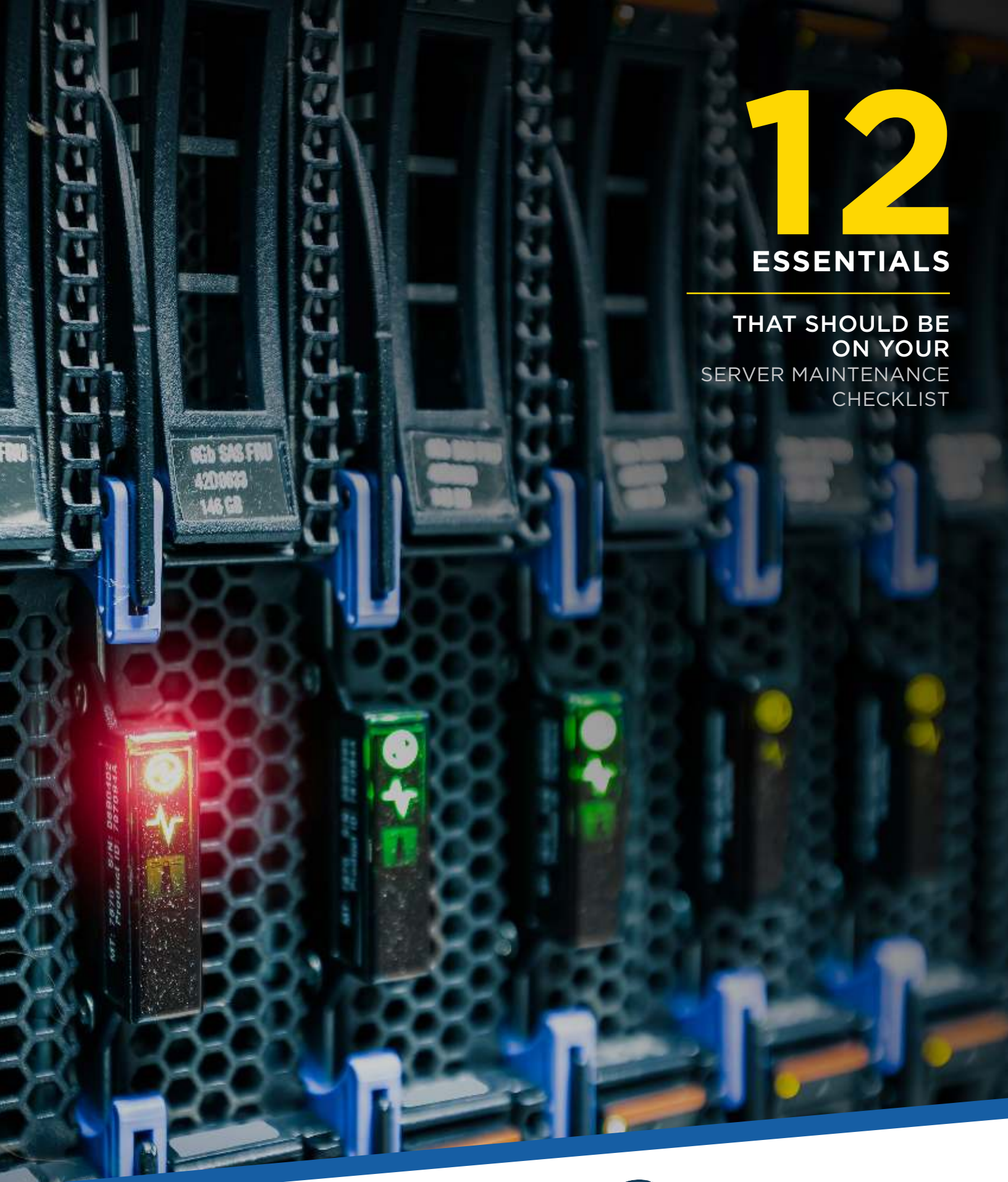

12 ESSENTIALS

THAT SHOULD BE ON YOUR SERVER MAINTENANCE CHECKLIST

WORLDWIDE SERVICES
MANAGED IT SERVICES & SOLUTIONS

SERVER MAINTENANCE CHECKLIST

Now that you understand what server maintenance means and why it's important, the next step is implementing a server maintenance plan. So how do you maintain a server?

To keep up with regular server maintenance, your business needs to create a server maintenance administration plan. This plan details what maintenace tasks you need to perform and how often you need to do them.

