

UNIX HEALTHCHECK

The number one in UNIX Health Checks

UNIX Health Check for Red Hat Enterprise Linux Data Sheet

What is UNIX Health Check for Red Hat Enterprise Linux ?

Usually, organizations monitor their computer systems automatically. So, when something goes wrong, an automated alert will be sent out. However, it is better not to wait until something goes wrong.

How about knowing up front if the Red Hat Enterprise Linux systems are installed, configured and maintained according to best practices? Even before monitoring alerts about it?

That's where UNIX Health Check for Red Hat Enterprise Linux comes in. We provide UNIX Health Check for Red Hat Enterprise Linux software to scan entire systems. It's software that runs on a Red Hat Enterprise Linux system to scan for issues. Just like going to a doctor for a full check-up.

A report of all features of the Red Hat Enterprise Linux system is generated, and it shows how the system is doing. If the system is properly installed, configured and maintained, an all green report with a score of 100% will be given. If for some reason, some things are off, we'll let you know in the report what is wrong, and how to fix it.

Highlights

- Based on best practices and years of experience supporting Linux systems.
 - Improves system health by automatically scanning the system for any known issues and providing suggestions to resolve any issue found.
 - Runs hundreds of checks in minutes.
 - Reduces manual checking and monitoring systems.
 - Avoids system outages by discovering misconfigurations pro-actively.
 - Can be automated to run at set intervals.
 - Verifies systems audit and federal regulations compliancy.
 - Inventories the configuration of the system.
 - Creates reports in CSV, text, HTML or XML format and is capable of sending email reports.
 - Helps to standardize system configurations.
 - Educates administrators on best practices.
-

When to use UNIX Health Check for Red Hat Enterprise Linux ?

UNIX Health Check is beneficial in several stages of a system life-cycle. Most of our customers simply run the entire health check daily, to provide them with a report of their server status. But doing a health check on your systems can also be very useful at certain other important points in time:

- Before putting a new system into production - to make sure the system was installed and configured correctly.
- Before and after doing a change on a server - to make sure no issues exist before applying patches/changes, and that no adverse situations were introduced as part of a change.
- Before or during audits - to make sure a system is compliant with company and federal regulations.
- During yearly performance reviews - to determine if the system administrators have taken good care of the servers.
- Before or during any Bare Metal Restore or Disaster Recovery exercises - to validate that a server has been recovered correctly.
- When doing a security review of a system - ensuring your system's security against outside vulnerabilities, such as hackers.
- When taking over support of systems from others or other accounts to perform an initial system scan.

... and of course:

- As part of the daily routine to check and monitor systems, because not daily reviewing systems, can have costly consequences.

Included

- Red Hat Enterprise Linux operating system, performance, clustering and security scans.
 - Support for a wide variety of operating system levels and hardware.
 - Years of combined experience supporting Red Hat Enterprise Linux systems.
 - Reports generated in CSV, text, HTML or XML output. Reports can be sent out to one or more email addresses.
 - Online documentation and quick start guide.
 - One year support from our technical experts.
 - One year software updates.
 - A fixed price (\$3,750), to plan IT budgets more easily.
 - Absolutely no hassle: It's easy to use!
-

What are UNIX best practices ?

We only employ the best of the best experts on Linux. All our experts are certified and have all gained the highest certification level possible. This requires significant training, reading, and passing at least 5 exams. And most of all, it requires years of on the job experience.

We have seen it all. From minor issues to large system outages; from wrong configurations to large disaster recovery efforts. We have built up an extensive experience on how to configure and maintain servers. We have gathered all this expertise in our products, UNIX Health Check for Red Hat Enterprise Linux.

Also, we derive our best practices from other sources:

- SAS70 audits
Statements on Auditing Standards No. 70, or short SAS70, is developed by the American Institute of Certified Public Accountants (AICPA), and widely recognized as an auditing standard.
- HIPAA
HIPAA, short for Health Insurance Portability and Accountability Act, is a United States law regarding security and privacy of electronic patient information in the healthcare industry, issued in 2003.
- DISA
The Defense Information Systems Agency (DISA) is a United States department of defense agency that provides guidelines for (amongst others) information technology.
- PCI DSS
Payment Card Industry Data Security Standard (PCI DSS) is a security standard accepted worldwide.
- FFIEC
Federal Financial Institutions Examination Council (FFIEC) defines a set of standards for financial service sectors such as online banking.
- Red Hat
Obviously, we also follow Red Hat's (and other vendor) recommendations, and service and support best practices and advisories published by Red Hat.

