
Confident professional with proven networking, troubleshooting, customer relations, and leadership skills!

Summary of Qualifications

- 26+ years of technology leadership overseeing hundreds of Microsoft, Hypervisor, VMware, Citrix, Linux, and other IT projects in both large enterprise environments and small businesses alike. Adapt at working through difficult situations and coordinating diverse groups to achieve successful outcomes.
- Experience installing and configuring a variety of operating systems, including: **Windows NT4.0/2000/2003/2008/2012 Server/Enterprise, Share Point 2003/2007/2010, Microsoft Dynamics CRM 4.0/2011, Windows XP Pro/Vista/7/8.1/10, Citrix, ESXi 4.0/5.5/6.0, VM Ware Server 4.0/5.5/6.0, SCO UNIX, Ubuntu Linux, Red Hat, Mobile Programming Android/IOS and Novell Netware.**
- Network management, Satellite Communications including: user and security administration, PowerShell, group policy, active directory, MS Exchange, ISA Server, CA, NetApp, VM Ware, Virtual Server, Virtual PC, Big Fix, Dameware, VNC, NetApp, Verities Backup and remote access service.
- Experience with various networking protocols/systems, including: TCP/IP, NetBEUI and Cisco Routers, VOIP, Catalyst and Switching, Air Defense Wireless, Cranite Wireless.
- Retina Network Security Scanner; ACAS; OCRS; Telnet; SSH; SSL Certificate; Self Signed Certificate; Digital Certificates; DNSKEY/DNSEC/KSK; Anti-Virus Tools (Norton, Symantec, Ghost, Solarwinds, ADTP, Hyena, etc.)
- Industry certifications include CCNA, CCNAS, CCNP, MCT, MCSE, MCSA, MCDBA, MCITP Enterprise, A+, Network+, Security+, CASP+ CE, Tanium and others.
- **Fluent in Indonesian – verbal and written.**

Core Competencies:

IAO/ISSO, IA Policy, COMSEC, System Analyst & Design, Network/Databases/System Administrator and Engineer, Web Development, Help Desk Support/Technician, Project Management, Troubleshooting, System Installation, End-user Training, Procedural Documentation, Computer Information System, Inventory Control, Cost Management.

Professional Experience

United Forces Command, Fleet Weather Center San Diego

2/2021 – Present

System Engineering Division Head

Analyzes hardware and software malfunctions to resolve physical and logical processing problems. Provides on-going optimization and problems solving support; continually surveys system operation to identify potential systems problems which could lead to loss or serious interruption of service. Initiates corrective or preventative measures to rectify immediate problems and prevent future occurrences. Troubleshoots and diagnoses system failures to isolate source of problems. Perform testing, troubleshoots, and corrects problems relative to interface and interoperability of system components such as hardware, systems software is, and applications programs.

Provides proactive consultation and instruction with system users to ensure seamless implementation of changes. Assesses the security of installed systems. Develops, reviews, and maintains systems documentation, including IT project implementation plans, security policies and procedures, hardware, software, and network diagrams. Maintains documentations of network configuration including schematic diagram with layout and location of all components. Establishes, reviews, and maintains configuration management controls, and database administration controls, ensures compliance with applicable standard. Prepares and updates manuals, instructions, and operating procedures for systems.

Serves as a senior customer technical analyst with responsibility for resolving the most complex customer problems. Provides advice and assistance to customers; troubleshoots complex problems; and provides support in a manner that minimizes interruptions in customers' ability to carry out critical activities. Provides ongoing technical support to customers to ensure proper functional use of equipment and programs to preclude undue

interruptions to IT and communications services. Coordinates efforts between system customers, system support personnel, and commercial vendors to identify and resolve hardware, software, and other system anomalies.

Records problem reports as they occur and analyzes data to determine trends in use or performance that could lead to future problems.

