HP Server Automation 10.1 Release

Performance Characterization of FIPS security configurations in SA Core

Product	HP Server Automation (SA)
Functional Area	FIPS Security Configurations
Release	HP SA 10.1 build 55.0.48777.0
Characterization Description	Performance Characterization of FIPS security configurations in HP SA
Document ID	SA10 1-FIPSstudy_v1.2.docx
Version Date	May 15, 2014
Document Author	SA Performance Team (*SA_Perf@hp.com*)

Table of Contents

Executive Summary

Server Automation can now support different configurations of the FIPS security standards. As these different configurations use distinct and possibly stronger encryption methods, there are different associated resource costs. These differing resource costs may affect the overall performance and job throughout capability of Server Automation. The purpose of this program is to quantify these effects and to provide guidance on the impact of choosing and changing FIPS configurations.

For the noted SA use cases and characterization environment, the following performance deltas are measured across the tested FIPS configurations:

Performance Impact of FIPS configurations		
Use Case	**Performance delta**	**Notes**
AppConfig	small delta	SHA1/FIPS1 or SHA256/FIPS0 compared to baseline configuration at 200 managed servers
Audit	small delta	SHA1/FIPS1 or SHA256/FIPS0 compared to baseline configuration at 200 managed servers
Remediate	~ 8% delta ~ 20% delta	SHA1/FIPS1 compared to baseline configuration at 70 managed servers SHA256/FIPS0 compared to baseline configuration at 70 managed servers

Overview

For this study, several configurations were selected to allow representative characterizations across the supported FIPS methods. The following configurations were characterized in this study:

FIPS Configurations

FIPS configurations		
SHA1	key size 2048	fips=0
SHA1	key size 2048	fips=1
SHA256	key size 4096	fips=0

The most important comparisons are to compare 1) SHA1/Key size 2048 across the FIPS enabled/disabled flag settings, and to compare 2) SHA1/Key size 2048/fips=0 to the SHA256/Key size 4096/fips=0 configuration.

SA Use Cases

Different SA use cases exercise the encryption components in different ways and use different code paths. This program characterizes FIPS impacts across several representative code paths for Java, Python, and scripts. The following criteria were used to select representative use cases:

- Coverage across representative Python and Java intensive code paths in SA
- Coverage across representative Network intensive vs. CPU intensive on SA Core
- Coverage using existing use cases with performance baseline over multiple SA releases

The following use cases were selected for this study:

Use Case	Selection criteria
Linux AppConfig with 100 rules pushed	Java code path, SA Core intensive
Linux Audit with PCI DSS v2 (192 rules)	Java code path, SA Core and Target intensive
Linux Remediation with 500MB zip file	Python code path, Network intensive

Overall Performance Characterization Summary

SA overall Job throughput is plotted as the number of managed servers in the Job increases. This plot provides a good representative diagram of overall SA job behavior as the workload size increases, and is most important to the SA customer. In each of the following plots, the job throughput curves are presented for the three tested configurations.

