**White Paper: Cloud Platform Expertise**

Designing Multi-Cloud Systems with AWS and Salesforce Integration (VA Context)

White Paper: Cloud Platform Expertise – Designing Multi-Cloud Systems with AWS and Salesforce Integration (VA Context)

## Executive Summary

As the Department of Veterans Affairs (VA) accelerates digital modernization, the need for secure, scalable, and standards-compliant multi-cloud architecture has become foundational. Cloud platform expertise enables the VA to design systems that integrate AWS, Salesforce, and hybrid infrastructures across mission-critical domains such as claims processing, identity management, case tracking, and benefits delivery.

This white paper outlines multi-cloud design principles and implementation strategies tailored to federal compliance mandates, identity federation models, and VA enterprise architecture standards. It also explores integration patterns between AWS and Salesforce using event-driven architectures, and shows how platform abstractions and observability help reduce vendor lock-in, improve resilience, and support cost optimization in a mission-driven environment.

1. Multi-Cloud Design

## 1.1 Why Multi-Cloud in VA?

- Avoid Lock-In: Ensures VA OIT can shift workloads between vendors based on cost, security, and policy flexibility.

- Resilience and Continuity: Multi-cloud strategies enable redundancy across GovCloud, VA private clouds, and on-prem systems like Corp DB.

- Leverage Strengths:

- AWS: Scalable compute, KMS encryption, and FedRAMP High.

- Salesforce: Veteran case management and appeals tracking.

- Azure: Integrations with Office 365, Sentinel, and ML services.

## 1.2 Abstraction Strategies

- Service Meshes (e.g., Istio): Decouple service discovery and traffic routing.

- CI/CD Pipelines: Jenkins and GitHub Actions abstract deployment logic using Terraform.

- API Gateways: AWS API Gateway or Kong allow for unified traffic management.

- Storage Abstraction: MinIO and cross-region S3 provide vendor-neutral object storage.

## 1.3 Federated Identity Across Clouds

- SSO Tools: Okta, PingFederate, and Azure AD ensure consistent access control.

- IAM Policies: Use AssumeRole and policy boundaries to secure AWS environments.

- Protocols: SAML 2.0 and OIDC standardize token-based auth across Salesforce and AWS.

2. AWS Core Services (Federal Context)

## 2.1 Compute: EC2 & Lambda

- EC2: Powers lift-and-shift systems and supports auto-scaling.

- Lambda: Enables scalable, serverless workflows (e.g., processing Veteran case data).

## 2.2 Networking: VPC

- VA Use: Segregated environments using NAT Gateways and Transit Gateways.

- Benefits: Improved security zones and shared service architectures.

## 2.3 Identity: IAM

- Practices: JSON-based policies, IAM Identity Center, MFA enforcement.

- Usage: Aligns with VA TRM compliance for cross-account management.

## 2.4 Storage: S3

- Scenarios:

- Static VA.gov content.

- Analytics lake for Redshift and Athena.

- Security: KMS encryption, S3 Access Points, lifecycle rules.

## 2.5 Encryption: KMS

- Functions:

- Key management.

- Access control logging.

- Encryption at rest for PII.

3. Salesforce Integration in VA

## 3.1 Platform Events

- Integration Model: Asynchronous messaging to Lambda, Kafka, or SQS.

- Usage: Real-time data flow between Salesforce and backend adjudication.

## 3.2 Salesforce Flows

- Use Case: Low-code workflows for Veteran-facing logic.

- Integration: AppFlow and Mulesoft used to trigger AWS actions.

## 3.3 Integration Tools & Patterns

- Salesforce Connect: External OData access to VA-owned databases.

- External Services: Auto-generated integrations via OpenAPI.

- Middleware: MuleSoft for data orchestration; AppFlow for native AWS sync.

## 4. Architecture Patterns

| Pattern | Description |

|---------|-------------|

| Event-Driven CRM Sync | Platform Events trigger Lambda and persist to S3/Redshift. |

| Hybrid Identity Broker | Okta federates identity across VA systems. |

| Data Ingestion Pipeline | Events from Salesforce flow to AWS analytics pipelines. |

| Cost Optimization Broker | Multi-cloud load balancing by SLA/cost metrics. |

## 5. Resources and References

| Resource | Link |

|----------|------|

| AWS Architecture Center | https://aws.amazon.com/architecture/ |

| Salesforce Integration Guide | https://developer.salesforce.com/docs |

| AWS Lambda Docs | https://docs.aws.amazon.com/lambda/latest/dg/ |

| IAM Policy Reference | https://docs.aws.amazon.com/IAM/latest/UserGuide/access\_policies.html |

| Salesforce Platform Events | https://developer.salesforce.com/docs/atlas.en-us.platform\_events.meta/platform\_events/ |

## Conclusion

Cloud platform expertise at the VA must align to mission delivery, security mandates, and enterprise architecture policies. By leveraging cross-platform tools, decoupling logic, and federating identity across clouds, the VA creates robust, compliant systems that improve delivery of Veteran services.

## Next Steps:

- Perform multi-cloud maturity assessments.

- Align Salesforce and AWS workflows for case management.

- Define Terraform-based blueprints for cross-cloud pipelines.

- Expand platform event-based integrations.

- Maintain architecture review criteria for FedRAMP, FISMA, and TRM standards.

## For related topics:

- NIST 800-207: Zero Trust

- DevSecOps & CI/CD

- VA EA Repository

- Salesforce + API Strategy