ULTIMATE SERVER HEALTH CHECKLIST

GROSSMENDELSOHN
TECHNOLOGY SOLUTIONS GROUP

Baltimore, MD 21202
410.685.5512
Contact Us

Fairfax, VA 22030
703.537.0576
Contact Us

What is Server Health?

There are several factors that determine server health. For the purposes of this checklist, we'll define server health as the level at which your server and network is performing. If your server is in good health, it means that your server is running at optimal performance.

Server maintenance requires checking multiple aspects of your network, including hardware, software and user activity. Not only do these elements have to be functioning properly in your network, they also have to be communicating with each other effectively. If the pieces aren't communicating with each other correctly, you could have a disaster on your hands.

Another important aspect of good server health is a disaster preparedness plan. You'll need to be prepared for an emergency, such as a flood, hurricane or hack. Having a disaster preparedness plan could define whether that emergency becomes a cakewalk or a nightmare.

Your networking provider may have given you further maintenance tasks to promote wellness in your custom networking setup. For help on completing the following tasks or further server health advice, we recommend contacting our trained networking engineers.

CONTACT OUR NETWORK ENGINEERS HERE

- [ ] Check for and Install Operating System (OS) Updates Monthly. System updates are important to keep up on. They're created by the manufacturer to improve the software process to maximize efficiency and safety or the user experience.
    - Update Outside Of Peak Business Hours. This process can take several hours to complete and could lag the network system. It's much easier to perform updates when you're not getting inundated with staff calls about the computer lag time.

- [ ] Check for and Install Applicable Hardware Updates Quarterly. In order to function at optimal performance and combat emerging threats, all hardware in a server needs to be checked and updates installed every quarter. All mainstream server hardware manufacturers have management software specific to their systems. Though diagnostic programs such as the management software show update levels and track the server functions, it's essential to physically check out the server to ensure that everything looks like it is working properly.

- [ ] Visit Your Server Management Program Dashboard Monthly. Your server management program monitors and logs each component of your server in a dashboard.
    - Review The Dashboard, which should detail various data points about your server performance, including important events and usage statistics.
    - Check Email Notification Settings. You should double check that the correct email is setup in the program so that emails get sent to the right person when there is an error that warrants immediate attention. It's imperative to make sure the existing notification emails are correct.

- Check To Make Sure The Dashboard Is Installed. The server management program is usually supplied by the hardware manufacturer. Sometimes we've seen that companies forgot to install this component in their network. Your server manufacturer might be able to supply another copy of the dashboard; it's a big help for monitoring server functions.

☐ Check Your Free Disk Space Monthly. A lack of free disk space can spur a variety of issues. If there is less than 15% free disk space on your server, then you need to archive some data or upgrade your storage.

When disk space reaches that level of capacity, it tends to slow down server processes and put your network at risk for a crash. The best way to reduce this risk is to ensure that the free disk space occupies at least 20% of the drive.

☐ Verify Your Server Backups Monthly. Backup data is there for us when an important file is accidentally deleted. Backup data should be double checked by restoring a few random files to a temporary location.

- Perform Frequent Data Backups to ensure that you'll be covered in case of an emergency. Though we like to think of our backup data as a recovery to the simple, "Oops, I deleted this file" conundrum, it is essential for the occasion when company data is put into a disastrous situation.

☐ Check Your Antivirus Security Monthly. Antivirus is the first line of defense when it comes to large server networks. You'll want to make sure your subscriptions are current and there are no critical messages that need attention.

☐ Follow Security Best Practices. Though antivirus software is important, there are additional best practices that are even more so to ensure network security. These best practices include:

- Update User Permissions and admin rights on your network so that your staff only has permission to what they need.
- Remove Inactive Users From Your Network. It's risky to allow past employees to have access to your company data.
- Train Your Employees on Network Safety procedures frequently so they understand how to handle risky emails, websites and more.
- Read This Blog Post to learn more about the best practices you can take to safeguard yourself against harmful malware.

☐ Check the Battery Backup Management Software Quarterly. The battery backup management software is synced with your uninterruptable power supply (UPS) units. This software is usually supplied by the UPS manufacturer.

- Review Your UPS Dashboard. Depending on the battery backup management software your company has chosen, you can receive information regarding the battery power status, power management events, power disruptions sources and more.
- Identify Where Error Messages Are Sent. Like the server management program, most battery backup management software identifies critical errors and alerts registered users. When checking this software, make sure the right personnel are getting notified and that there are no outstanding errors that need attention.
- Test Your Uninterruptable Power Supply (UPS) System Annually. Testing the UPS system can be tricky. The simplest way to test if your UPS is working correctly is to simply unplug the unit and see if the appropriate server alarms sound and if the server continues to power the device.
- Don't Forget To Backup. Though unplugging is the easiest way, you need to ensure that your data is 100% backed up before testing your UPS. If the UPS fails, then your test could turn into a nightmare to deal with.

☐ Review the Application and System Logs Monthly. The application log and the system log need to be checked frequently for any signs of critical errors or warning entries. The errors and warning entries provide insight to where problems are coming from and provide a stepping stone for pinpointing solutions.

- Monitor User Activity. Reading these logs can also give networking personnel insight into users' activity on the network. Understanding user activity can identify potential security risks and allow network experts to proactively address risky activities.

☐ Ensure Your Operating System Is Current Annually. Having an updated operating system is not only critical to network safety, but also it adds to the overall efficiency of your business. An outdated operating system lacks the sophistication required to handle the modern-day server safety risks.

- Chat With Your Network Advisor about Your Operating System. Your networking advisors will be able to tell you the limitations of an antique operating system. Software manufacturers stop issuing security patches for end of life systems. Without these patches, your network is vulnerable to attack.

☐ Enforce complex passwords. Research has shown that using a complex, randomly generated password is vastly more secure.

- Ensure That You Have Rules Set For Your Company Passwords. Any password that is simple to guess can be cracked in seconds. Randomly generated passwords are far superior. They should be 8 or more characters in length with upper and lower case letters and at least one number plus a special character.
- Don't Go Overboard with Employee Password Changes. That same research mentioned before shows that too many password changes forces users to choose predictable and easy passwords to guess.

Yearly Server Examination with Our Professionals

Performing regular maintenance to your server is the first step to protect your investment. This checklist should serve as a starting point to your server health journey in conjunction with an annual server examination from your networking provider.

The annual server examination is a chance for an expert to identify how each networking component is functioning and if it is the right setup for your company needs. We offer a Yearly Server Checkup to our clients to make sure that the service they are getting is always at high performance. Our networking gurus' expertise qualifies them to understand each server setup, no matter how complex, and determine how it can be improved.

Additionally, we offer a free network assessment with our trained network engineers. In our network assessment, your specialist will provide a complimentary report that will identify your network information, including:

- Password complexity
- Low disk space
- Missing security patches
- Missing antivirus and anti-malware protection
- Outdated operating systems
- User account inactivity
- Ports exposed to external vulnerabilities

To contact our lead networking engineer, Bill Walter, MCP, MCSE, click here or give us a call at 800.899.4623.