SimplStor® Management Best Practices Checklist

SimplStor systems are engineered to meet the requirements of our global clients in a variety of network storage environments. Based on customer support tickets over the last 30+ years we have created a list of best practices for our customers to use as a guide as they create or update their own Best Practices for their critical storage environments and ensure a clean, safe, secure environment for your data storage.

3-2-1 Backup

SimplStor systems are designed to provide secure and reliable data storage. However, nothing is fault-proof. Verify that Backups and Mirrors are completed on time without file corruption.

Security, Security!

Ensure the default SimplStor passwords have been changed. Zerowait Engineering can guide you through the entire process to ensure your data is safe.

Patch It Up!

Ensure that the SimplStor components have current firmware and software updates to keep you updated on security and bug fixes. Before patching systems, verify that the updates will not negatively affect your environment.

Everything Has Its Capacity!

Ensure aggregates and volumes are never at total storage capacity (less than 85% is recommended). A storage system at 100% capacity will most likely have performance issues and other potential problems down the road.

Monitor the Monitor!

Ensure that SimplStat monitoring is regularly sent to the designated system administrators and Zerowait support. Actively receiving error logs is imperative to identify potential issues.

Don't Get Caught on the Side of the Road with a Flat Tire!

Always ensure the SimplStor has spares available. We always advise having at least (1) hot spare available for each drive type to avoid the risk of data loss. For larger systems, one spare minimum per RAID group. Cold spares are also encouraged for more critical components that fail frequently.

SimplStor

NETWORK STORAGE SOLUTIONS BY ZEROWAIT

Schedule the Update!

Complete monthly update(s) of the SimplStor operating system and reboot when applicable. Updates and Reboots are always an excellent strategy to avoid lingering issues that grow over time.

Keep the Bad Apples Out!

Ensure the prompt replacement of any failed components. Failed components can sometimes have a domino effect on the NAS device and cause additional failures in the system.

Clean Your Room!

IT departments are always concerned with cyber security paralyzing your network infrastructure. However, no one considers the dust and debris that is collecting in your server room, which can shut down your SimplStor without notice. Ensure you have a quarterly cleaning schedule to remove any dust and moisture from your data room. Ensuring adequate ventilation and temperature settings is essential to avoid data loss on your NAS equipment.

Keep Your Emergency Checklist, Contracts, and Contacts Updated!

Who are you going to call in an emergency? Create an up-to-date system to maintain equipment support contracts and contacts. Equipment and contact information often change regularly and when things go wrong you need to know who to call to get your systems back online!

If you need assistance with installation, configuration, or anyother aspect of SimplStor email support at support@simplstor.com

707 Kirkwood Highway | Wilmington, DE 19805 | P: 888.850.8008 | E: sales@zerowait.com | W: www.SimplStor.com