**ACME LLC – Azure Kubernetes Service:  
 Non-Functional Requirements Definition**

**Last Date Modified:** December 10th, 2021

**Version: 1.4**

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Change** | **Change Reason** |
| 1.0 | Matthew Fiallos | 10/1/2021 | Initial Non-Functional Requirements Definition draft |  |
| 1.1 | Matthew Fiallos | 11/12/2021 | Incorporate feedback and direction provided by ACME LLC | Additional information, scope clarification, and corrections |
| 1.2 | Matthew Fiallos | 11/22/2021 | Incorporate feedback and direction provided by ACME LLC, Big Data App, and internal discussions | Additional information, scope clarification, and corrections |
| 1.3 | Matthew Fiallos | 12/6/2021 | Incorporate feedback and direction provided by ACME LLC, Big Data App, and internal discussions. 3.1.1.4, 3.1.2.1, 3.1.2.2, 3.1.2.3, 3.1.2.4, 3.1.4.1, 3.1.4.2, 3.1.11.1, 3.1.11.2, 3.1.11.3, 3.1.12.1, 3.1.13.2, 3.2.1.1, 3.2.1.2, 3.2.2.1, 3.2.2.2, 3.2.3.1, 3.2.3.2, 3.2.3.3, 3.2.3.4, 3.2.4.1, 3.2.4.2, 3.2.5.2, 3.2.5.3, 3.2.5.4, 3.2.5.5, 3.2.6.1, 3.2.6.2, 3.2.8.2, 3.2.9.2, 3.2.9.8, 3.2.10.3, 3.3.3.2, 3.3.7.1, 3.4.1.1, 3.6.3.1, 3.6.6.1, 3.6.6.2, 3.6.6.3, 3.6.7.2, 3.7.4.1 | Additional information, scope clarification, and corrections |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

