

Cloud Computing Patch Automation Checklist



PHYSICAL HARDWARE CHECKS

- Check hardware termination.
- Check cloud computing hardware interoperability.
- Identify any hardware faults on servers, printers, etc.
- Check functionality of other cloud computing peripherals.
- Investigate any disconnected cables.
- Check for incorrectly connected cabling.
- Check for error indicators.



EVENT LOGS AND SERVICES

- Check system, application, Domain Name System (DNS), Functional Requirement Specification (FRS) and security logs.
- Archive old events with appropriate dates.
- Troubleshoot error events and warnings that arise in your cloud computing environment.
- Check cloud computing services for failed startups.
- Check the correct services are starting up.
- Disable unnecessary services.



BACKUP AND RESTORE

- Check Backup logs for errors.
- Verify Backup Job Consistency.
- Perform Test Restore using recent Backup Media.
- Ensure Backup is running on schedule.
- Run a cleaning tape when required.



DISK MANAGEMENT

- Check disks for data integrity and consistency. Analyze disk performance and usage.
- Check status of Redundant Array of Inexpensive Disks (RAID) configuration if applicable.
- Perform and or schedule a chkdsk and defragment disks if required.
- Check disk capacity.
- Clear temp files.
- Check network shares and disable any unnecessary shares.



CLOUD COMPUTING SOFTWARE UPDATES AND LICENSING

- Check for operating system updates.
- Assess cloud computing components for application updates.
- Check any third-party applications for updates.
- Ensure antivirus definition update scheduling is operational.
- Check for updated printer drivers.
- Ensure product licensing is current and valid.



ANTIVIRUS

- Check event, history and virus logs in your cloud computing environment.
- Check scan schedule times.
- Clear quarantined items.
- Ensure antivirus definition updates are occurring in your cloud computing environment.



CLOUD COMPUTING SECURITY

- Enable and check firewall and router logs. Troubleshoot findings.
- Perform penetration tests on network/servers.
- Perform security checks on other cloud computing applications and files.
- Check wireless authentication, encryption, access control and logs.
- Check for password strength policies.



ACTIVE DIRECTORY

- Check Active Directory replication.
- Check Active Directory using replmon, dcdiag, and/or netiq tools.
- Monitor Active Directory performance.
- Audit and remove unnecessary user accounts.



MICROSOFT EXCHANGE MAIL SYSTEM

- Check Exchange event logs.
- Clear dead and/or bad mail.
- Check individual mailbox space usage and note any large mailboxes.
- Ensure replication and routing events are successful.
- Schedule a database compact using either isinteg or eseutil tools.



CLOUD COMPUTING NETWORK PERFORMANCE

- Check network utilization rates.
- Monitor any excessive broadcast traffic.
- Identify any network bottlenecks.



MISCELLANEOUS MAINTENANCE TASKS FOR CLOUD COMPUTING

- Check server performance using perfmon.
- Check (Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS) and Windows Internet Name Service (WINS) configurations.
- Check Windows Server Update Services (WSUS) synchronization logs.
- Approve any necessary updates to your cloud computing environment.
- Confirm group policies settings.
- Check the uptime of servers, switches, and routers.
- Test Universal Power Supply (UPS) battery performance.
- Make a hardware profile in case you need to roll back your cloud computing environment to the last known working config.
- Test your contingency remote access mechanism(s). Examples are PCAnywhere, Terminal Services, Virtual Network Computing (VNC), HP Integrated Lights-Out (iLO) management port.

CompTIA's vendor-neutral Cloud+ certification validates the skills needed to maintain your cloud computing environment and automate patching tasks.