Frantz Honore

Hanover Maryland

301-252-8634

Frantzhonore1@outlook.com

**SUMMARY:**

TS/SCI Full scope Architect Professional/ Systems Engineer with 20+ years of experience. Background skills include Cloud, Big Data, DevOps, AI, Splunk, Virtualizations, Cyber Security and Networking,

|  |  |
| --- | --- |
| Operating Systems | Windows 2008/2012/2016 /Win7, AIX, Linux CentOS Red-Hat, Ubuntu, Fedora OSX and Solaris |
| IBM ECM/BPM/ICM | ECM 4.x/4.5.x/5.1x/5.2x, BPM 4.x/4.5.x/5.1x/5.2x, IBM Case Manager (ICM), IBM Content Navigator (ICN), Business Process Framework (BPF), Infosphere Content Collector Records Manager(ICC) |
| RDBMS | Oracle 10/11g/12c, MS-SQL Server 2005/2008/2012, 2016 DB2 9.7,10.1 |
| VMWARE | ESX 3.5, Vsphere 4.0, Vcenter 5.0 , 6.0 Workstation 6.0/6.5/7.0 |
| Cloud | AWS , AZURE , OpenShift,OpenStack,PCF |
| TECHNICALSKILLS: | UNIX (Solaris, SGI, HP AUX, AIX Centos , Ubuntu,), Linux Red Hat, AWS, Cloudera, Windows Server 8R2 , 2012 , 2016 ,OpenStack, Puppet, Hadoop, EMC Isilon, VNX, NetApp, Html, Internet Explorer, Netscape Navigator, McAfee, Heat Management Tools, Lotus Notes, Pine, Hummingbird exceed (NETBackup, VMWare Citrix XenApp / XenDesktop) EMC, Isilon, VNX, Cisco Nexus, SQL Server 2012, ,Active Directory , Certification and Accreditation Process (C&A), Security Scanning Tools, Varonis, LINUX Server and workstation Administration, HPC Administration, NAS and SAN Administration and Engineering, System Security Administration and Engineering, System integration, Data Migration, Computer Systems Certification and Accreditation, Data Center Management, Data Center Migration, Big Data Management, Tanium Foundation, Operations, & IR Deep Dive |

**EDUCATION:**

**University of Maryland at Baltimore County**

Computer Certification Program

Howard High School Ellicott City MD 1993

**IT Certifications:**

**Project Management Institute**

Project Management Professional (PMP) 2021

**Amazon Web Services Certifications**

AWS Certified Developer Associate 2020

AWS Certified Solutions Architect Professional 2020

AWS Certified Security Specialty 2021

AWS Certified DevOps Engineer Professional 2021

AWS Certified Data Analytics Specialty 2021

AWS Certified Machine Learning Specialty 2021

AWS Certified Machine Learning - Specialty

**ISACA Certifications**

CISM Certified Information Security Manager 2021

CRISC—Certified in Risk and Information Systems Control 202

CISA—Certified Information Systems Auditor 2022

CGEIT—Certified in the Governance of Enterprise IT 2021

CDPSE—Certified Data Privacy Solutions Engineer. 2022

**EC-Council**

Certified Ethical Hacker 2022

**Microsoft Certifications**

Azure Administrator Associate 2021

Azure Architect Design 2021

Azure AI -Artificial Intelligence 2021

Azure Security Engineer Associate 2021

Azure Solutions Architect Expert 2021

Azure DevOps Engineer Expert 2021

**Splunk Certifications**

Splunk Core Certified User 2021

Splunk Core Certified Power User 2021

Splunk Enterprise Security Certified Admin

Splunk Enterprise Certified Admin

**Google Cloud Certifications**

Google Professional Cloud Architect

Google Cloud Certified-Professional Data Engineer

Google Professional Cloud Security Engineer

Google Professional Cloud Network Engineer

**CompTIA Advanced Security Practitioner (CASP+) 2021**

**Kubernetes Certifications**

Certified Kubernetes Administrator (CKA)

Certified Kubernetes Application Developer (CKAD)

Certified Kubernetes Security Specialist (CKS)

