# Azure Monitor Automation Solution

Prepared for Client Review

## ARCHITECTURE DIAGRAM

+-------------------------------------------------------------------+

| AZURE CLOUD ENVIRONMENT |

| |

| +----------------------------------------------------------+ |

| | AZURE KEY VAULT | |

| | (Secure Credential Storage) | |

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

| | Service Principal App ID | |

| | Encrypted Passwords | |

| | Tenant ID | |

| | Military-Grade Encryption | |

| +----------------------------------------------------------+ |

| | |

| | Retrieves Credentials |

| v |

| +----------------------------------------------------------+ |

| | BASTION SERVER | |

| | (24/7 Automation Hub) | |

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

| | Scheduled Tasks: | |

| | Mon/Thu 8AM: Monitor Reports | |

| | Monthly: Key Rotation | |

| | Weekly: Security Audits | |

| | Daily: Cost Optimization | |

| +----------------------------------------------------------+ |

| | |

| | Authenticates |

| v |

| +----------------------------------------------------------+ |

| | SERVICE PRINCIPAL | |

| | (Secure Machine Identity) | |

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

| | Read-Only Monitor Access | |

| | Create/Update Alerts | |

| | NO VM or Data Access | |

| | Auto-Rotates Monthly | |

| +----------------------------------------------------------+ |

| | |

| | Queries Performance Data |

| v |

| +----------------------------------------------------------+ |

| | AZURE MONITOR | |

| | (Intelligence and Alerting) | |

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

| | VM Performance (CPU, Memory, Disk) | |

| | Security Events and Cost Metrics | |

| | Proactive Alerts | |

| +----------------------------------------------------------+ |

| | |

| | Monitors All Resources |

| v |

| +----------------------------------------------------------+ |

| | YOUR AZURE RESOURCES | |

| | +----------+ +----------+ +----------+ +---------+ | |

| | | Virtual | | Storage | | App | | SQL | | |

| | | Machines | | Accounts | | Services | | DBs | | |

| | +----------+ +----------+ +----------+ +---------+ | |

| +----------------------------------------------------------+ |

| | |

+----------------------------+--------------------------------------+

|

| Generates Reports and Alerts

v

+------------------------+

| ADMINISTRATORS |

| Email Reports |

| HTML Dashboards |

| CSV Data Files |

+------------------------+

## What We Are Solving

Manual Azure monitoring takes 2-3 hours daily using admin accounts. This wastes time and creates security risks.

Current Issues:

- 2-3 hours daily manual checking

- Passwords in scripts

- Admin accounts with excessive access

- No automatic alerts

- Missing cost savings

## My Recommended Solution

3-part system working together:

### Part 1: Azure Key Vault

Stores all passwords encrypted. Only automation server can access.

Why safe:

- Military-grade encryption

- Only Bastion can access

- Full audit trail

- Meets SOC 2, ISO, HIPAA

### Part 2: Bastion Server

Dedicated server running monitoring 24/7 separate from production.

What it does:

- Monday/Thursday 8AM: Monitor reports

- Monthly: Rotate keys

- Weekly: Security audits

- Daily: Cost optimization

### Part 3: Service Principal

Limited-permission account for monitoring only.

Why better:

- Minimum permissions

- Cannot be phished

- Auto-rotates monthly

- Limited damage if compromised

## How It Works

1. Key Vault stores passwords encrypted

2. Bastion retrieves credentials on schedule

3. Service Principal logs in with limited access

4. Azure Monitor collects data

5. Reports emailed automatically

## What Gets Monitored

Virtual Machines:

- CPU over 85 percent

- Low memory

- Disk issues

- Network problems

Storage:

- Running out of space

- Slow performance

- Availability issues

Apps:

- Slow response times

- Errors

- High CPU/memory

Databases:

- Performance issues

- Storage full

- Deadlocks

Cost:

- Idle VMs

- Unused storage

- Oversized resources

## Savings

Time: 500 hours per year ($50,000)

Cost: 15-30 percent reduction ($10,000-30,000)

Uptime: 95 percent to 99.9 percent

Total Annual Benefit: $80,000-100,000

Investment: $2,000

ROI: 40x

## Implementation

Week 1: Deploy Bastion, Key Vault, Service Principal

Week 2: Configure monitoring and alerts

Week 3: Test and validate

Total: 3 weeks

## Why Bastion Server

Security:

- Isolated from production

- Limited to one purpose

- Easy to audit

- Limited damage if compromised

Practical:

- Runs 24/7

- No human error

- Easy to rebuild

- Consistent execution

Compliance:

- Complete audit trail

- Proves key rotation

- Continuous monitoring

- Separation of duties

## My Recommendation

This is the right way to do Azure monitoring:

- Microsoft best practices

- Enterprise-proven

- Immediate ROI

- Improved security

- Low maintenance (15 min/month)

Bottom line: Saves 500+ hours per year, improves security, reduces costs.

Ready to start when you approve.

## Questions

Q: What if Bastion goes down?

A: Alerts immediately. Rebuild in 1 hour. Production unaffected.

Q: What if Service Principal compromised?

A: Read-only access. Cannot access VMs or data. Disable instantly.

Q: How do we know if issues occur?

A: System monitors itself. Alerts on failures.

Q: Can we customize monitoring?

A: Yes. Add/remove alerts anytime.

Q: Current monitoring during transition?

A: Run parallel for 2 weeks. Zero disruption.

Next Steps: Schedule 15-minute call to discuss.

Microsoft Azure Well-Architected Framework compliant.