> **It can be difficult to filter through** server maintenance tips to develop a cohesive plan. To help, we've created a **server maintenance checklist.**

1. CHECK BACKUPS

Backing up data is one of the single most important things your business can do to prevent catastrophic data loss. The last thing your business needs is for your backup system to fail just as a major event occurs. For this reason, regularly checking that your backup system is working is essential.

Test your backup system either by running test recoveries or by mirroring the server environment in a virtual machine. While testing the backup system, also assess where the backups are located and determine if they need to be moved.

Backups should be checked very frequently. A few minutes a day is ideal, though your business should be checking them every week at a minimum. Though this may seem overly frequent, it is better to have a great backup system and not need it than to need it and not have it.

2. CHECK THE RAID ARRAY

RAID stands for Redundant Array of Independent Disks, and many dedicated servers run a RAID array. This array serves as a storage device in the event that one disk fails, preventing data losses. Without a functioning RAID array, the entire system may fail, resulting in massive losses. This is easily prevented by regularly checking the RAID array.

In many cases, RAID arrays have built-in advanced monitoring tools. To check in on your RAID array, you simply need to check your monitoring tool, which alerts you to potential failures ahead of time. By checking the RAID array daily, semi-daily or weekly, you can plan replacements and rebuilds proactively, minimizing downtime.

3. CHECK SERVER UTILIZATION

Regularly review server resource usage, as these numbers indicate how well your system is functioning and lend clues as to how to improve performance. The three primary utilization numbers to look at are:

Memory: Servers are meant for production, not archiving. If your system is storing useless information on its hard drives, it is unnecessarily slowing down your system. Regularly check your server for old log files, old emails and outdated software versions and delete what you can. If you need to keep old log files or emails, consider archiving them to external storage instead. You can do this manually or use a cleanup protocol to move these files to an archive automatically.

CPU: Processing power is essential for servers, but the closer servers get to 100% processing power, the more likely they are to shut down.

Network use: Server loads have a network capacity as well. This is the maximum amount of hardware a network can support before it starts to encounter errors and failures. If the server reaches 100%, the likelihood of data loss increases substantially.

Look at your utilization numbers on a weekly, if not daily, basis. If any of these numbers are regularly approaching 100% utilization, look into how to improve each individually. If two or more frequently approach 100%, this is an indicator that the server is overburdened. You can fix this by upgrading or adding additional servers.

4. UPDATE THE CONTROL PANEL

If your business uses a hosting or server control panel, update it regularly. This includes updating the control panel itself as well as all the software it controls. Usually, this needs to be done manually, as updating a control panel does not automatically update the applications it controls.

5. UPDATE SOFTWARE APPLICATIONS

Servers may host any number of software applications, but all of them need to be updated regularly to take advantage of new functions, integrations and security measures. While some systems have package managers that automatically update software, others require you to review and manually apply software updates.

Web-based software applications are particularly crucial to update regularly. Web applications are the area of greatest cybersecurity risk for companies, with 20% of vulnerabilities associated with these applications. Regularly updating these applications takes advantage of new security measures from the production teams.

6. CHECK REMOTE MANAGEMENT TOOLS

Remote management tools allow users to log into, manage or monitor a server without being physically present, which is essential if the user runs a cloud-based virtual server environment or manages servers remotely. These tools include the remote console, remote reboot and rescue mode. If you use these tools, check up on them regularly to ensure that they are updated and functional. If any remote management tools are showing errors, reboot or update these systems.

7. UPDATE OPERATING SYSTEMS

Operating system updates are essential but tricky to navigate. Regular updates are necessary for protecting your systems from new cybersecurity threats, but depending on how you manage your operating system, updates pose different problems:

+ **Official patches:** While official patches and updates can resolve security problems and improve performance, hackers often plan attacks around OS patches, attacking weaknesses before they can be caught and patched.
+ **Custom software:** In some cases, administrators may choose to customize their software to fit their specific needs. However, this can pose serious problems when it comes time to update the system. Custom software may conflict with the updates, resulting in software instabilities that can put data at risk.

> **Regardless of the OS route you choose,** dedicate time to review OS updates regularly. If you are especially concerned, **you can create a test environment** to test any system updates before rolling them out.

8. CLEAN AND CHECK SERVER HARDWARE

Server hardware needs physical maintenance as well as virtual maintenance. Dust and debris can quickly build up inside and outside the server, getting into circuit boards and fans. This dust buildup interferes with the server's ability to manage heat, resulting in the server getting hotter over time. The hotter the server, the worse the server performs, and the more likely the server is to fail.