Marines Corps Cyberspace Operations Group

6/2017 – 2/2021

Enterprise Directory and Messaging Triage Lead, West

- Supervises, directs, plans, manages, and coordinates the work efforts of military, civilian and contractors. Independently plans and implements assigned functional responsibilities.
- Supervises professional employees (military and contractor) highly skilled in specialized network related technical disciplines.
- Takes an active role in the discussions and subsequent task that emerge as a result of network defense working group meetings. Prioritizes work group requirements based on available resources.
- Stay informed of current development in the dynamic and changing technical field of Computer Network Defense by studying technical literature, attending and participating in meetings and symposia, formal training/education, and through correspondence with other professional.
- Recommends project priorities along with phasing, resource requirements, special project considerations, and is then permitted latitude in accomplishing approved projects.
- Oversees the development and integration of functional supporting plans into regional support to a coordinated enterprise-level network defense, detection and vulnerability management effort. Coordinates budget requirements, performance measurements, staff planning and resource allocation for the purposes of accomplishing successful operations.
- Oversees the timely reporting and tracking of all incidents occurring in the AOR in coordination with the MCNOSC per applicable DoD, DON and USMC policies.
- Serve as lead of the Crisis Action Team (CAT) working non-standard hours and shifts as necessary in response to ongoing critical incidents or attacks against or impacting computing assets or services in the AOR.
- Coordinate with Marines Corps IT support vendors to ensure compliance with DoD and USMC standards and policy relating to CND incident monitoring, analysis, detection, response and reporting standards as outline in CJCSM 6510.01
- Ensure local scanning systems and network sensor feeds are maintained in an operational status and that incident monitoring, analysis, detection and reporting is accomplished in accordance with applicable Marine Corps and DoD Policy.
- Manage the local maintenance and troubleshooting of all hardware and software based sensor systems in coordination with the MCNOSC in support of the overall enterprise-level MCEN detection strategy.
- Maintains current documentation on Federal Government, DoD and Marine Corps policies, procedures, and regulations related to CND standards, software, techniques and processes to ensure compliance for provisioning, funding, and management practices.
- Coordinate with the appropriate IT service vendors to ensure compliance with DoD and USMC standards and policy relating to IAVM.
- Develop and maintain MCNOSC enterprise INFOCON management process and supporting policies.
- Serve as AOR lead for management of host-based defense software capabilities and implementation.
- Provide periodic reporting to Operations Center regarding general Marine Corps readiness for implementation of INFOCON level, and potential operational impacts.

Naval Facilities Engineering Command South West San Diego

5/2016 – 5/2017

System Administrator, Network Administrator and Engineer, and Technical Support

- Certification Authority (CA) is official responsible for performing the comprehensive evaluation of the technical and non-technical security features and safeguards of an IT system, application, or network. This evaluation is made in support of the accreditation process, to establish the extent that a particular design and implementation meets information assurance requirements. On other responsible with CA for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and issuing a certification statement for the system. The CA is responsible for managing the certification process.
- Participates in identifying IT requirements applied to the planning, development, testing, implementation, and support of systems and networks. Performs installation, testing, troubleshooting and maintenance of hardware or software. Reviews systems and network vulnerabilities. Make recommendations for acquisition of IT products or services.

