



Landing Zone Design and Implementation

2024

Landing Zone Design Phase

1 Tenant Model

- Resource Hierarchy (Organization/Management Groups)
- Tagging and policies
- Resource Deployment
- Shared Subscription/VPC structure with Prod/Non-Prod/BU

2 Networking

- Network Topology / IP Schema
- WAN/LAN Connectivity and redundancy
- Internet connectivity (To/From)

3 Access & Identity Management

- Identity and Access Management (Authentication)
- Domain Join / ADDS / DNS / Private DNS
- PIM (Conditional Access , Multi-Factor Authorization, Role Based Access Control (RBAC))

4 Security

- Security best practices, and Cloud Security Posture management (CSPM)
- Data protection/Encryption/Secret Management
- Networking Security (Perimeter , Inside cloud , Visibility)
- End Point Security / Observability
- NSGs/ASGs/Security Groups (Micro Segmentation)

Landing Zone Design Phase

5 Monitoring

- Azure dashboard / Alerts
- Monitoring and Observability using all Third-party Tools
- Operational and Security Logging
- Application/VM Insights

6 IAC/DevOps

- Base Services / Core Services / Shared Services prioritization
- IAC Practices (Terraform/Ansible/Cloud Formation/ARM)
- Code Repository (GitHub/ADO)
- CI/CD Tool (Jenkins/DevOps/Bamboo)
- Self-Service for rapid Cloud Adaption

7 Resiliency H/A-BCDR

- Resiliency for each IaaS/PaaS/SaaS Service , RTO/RPO and DR Classification
- BCDR -H/A Requirements
- Design / Approach for each service

Landing Zone Implementation Phase

1

Landing Zone Enablement

- Build the Landing Zone as per the agreed architecture by Client
- Define MG/Organization hierarchy structure
- Subscription/VPC setup for Landing Zone (Hub/Spoke Architecture)
- Prod/Non-Prod Separation at each Layer
- VNET/VPC setup with subnets & NSGs
- Create or leverage existing express route / Direct Connect
- Deploy/Modify BCDR region Landing Zone
- Enable Logging, Monitoring and Alerts.

2

Base Services Enablement

- Prioritize Base services in cloud
- Build Base Services (up to 10 services)
- Create policies/Protective/Detective controls to enforce Cloud Governance/compliance
- Setup IAM roles and policy assignments
- Security & Audit logging
- Resiliency implementation for each service based on RTO/RPO and DR Classification