SOP-AZ-001_Azure_VM_Admin_v1.0.0

SOP-AZ-001_Azure_VM_Admin_v1.0.0

Standard Operating Procedure: SOP-AZ-001

DOCUMENT CONTROL

SOP ID	SOP-AZ-001
Title	Azure VM Infrastructure Administration
Version	1.0
Status	Final
Author	IT Department
Approver	IT Management
Effective Date	2025-12-02

1.0 PURPOSE

To establish a standardized process for the secure and efficient administration, migration, and management of Azure Virtual Machines (VMs) and related compute infrastructure. This SOP ensures consistency, high availability, and adherence to security best practices.

2.0 SCOPE

This SOP applies to all IT personnel responsible for deploying, managing, and securing the Azure VM environment. It covers procedures for VM migration, load balancing, ADFS management, network troubleshooting, topology management, and identity/access control.

3.0 RESPONSIBILITIES

Role	Responsibility
IT Administrators	Execution of the procedures outlined in this SOP, including VM management, migration, and monitoring.
Network Team	Management of Azure networking components, including VNet, NSGs, Load Balancers, and topology.
Security Team	Auditing and enforcement of RBAC, MFA, and other security policies. Management of Azure AD PIM.
IT Management	Ensuring compliance with this SOP, approving significant changes, and allocating necessary resources.

4.0 PROCEDURE

4.1 Virtual Machine Migration This procedure outlines the steps for migrating on-premises VMs to Azure using Azure Migrate.

1. **Preparation and Assessment:**
   - In the Azure Portal, navigate to **Azure Migrate** and create a new project.
   - Select the appropriate migration scenario (e.g., VMware, Hyper-V, physical).
   - Perform discovery and assessment using Azure Migrate tools to evaluate VM dependencies, sizing, and readiness. Utilize the **Dependency Visualizer** for a comprehensive dependency map.
2. **Set Up Azure Migrate Appliance:**
   - Deploy the Azure Migrate appliance (OVA or setup file) in the on-premises environment.
   - Register the appliance with the Azure Migrate project and allow it to complete discovery.
3. **Configure Replication:**
   - In the Azure Migrate project, select the VMs to be replicated.
   - Configure target settings: Azure subscription, region, resource group, VM size, and availability options (Availability Zone/Set).
   - Define target disk types and select which disks to replicate.
   - If applicable, enable **Azure Hybrid Benefit** to reduce licensing costs.
4. **Start and Monitor Replication:**
   - Initiate replication for the selected VMs.
   - Monitor replication health and status through the Azure Migrate portal.

5. **Conduct Test Migration:**
    - Perform a test migration on replicated VMs to create a sandboxed test environment in Azure.
    - Verify VM boot, network connectivity, and application functionality within the test environment. This step does not impact production workloads.
6. **Perform Full Migration (Cutover):**
    - Schedule and perform the final cutover. This transitions the Azure VMs to the production environment.
    - Shut down the on-premises source VMs.
    - Update DNS records, firewall rules, and application connection strings to point to the new Azure VMs.
7. **Post-Migration Validation and Optimization:**
    - Verify the health, performance, and connectivity of the newly migrated VMs in Azure.
    - Implement **Azure Backup** for the VMs.
    - Configure monitoring and alerting using **Azure Log Analytics**.
    - Optimize VM sizes and disk types based on post-migration performance data to manage costs effectively.
    - Implement **Just-in-Time (JIT) VM Access** to enhance security by controlling port access.

4.2 Load Balancing

1. **Deployment:**
    - Deploy **Azure Load Balancer** (for Layer 4 traffic) or **Azure Application Gateway** (for Layer 7 traffic) to distribute traffic across VM instances.
2. **Configuration (for Windows Clusters):**
    - Use PowerShell to configure the `AutoBalancerMode` and `AutoBalancerLevel` for VM clusters.
        - `AutoBalancerMode`: `0` (Disabled), `1` (On Join), `2` (Always)
        - `AutoBalancerLevel`: `1` (Low - move at 80% host load), `2` (Medium - move at 70%), `3` (High - move above 5% average).
    - **PowerShell Commands:** `powershell (Get-Cluster).AutoBalancerMode = <value> (Get-Cluster).AutoBalancerLevel = <value>`

4.3 ADFS Management

1. **Security:**
    - Isolate ADFS servers from direct internet access. Use Web Application Proxy (WAP) for external federation.
    - Protect ADFS servers behind internal firewalls and apply regular security patches.
    - Enforce the principle of least privilege for service accounts.
2. **Modernization:**

- Evaluate migrating from ADFS to **Azure AD** for identity federation to reduce on-premises complexity and improve resilience.

