Senior Linux Systems Administrator and Security Analyst Senior Linux Systems Administrator and Security Analyst Senior Linux Systems Administrator and Security Analyst - Department of Interior, USGS Rockville, MD Authorized to work in the US for any employer Work Experience Senior Linux Systems Administrator and Security Analyst Department of Interior, USGS July 2017 to Present Performed system administration including troubleshooting, fault isolation, system tuning, and Maintenance ? Patch management- Developed patching procedures for critical production servers. Used Ansible script to automate patching for staging, development and production Ubuntu servers ? Developed and set up backup and patching methods for entire linux environment ?Management of the Red Hat Satellite- Attached subscriptions, added hosts, managed all hosts, deployments ? Used Red hat Satellite to deploy and automate patches to environment ? Setup cronjobs to cleanup any zombie processes left running from hung sessions ? Created snapshots for backup and cloning of instances ? Design, and implementation of customized technical virtualization solutions for clients taking into account size, infrastructure, data protection, disaster recovery, and application requirements. ? Created patching and backup baseline/work flow ? Installed and configured both local and external repos to get packages for installs and updates ? Cloning to templates, modifying vm templates, creating vm snapshots ?Performed datastore migrations ?Building servers using VSphere VmWare (either by attaching specified images to the datastore or using configured preexisting templates. ?Recovering replicated virtual machines from original datacenter during migration ?Configuration of virtual machine network cards per associated VLan environments ? Logical volume management ?Provide support to clients on security team - Fixed vulnerabilities found on systems after reviewing Nessus scan results ? Installed and configured postfix and mailman from scratch and integrated both to create a fully functional mailing list server and provide continuous support to hundreds of users of said server ? Configured firewall to allow access for both local and external users ? Researched client best server monitoring application with power point presentations on best approach ? Monitoring, fine tuning and setting up alerts ?Configuring firewall ports ? Swapped damaged disks and removed old ones and replace with new disks ? eFTP migration from physical servers to virtual ? Added hosts on satellite server using keys ?

Opened client firewall ports ? User management ? Manually excluded packages for updates and installs ? Manually applied package updates to RHEL Systems to meet updated standards ? Configured login for users so that they can use their AD credentials to SSH into servers ? Configured passwordless login for customers to fulfill security controls ? Install and configure antivirus on linux systems ,edit configuration files and setup cronjob to run scripts and scans on a daily basis ? Analyze problems and make sound decisions for solutions ? Monitor servers using Xymon monitoring tool and respond to alerts depending on how critical ? Provide support to database admin, and application developers ? Reviewing, maintaining, and ensuring all Assessments and Authorizations (A&A) documentations are included in the system security package. ? Oversee the preparation of the C&A (Certification and Accreditation) packages for the approval of an ATO. ? Perform updates and review the System Categorization using FIPS 199, E-authentication, PTA, PIA, SAR, SAP, ISCMP and Initial Risk Assessment. ? Collaborate with external security auditors to conduct in-depth compliance audits and present findings to upper management ? Ensure proper system categorization using FIPS 199 and NIST 800-60; Implementation of applicable security controls for Information System based on NIST 800-53 rev 4, FIPS 200 ?Run Continuous Monitoring & Risk Scoring (CMRS) compliance reports to maintain the Authority to Operate (ATO). ? Review procedures for responding to new threats to systems to ensure confidentiality, integrity, and availability. ? Review and update remediation Plan of Action & Milestones (POA&Ms) in Organization CSAM, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist with the closure of the POA&M. ? Assess, analyze, and document vulnerabilities to information systems to help customers make an informed risk based decision. ? Analyze vulnerability scan results from Tenable Nessus and document findings in the POA&M. ? Remediate POA&Ms findings. ? Update the Security Assessment Report (SAR) on a regular basis with the continuous monitoring assessment results. ? Perform Risk Assessments of information systems based on RMF and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and make recommendations to customer. ? Conduct Security Assessment interviews to

determine the Security posture of the System and develop a SAR in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization to Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Information System Security Officer ISSO January 2014 to May 2017 Manage and coordinate a team of information security professionals to conduct Security Authorization packages based on NIST standards for general support systems and major applications. ? Risk assessment for overall environment -Assessment and Authorization (AA) based on FISMA Compliance. ? Provide input to management on appropriate FIPS 199 impact level designations and identify appropriate security controls based on characterization of the general support system or major applications. ? Develop and maintain artifacts supporting the Risk Profile SP, CP, CM, IR and POA&Ms ? Develop and maintain Plan of Action and Milestones (POA&MS) of all accepted risks upon completion of system (A&A) ? Prepare system documentation for assessment in accordance with the Risk Management Framework (RMF) and NIST Special Publications (800-37, 800-53 and others); identify deficiencies and provide recommendations for solutions ? Managed system security using Iptables and port ? Create and maintain existing information system security documentation, including System Security Plan (SSP), Security Controls Matrix and/or Assessment ? Assist external auditors with OMB A-123 Audits, and Financial Statements Audits. ?Track findings with Plan of Action and Milestones (POA&M) through mitigation and/or risk acceptance ? Provide guidance and quality assurance to the system owner on the development of A&A documentation Linux Systems Administrator Qota Systems January 2012 to January 2014 Configure passwordless login between database servers ?Install, configure, upgrade linux operating systems and kernels. ?Install, upgrade and manage packages via RPM and YUM package management ?Created filesystems using logical volume and updated stab. ?Building servers using Vsphere Vmware (either by attaching specified images to the datastore or using configured preexisting templates. ?Installation of atlassian agile apps like bitbucket, jira, confluence ?Recovering replicated virtual machines from original datacenter during migration ?Using logical volume tools to create local filesystem e.g lvcreate,pvcreate ?Online migration of data from active