-
- Check and monitoring Individuals who have access to system control, monitoring, or administration functions (e.g., system administrator, IAO, system programmers, etc.) are Privileged Users and make sure the privileged users are responsible for providing IA safeguards and assurances to the data they control as well as their personal authentication mechanisms.
 - Supports the development of new methods and procedures and provides advice and guidance on a variety of IT issues. Reviews IT standards, and guidelines. Participates in analysis and recommends solutions to IT issues, new or enhanced products and approaches to IT programs or services.
 - Oversees capacity planning to determine enterprise and agency needs; analyzes DoD business needs; assesses industry direction and analyzes new capabilities that may be applied to the business units within the enterprise; evaluates new products, documents characteristics, and makes recommendations for, and takes the lead in, the integration of new or improved techniques.
 - Designs, coordinates and implements complex installation projects for major, statewide systems that have high risk/high impact on public services, implements new development or major maintenance that have executive sponsorship; integrates and certifies software/hardware for enterprise-wide systems.
 - Identifies and independently resolves operational problems for major, enterprise-wide systems that have high risk/high impact on public services, coordinates the resolution of inter-agency operational problems from Information Technology Services.
 - Oversees the development of requests for information and/or requests for proposals, feasibility studies and decision packages for high visibility/impact or multi-agency initiatives; leads the implementation of information technology policies and strategies; defines project charters, conducts cost/benefit analysis, oversees requests for proposals and evaluates responses for major information technology systems.
 - Analyzes statewide trends and makes recommendations for improvements and efficiencies in system performance; develops and writes enterprise and volume purchase acquisition plans for review and implementation by Information Technology Services.
 - Develops service level agreements with clients and vendors; develops measurement and monitoring methods and prepares operational and performance reports on major information technology systems and processes.
 - Creates and supports processing environment (e.g., test, demonstration and production) for enterprise-wide and agency-wide systems. Supervises and evaluates the work of subordinate staff; effectively recommends personnel actions related to selection, disciplinary procedures, performance, leaves of absence, grievances, work schedules and assignments, and administers personnel and related policies and procedures.
 - Plans, coordinates, and directs the activities of technical and clerical personnel engaged in operating a computer system, related peripheral equipment, data entry devices, and controlling document and record distribution. Confers with other information technology processing staff to establish operation requirements and procedures for testing and debugging programs.
 - Develops long range plans (or phases of plans) for the operations unit by considering work methods, scheduling of priorities, and capabilities of equipment to produce desired results efficiently and effectively; informs administrator of recurring or projected resource and capacity problems for planning purposes and corrective action.
 - Develops and maintains operating schedules to provide the most efficient use of personnel and equipment; establishes maintenance schedule for all equipment.
 - Maintains records and prepares reports of production, equipment operation, and downtime; orders and regulates the use of supplies used in computer operations and in data entry. Reviews finished products of computer and data entry operations to ensure conformance to established quality and operational standards.
 - Establishes and enforces standards for controlling the workflow and integrity of data through the production processes and for ensuring the quality of production work and security of materials, equipment, and files located within the facility.
 - Managed Design, Troubleshooting, Analyzed, and Administering and resolved Operates any issue in electronic computer and peripheral equipment as required.

Joint Project Manager Information Systems (JPMIS)/SPAWAR San Diego

8/2015 – 05/2016

System Administrator and Engineer, Network Administrator and Engineer, and Technical Support

- Design, Implementation Updating and Troubleshooting of ESXi Server, VMware ESX 5.1/5.5 Hosts, VMware vSphere virtual center and windows virtual machines.
- Managed VMware ESXi hosts using vSphere client and Web client. Performing VMotion and storage VMotions. Creating Clusters for High Availability and Dynamic Resource Scheduling. Played a vital role in Creating Virtual Machines, Cloning virtual machines, VM-Provisioning (Linked clones, thin disks, de-duplication) taking Snapshots of virtual servers, HA, DRS, VMotioning.
- Experience in Installation and Configuration of ESXi, Single Sign on Sever (SSO), vCenter Inventory Services and vCenter5.1/5 also install separation database with MS SQL Server 2012 for each component of VMWare system.
- Check and Update on all IAVA compliance requirements thru DISA, and create POAM for outstanding IAVA.

-
- Provides assistance and advice to users of IT systems. Provides guidance to resolve processing problems. Conducts interviews with users and generates requirements for new or modified IT systems/services, software and/or hardware.
 - Participates in identifying IT requirements applied to the planning, development, testing, implementation, and support of systems and networks. Performs installation, testing, troubleshooting and maintenance of hardware or software. Reviews systems and network vulnerabilities. Make recommendations for acquisition of IT products or services.
 - Performed Data Migrations using Volume Snap-mirror, Flash Copy, and Image Mode Copy Technologies. Analyzing and Troubleshooting Filer, Array and Server Related Issues in The Environment Using Monitoring and Reporting Tools.
 - Supported and Implemented NetApp SAN/NAS in an existing environment of windows, VMware, and Linux systems.
 - Check and monitoring Individuals who have access to system control, monitoring, or administration functions (e.g., system administrator, IAO, system programmers, etc.) are Privileged Users and make sure the privileged users are responsible for providing IA safeguards and assurances to the data they control as well as their personal authentication mechanisms.
 - Supports the development of new methods and procedures and provides advice and guidance on a variety of IT issues. Reviews IT standards, and guidelines. Participates in analysis and recommends solutions to IT issues, new or enhanced products and approaches to IT programs or services.
 - Technical Support, Setup/installation/maintenance, configure hardware, software, network printing, network account and IP for JPMIS. Provides network/security checks for equipment entering/exiting JPMIS
 - Deputy IT Manager for JPMIS. Manages and configure all VPN application and systems for JPMIS.
 - Perform routine audits, analyze of system logs and software. Perform backups, Install and configure new hardware and software.
 - Add/remove/update user account information. Document the configuration of the system and Fine-tune system performance.
 - Make recommendations on long-range plans, organize, prioritizes in support of JPMIS objectives and prepares reports as necessary. Proven ability to create and deliver solution tied to business growth. Led-in-house and consultant team in large-scale infrastructure for JPMIS, which significantly enhanced system performance.

