Hewlett Packard Enterprise

HPE System Healthcheck

Security Impact Statement

A statement regarding the security and confidentiality of information collected by HPE System Healthcheck (SHC).

HPE's commitment to you

HPE is fully committed to alleviating customers concerns regarding data privacy and security. It is the policy of HPE to prohibit unauthorized access, disclosure, duplication, modification, or misuse of customer supplied information. In addition, it is the policy of HPE to protect information belonging to third-parties that have been entrusted to HPE in confidence, in the same manner that HPE sensitive data is protected.

System Healthcheck (SHC) is a tool used by HPE Services to analyze a system's configuration, performance, and security status. The operation of SHC requires data exchange between SHC components at the customer's premises and HPE.

Because SHC customers have a high degree of sensitivity regarding the confidentiality and handling of their support data, HPE has a custodial responsibility to ensure that any use of this data for support purposes protects the confidentiality of the data during its useful lifetime. This includes controlling what data is collected, who has access to the data, for what business purposes, and how the data will be properly disposed.

System Healthcheck Operation

- SHC is an Operating System analysis and reporting tool only.
- SHC reads various Operating System data structures and configuration only as part of its analysis.
- SHC does not read any private data reading on a host system.
- SHC does not make any changes to the system as a result of analysis.
- SHC does not read, alter or extract any customer data.
- SHC does not make any temporary or permanent modifications to privileged areas of the OS in any way.
- SHC analysis is designed to have a minimal performance impact. Where possible, SHC runtime analysis occurs at a priority level below the normal process priority in order to reduce impact on system performance.
- SHC data that is transported to HPE for the SHCA Detailed report is packaged in an encrypted ZIP file. This data contains results of analysis (problems detected) along with accompanying evidence.
- SHC must send data back to HPE in order to generate the SHCA Detailed and Management Summary reports. This data contains results of analysis (problems detected) with accompanying evidence.
- SHC uses one of the following transport options to transport its analysis data. These are SMTP or manual.
- SHC analysis data may be transported via an alternative medium if no network connection exists.

January 2016

Examples of Operating System data structures examined by SHC during an analysis:

Windows

- Memory performance metrics
- Process performance metrics
- CPU performance metrics
- Disk performance metrics
- Windows security settings (Audit settings, policy settings, Internet Explorer configuration)
- IIS Metabase network settings
- TCP/IP, WINS, DHCP DNS settings
- Boot settings
- Active Directory configuration
- Microsoft Cluster Service settings
- Registry settings
- Network Load Balancing settings

HP-UX/Linux

- Memory/Swap configuration and performance metrics
- Process performance metrics (/proc)
- CPU performance metrics (pstat, /proc)
- Disk performance metrics (/proc)
- Network configuration (ndd, netstat)
- Processor performance metrics
- Hardware configuration (ioscan, dmi)
- Security setting (.rhosts, ftpusers) and log files
- LVM/VxVM/LSM configuration and performance metrics
- Kernel tunable parameters
- Serviceguard configuration (HP-UX)
- Unauthorized logins, missing user passwords

How SHC Analysis data is handled by HPE

SHC analysis data is transported back to HPE for the purposes of generating an SHCA Detailed report. This data is stored for a period of time on a restricted and secure HPE site. Access to this site is restricted to authorized personnel.

SHC professional reports are delivered in electronic from only to the Customer Account Support specialist.

SHC analysis data is periodically archived and removed from the HPE site.

No hard copies of the SHC professional report are produced.

SHC analysis data and/or SHC reports are not used for any other purpose or made available to any other party, internal or external to HPE.

Usage of SHC, and data transported to HPE through SHC, is bound by policies prescribing acceptable use of SHC and the data collected, and by HPE’s Standards of Business Conduct. Failure to adhere to these Standards by HPE staff or representatives is potential misconduct, and is subject to management review and disciplinary action.

HPE continuing commitment

HPE is fully committed to safeguarding all data used within SHC analysis and maintaining the highest level of Security, Confidentiality, and Trust thereof.

HPE will strive to improve its processes going forward to ensure the customer’s data privacy continues to be preserved.