**PROFESSIONAL EXPERIENCE:**

**Insight Global** **Remote Engineer**

**DevOps Cloud Automation Engineer**

**5/2020-** Present

* Focuses on optimizing existing systems, build and secure cloud infrastructure, while eliminating work through automation.
* Configured user permissions in Red-Hat IDM/ and control Minder on customers current environment
* Supported and made sure applications are NIST SP 800 Series, FedRAMP and FISMA certified
* Wrote, edited, and manage wide variety of IT security documentation and familiarity with federal IT standards such as Federal Information Security Management Act (FISMA)
* Worked on technical documentation related to FIPS 199, NIST SP 800-37, NIST SP 800-53 REV 4, FISMA A&A, and continuous monitoring, and POA&M management
* Worked with Amazon Document DB, to set up, secure, and scale MongoDB-compatible databases in the cloud without worrying about manually setting up and securing database clusters, running cluster management software, configure backups, and monitor production workloads.
* Implemented and enhanced CRUD operations for the applications using the MVC Model View Controller architecture of Rails framework and Ruby conducting code reviews.
* Develop new functionality of the Ruby and Rails service that power our backend
* I’ve worked with IRONSCALES cloud-native, API-based email security platform to continuously learn, detect and remediate advanced threats at the mailbox level, before and after email delivery.
* Designed Infrastructure and Security requirements for ArcGIS Geospatial Software-as-a-Service built on AWS in accordance with FedRAMP control requirements.
* Identified solutions for Load Balancing, Disaster Recovery\COOP, Access Control
* Identity Management, Encryption and Federal Compliance (FedRAMP)
* Worked on the infrastructure supporting a global deployment of HashiCorp’s Vault Enterprise hosted in GCP. Automated distribution of SSL certificates. Improved the processes for managing vault policies by migrating them into Terraform. Refactored infrastructure deployment to support in-place rolling upgrades to Vault and Consul clusters.
* Worked closely with the monitoring team to ensure services and backups were being correctly monitored.
* Used Terraform as a tool for building, changing, and versioning infrastructure safely and efficiently. manage existing and popular service providers as well as custom in-house solutions.
* Authored Terraform modules for infrastructure management. Authored and published a module to the Terraform registry for enterprise customers to deploy our product inside their AWS environment.
* Developed Scripts for AZURE/AWS Orchestration Developed Scripts for AZURE/AWS Orchestration Designing and developing new back-end services, maintaining and expanding our AWS infrastructure, and providing mentorship to others on my team.
* Performed security assessment on a newly proposed Azure AD structure
* Performed security assessment on a proposed Azure Hub-Spoke environment
* Performed automation tasks using Azure Devops to implement security solutions
* Design and develop cloud specific security policies and procedures for SIEM tools (QRadar,splunk), Vulnerbility Management tools(Qualys), Data Loss Prevention, Encryption, cloud compliance tool(Redlock), monitoring tools(Data dog).
* Involved in building Azure Security Controls for onboarding on-prem applications to Azure.
* Involved in determining Encryption Policies for Azure Resources.
* Performed security assessments for products like Palo Alto VM Series, Zscalar, Azure firewall.
* Involved in security assessment while moving on-prem applications to cloud.
* Identify risks and vulnerability reported in Azure security center and Redlock and remediate them.
* Involved in firewall deployment and management in Azure such as Palo Alto, Azure FirewallMaintained and developed Docker images for a tech stack including Cassandra, Kafka, Apache, and several in house written Java services running in Google Cloud Platform(GCP) on Kubernetes.
* Set up a **GCP** Firewall rules in order to allow or deny traffic to and from the **VM's** instances based on specified configuration and used **GCP** cloud **CDN** (content delivery network) to deliver content from **GCP** cache locations drastically improving user experience and latency.