Use Case: AppConfig

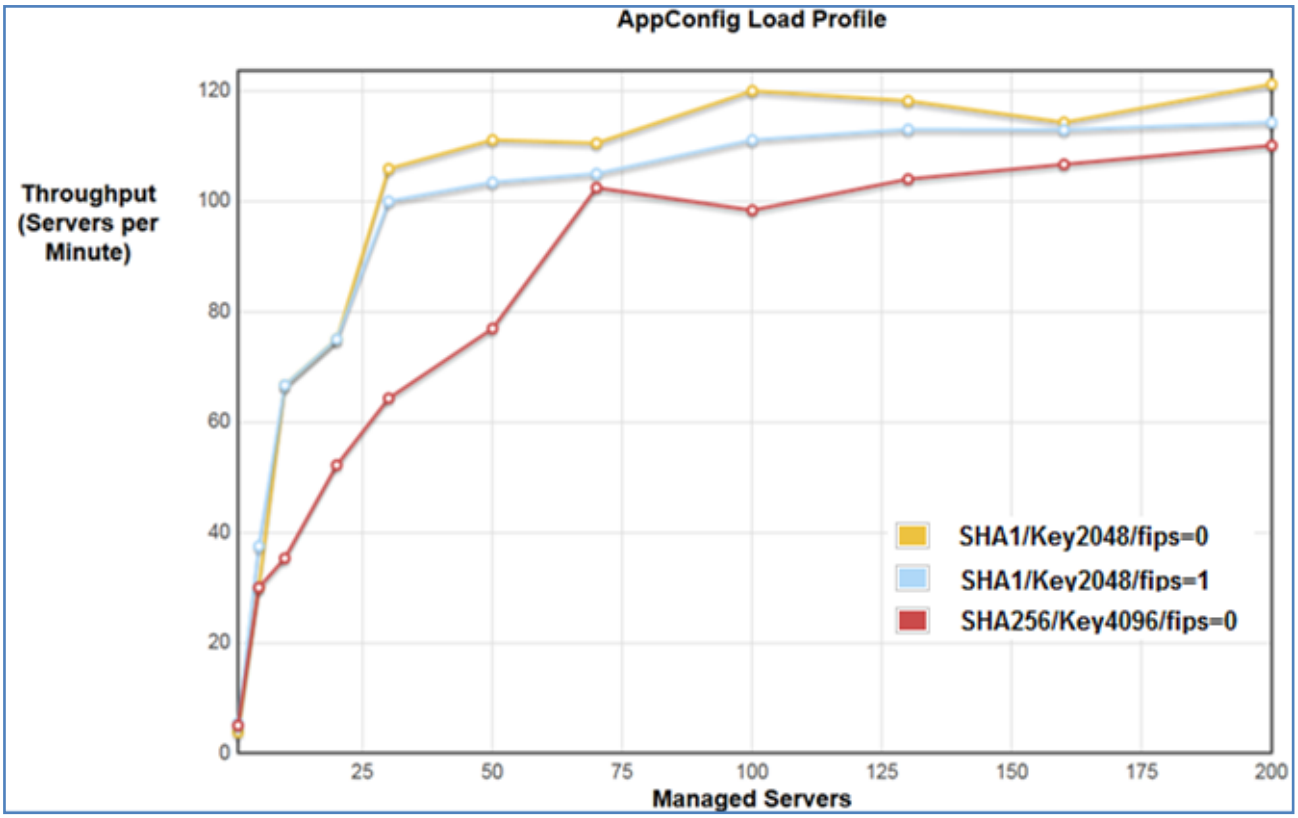


Figure 1: AppConfig with 100 rules pushed

The diagram shows that the overall SA Job throughputs for all three FIPS configurations are about the same. No significant degradation observed for SHA1, fips=1 and SHA256, fips=0 cases as compared to the default configuration of SHA1, fips=0 in the SA 10.1 release.

AppConfig is a lighter weight SA use case and makes low network demands, so the effects of the FIPS settings tend to be dominated by the overall SA job characteristics.

