

Job Title: Systems Administrator
Location: Fort Carson, CO
Type: Full-time
Salary: Commensurate with experience

Required:

- Minimum of 3 years System Administration services and support experience.
- IAT Level II certification
- Active/recent U.S. government security clearance.

Desired:

- Microsoft Endpoint Configuration Manager (MECM)/INTUNE Training
- PowerShell Training or Experience

Job Description:

Candidate shall have knowledge of a large variety of end-point management toolsets to include but not limited to Microsoft Azure Active Directory, Intune, Microsoft Endpoint configuration Manager (MECM/INTUNE), and Defender for Endpoints (MDE) in order to implement configurations and troubleshoot product sets. The candidate shall utilize the aforementioned toolsets to install, configure, operate and administer the patch management, update distribution, computer image deployment configuration, compliance, and Network Access Control (NAC) application services of a large enterprise network consisting of both physical devices and Virtual Desktop Infrastructure (VDI) to include but not limited to VMware Horizon, Azure Virtual Desktop (AVD), and Microsoft Hyper-V. The candidate shall monitor Network Access Control (NAC) administration, management, and control to assist the Government in ensuring accurate compliance standards are set in keeping with released software patches and current IAVM alerts, bulletins, and technical guides

- Develop innovative technical solutions, troubleshoot MECM/INTUNE faults, and leverage MECM/INTUNE and PowerShell to collect needed data from client assets.
- Create MECM/INTUNE management reports an average of 5 times per month as assigned through the AESD ticket; gather data to support daily operations for the IT enterprise leveraging reports; run compliance and troubleshooting reports in MECM/INTUNE an average of 25 times per month.
- Package software using MECM/INTUNE and other methods, including PowerShell scripts, command line batch files, and other packaging software, to develop, evaluate and deploy software to all applicable MECM/INTUNE supported platforms (approximately 14,000 devices) using Windows Installer technologies. The average number of deployments using MECM/INTUNE is approximately 30 software packages per month. Accomplish Microsoft Windows software patches and updates, third-party software updates, and remediation based on vulnerability scan results provided by Cyber Security Division. Manually update, patch, or remediate any devices that fail to receive a packet.
- Gather requirements, as assigned through the AESD ticket, for desktop applications and automate the installations so that little to no end user interaction is required and to time required restarts to minimize customer impact. Coordinate with Customer Management Branch team to ensure that software gets deployed and installed to advertised devices, and provide reports and analysis upon request of the COR. Install service packs, hot-fixes, and application updates for all MECM/INTUNE infrastructure and clients; create and maintain documentation for application deployment/packaging, administrative procedures, MECM/INTUNE architecture, and troubleshooting client issues using system CONOPS.
- Maintain and create new OS deployment task sequences for computer image deployment and use User State Migration Tool (USMT) to backup user data for post-image data restoration on newly imaged computers. Assess, implement and document complex tools and utilities (e.g. compatibility, identification, diagnostic, monitoring, etc.) to automate desktop tasks and actions; troubleshoot and resolve MECM/INTUNE performance issues; configure MECM/INTUNE infrastructure through client agent installation and configuration, site boundaries and system roles, and discovery methods; schedule client maintenance tasks to minimize computer user service interruptions; and manage MECM/INTUNE asset inventory by validating the data and inputting it into change management databases.
- Perform tasks using IT management tools and applications such as: Microsoft Operating System Deployment (OSD), Windows Deployment Services (WDS), Windows Administrator Deployment Toolkit, Windows Server Update Services (WSUS), Forescout, Azure technologies. Microsoft Office 2016/2019/365 suites, Windows 10/11, Windows Server 2019 operating systems and Microsoft Management Console (MMC). Integrate these listed tool sets with MECM/INTUNE for a comprehensive, overall administration and management solution for enterprise assets. Use Windows Management Instrumentation (WMI), Visual

Basic, Windows PowerShell, and PSEXec scripting tools for both data collection and workstation administration across the enterprise.

- Plan and execute unit and systems testing; install applications and images remotely; provide technical support on execution problems; troubleshoot applications packages; and modify applications, as necessary.
- Access permissions on computers; reconfigure file structures; ensure systems are configured according to policy, and computers on the installation are protected from viruses. Use local group policy objects and domain group policy objects to ensure a secure, yet functional, user computing experience.
- All of the above requirements will be assigned through the AESD ticketing system consisting of approximately 75 work orders/trouble tickets averaged per month.
- The LNECs process approximately 200 tickets per month. This number is only utilized as an awareness that travel may need to be utilized to support the O&M at the LNECs as prescribed in the Scope paragraph.

Physical & Mental Requirements: Performance of essential and ancillary functions may require:

- Bending, stooping, and sitting.
- Walking or standing for prolonged periods.
- Ability to lift up to 50 pounds.
- Requires near vision acuity to review written documentation.
- Ability to hear and understand speech at normal room levels and on the telephone.
- Manual dexterity to operate a telephone and keyboard.
- Ability to lift horizontally and vertically.

Clearance:

Selected applicants will be subject to a government security investigation and must meet eligibility requirements for access to classified information. Hire dates are dependent upon the issuance of an interim or final government security clearance.

Background Check:

Offers are contingent on successful completion of professional reference checks, employment history verification, and background screening.

GStek, Inc. is proud to be an Affirmative Action/Equal Opportunity employer. All qualified applicants will receive equal consideration for employment. GStek encourages veterans, disabled veterans, and disabled individuals to apply for any open position for which they feel they are qualified.

EOE Minority/Female/Veteran/Disabled