* Work with VMware Tanzu to enable and operator to [curate a secure set of container images](https://tanzu.vmware.com/application-catalog) that’s grab-and-go for developers, which speeds development and delivery.
* Analyze endpoint application data in real time to identify potential threats, rogue systems, vulnerabilities, unauthorized devices and/or system changes, and data loss prevention. Report cyber incidents to SOC incident responders
* Responsible for operating and maintaining Symantec Endpoint Security Manager
* Use Data Protection Manager (DPM) backups in Windows Azure Backup. Which provided Dashboard of centralized gateway to view servers protected by backup vault
* Guide the cloud security group, identifying opportunities for improvement and then driving those improvements through the enterprise
* Ensures that Integration architecture is consistent with Application Reference architectures, and infrastructure architecture and standards
* upport help automate and be responsible for how SaaS and PaaS products relate to each other.
* Develop, maintain, and report on key cloud security metrics – both as a program and on an individual basis, creating metric templates and scoring models
* Work with Visio to configure and design drawings for current customer environments
* Engage improve the complete lifecycle of services inception and design, through deployment, operation, and refinement.
* Support services before going-live through the process of developing automation, developing security frameworks, and planning continuous delivery cycles.
* Maintain services that are live by helping to measure and monitor availability, security, and overall system health.
* Assisted in the development of the framework to manage the Integration Architecture for UBS
* Configure Helm to deploy applications in various environment
* Used Kubernetes to orchestrate the deployment, scaling and management of Docker Containers.
* Utilized Kubernetes for the runtime environment of the CI/CD system to build, test deploy.
* Provides security expertise for cloud-based DevOps development and deployment
* Managed Docker orchestration and Docker containerization using Kubernetes.
* Supported Middleware application deploying VMWare builds
* Scale systems sustainability through mechanisms like automation and evolve systems by pushing for changes in reliability, security, and velocity. Implemented a **'server less'** architectureusing **API Gateway, Lambda, and Dynamo DB** anddeployed **AWS Lambda code** from Amazon S3 buckets. Created a Lambda Deployment function, and configured it to receive events from your S3 bucket
* Design the data models to be used in data intensive **AWS Lambda** applications which are aimed to do complex analysis creating analytical reports for end-to-end
* Create and maintain highly scalable and fault tolerant multi-tier AWS and Azure environments spanning across multiple availability zones using Terraform and CloudFormation.
* Manage existing application and create new applications (visual and non-visual)
* Manage SPLUNK user accounts (create, delete, modify, etc.)
* Create data retention policies and perform index administration
* Assist with the cloud implementation, modification and improvement of the Sponsor's Risk Management Framework (RMF) workflow and its component parts
* Exploit Tool development: Developing the security toolset to exploit newly found vulnerabilities in order to perform real-world Cloud issues
* Involved in Cloud Security Infrastructure and design for client’s in-house Azure Applications
* Perform cloud security risk assessment for cloud applications already in Azure
* Involved in defining cloud security controls for an Azure environment at an Enterprise level
* Implemented Cloud security controls in SecOps including but not limited to Encryption, Tagging, Container security, Golden AMI policy, IDS/IPS, NSG management, Service Endpoints, DDoS, Integrating 3 rd party services such as QRadar, Qualys, Redlock
* Configured Azure Key vault and key management policies
* nvolved in implementing security agents in Azure Golden Images to be enforced company wide

