MICHAEL URREA

murrea@msn.com

(520) 234-1004

Cochise County, AZ

CERTIFICATIONS/CLEARANCE

- CompTIA Advanced Security Practitioner (CASP+) CE [exp. 2021]
- CompTIA Security+ CE [exp. 2021]
- CompTIA Linux+
- Microsoft Certified: Azure Administrator Associate (AZ-103)
- Microsoft Certified Solutions Associate (MCSA): Windows Server 2016
- NetApp Certified Data Administrator (NCDA)
- SUSE Certified Linux Administrator (SCA)
- LPIC-1 Certification
- Certified Ethical Hacker V.8 (CEH) [exp. 2021]
- DISA ACAS 4.8 Certification

- Clearance: TOP SECRET/SCI (SCI adjudicated 04/2018)

PROFESSIONAL EXPERIENCE

Intelligent Waves LLC 01/2020- Present

Systems Administrator - Remote

- Develop and maintain full infrastructure of lab environment used to test patches and updates before production
- Install and configure Cisco UCS rack servers used for hosting virtual machines
- Deploy application updates using Ansible
- Install and configure Graylog server utilizing Redis and Elasticsearch to monitor multiple assets and store logs
- Harden all systems per DISA STIGs including infrastructure, hardware, and software
- Manage Dell EqualLogic Network Attached Storage (NAS)
- Configure and manage vCenter HA cluster using ESXi 6.7 managed by Vcenter
- Integrated an HTML5 web application used to access computers via RDP, VNC, and SSH from a web browser
- Install and maintain Microsoft SQL 2016 and MySQL
- Maintain Web Servers running Apache, NGINX, IIS, and Tomcat
- Create backup policies on multiple environments using NetBackup
- Manage layer 2 and 3 Cisco (3560) switches
- Perform daily ACAS SecurityCenter scans daily

NCI Inc. 09/2018- 12/2019

Sr. Systems Engineer – Enterprise Service Management System (ESMS)

- Develop and maintain full infrastructure of lab environment used to test patches and updates before production
- Deploy and manage multiple Virtual Machines on Amazon Web Services (AWS) Elastic Computing (EC2)
- Prepare and submit Risk Management Framework (RMF) packages for the entire BMC Remedy infrastructure
- Install and configure F5 BIG-IP systems utilizing Local Traffic Management (LTM) for load balancing
- Administer and create F5 iRules
- Install and configure Cisco UCS rack servers used for hosting virtual machines
- Install and configure BMC Atrium Discovery and Dependency Mapping (ADDM) on RedHat 7 using OpenShift
- Deploy application updates using Ansible
- Install and configure Graylog server utilizing Redis and Elasticsearch to monitor multiple assets and store logs
- Harden all systems per DISA STIGs including infrastructure, hardware, and software
- Manage Dell EqualLogic Network Attached Storage (NAS)
- Configure and manage vCenter HA cluster using ESXi 6.7 managed by Vcenter
- Integrated an HTML5 web application used to access computers via RDP, VNC, and SSH from a web browser
- Install and maintain Microsoft SQL 2016 and MySQL
- Maintain Web Servers running Apache, NGINX, IIS, and Tomcat
- Troubleshoot Java errors within the Remedy application
- Manage multiple Subscriptions and Resource Groups in Microsoft Azure
- Create backup policies on multiple environments using NetBackup
- Install and maintain BMC Remedy application suite 9.1
- Configure ARSsytem, Mid-Tier and RSSO for the Remedy application on Windows 2016 servers
- Manage layer 2 and 3 Cisco (3560) switches
- Perform daily ACAS SecurityCenter scans daily

Artic Slope Mission Services 10/2016-09/2018

I.C.E, INC. 02/2016- 09/2016

Principal Systems Engineer – Intelligence Battle Laboratory

- Design and implement cloud solutions for enterprise applications and storage using the DoDAF Meta Model (DM2)
- Work directly with developers and engineers to determine the best approach to for new application development
- Configure and manage Hyper-V HA cluster using Windows Server 2012 R2 Datacenter
- Configure and manage vCenter HA cluster using ESXi 6.0/6.7
- Lead technical team in multiple events including Enterprise Challenge (EC) and Unified Challenge (UC)
- Successfully lead team in an accreditation (2017), awarded for exceptional effort
- Oversee technical team including three system administrators and two network administrators
- Suggest and purchase new hardware to replace end-of-life equipment
- Migrated 50+ Windows desktops from Windows 7 to Windows 10 using Snap Deploy saving 240+ hours
- Migrated 20+ Red Hat Enterprise Linux servers (RHEL) to Community Enterprise Operating System (CentOS) saving over $6000 in yearly subscriptions
- Integrate commercial technologies in DOD networks including Google Earth, ArcGIS, MAK, Guacamole
- Integrated an HTML5 web application used to access computers via RDP, VNC, and SSH from a web browser
- Secure operating systems and applications per DISA STIGs
- Manage 20+ Dell physical servers (R820, R910), 40+ virtual machines, 50+ workstations all mixed Windows/Linux
- Install and configure Nexus (N55) switches used from Fiber Channel over Ethernet (FCOE)
- Manage Distributed Common Ground System-Army (DCGS-A) IFS (3.2.5) and 20+ Multi-Function workstations
- Manage Intelligence Electronic Warfare Tactical Proficiency Trainer (IEWTPT)
- Install and maintain SQL databases including Oracle DB and MySQL
- Maintain Web Server running Apache, Tomcat, and Wildfly
- Install and maintain ACAS/Nessus scanners for multiple networks
- Install and maintain WSUS, AD, OneSAF, NightVision, SitaWare, DHCP, DDS, CPOF, and Linux repository
- Manage layer 2 and 3 Cisco (3560) switches on multiple classified and unclassified networks
- Manage 20+ Cisco VOIP (CP-9951) phones and 3 VTC (SX-80) systems
- Manage 6 NetApp (FAS2552) Storages on multiple networks

