bit 1x Virtual CPU 512 MB Virtual Memory 5 GB disk space
Agent Version	40.0.0.0.22
Network	Network: 1 Gbps LAN

Appendix C: Environment Diagram