**Prime Technical Services Inc. Atlanta, GA**

**Architect**

**3/2019- 5/2020**

* Deploy cloud infrastructure (Security Groups and load balancers needed to support EBS environment)
* Designed\Architected FedRAMP Compliant Infrastructure-as-a-Service Cloud, Created FedRAMP A&A documentation package, Identified required Hardware\Software inventory for BOM, Selected strategic products such as VMWare vCloud Enterprise (vCNS), NetApp, Cisco Nexus 7009, F5 BIG IP 11050, Palo Alto, AlienVault, Nessus, AppSec, DigiCert, Vormetrics. Identified FedRAMP artifacts for FedRAMP 3PAO preparation
* Performed Security Assessment, Compliance Analysis and Documentation for FISMA (Moderate) and FedRAMP.
* Prepared FedRAMP Security Authorization Package for Third Party Review
* Configure following services in AWS Cloud9 environments starting with AWS security group to create Amazon Document DB cluster for HA while installing mongo shell for ability to connect to Amazon Document DB cluster
* Work with Ruby gems such as ruby-pg for Oracle- PostGRE-SQL
* Database modeling and design. Involved in developing and implementation of the web application using Ruby on Rails.
* Utilized Kubernetes for the runtime environment of the CI/CD system to build, test deploy.
* Worte Terraform based instructions to orchestrate cloud server provisioning
* Leverag AWS, Terraform, Python and bash to rapidly provision multi-team cloud environments.
* Set up Terraform backends, modules and varfiles to manage multiple environments with same Infrastructure code.
* Work with Kubernetes to orchestrate the deployment, scaling and management of Docker
* Created and managed Windows Azure Subscriptions
* Design and Implemented Azure Infrastructure environment according to the customer requirements
* Configured RBAC and Azure Monitor for adding security in Azure Cloud.
* Configured Network Security Groups for Subnet and NIC level for Azure Virtual Machines
* Supported configured User defined routes to route traffic between the Azure Networks
* Reviewed configured Azure VPN gateway and established Site-to-Site connectivity, Express Route with On Premise Networks and Azure
* Deployed and configured Firewall Appliances (Barracuda, Palo Alto, Fortinet) to secure Azure Cloud
* Deployed and configured virtual networks and storage accounts in Azure
* Extended and Integrated On-Premises AD to Azure Active Directory
* Maintained and managed User’s access using custom RBAC roles
* Deployed and configured virtual Machines in Windows and Red Hat Enterprise Linux 7 and 8
* platforms using PowerShell Scripting, JSON templates and Azure Resource Manager portal.
* Configured Network Security Group for azure security and route traffic between virtual machines
* Implemented and configured Express Route connectivity from On-Premises to Azure Cloud
* Deployed and configured Azure Backups for Virtual Machines and files & folders backups on Windows and Red Hat Enterprise 7 and 8.
* nux operating systems using Recovery Services Vault in Azure Resource Manager
* Performed migration of servers from On-Premises to Azure Cloud, servers from Classic to Azure Resource Manager
* Configured Virtual Machines scale sets, Availability sets to manage virtual machines
* Implemented custom RBAC roles, Resource Group Policies based on Customer’s requirements to manage the User’s access
* Configured Virtual Network peering between the regions in different subscription Azure Encryption for Azure Storage and Virtual Machines, Azure Key Vaul
* Manage EndPoint Security environments and deliver services using End point Security tools (EPTM, HIDS, HIPS)
* Work with Monitor DPM in Operations Manager to monitor and report on the health and status of DPM servers using System Center Operations Manager Management Packs for DPM
* Integrate the Cloud Platform with the firms Identity and Access Management systems (Active Directory & SSO) and leverage industry best practices for Authentication and Authorization
* Deep and broad understanding of services and architecture required to build secure Cloud computing platforms; especially using encryption for data at rest and in transit
* Identity Management, authorization and authentication expert – including using SSL, IPSEC and PKI frameworks for securing and encrypting communications
* Perform the integration architecture assessments during Solution Gate Review
* Used Cloud watch to monitor various issues within Applications in AWS
* Documented customers entire integration architecture design and analysis work
* Design network diagram using Visio
* Define security best practices for our cloud platform and provide guidance to application development teams
* Identify security security gaps and provide recommendations to address gaps on both new and existing cloud platforms
* Document security policy for our cloud environments and build tools to automate enforcement of policy
* Design, test, certify and document new cloud services, environments and systems
* Collaborate with business units to help architect secure applications
* Implemented a **'server less'** architectureusing **API Gateway, Lambda, and Dynamo DB** anddeployed **AWS Lambda code** from Amazon S3 buckets. Created a Lambda Deployment function, and configured it to receive events from your S3 bucket
* Design the data models to be used in data intensive **AWS Lambda** applications which are aimed to do complex analysis creating analytical reports for end-to-end
* Create and maintain highly scalable and fault tolerant multi-tier AWS and Azure environments spanning across multiple availability zones using Terraform and CloudFormation.
* Manage existing application and create new applications (visual and non-visual)
* Manage SPLUNK user accounts (create, delete, modify, etc.)
* Provided technical support in planning, designing and developing Enterprise Integration architecture.
* Create data retention policies and perform index administration, maintenance and optimization
* Work with third party application, hosting and CDN providers to integrate data feeds to a centralized Splunk platform
* Provide overall management of the SPLUNK platform
* Assist with design of core scripts to automate SPLUNK maintenance and alerting tasks. Support SPLUNK on UNIX,