Use Case: Linux Audit

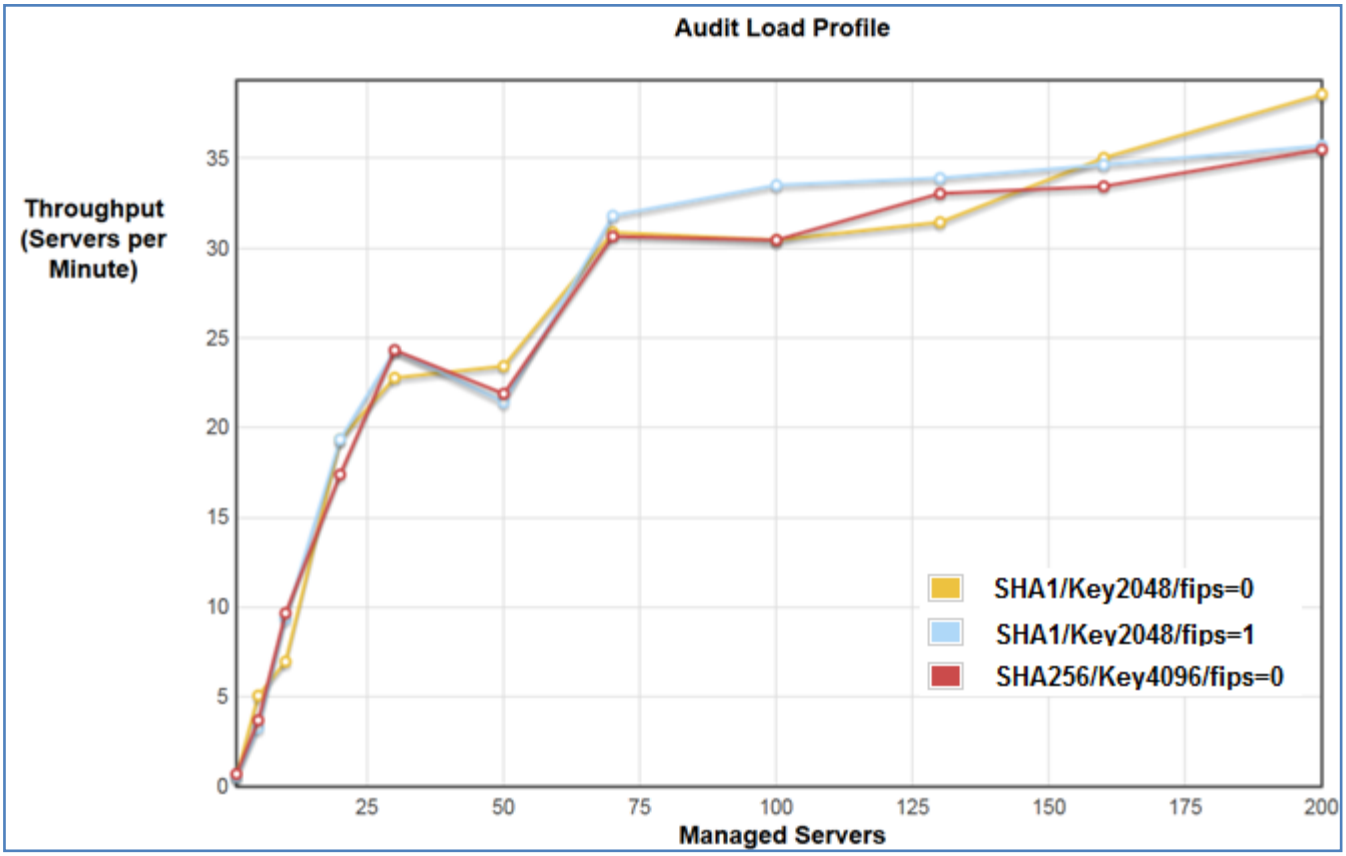
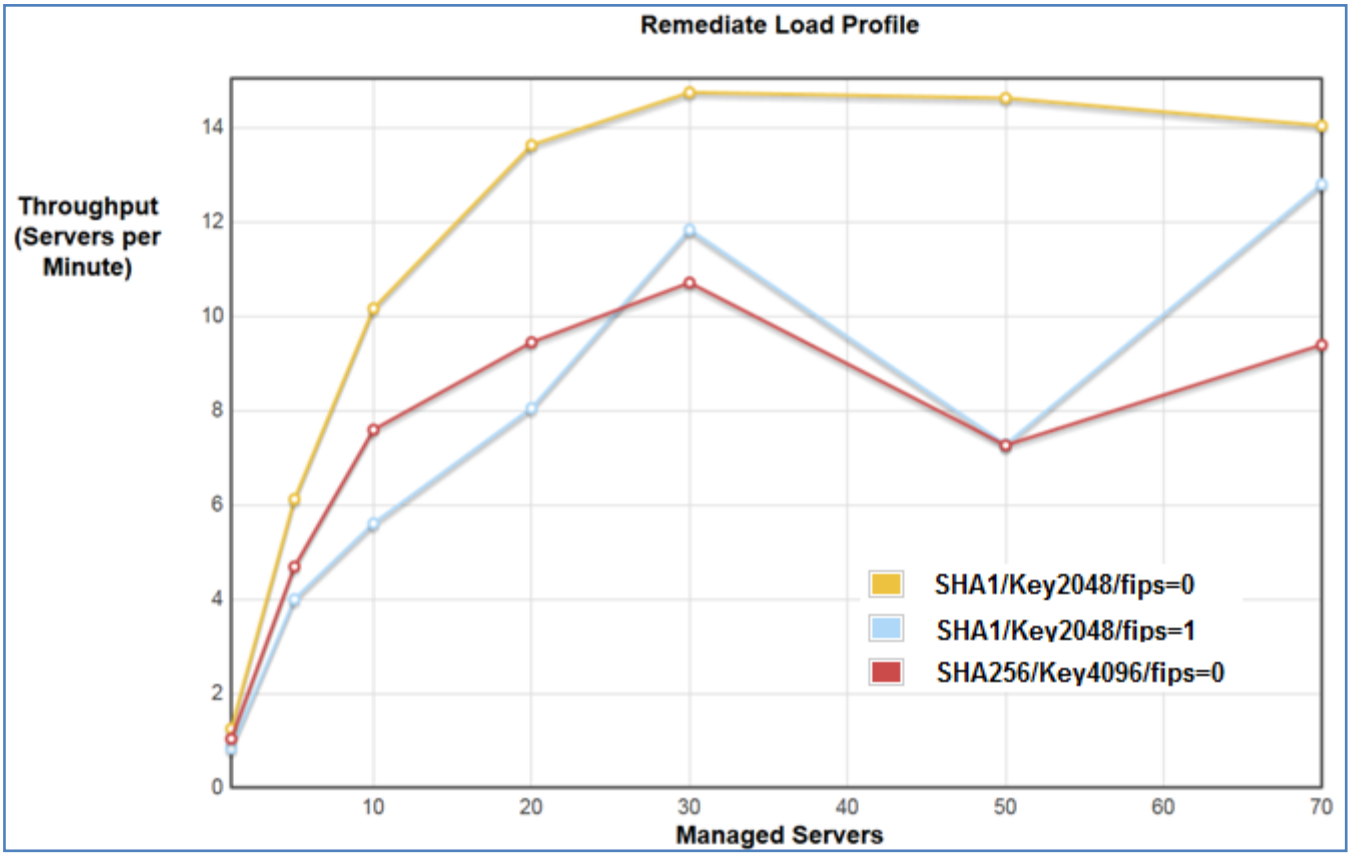