What happens with the reports generated by UNIX Health Check for Red Hat Enterprise Linux ?

We understand that Red Hat Enterprise Linux systems are critical to the businesses they operate in. UNIX Health Check doesn't transmit any information of Red Hat Enterprise Linux systems. Our software is built to run standalone on Red Hat Enterprise Linux servers. You decide what to do with the information produced by the health check software. All of our software is written in scripting language. It can be reviewed up front, to make absolutely sure that no system information is transmitted outside your company. We don't access client system(s), and we don't get access to system information.

How long does it take to run UNIX Health Check for Red Hat Enterprise Linux ?

Performance is a big issue with us here at UNIX Health Check. We've taken every possible opportunity to make sure UNIX Health Check software runs smoothly and quickly, and without consuming too many system resources. But it depends on the system you're running UNIX Health Check for Red Hat Enterprise Linux on. Obviously, an older system takes more time to run, compared to a new powerful multi-core system. It also depends on the number of users and the number or devices that are configured.

On average, a Red Hat Enterprise Linux system takes a couple of minutes to run UNIX Health Check for Red Hat Enterprise Linux. Some of the latest systems can get close to running it within 90 seconds. Large enterprise systems, with thousands of users and thousands of devices, may take up to 30 minutes to run a full health check.

System requirements

Hardware supported:

- All Red Hat supported hardware is supported by UNIX Health Check, as well as virtual environments.

RHEL levels supported:

- RHEL 5.1 through 5.11
- RHEL 6.1 through 6.9
- RHEL 7.1 through 7.6
- RHEL 8.0
- And matching levels of CentOS, Oracle Linux and Scientific Linux

UNIX Health Check for Red Hat Enterprise Linux needs to be run as user root, and cannot be used by any other user account. This is since several root-level access commands are run by UNIX Health Check for Red Hat Enterprise Linux. Of course, UNIX Health Check for Red Hat Enterprise Linux does not change anything on the Red Hat Enterprise Linux server; it only reports.

To view HTML reports created by UNIX Health Check for Red Hat Enterprise Linux, one of the following browsers is required:

- Microsoft Internet Explorer 8 or higher, or Microsoft Edge
 - Mozilla Firefox
 - Google Chrome
 - Microsoft Outlook or Windows Live Mail (to receive HTML-style reports)
-

What items are checked by UNIX Health Check for Red Hat Enterprise Linux ?

Listing all items checked by UNIX Health Check for Red Hat Enterprise Linux would simply be too much. The software consists of hundreds of checks. Some examples of items that are checked by UNIX Health Check for Red Hat Enterprise Linux are:

- Are the paging spaces set up correctly with the correct sizes?
- Are any unnecessary daemons properly disabled?
- Are the correct levels of openSSH and openSSL installed?
- Is the 64 bit kernel running on a 64-bit capable system?
- Are the firmware levels up to date?
- Are the settings correct for user accounts and passwords?
- Are the retention settings correct backups?
- Are permissions of files and folders correctly set?
- Are the latest updates correctly installed?
- Are all the file systems writeable?
- Are all disks in disk arrays available and functional?

Sample reports and a demo version are available on our website, www.unixhealthcheck.com.

Contact and more information

UNIX Health Check

P.O. Box 6153
McKinney, TX 75071
United States of America

Stratumsedijk 23-H
5611 NA Eindhoven
The Netherlands

Sales: sales@unixhealthcheck.com
Customer Service: support@unixhealthcheck.com
Phone: +1 (469) 343-4311
www.unixhealthcheck.com



Please Recycle

Also available:

[UNIX Health Check for AIX](#)

Use the same functionality of UNIX Health Check for Red Hat Enterprise Linux on all your AIX systems.

A discount of 20% applies if both UNIX Health Check for Red Hat Enterprise Linux and UNIX Health Check for AIX are licensed together.