Center for Information Dominance/FITC San Diego

8/2014 – 8/2015

ISSO, System Administrator and Engineer, Network Administrator and Engineer, and Technical Support

- Design, Implementation Updating and Troubleshooting of ESXi Server, VMware ESX 5.1/5.5 Hosts, VMware vSphere virtual center and windows virtual machines.
- Managed VMware ESXi hosts using vSphere client and Web client. Performing VMotion and storage VMotions. Creating Clusters for High Availability and Dynamic Resource Scheduling. Played a vital role in Creating Virtual Machines, Cloning virtual machines, recompose P20/VDI (used standard VMware recompose tool), VM-Provisioning (Linked clones, thin disks, de-duplication) taking Snapshots of virtual servers, HA, DRS, VMotioning.
- Experience in Installation and Configuration of ESXi, Single Sign on Sever (SSO), vCenter Inventory Services and vCenter5.1 also install separation database with MS SQL Server 2012 for each component of VMWare system.
- Installing Citrix Presentation/XenDesktop 4.5/6.5 and manage the farm through Presentation and Access Management Console.
- Designed the architecture, deployed, and maintained all Citrix Provisioning Services and Citrix XenDesktop virtualization environments in CID/FITC.
- Developed and implemented a security patching procedure for Citrix, VMware, and Microsoft Windows servers/Windows 7. Brought all servers up to current patch levels and created a detailed plan for deploying monthly security hotfixes to all development, test, and production server environments. Maintained ACAS compliance through this work.
- Responded to Information Assurance Vulnerability Alerts (IAVA) regarding system integrity. Made appropriate updates, changes, modification as necessary to meet security requirements and update on all IAVA compliance requirements thru DISA, and create POAM for outstanding IAVA.
- Participates in identifying IT requirements applied to the planning, development, testing, implementation, and support of systems and networks. Performs installation, testing, troubleshooting and maintenance of hardware or software. Reviews systems and network vulnerabilities. Make recommendations for acquisition of IT products or services.
- Installation, Configuration and Administration of NetApp with 7 mode, Single Cluster, Two Node Cluster and Switchless.
- Performed Data Migrations using Volume Snap-mirror, Flash Copy, and Image Mode Copy Technologies.
- Analyzing, implementing and Troubleshooting NetApp for CIFS,, NFS, Filer, Array and Server Related Issues in The Environment Using Monitoring and Reporting Tools for Windows, VMware and Solaris Systems
- Develop Continuity of Operations (COOP) and Disaster Recovery (DR) operations and conduct evaluation of COOP and DR during annual incident response training. Network connectivity troubleshooting, ping, tracer, telnet, Solar Winds, and Wireshark.
- Cisco switch configuration in particular VLAN, Net-Timing/Bridge Network, LACP, PAGP configuration/troubleshooting.
- Analyzed and solved configuration issues on Cisco 2950, 2960. 3500 Series, 3550, router and switched network platform.