Figure 2: Linux Audit with PCI-DSS Policy, 192 rules

The diagram shows that the SA Job throughputs for all three FIPS configurations are about the same. No significant degradation observed for SHA1, fips=1 and SHA256, fips=0 cases as compared to the default configuration of SHA1, fips=0 in the SA 10.1 release.

Use Case: Linux Remediation



The overall Job throughput diagrams for all three configurations show the following differences in the throughputs amongst the three FIPS configurations:

- At the level of 70 managed servers, it is roughly about 8% degraded for SHA1, fips=1 case compared to the default configuration SHA1, fips=0.
- Also at the level of 70 managed servers, it is roughly about 20% degraded for SHA256, fips=0 case compared to the default configuration SHA1, fips=0.

Additional analysis shows how SA internal job states are affected in this network-intensive job. Please see this additional information in the Appendices.

Conclusions

SA operation and performance is affected to a greater or lesser degree by the selection of different FIPS encryption options. The effect of this performance overhead is quantified.

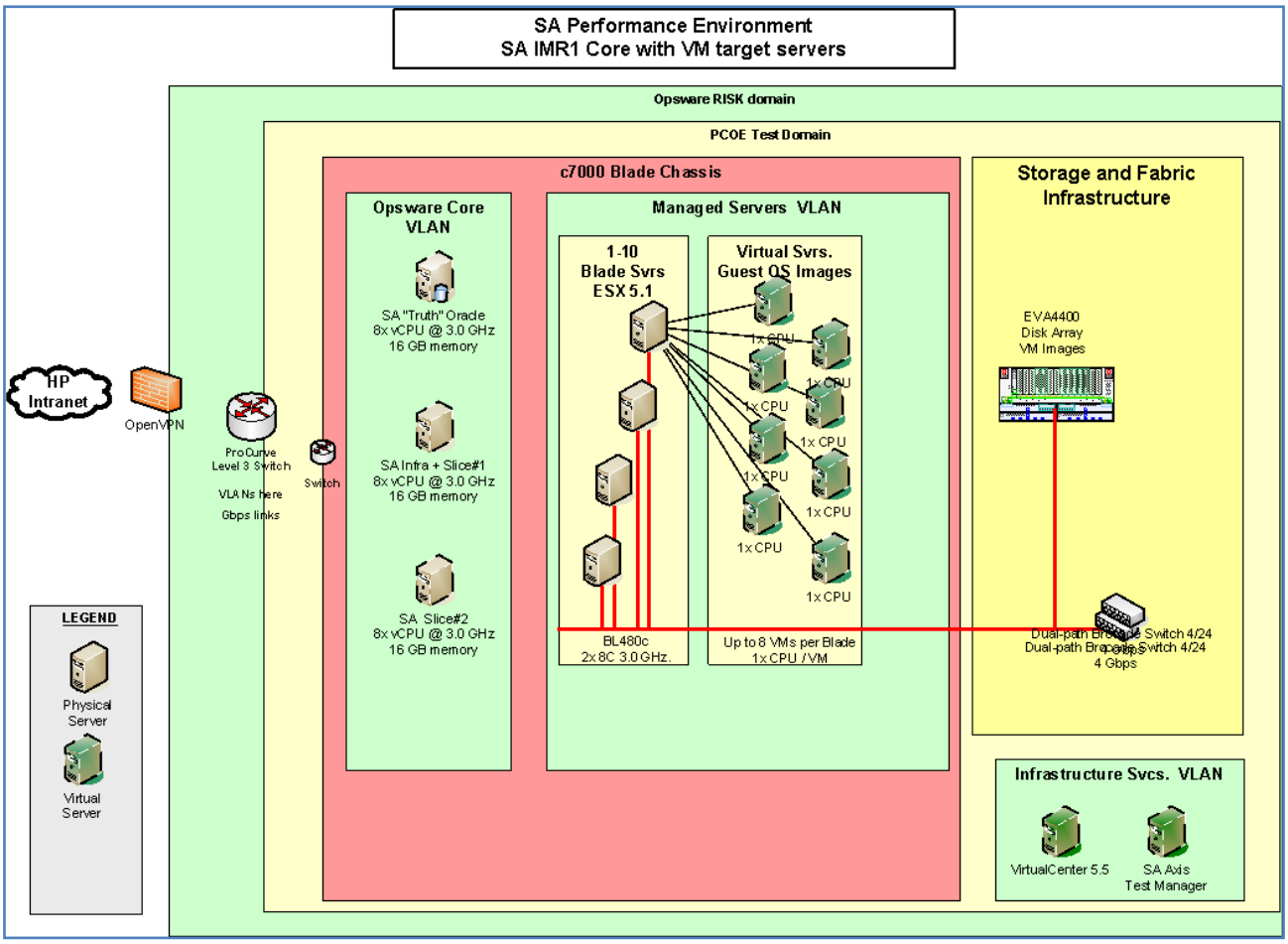
The effects of varying the FIPS configurations can be minor (AppConfig and Audit use cases), or moderate (Remediate use case). The most performance impact is observed for the Remediate use case, which can be the most network-intensive SA operation. For a representative SA job of Remediation of 500 MB content to targets at a server group size of 70, up to 20% performance degradation is observed.

