**SMBCTEX-002 – Solution Configuration Document**

**SMBCTEX-002 – Solution Configuration Document**

**Project Name:** IX-RD-PS-Infinity-01 Migración y modernización infraestructura Infinity  
**Client:** Infinity Gifts Souvenirs  
**Prepared by:** Intcomex Cloud  
**Date:** June, 2025

**1. Introduction**

This document provides a detailed configuration overview of the AWS environment implemented for Infinity Gifts Souvenirs. It complements the Design Document (SMBCTEX-001) and serves as a reference for technical staff managing the infrastructure.

**2. AWS Region and Availability**

* **Region:** us-east-1 (N. Virginia)
* **Availability Zone(s):** Single AZ (Cost-saving strategy)

**3. Core AWS Services and Configurations**

**3.1 Amazon EC2 Instances**

| **Purpose** | **Instance Type** | **OS** | **Key Configurations** |
| --- | --- | --- | --- |
| Active Directory | t3.medium | Windows Server | Joined to VPC, static IP, domain controller setup |
| IIS Web Server | t3.medium | Windows Server | Hosted internal web application, SSL |
| Patch Manager Agent | N/A | Installed on all EC2 | Connected to AWS Systems Manager |

**Tags:**

* Environment: Production
* Application: InfinitySouvenirs
* Owner: ITDept

**3.2 Amazon RDS (SQL Server)**

| **Parameter** | **Value** |
| --- | --- |
| Engine | SQL Server Standard Edition |
| Instance Type | db.t3.medium |
| Multi-AZ | No (Single AZ for cost efficiency) |
| Storage Type | General Purpose (gp2) |
| Storage Size | 100 GB |
| Backup Retention | 7 Days |
| Encryption | Enabled (AWS-managed keys) |

**3.3 AWS Systems Manager**

| **Feature** | **Configuration** |
| --- | --- |
| Patch Manager | Patch scan enabled (manual install only) |
| Compliance | Reports reviewed before applying patches |
| Inventory | Enabled to track software and instances |

**3.4 Amazon Elastic Block Store (EBS)**

| **Volume Type** | **Purpose** | **Size** | **Encrypted** | **Attachment** |
| --- | --- | --- | --- | --- |
| gp2 | OS & App Data | 100GB | Yes | EC2 Web/App |
| gp2 | AD Database | 80GB | Yes | EC2 AD |

**3.5 AWS IAM**

| **Element** | **Configuration** |
| --- | --- |
| Root User | MFA Enabled, used only for break-glass |
| IAM Policies | Least privilege, role-based |
| Admin Access | 1 Named User (Terraform Only) |
| Partner Access | Dedicated user, access scoped by EC2 |

**3.6 AWS Certificate Manager**

* SSL certificates issued for IIS-hosted web apps.
* Certificate bound to Elastic IP on IIS server.

**3.7 Amazon CloudWatch**

| **Metric Monitored** | **Alarms Configured** |
| --- | --- |
| CPU Usage | Yes (90% threshold) |
| Memory Usage | Yes (RAM agent setup) |
| Disk Space | Yes |
| Log Forwarding | Enabled via CloudWatch Agent |

**Log Groups:**

* /rds/error-logs
* /iis/logs
* /event-viewer

**3.8 AWS CloudTrail**

* Enabled for all regions.
* Stores activity logs in an encrypted S3 bucket.
* Reviewed periodically for compliance events.

**3.9 AWS Backup**

| **Parameter** | **Value** |
| --- | --- |
| Backup Plan Name | InfinityBackup |
| Frequency | Daily |
| Retention | 7 Days |
| Recovery Test | Manual RTO/RPO review monthly |

**Recovery Objectives:**

* **RTO:** 2 hours
* **RPO:** 24 hours

**3.10 Terraform Deployment**

* IaC Codebase: Stored in private Git repository.
* CI/CD: Pipeline using GitHub Actions.
* Secrets managed with environment variables.
* Version-controlled deployments with rollback.

**4. VPC and Network Configuration**

| **Component** | **Details** |
| --- | --- |
| VPC CIDR | 10.0.0.0/16 |
| Subnets | Public and Private (1 AZ) |
| Internet Gateway | Attached to public subnet |
| NAT Gateway | Not used (all resources in 1 AZ) |
| Security Groups | Ingress rules limited to required ports only |
| NACLs | Default, reviewed for known risks |

**5. Backup and Recovery Procedures**

* Daily backup schedules applied using AWS Backup.
* Monthly verification of recovery capability.
* Quarterly DR test involving partial restoration.
* Manual snapshots for major application changes.

**6. Training and Handover**

* 3 Sessions held over Microsoft Teams.
* Covered: EC2, RDS, IAM, Backup, Patch Management.
* All sessions recorded by client team.
* Handover document and runbooks provided.

**7. Compliance & Best Practices**

* IAM policies follow least privilege principle.
* Encryption used for all data at rest and in transit.
* Monitoring and alerting in place.
* Manual checklist for changes to production.
* QA environment isolated from production.