General Dynamics 06/2015- 02/2016

Systems Administrator – HBSS Server Support

- Remotely managed ePO, Functional, NCR, E-SADRs, and Agent Handlers
- Daily checks on Windows 2008 R2 servers to monitor the status and the state of the servers
- Installed, configured, and administered servers and troubleshot issues as needed
- Performed IAVA vulnerability scans using SCAP and ACAS scanning software
- Powershell scripting for running various DISA STIG checks
- Ensured health of servers using SCOM agent
- Participated in monthly ASIs for patching and sustainment as needed
- Provided assistance to HBSS application team

General Dynamics 07/2013- 05/2015

Domain Administrator - Active Directory

- Secured remote administration of the DCs and member servers managed by the Infrastructure Group
- Managed group policy at root of domain and for Domain Controllers OU
- Created, tested, and managed GPOs used by multiple OU Admins
- Managed the Users and Computers Containers
- Installed and managed security reporting tools used to monitor changes to the Active Directory
- Monitored data and elevated privileges to others as needed
- Provided PKI support to all domains within the forest
- Planned and managed all migrations and upgrades related to the AD or the DCs
- Monitored changes to domain root and domain controllers OU to ensure unauthorized changes did not occur
- Monitored connectivity, synchronization, replication, netlogon, time services, FSMO roles, schema, NTDS database partitions, DNS settings, SRV records, and trust relationships
- Reviewed DC event and security logs and take corrective actions
- Monitored and resolved security situations at all levels of domain to ensure stable and secure domain

General Dynamics 04/2013- 06/2013

Systems Administrator - Desktop Support

- Identified and resolved a wide range of technical computer-related problems
- Provided basic imaging of end user equipment
- Migrated users from physical workstations to thin clients
- Provided support to Level 3/4 techs for advanced remote access/VPN support
- Supported remote access connections using VMware View
- Supported Multifunction Printing and driver updates for end users
- Responded to all technical emergencies outside of normal working hours as needed
- Responded to Security incidents and actions
- Maintained software and hardware registration and inventory to provide upgrades as necessary and ensure appropriate security levels were maintained
- Performed IAVA vulnerability scans using Retina scanning software
- Participated in rotational on-call duties to provide after-hours support

General Dynamics 10/2011- 03/2013

Accounts Administrator - Access Management

- Team Member of Security Access Management for the CONUS-TNOSC.
- Responsible for all internal and external account requested including Remedy, HBSS, ACS, E-health, Spectrum, UNIX/Linux, Netcool, ARCsight, Portal, and OU accounts
- Reviewed all DD2875 forms pertaining to accounts as an IASO (Information Assurance Support Officer) for the organization
- Created, modified, and deleted Remedy legacy, 7.1, and 7.6 accounts
- Provided building access to employees using the proxy system
- Managed UNIX servers on NIPR and created user accounts on all UNIX servers
- Worked with Tivoli, DNS, syslog, SNORT, and VM servers
- Used JPAS/JCAVS to verify security clearances
- Managed IPs for the C-TNOSC organization
- In-process and out-process employees
- Provided excellent customer service using Remedy ITSM 7.6

Coca Cola 09/2009- 10/2011

Junior Systems Administrator

- Managed users, computers, and printers using Microsoft Active Directory
- Patched workstations and servers (Microsoft Server)
- Managed LAN network for the headquarter office
- Used Microsoft Office for managing supplies
- Managed VOIP phones
- Provide On-Call support
- Supplied stores with merchandise when needed

TECHNICAL SKILLS

Operating Systems
Windows 7/10
Windows Server 2008/2012/2016
RHEL 6/7/8
CentOS 6/7/8
MacOS
ONTAP 9
Ubuntu 18.04

Software
MySQL
Apache
OneSAF
ArcGIS
Solarwinds Kiwi
MakLogger
Google Earth
Remedy ITSM
Tomcat

Accreditation
DISA STIGS
SecurityCenter
SCAP Tool
RMF process
eMASS

Virtualization
Microsoft Hyper-V
Microsoft Azure
AWS
VMware vSphere
VMware ESXi

Offensive Security
Wireshark
Metasploit
Aircrack-ng
Nmap