SA system architects should plan and provision servers appropriately when changing their FIPS configurations. In network intensive SA Cores (for example, where there are heavy workloads for Remediation or Patching), CPU resources should not be minimized or else the CPU may become a bottleneck and limit overall job throughout.

SA system architects should plan appropriately when estimating their expected SA job throughout.

Appendices

Appendix A: Representative Performance Characterization Environment



Appendix B: System Configurations

SA Core Slice #1	Infrastructure & Slice services, 8 CPU, 32 GB RAM VM on ESXi 5.1 Model Repository Multimaster Component (vault) Data Access Engine (Spin - primary) Media Repository (Word storage on NFS, SMB) Gateways (mgw, cgw, agw) Command Engine (Way) Web service API (Twist) Opsware Global File System (Hub) Word Tsunami Build Manager
Machine Specs	Local Disk: 200 GB Linux ext3 on VMFS CPU: 8x vCPU @ 3.0 GHz. , Memory: 32 GB HW: Model: HP BL480 G8
Network Config	Network: 10 Gbps LAN, dedicated VLAN
Software Specs	OS: RHEL6.3 64-bit SA 10.1 - Build 55.0.48777.0
SA Core Slice #2	"Slice" scalable services, 8 CPU, 32 GB RAM VM on ESXi 5.1 Command Engine (Way) Secondary Spin Web service API (Twist) Opsware Global File System (Hub) Word Tsunami Gateways (cgw, agw)
Machine Specs	Local Disk: 200 GB Linux ext3 on VMFS CPU: 8x vCPU @ 3.0 GHz. , Memory: 32 GB HW: Model: HP BL480 G8
Network Config	Network: 10 Gbps LAN, dedicated VLAN
Software Specs	OS: RHEL6.3 64-bit SA 10.1 - Build 55.0.48777.0
SA Database	Model Repository Database (Truth, 8 CPU, 32 GB RAM VM, ESXi 5.1)
Machine Specs	Local Disk: 200 GB Linux ext3 on VMFS CPU: 8x vCPU @ 3.0 GHz. , Memory: 32 GB HW: Model: HP BL480 G8
Network Config	Network: 10 Gbps LAN, dedicated VLAN
Software Specs	OS: RHEL6.3 64-bit Oracle 12.1.0 Enterprise Edition (64-bit)
Additional Notes	SA 10.1 - Build 55.0.48777.0
Managed Servers	Blade servers, hosting VMware VMs
Machine Specs	Local Disk: Linux ext3 on VMFS SAN Attach: 4Gbps dual path FC, EVA4400 Array (VM images) Memory: 32GB OS: VMware ESX Server 5.1 CPU: 2x 8Core 3.0 GHz Intel Xeon Model: HP BL480 G8
Network Config	Network: 10 Gbps LAN, dedicated VLAN
Software Specs	RHEL Server 6.3 64-bit 1 vCPU, 2 GB vMemory
Additional Notes	VMs are evenly distributed across 10 VMware ESXi hosts

