10 Ways to Keep Your Video Server Running Optimally

IT Brief

Any security manager who has been tasked with overseeing a network can understand the frustration of server and other equipment failure. Sometimes, these malfunctions are a result of manufacturing errors or electrical issues, but more times than not, server issues are a result of user negligence. Servers are a lot like cars; it is important to perform periodical maintenance to ensure they are running optimally and more importantly, to ensure their longevity.

Failure to consistently check the overall condition of your servers can lead to a variety of problems such as overheating, network inefficiency, and unauthorized security breaches.

To ensure your video servers continue to run like a well-oiled machine, we created a monthly IT maintenance checklist that will help you save both time and money.

More times than not, server issues are a result of user negligence.

1. Visually Inspect Servers

Conducting visual checks on servers and hard drives is an important aspect in ensuring they run optimally. Most servers have intuitive lights (or LEDs) externally displayed so that an end-user is always aware of the server's status and can spot any immediate red flags. Typically, blue or green lights signal good status, while red or orange lights often signal some sort of failure - whether it is the device or connection. Some servers can email you alerts whenever there is a hardware failure. Ignoring the server status lights could result in system failure and the potential for video loss if it's a hardware malfunction.

2. Update and Schedule your Operating System and Anti-Virus Software

Just like your home computer, servers are susceptible to viruses. If you have a publically accessible server, be sure to consistently keep your operating system up to date and frequently run an anti-virus scan on it. Your anti-virus software should be the most current version and should meet all industry standards. A corrupt server is not only prone to slower performance and internal server errors, but also leaves your server open to possible external security risks. Finally, it is important to ensure that your firewall software is properly configured and turned on.

3. Schedule a Defragmentation

When a server attempts to locate files that are fragmented across the hard drive, the bandwidth it takes to locate and group individual files into one can slow down your entire system. Scheduling and performing a defragmentation to your server's hard drive will pool all fragmented files together, making them easier to find. Keep in mind that some servers, such as Avigilon's, do not require users to perform a defragmentation because fragmented files are already blocked together and written to the hard drive in the same place upon installation.

4. Review Operating System Logs

The practice of reviewing operating system logs is standard to server operation. If you have a Windows-based system, make sure you check the activity logs to ensure there are no out-of-the-ordinary or suspicious audit entries. Not following up with "Critical" or "Warning" events may lead to system failure, resulting in loss of video and disconnected system access.

5. Audit the Active Accounts

In organizations of all sizes, over time there is bound to be turnover. As a security measure, it is important to keep track of the employees that have access to servers and ensure that former employees do not have access to your system. Be sure to delete old users and change passwords when necessary.

6. Verify Retention

Make sure you have record of your servers' storage capacity. Since cameras typically record on motion detection, if there is an increase in activity in the area you are monitoring, your retention time may be affected. To verify the amount of storage you have, check out your software's timeline and confirm the number of days that are being recorded. You don't want to try to locate important footage from a few weeks back only to find out it has been erased.

7. Delete Unnecessary Bookmarks

Managing your server's saved footage is very similar to using your TV's DVR. Keeping old bookmarks for surveillance video in your server is the equivalent to hoarding a stockpile of recorded TV shows you don't watch. Too much data saved unnecessarily will impact your storage space and the amount of footage you are able to retain. Be sure to delete and/or export saved footage you don't need to maximize your server's storage space.

> Keeping old bookmarks for surveillance video in your server is the equivalent to hoarding a stockpile of recorded TV shows you don't watch.

8. Check UPS Battery

Power outages happen. As a result, it is important to ensure your security and your servers are not compromised in the event of electrical failure. When installing a server, customers should add a UPS or backup power supply to protect their information in the event of a power failure. Upon installation, customers should also perform a quick test to confirm the backup battery is working correctly.

9. Ensure Software is Up to Date

Verify that software is up to date for both the video management client and the server. This will enable you to optimize your software and ensure that bugs from previous versions do not affect your current system. Being negligent with software updates could be a security risk as updates may fix important issues in previous versions of your software.

10. Auditing Logs of Users activity

It is always a good idea to audit user activity on a site to ensure users are adhering to protocol. Check activity logs to be sure users are being responsible and ethical with their access.