SMC/MILSATCOM Los Angeles Air Forces Base

12/2011 – 8/2014

ISSO/IAO/System Administrator, Network Administrator, and Technician Support

- Protected vulnerable networks following detailed risk assessments. Guided cross-functional teams in the design, validation, acceptance testing and implementation of secure, networked communications across remote sites for several key clients.
- Responsible for developing and implementing IA-related programs and controls, ensuring that IA is incorporated throughout the system development lifecycle, assigning by IAM, providing enterprise-wide vulnerability
- Certification Authority (CA) is official responsible for performing the comprehensive evaluation of the technical and non-technical security features and safeguards of an IT system, application, or network. This evaluation is made in support of the accreditation process, to establish the extent that a particular design and implementation meets information assurance requirements. On other responsible with CA for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and issuing a certification statement for the system. The CA is responsible for managing the certification process.
- As IA Officers (IAOs) are responsible to an IAM for ensuring the appropriate operational IA posture is maintained for a command, organization, site, system, or enclave. IAOs assist in creating accreditation packages. They implement and enforce system level IA controls in accordance with program and policy guidance.
- Assist in the development of System Security Accreditation Agreement (SSAA) documentation in accordance with the DITSCAP/DIACAP guidelines
- Ensure that all monitored systems comply with the DoD Gold disk, STIGs, IAVA, IAVB, IAV-TA, Security Control procedures in addition to FISMA requirements and Report on all security, IA, and C&A compliance requirements
- Check and monitoring Individuals who have access to system control, monitoring, or administration functions (e.g., system administrator, IAO, system programmers, etc.) are Privileged Users and make sure the privileged users are responsible for providing IA safeguards and assurances to the data they control as well as their personal authentication mechanisms.
- Supports the development of new methods and procedures and provides advice and guidance on a variety of IT issues. Reviews IT standards, and guidelines. Participates in analysis and recommends solutions to IT issues, new or enhanced products and approaches to IT programs or services. Perform and create procedures for system security audits, penetration-tests, and vulnerability assessments, than develop scripts to maintain and backup key security
- Install and maintain security infrastructure, including IPS, IDS, log management, and security assessment systems. Assess threats, risks, and vulnerabilities from emerging security issues.
- Performance tuning tools, database management, and project management methods sufficient to optimize systems performance, troubleshoot database performance problems, and perform a wide range of systems administration functions.

Defense Contract Management Agency Sepecial Program

10/2009 – 12/2011

**Network Engineering, System Administrator, Databases Administrator,
Web Development/Master, Computer Security, Helpdesk Support, and Technician Support**

- Provided message traffic administration, support and service, and implemented the PKI (Public Key Infrastructure) certificate program to provide secure/encrypted messaging communication using Blackberry, CAC Card and MS Outlook.
- Administered Video Teleconference secure and non-secure, encryption device, firewall and backup systems, providing access to customers via ports and policies based on preapproved conditions.
- Responded to Information Assurance Vulnerability Alerts (IAVA) regarding system integrity. Made appropriate updates, changes, modification as necessary to meet security requirements (JAFAN 6/9).
- Research and proposed an upgrade to increase bandwidths speed from 10/100 Mbps to 1 Gbps and TACLANE upgrade or modification. Resulted in the infrastructure being overhauled and created a maintainable upgradeable infrastructure.
- Upgrade Infrastructure from Windows 2003 to Windows 2008 R2 Clustering, VM Ware, Novell 6.0 and Red Hat Linux with Setup Clustering and Load Balancing or hot spare on 6 Server for Domain Controller, 6 Server for Exchange Server, 6 Server for Distribution Server, 24 Server for Oracle and SQL Database and 8 NAS/SAN for data backup. Resulted in receiving Individual Time off Award.
- Providing SharePoint training to individuals or groups; migrating and upgrading current EPM infrastructure from 2003 to 2007.
- Managing system security; system patching and upgrades; deploying custom developed and third-party SharePoint solution packages; Configuring SharePoint services and settings; Documenting SharePoint configuration and architecture; Managing site quotas and file size limits; Reviewing and monitoring usage reports; Managing content databases and creating new ones as

required; Administering and maintaining sites and sub-sites; Managing security for sites and sub-sites; Managing the site layout structure and content; Provide SharePoint support to end users; Provide Microsoft Project support to project leaders.

- Installed workstations on NAS/SAN and a routable LAN with non-routable protocols providing limited access to secure information and Develop Continuity of Operations (COOP) and Disaster Recovery (DR) operations
- Maintained network to include implementation of back-ups utilizing NetApp and VERITAS; creating and implementing procedures for setting up auditing, firewall monitoring and maintenance, Symantec Anti-virus server maintenance and log review, IP/DNS block lists and Web Inspector auditing.
- Developed data model describing data element, modified existing databases management systems than directed programmers and analysts to make changes. Reviewed workflow charts developed by programmer analysts to understand tasks computer would perform, such as updating records. Selected and entered codes to monitor database performance and to create production databases. Specified users and user access levels for each segment of database.