Appendix C: Detailed analyses for the SA Remediate Use Case

System Resource Demands for FIPS configurations

The effect on CPU consumption for the Remediate use case with 500 MB Zip package and for a 70-server target set in the different FIPS configurations may be viewed in the following diagrams. Each row of the table depicts % Consumption of the CPU computing resources over the Job lifetime for a tested FIPS configuration. The left column plots CPU usage for the Primary Slice #1 server, and the right column plots CPU usage for the Secondary Slice #2 server. Overall job time increases for the SHA1/FIPS1 and SHA256/FIPS0 modes versus the baseline SHA1/FIPS0 configuration (x-axes are not to the same scale for the 3 plots).

For all test cases, the initial peak in CPU load roughly corresponds to the SA Staging work phase where the 500 MB content is transferred across the network to each of the 70 target servers. CPU resources are consumed for encryption of the content across the secure network link.

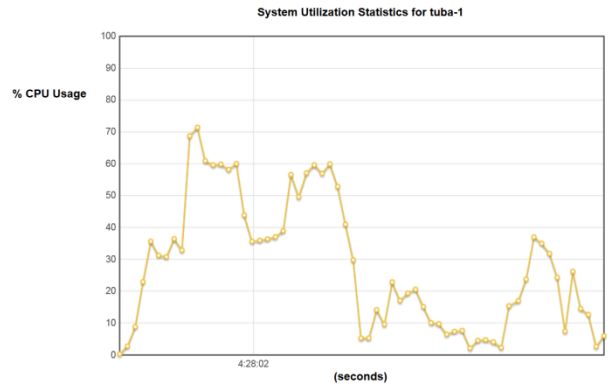
The top row plots CPU consumption for the baseline configuration of SHA1 encryption, Keylength 2048, and FIPS mode disabled (fips=0). CPU consumption is moderate across the job lifetime.

The middle row plots CPU consumption for the configuration: SHA1 encryption, Keylength 2048, FIPS mode enabled (fips=1). CPU demand increases and the initial workload peak become essentially CPU bound for this Job phase.

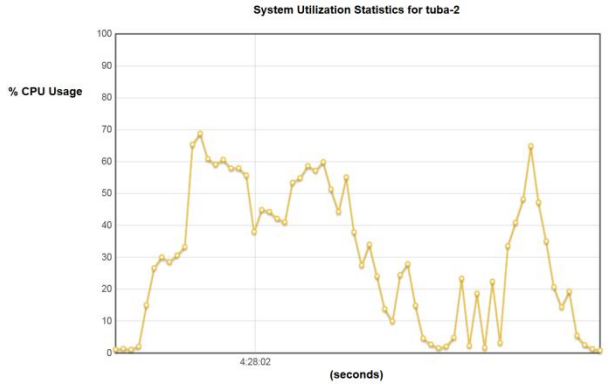
The bottom row plots CPU consumption for the configuration: SHA256 encryption, Keylength 4096, FIPS mode disabled (fips=0). CPU load is moderately high.

These diagrams illustrate that CPU consumption may increase for configurations in the FIPS enabled mode. SA system architects should consider this in their deployment planning and ensure that SA Core servers are appropriately sized and are not configured with minimal CPU resources.

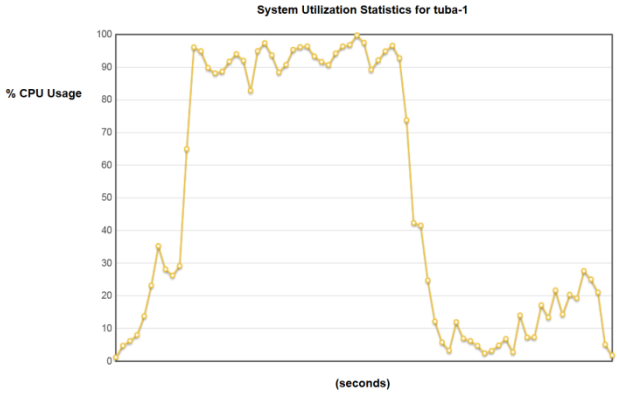
For all test cases, CPU load is roughly balanced across the 2 Slice servers, demonstrating that SA Remediation exhibits good balanced job distribution across the available Slice servers.