4.4 Network Troubleshooting

1. **Monitoring:**
   - Use **Azure Network Watcher** to diagnose VM connectivity, packet loss, and latency issues.
   - Leverage **Azure Log Analytics** for real-time network traffic analysis.
2. **Diagnostics:**
   - Review network topology, VNet peering, Network Security Groups (NSGs), User-Defined Routes (UDRs), and VPN configurations when troubleshooting connectivity.

4.5 Topology Management

1. **Design:**
   - Follow Azure reference architectures (e.g., Hub-Spoke, Virtual WAN) for scalable and secure network design.
   - Use discrete resource groups for logical segmentation of compute, storage, and networking resources.
2. **High Availability:**
   - Distribute VM instances and related services across multiple Availability Zones.
3. **Automation:**
   - Automate infrastructure deployments using **ARM templates** or **Bicep**.
   - Integrate templates with a version control system (e.g., Git) for repeatable and documented infrastructure management.

4.6 Security and Access Control

4.6.1 Role-Based Access Control (RBAC)

1. **Principle:**
   - Assign permissions using role assignments that consist of a **security principal** (user/group), a **role definition** (permissions), and a **scope** (resource/group/subscription).
2. **Implementation:**
   - Assign roles based on the principle of **least privilege**. Use built-in roles (e.g., `Virtual Machine Contributor`) where possible, or create custom roles for specific needs.
   - **Assign roles to Azure AD groups** rather than individual users to simplify management.
3. **Procedure (Portal):**
   - Navigate to the resource and select **Access control (IAM)**.

- Click **Add > Add role assignment**, select the desired role, and assign it to the appropriate security group or user.

4. **Auditing:**
   - Periodically audit role assignments to remove obsolete or excessive permissions.
   - Limit the number of users with the `Owner` role on subscriptions.
   - Use **Azure AD Privileged Identity Management (PIM)** to enable just-in-time (JIT) privileged access and time-bound role activations.

4.6.2 Multi-Factor Authentication (MFA)

1. **Enforcement:**
   - Enforce MFA on all user accounts, especially those with privileged roles.
2. **Policy:**
   - Use **Azure AD Conditional Access** policies to require MFA based on conditions like user location, device compliance, or sign-in risk.
   - Ensure compliance with Microsoft's requirement for MFA on all Azure resource management operations.
3. **Monitoring:**
   - Enable logging and alerting to monitor sign-in activity, detect MFA bypass attempts, and investigate suspicious behavior.

5.0 QUICK REFERENCE CHEATSHEET

Task	Tool / Command	Best Practice
Discover/Assess VMs	Azure Migrate, Dependency Visualizer	Map all dependencies before migration.
Test Migration	Azure Migrate: Test Migration	Validate all applications before cutover.
Load Balancing (PS)	`(Get-Cluster).AutoBalancerMode = <value>`	Set to `1` (On Join) or `2` (Always).
LB Aggressiveness (PS)	`(Get-Cluster).AutoBalancerLevel = <value>`	Use `1` (Low), `2` (Medium), or `3` (High).
Assign RBAC Role (CLI)	`az role assignment create`	Script assignments for automation and consistency.
ADFS Security	Harden ADFS, use WAP	Eliminate direct public internet exposure.
Network Troubleshooting	Azure Network Watcher, Log Analytics	Monitor connectivity, routing, and packet loss.
Topology Management	ARM/Bicep Templates	Automate deployments; use Hub-Spoke design.

Task	Tool / Command	Best Practice
Enable PIM	Azure AD > Privileged Identity Management	Implement Just-In-Time (JIT) privileged access.
Enable MFA	Azure AD > Conditional Access	Enforce MFA for all users, especially administrators.

6.0 REVISION HISTORY

Version	Date	Author	Description of Change
1.0	2025-12-02	IT Department	Initial document creation.