* Write terraform scripts from scratch for building Dev, Staging, Prod and DR environments.
* Installed configured Big Query application in the cloud
* Supported issues with Big Query as needed
* Supported large big data applications hosted on Big Query
* Made sure large applications in customers environment are on BigQuery is used for handling or analyzing big data. ,
* Work with customer application on BigQuery to manage data using fast SQL-like queries for real-time analysis
* Design and developed various Web forms using HTML, CSS, Bootstrap and JavaScript, React.JS
* Created documentation for all the components which is included in React-Bootstrap page.
* Provided tailored designs to multiple teams using the service mesh.
* Designed and implemented solutions for scaling DNS, auditing and authentication on the service mesh
* Support work with API management, RESTful APIs and/or managed API gateways
* Support Monitor ESB and API usage and effectiveness
* Ensure security and compliance of APIs and assist with discovery efforts •
* Provided Tier 3/troubleshoot support for API capabilities for enterprise services (e.g., ESB, API Manager, performance and utilization reporting systems)
* Maintain and support PaaS and API gateway infrastructure and associated tools
* Lead API lifecycle development; responsible for software development and code quality
* Set up an API Gateway installation.
* Design, implement, test and deploy APIs using the latest technologies and best practices.
* Implement API management using API management software (like Apigee or others) to include API proxies, mashups, rate limiting, security, analytics, monetization and developer portals
* Set up processes for Policy generation using various techniques
* Set up error management and log management processes
* Set up a onboarding, roll out to production and support processes using the API gateway tool.
* Work with various network/ security engineers to maintain security CA Layer7 to setup infrastructure, install Layer7 products, patches, and design, develop, modify, configure, debug and evaluate application programs for functional business areas.  Provided strict adherence to change control and process documentation is required.
* Enable users to understand the usage of API gateway platform.
* Gather requirements and build, test and roll out projects using API Gateway tool.
* Support current installation of API Gateway projects.
* Developed API services in an Agile environment
* Manage the Openshift cluster that includes scaling up and down the AWS app nodes.
* Develop course work that’s designed customers looking to learn DevOps.
* Teach Clients to learn the ins and outs of Cloud Foundry.
* Wrote ansible scripts to ensure Openshift container platform works in sync with Bank system of records.
* Implemented Microservices on RedHat OpenShift based on Kubernetes, Etcd, and Docker to achieve Continuous Delivery.
* Provide day to day training on Cloud Foundry architecture and various components of Cloud Foundry,
* Worked on OpenShift for container management and to enhance container platform multi - tenancy.
* Design a patch process and wrote ansible playbooks for patching openshift -RHEL, atomic OS and also for bug fix for Openshift.
* Provide training on how to tailor apps to ensure that they will run correctly when you execute a cf push, and how to write a manifest that will make your deploy process repeatable and predictable.
* Teach clients how to perform blue-green deployments of your apps already running in Cloud Foundry. Last but not least, this course will prepare you for taking the Cloud Foundry Certified Developer exam.
* Create and manage TFS Continuous integration builds on VSTS
* Responsible for installation & configuration of Jenkins to support various Java builds and Jenkins plugins to automate continuous builds and publishing Docker images to the Nexus repository.
* Manage Docker orchestration and Docker containerization using Kubernetes.
* Used Kubernetes to orchestrate the deployment, scaling and management of Docker Containers.
* Responsible for maintaining AWS instances as part of EBS deployment
* Developed business logic using Python
* Build/Maintain Docker container clusters managed by Kubernetes Linux Red Hat Enterprise Linux 7 and 8, Bash, GIT , Docker, on AWS/AZURE .
* Utilized Kubernetes for the runtime environment of the CI/CD system to build, test deploy.
* Provided support on AWS services and DevOps deploying applications in AWS to help take full advantage of the AWS platform
* Develop serverless applications on AWS instances (Lambda, ECS, SNS/SQS/Kinesis, RDS, DynamoDB, etc)
* Develop microservice applications using Java
* Developed business logic using Python
* Supported and Work with both relational and NoSQL databases
* Configured, test, deploy, and upgrade software for production EC2 servers in AWS
* Lead initiatives for automating and scaling our systems
* Participated in technical architecture design
* Improve the security, reliability, and performance
* Administer, monitor, and deploy cloud-based systems
* Collaborate with application engineers to design robust systems
* Take ownership of infrastructure projects and internal tools
* Exert automated test approaches through CICD
* Communicated and collaborate with Product Manager, Engineers, Stakeholders, et
* Deploy, automate, maintain and manage AWS cloud-based production system, to ensure the availability, performance, scalability and security of productions systems.
* Establish, maintain and evolve concepts in continuous integration and deployment (CI/CD) pipelines for existing and new services.
* Ensured security compliance with appropriate NIST and ICD requirements
* Assisted in the architecture, design, implementation, and lead AWS public cloud build (connectivity, network, security, containerization, monitoring)
* Provided guidance on security configurations and risk and compliance procedures (Identity Management, Network Configuration, Data Protection, Segregation of Duties)
* Work with in-house cloud security experts to implement a security framework that satisfies ISO standards for implementing cloud solutions in public clouds