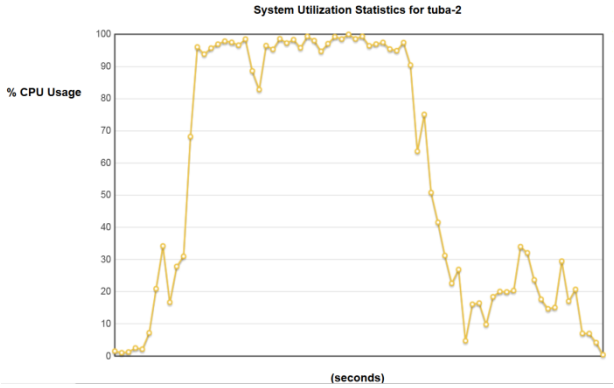
SHA1, Keylength 2048, FIPS=0 Slice 1



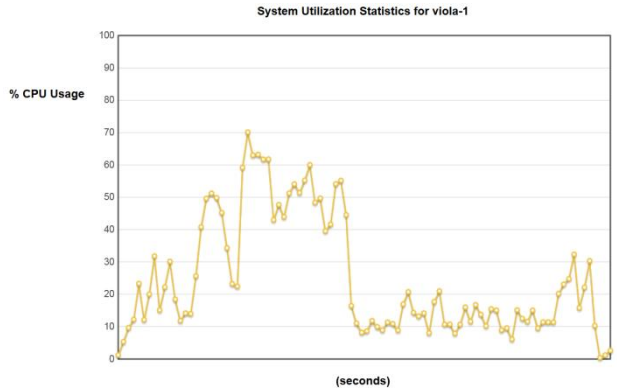
SHA1, Keylength 2048, FIPS=0 Slice 2



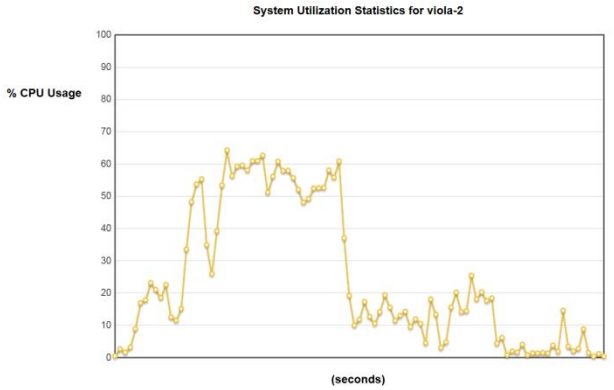
SHA1, Keylength 2048, FIPS=1 Slice 1



SHA1, Keylength 2048, FIPS=1 Slice 2



SHA256, Keylength 4096, FIPS=0 Slice 1



SHA256, Keylength 4096, FIPS=0 Slice 2

Table 1: CPU consumption over SA Remediate Job lifetime

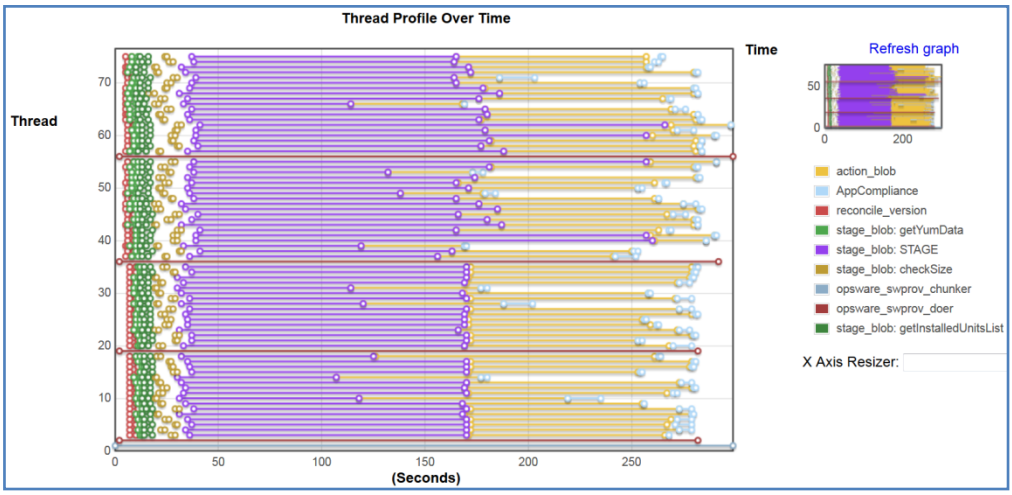
SA Job Thread Diagrams for Remediate Use Case

SA job threads may be used to understand the internal job states for a job, and how these certain (but not all) job states may change depending on the FIPS configuration under test. The following diagrams plot the internal job states for SA Remediation for the three tested configurations. Note that in the following diagrams, the time (X) axis increases from Plot 1 to Plot 2 and from Plot 2 to Plot 3, so that the overall job times for these configurations increase.

