# Server Hosting Basic Services System Administrator Duties

## Project/Workloads

- Tune the operating system (OS) kernel
- Monitor system logs: DISA provides auditing services of operating system level log files via the Log Aggregation-Single Service Environment (LA-SSE) program. LA-SSE provides automated auditing and notification of events identified as warranting investigation per established cyber assurance threat signature patterns.  Signature patterns and criticality of events are determined by DISA Cyber Assurance and DISA subject matter experts.  LA-SSE provides capability for immediate notification as well as historical recaps of auditable events. Actionable events are escalated to the Global Service Desk monitoring views and routed to appropriate Command and Control (C2) groups for action. C2 assignees determine if an audit event warrants notification to the mission partner Cyber Assurance group for informational purposes and action. Historical notifications are routed to the DISA site security element for informational purposes and pattern/trending analysis.
- Install software and associated patches
- Perform Windows server admin and secure Internet Information Services (IIS)
- Provide after-hours support for incidents and authorized service interruptions (ASIs)
- Monitor console messages and system logs
- Configure and manage replication and/or cluster environment software
- Assist vendor during troubleshooting/hardware repair
- Ensure Netbackup software is installed and configured
- Schedule backup for file systems
- Coordinate with application/database administration
- Review backup reports daily
- Change disk space allocations
- Update technical leads and management

## Incident Management

- Perform break/fix actions
- Work with service desk personnel
- Escalate incidents
- Review/update all assigned tickets

## Problem Management

- Perform root cause analysis (RCA)
- Develop workarounds and publish to the Known Error Database (KEDB)
- Update assigned tickets
- Escalate tickets to Tier III

**Change Management**

- Provide system and component information
- Add all new systems to the Configuration Management Database (CMDB)
- Remove all decommissioned systems or components
- Document all changes to include a Continuity of Operations (COOP) plan
- Coordinate with application, database, and web administrators

**Enterprise Information Services (EIS) & Enterprise System Management (ESM) Tools**

- Monitor the operations status of production systems
- Ensure Host-Based Security System (HBSS) is installed and functioning
- Configure all systems to Sensage
- Ensure the ESM agents are configured and installed
- Ensure Tivoli components are configured and installed

**Security**

- Verify Communications Tasking Order (CTO)/Fragmentary Order (FRAGO)/Information Operations Condition (INFOCON) requirements
- Resolve vulnerability scan results
- Validate all applicable postures within the Vulnerability Management System (VMS)
- Ensure timely updates to findings for assigned systems
- Perform annual Secure Readiness Reviews (SRRs)
- Apply all required patches
- Adhere to US Cyber Command (CyberCom) Information Assurance Vulnerability Alerts (IAVAs)/bulletins/tech advisories
- Participate in audits for partner/site accreditation
- Create and update VMS Plan of Action and Milestones (POA&M)
- Ensure anti-virus software is installed/configured
- Schedule anti-virus scans and definition updates

**Account Management**

- Manage user accounts at the OS level
- Ensure admin/root passwords are changed/maintained