**Open Systems Technologies Corp Herndon VA**

**Architect**

**10/2018- 3/2019**

* Deploy, monitor and maintain Amazon AWS GOV cloud infrastructure consisting of multiple EC2 nodes in rapidly changing R&D environment
* Used MAVEN as build tools on Java projects for the development of build artifacts on the source code. Completed a FedRAMP \ FISMA A&A Package based on NIST 800-53R3 and Confidential issued FedRAMP controls
* Performed Security Assessment, Compliance Analysis and Documentation for FISMA (Moderate) and FedRAMP.
* Prepared FedRAMP Security Authorization Package for Third Party Review
* Used **Bash** and **Python** , included **Boto3** to supplement automation provided by **Ansible** and **Terraform** for tasks such as encrypting **EBS volumes** backing **AMIs** and scheduling **Lambda** functions for routine **AWS tasks** .
* Wrote terraform scripts for Cloudwatch Alerts.
* Created develop and test environments of different applications by provisioning Kubernetes clusters on AWS using **Docker**, Ansible, and Terraform
* Automate Datadog Dashboards with the stack through Terraform Scripts.
* Implemented AWS **Code Pipeline** and Created Cloud formation **JSON** templates in **Terraform** for infrastructure as code.
* Work with Scheduling, deploying, managing container replicas onto a node using Kubernetes and experienced in creating Kubernetes clusters work with Helm charts running on the same cluster resources.
* Design customers distributed private cloud system solution using Kubernetes (Docker) on CoreOS and used it to deploy scale, load balance and manage Docker containers with multiple name spaced versions.
* Developed Scripts for AWS Orchestration Developed Scripts for AWS Orchestration Designing and developing new back-end services, maintaining and expanding our AWS infrastructure, and providing mentorship to others on my team.
* Wrote Puppet manifests for deploying, configuring, install shield and managing collected for metric collection and monitoring.
* Used Ansible-Playbook (Python base) to automate build/setup LAMP Stack and manage 1000+ RedHat and Windows cloud servers Identify and architect the
* Setup and configure Splunk and Logstash/Kibana to monitor all provisioning logs.
* Design and Develop Bamboo Build deployments on Docker containers.
* Provided support for development in Microsoft Azure and Google Cloud environments
* Work with the team as a Cloud Engineer within the Google environment.
* Collaborate with the team on GCP Cloud to support infrastructure support requests. •
* Provision, administer and manage GCP cloud infrastructure for a DoD client
* Responsibile to architect, engineer, support, configure, and implement endpoint security controls, of which the CA for Microsoft Certificate Services is an important example
* Coordinate between various business functions which includes the incident management team, business owners, endpoint security team
* Manage all endpoint security implementation and deployment projects
* Attended customer/project meetings, review system documentation (e.g., system requirements, detailed design/architecture, interface documents, etc.), identify security gaps and provide security recommendations to address gaps, and complete risk profiles for cloud computing solutions
* Provided security input in architecture/design/process documentation and will work with project teams to identify and implement security controls to meet FISMA compliance requirements, i.e., NIST SP 800-53 Rev4
* Work with Cloud watch to collect data that would be push in the customers SEIM and Splunk environment Draft design various customers environment in DEV, Test and Prod in Visio
* Work with Kinesis within the cloud for various projects I’m supporting
* Maintain an AWS Lambda@Edge interceptor in order to simplify the deployment of Amazon-authenticated websites using serverless technologies.
* Automate Datadog Dashboards with the stack through Terraform Scripts.
* Work within the software engineers to implement API Management platform to focus on enabling the platform for enterprise.
* Work within AWS GOV cloud to improvement in system interfaces while Monitoring ESB and API usage and effectiveness Ensure security and compliance of APIs and assist with discovery
* Write terraform scripts for Cloudwatch Alerts.
* Assisted in the development of technology roadmaps to evolve the API estate in conjunction with internal and external solution providers
* Created Windows and Linux Red Hat Enterprise Linux 7 and 8 desktop using AWS Workspaces
* Setup Amazon Work Spaces that’s available different Regions P
* Provided access to high performance cloud desktops wherever the teams needed work done
* Operated on several prototype OpenShift projects involving clustered container orchestration and management.
* Implemented cloud services IAAS, PAAS , and SaaS which include Openstack , Docker and Openshift .

**Lockheed Martin Herndon VA**

**Sr Engineer /** Architect

**8/2016- 10/2018**

* Automate and manage our AWS infrastructure and deployment processes, including production, test and development environments.
* Created a Decision Tree Process Model for Cloud services and FedRAMP vendor selection
* Made Virtualization Security Recommendations to ensure FedRAMP compliance before submitting
* Addressed all FedRAMP controls and created matrix for control delta
* Authored Cloud Assessment of Salesforce.com, Oracle and Microsoft offerings
* Presented overview of Cloud Security requirements, FISMA and FedRAMP
* Work with Jenkins to deploy .net apps to AWS and AZURE
* Monitor all cloud issues using cloud watch and cloud trail
* Deploy configure and implement Kinesis in AWS
* Design and implement Splunk infrastructure, deployment, products, apps, reports, alerts, and dashboards