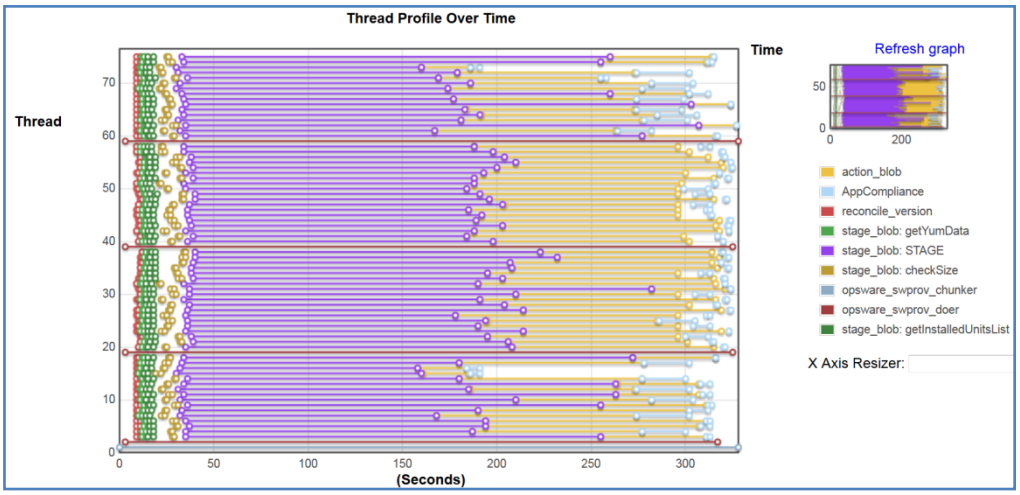
Comparing the thread diagrams for SHA1/Key2048/fips=0 and for SHA1/Key2048/fips=1 modes, the pattern of the different job stages are about the same. The overall time is longer for the job with SHA1, fips=1 configuration which results in about an 8% degradation in throughput.

Also, comparing the thread diagrams for the configuration SHA1/Key2048/fips=0, and for configuration SHA256/Key4096/fips=0, not only is the overall time longer for the SHA256, fips=0 configuration by about 20 percent when comparing to the SHA1, fips=0 case, but also the internal job states for both stage_blob: getYumData and stage_blob: getInstalledUnitsList phases need more time to complete.

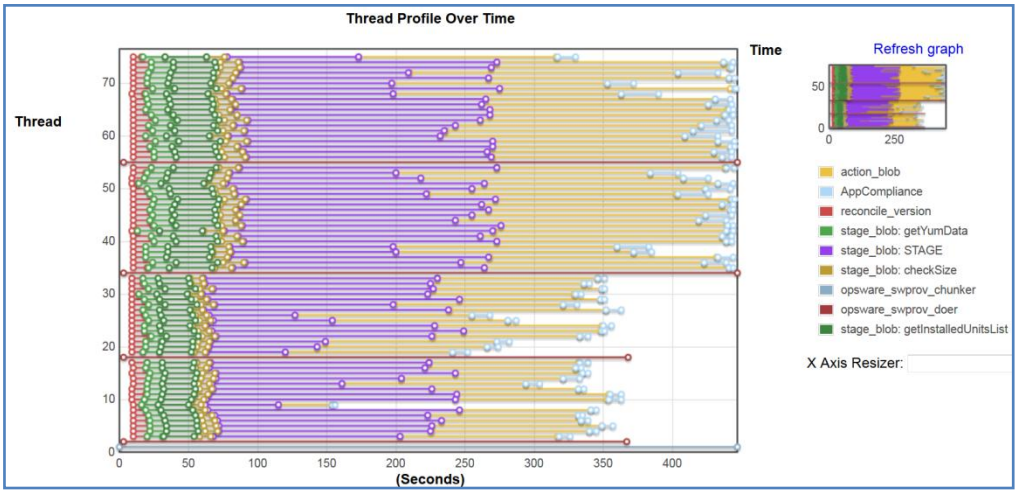
If further investigation is required, these two phases (stage_blob: getYumData and stage_blob: getInstalledUnitsList) may be analyzed in more detail to see why more time has been spent for the SHA256/Key4096/fips=0 case.



Plot 1: SHA1/Key2048/fips=0



Plot 2: SHA1/Key2048/fips=1



Plot 3: SHA256/Key4096/fips=0

Appendix D: SA Performance Documentation

Selected SA Performance Whitepapers are published on the HP SW Portal

SA Customer Access

Valid HP Support Contract/HP Passport login required to access.