Education

California State University San Marcos in Computer Science with GPA 3.7

University of the District of Columbia in Computer Science with GPA 3.7

Grossmont College in C++, Java, JavaScript, Visual Basic, UNIX, Linux and Web Design Class with GPA 3.4.

The University of Trisakti, Indonesia, Bachelor of Science in Economics Management, with honors.

Technical Training

- CEI Computer Networking Certification, Los Angeles, CA – GPA 4.00-Graduated with highest Honors.
- CompTIA: A+, Network+, Security+, CASP+ CE Certification.
- CCNA (2003-22), CCNAS (2015-22), CCNP (2003-22).
- MCP 2000, MCSA 2000-2003, MCSE 2000-2003, MCDBA 2000.
- MCTS Windows 2008 Active Directory, Network Infrastructure Configuration, Applications Infrastructure Configuration, Windows Vista.
- MCITP Windows 2008 Server Administrator, Windows 2008 Enterprise Server Administrator.
- MS Exchange, Lotus Notes/Domino Training.
- Novell, UNIX /XENIX/Linux and TCP/IP
- Informix and ANSI C Training.
- AS/400 and OS/400
- Accounting Training.
- System Software Specialist Series by Department of Technology Service, State Personal Board California.
- Afloat Automatic Pay System/NEC-2905-Graduate with highest Honor 97.7.
- Assured Compliance Assessment Solution (ACAS).
- Tanium Certified.
- DoD CSWF: IAT Level III, IAM Level II, IASAE Level II.
- DoD DAWIA Level I.
- DoD DAWIA Level II in process (one more class).
- RMF Certification in Process

Technical Skills

O/S: Windows XP/Vista/7/8.1/10/2012, NT4.0, Server 2000/2003/2008/2012, Novell Netware 4.00, SCO UNIX, SCO XENIX, X-Windows, Ubuntu, ESXi Ver 4.1/5.5/6.0, VMware Ver 4.1/5.5/6.0, VM Player, Dameware, Citrix, VNC, Wave, Air Defense, Novell SUSE Linux 9, Macintosh, OS/400, and MS Dos 6.22.

Software: MS Office 2003/2007/2010/2013, MS Project, MS Visio, MS Exchange 5.5/2007/2010, MS SQL 2000/2005/2008/2012, Microsoft Dynamics CRM 4.0/2011, MS Share Point 2003/2007/2010, Lotus Notes, Lotus Smart Suite, PC Anywhere, Informix, Visual FoxPro, Ansi C, C/C++/C# Language, Visual Basic, Cobol, Pascal, Java Language, RPG, Assembler, Visio, Harvard Graphic, Macromedia Director 7.0, SPSS for Windows, Adobe Suite CS5, Adobe Photoshop CS3, Adobe Page Maker, Adobe Dreamweaver CS4, Adobe Flash CS4, MySQL, ColdFusion, Apache Server, IIS 6.0, JavaScript, PHP, AJAX, XML, HTML, Metric Studio, AutoCAD, Corel Draw 12, 3D Studio Max, VERITAS Backup, Abacus, Galileo.

Hardware: All relevant networking hardware, including: Reattach and 3Com LAN Card, Bay Network, 3Com switches, Cisco Switch/Routers/Server, NetApp 7-Mode/Clustering (NAS/SAN), Taclane, PKI Certification, Encryption Device, VTC, Jupiter Server, Dell Server, HP Server, Tandberg Video Teleconference, SmartBoard, and network printers.

Honors And Awards

- CEI: Highest Honors with GPA 4.0 Award 2003 and Perfect Attendant 2003.
- The Navy Good of Conduct Medal, 2006
- Afloat Automatic Pay System: Highest Honors Award 2007
- Cuyamaca College: Honor Award with GPA 4.0 spring 2008.
- Two Letter of Appreciation from USMC Marine Aviation Weapons and Tactics Squadron One.
- Individual Time off Award from DCMA Special Program.
- Individual Time off Awards from SMC/PIO, Los Angeles Air Forces Base.
- California State University of San Marcos Scholarship.
- JPMIS Team Award on 13 Jan 2016
- Monetary Awards from NAVFAC SW on May 2017.