systems, using rsync ?Creating new groups in RedHat Satellite server and adding servers to configured groups ?Managing and fixing Inactive, Out of date, Ungrouped and Duplicate systems in RedHat Satellite ?Installation, configuration, support and use of apache tomcat to deploy applications. ?Create and delete user accounts, enforce security and compliance rules regarding passwords and access to computer systems. ?Use of kickstart to build automation into daily processes, including server builds. ?Managing monthly patches for dev environment and bi monthly patches for the prod environment ?Using Satellite to update root password for critical server that could not be placed in single user mode ?Installed, configured and supported apache on virtual machines ?Configuration of ObserverIT application for test monitoring ?Monitoring filesystem use and fixing filesystems above threshold ?Configuring special group login in active directory ?Configure printers using linux lpr tools ?Worked on a highly sensitive project to change all running applications in the environment. ?Configuring sudo(group and wheel) access for users ?Performance tuning for oracle team, fixing issues with Hugepages and swap space modification. ?Fix broken links associated with start up scripts ?General troubleshooting fixing stale NFS handles, service management, fixing remote home directory issues, cron management and other duties assigned ?Filesystem investigation and management ?Responding to critical and major HPOV alerts ?Monitoring entire infrastructure and identifying points of failure before major escalation and reduction of downtime ?Configuring and setting up NFS filesystems ?Managed system security using Iptables and ports ?Managing and troubleshooting running processes and applications ?Hardware troubleshooting, replacement and support. ?Chron jobs setup and administration ?User administration ?Snmp (snmpwalk) installation, configuration and management. ?Network connection troubleshooting, management and support. ?Symantec Netbackup installation, administration, backup and restoration. ?Providing users with elevated privileges for special tasks(sudo) ?Server decommissioning using laid down procedures and scripts ?Physical data room walk-throughs server observation ?Creating maintenance windows within which physical server maintenance is performed ?Using RHEV manager to manage multiple concurrent tasks on multiple servers ?Reviewing servers for production by evaluating server

readiness ?Security and audit scans to limit cracking. ?VirtualBox VM setup for clients using centos vdi images ?Physical disk replacements (hot swappable) ?Provide on call support by rotation 24x7x365 Linux Systems Administrator MTN - CM August 2008 to July 2010 Hardware monitoring and performance evaluation. ?Tracking filesystem growth trends and capacity planning ?Bandwidth monitoring and utilization ?Network troubleshooting and maintenance. ?Automated installations using jumpstart methods. ?Service packs and security patches, Installation of recommended SUN patch clusters ?Performed data management using native Solaris utilities for archiving and compression. ? System troubleshooting and operating system support ?Security scan analysis and baseline analysis ?Disk quotas evaluation and system performance monitoring and tuning. ?Server administration - user management and support ?File restoration ?Hardware documentation and policy ?New purchase recommendation ?Oracle database support. ?Performance Monitoring and capacity planning. ?Veritas NetBackup support and Backup assistance. ?Role-Based Access control management. ?Familiarity with network systems such as servers, switches, firewalls and routers. ?Apache web server administration and support. ?Tracked and fixed problems using system logs ?Clean system shutdown administration Junior Linux Systems Administrator Alliance Tech Cyber Caf February 2008 to July 2008 User administration ? System monitoring, analysis -making recommendations regarding computer system security, monitor network, computer and disk utilization ?Conduct software and hardware evaluations, provide technical analysis and implement systems to meet the company's IT goals ?Planned and performed appropriate procedures, documentation, inventory assessment, and other procedures related to IT ?Performed scheduled backup and necessary restores ?Repaired and recovered hardware or software failures as well as coordinating and communicating with impacted constituencies. ?Performed troubleshooting on network connectivity issues ?Monitored and maintained email applications or virus protection software ?Implemented security measures to protect data, software and hardware ?Performed ongoing performance tuning, hardware upgrades and resource optimization as required. ?Configured CPU, memory, and disk partitions as required ?Performed periodic performance reporting to support capacity planning. ?Responsible for security - intrusion prevention ?Performed

additional duties as assigned by management ?Maintained professionalism, good attitude and appropriate behavior with personnel and clients. ?Operated master consoles in order to monitor the performance of computer systems Education MSc. in Computer Science NIST 2009 Skills System Administrator, Linux, Vmware, System Admin, Red Hat, Linux Administrator, Redhat

Name: Alexander Phillips

Email: elizabethrichardson@example.com

Phone: 603.883.8480x84559