On top of cleaning servers, also check the server's environment. Make sure that the server room temperature is properly maintained and that the cabinets have plenty of airflow to help with heat management. Also, check for any unusual wiring or unexpected equipment, such as flash drives, as these can be signs of errors or security breaches.

9. CHECK SERVER LOGS

Modern server systems maintain logs that track errors on the server system and in the hardware. Server error logs can include information on software errors, data loss, user access anomalies and more. Hardware error logs include logs on overheating systems, disk read errors, network failures and hard drive problems.

Logs keep detailed information on errors so that you can pinpoint and resolve these issues before they escalate into system crashes. Regularly review these logs for any signs of problems so that you can proactively address them. It's especially important to check these logs if your system has recently started operating outside of normal ranges.

10. EVALUATE USER ACCOUNTS

It is the nature of businesses to change, and that includes changes in staff and users. Any accounts that are no longer in use need to be removed, as they pose a security and legal risk to your business. Hackers or disgruntled former employees can exploit unused accounts to gain entry into your system.

Additionally, regularly check account permissions for existing users. Promotions and department transitions can result in users having access to databases that they no longer need for their daily duties, leaving open another access point for potential exploitation.

11. EVALUATE SERVER SECURITY

Regularly evaluate your server security software and policies and update them as needed. This includes the following:

+ **Testing existing systems:** Test your existing network from the outside to see how easy it is to gain access. You can do this using an internal tester or a third-party network security tool. Also, regularly audit your system for any potential risks or improvements.
+ **Training employees:** Review security training with employees regularly, including proper password hygiene, email protocol and safe internet usage.
+ **Reviewing password security:** Password hygiene is a must for all businesses, as this serves as the first line of defense against hackers. Regularly evaluate your company's password policy and communicate your expectations to users. You may also consider setting password change requirements in your software systems or establishing mandatory password changes every six to 12 months.
+ **Assessing new tools:** Regularly assess potential software or services that your business could use to improve security or functionality. Some examples include third-party security services and network monitoring tools.

BE SURE TO ASSESS YOUR SECURITY **AT LEAST QUARTERLY.**

12. REVIEW SERVER MAINTENANCE REGULARLY

Like all technology, servers and server systems change frequently and rapidly. Because of this, it is essential to regularly review and update your server maintenance checklist to meet the needs of your system. Especially important is updating how frequently you check certain aspects of your system. Whether you check an area of your server daily, weekly or monthly depends on several factors, including the following:

+ **Urgency:** Some server configurations impact your immediate daily functionality, while others don't. Some examples of more immediate configurations include data backups and email routing — if either of these went down, your company would feel the impact immediately. On the other hand, server memory and hard disk space don't impact your business' daily operations as directly, so they can be checked weekly or monthly unless an issue occurs. Assess which functions are most urgent for your company and base your server maintenance around these priorities.
+ **Automation**: Certain maintenance functions can be automated to handle the daily tasks needed to keep your server system running optimally. If your system automates certain functions, take this into account when judging when to manually check that function.
+ **Age:** The older your server equipment, the more frequently you will need to monitor it. Older systems may decline in function more quickly, so they require more frequent maintenance check-ups.

The network administrator should review maintenance protocols on an annual basis or whenever there are major changes to the server.

Work With a Server Maintenance Company

This checklist gives you an overall idea of how to maintain a server and what steps are involved. By following this checklist and tailoring it to your business's needs, you can ensure that minor server issues don't escalate into complete system failures. While these steps are essential, many companies don't have the time or resources to conduct proper server maintenance. IT server management from Worldwide Services can help.

Worldwide Services is a global provider of network and telecommunication services and equipment, and we offer IT server management that can help you keep your servers running smoothly. Our server maintenance plan handles all the steps of server maintenance for you, including security, so you can rest easy knowing that your servers are in good hands.

To learn more about Worldwide Services and our IT server management, contact us today.

Tel: +31 (0) 20 808 5138. E-mail: europesales@worldwideservices.net

Sources:

1. https://computer.howstuffworks.com/what-is-network-server.htm
2. https://www.webopedia.com/quick_ref/servers.asp
3. https://searchstorage.techtarget.com/definition/RAID
4. https://www.infosecurity-magazine.com/news/web-application-security/
5. https://blog.etech7.com/what-is-a-server-maintenance-plan-and-why-is-it-important
6. https://www.rackaid.com/blog/server-maintenance-checklist/
7. https://phoenixnap.com/blog/server-maintenance-checklist
8. https://worldwideservices.net/services/server-maintenance-services/