***Table of Contents***

[***Chapter 1***](#_heading=h.gjdgxs) ***Introduction 6***

[**1.1**](#_heading=h.30j0zll) **Purpose of this document 6**

[**1.2**](#_heading=h.1fob9te) **Style Guide for Written Requirements 6**

[1.2.1](#_heading=h.3znysh7) Requirement Structure 6

[1.2.2](#_heading=h.2et92p0) Requirement Numbering 7

[1.2.3](#_heading=h.tyjcwt) Requirement Types 7

[1.2.4](#_heading=h.3dy6vkm) Requirement Priority 8

[**1.3**](#_heading=h.1t3h5sf) **Reference Documents 9**

[**1.4**](#_heading=h.4d34og8) **Glossary 9**

[***Chapter 2***](#_heading=h.2s8eyo1) ***Project Overview & Scope 10***

[**2.1**](#_heading=h.17dp8vu) **Project Overview & Business Statement 10**

[**2.2**](#_heading=h.3rdcrjn) **Scope 11**

[2.2.1](#_heading=h.26in1rg) In Scope 11

[2.2.2](#_heading=h.lnxbz9) Out of Scope 11

[***Chapter 3***](#_heading=h.35nkun2) ***Non-Functional Requirements 13***

[**3.1**](#_heading=h.1ksv4uv) **Infrastructure 13**

[3.1.1](#_heading=h.44sinio) Environment Landscape 13

[3.1.2](#_heading=h.2jxsxqh) Server 14

[3.1.3](#_heading=h.z337ya) Operating System 14

[3.1.4](#_heading=h.3j2qqm3) Data Storage 15

[3.1.5](#_heading=h.1y810tw) Database 15

[3.1.6](#_heading=h.4i7ojhp) Data/Database Reporting Services 15

[3.1.7](#_heading=h.2xcytpi) Data/Database Analysis & Integration 15

[3.1.8](#_heading=h.1ci93xb) Network 15

[3.1.9](#_heading=h.3whwml4) Peripherals 16

[**3.2**](#_heading=h.2bn6wsx) **Software/Application 17**

[3.2.1](#_heading=h.2bn6wsx) Version 17

[3.2.2](#_heading=h.qsh70q) Function/Component 17

[3.2.3](#_heading=h.3as4poj) Configuration 18

[3.2.4](#_heading=h.1pxezwc) Implementation 18

[**3.3**](#_heading=h.49x2ik5) **Security 20**

[3.3.1](#_heading=h.49x2ik5) Authentication 20

[3.3.2](#_heading=h.2p2csry) Authorization 20

[3.3.3](#_heading=h.147n2zr) Accounting 20

[3.3.4](#_heading=h.3o7alnk) Security Levels 20

[3.3.5](#_heading=h.23ckvvd) Data Confidentiality 20

[3.3.6](#_heading=h.ihv636) Access Controls 21

[3.3.7](#_heading=h.32hioqz) User Account Provisioning 21

[3.3.8](#_heading=h.1hmsyys) Single-Sign-On (SSO) 21

[3.3.9](#_heading=h.41mghml) Domain/Directory 21

[**3.4**](#_heading=h.2grqrue) **Reliability 22**

[3.4.1](#_heading=h.2grqrue) Availability 22

[3.4.2](#_heading=h.vx1227) Accuracy 22

[3.4.3](#_heading=h.3fwokq0) Disaster Recovery 22

[3.4.4](#_heading=h.1v1yuxt) Failure Management 22

[3.4.5](#_heading=h.4f1mdlm) Recovery 23

[3.4.6](#_heading=h.2u6wntf) Failover / High Availability 23

[3.4.7](#_heading=h.3tbugp1) Scalability 23

[3.4.8](#_heading=h.28h4qwu) Service Levels 23

[**3.5**](#_heading=h.nmf14n) **Performance 24**

[3.5.1](#_heading=h.nmf14n) Response Times 24

[3.5.2](#_heading=h.37m2jsg) Throughput 24

[3.5.3](#_heading=h.1mrcu09) Volumes 24

[**3.6**](#_heading=h.46r0co2) **Maintainability 25**

[3.6.1](#_heading=h.46r0co2) Archiving 25

[3.6.2](#_heading=h.2lwamvv) Backups 25

[3.6.3](#_heading=h.111kx3o) Data Integrity 25

[3.6.4](#_heading=h.3l18frh) Release Upgrade Management and control 25

[3.6.5](#_heading=h.206ipza) Documentation and Help Systems 25

[3.6.6](#_heading=h.4k668n3) Operational Recovery 26

[3.6.7](#_heading=h.2zbgiuw) Data Refreshes 26

[3.6.8](#_heading=h.1egqt2p) Governance 26

[**3.7**](#_heading=h.3ygebqi) **Operations & Supportability 27**

[3.7.1](#_heading=h.3ygebqi) Service Levels 27

[3.7.2](#_heading=h.2dlolyb) System Support & Staffing 27

[3.7.3](#_heading=h.sqyw64) Deployments, Migrations, and Release Management 27

[3.7.4](#_heading=h.3cqmetx) System Administration 27

[3.7.5](#_heading=h.1rvwp1q) Troubleshooting 28

[3.7.6](#_heading=h.4bvk7pj) Environment Access 28

[3.7.7](#_heading=h.2r0uhxc) Monitoring 29

[**3.8**](#_heading=h.1664s55) **Legal & Compliance 30**

[3.8.1](#_heading=h.1664s55) Legal 30

[3.8.2](#_heading=h.3q5sasy) Regulatory 30

[3.8.3](#_heading=h.25b2l0r) Audit 30

[3.8.4](#_heading=h.kgcv8k) Privacy 30

[3.8.5](#_heading=h.34g0dwd) External 30

[**3.9**](#_heading=h.1jlao46) **Interfaces 32**

[3.9.1](#_heading=h.43ky6rz) Internal 32

[3.9.2](#_heading=h.2iq8gzs) External 32

[***Chapter 4***](#_heading=h.xvir7l) ***Signoff & Approval 33***

[**4.1**](#_heading=h.3hv69ve) **Peer Review 33**

[**4.2**](#_heading=h.1x0gk37) **Approvals 33**

# Introduction

## Purpose of this document

The Non-Functional Requirements Definition documents and tracks the necessary information required to effectively define non-functional and technical requirements. The Non-Functional Requirements Definition document is created during the Planning Phase of the project. Its intended audience is the project manager, project team, project sponsor, client/user, ACME LLC Team(s), and any stakeholder whose input/approval into the requirements definitions process is needed.

## Style Guide for Written Requirements

* + 1. **Requirement Structure**

Non-Functional Requirements are statements in terms of WHAT the system must do, the properties it must exhibit, qualities it must possess, and how the capabilities will be delivered. Non-Functional Requirements may be system agnostic and independent of system design.

There are four key components of a requirement statement: subject, focus word, capability, and criterion:

<Subject> <focus word> <capability> within <criterion\*>.

<Subject> <focus word> <capability>.

*\*Where criterion is assumed to be 100 percent of the stated capability.*

1. **Subject** is the person, place, or thing who performs the action. (E.g.; User, Customer, System)
2. **Focus Word** describes the requirement's significance. They are not and should not be confused with the priority of the requirement. Each documented requirement shall contain one of 4 focus words to be determined by the following definitions:

|  |  |
| --- | --- |
| **Focus Word** | **Definition** |
| **Shall** | * + - * Indicates a mandatory requirement to be met from the perspective of the solution       * Implies “is required to” |
| **Can** | * + - * Used to indicate the users have optional behavior choices       * Implies “is able to” |
| **MUST** | * + - * Used to indicate the requirement reflects a regulation       * MUST always appears in capital and bold-faced letters |
| **Will** | * + - * Used to indicate the requirement reflects a business rule or requirement |

1. **Capability** is a single verb that describes an action taken by the subject. (E.g.; Perform, Execute, Process, View, Select, Analyze)
2. **Criterion** is an optional quantitative or qualitative limit, range, or boundary condition. (E.g.; In two seconds or less, rate a four or better on a five-point scale or Reliability is greater than 99.5 percent)
3. **Example Requirement Statements using Focus Words:**
   * The system **shall** be able to answer requests within five seconds.
   * The user **will** be able to monitor the system transaction logs.
   * The user **can** select to add one or more attributes to a transaction.
   * The customer **MUST** receive notification via email when a system outage occurs.
   * The system **MUST** provide a PCI zone to accommodate sensitive data.

* + 1. **Requirement Numbering**

Numbering will be used to uniquely identify each requirement in this document and follow the requirement into traceability.

* + 1. **Requirement Types**

Each requirement will be categorized into a requirement type. Requirements types are logical groupings of requirements by common functions, features, and attributes.

Requirement types are as follows:

* **Infrastructure** - Describes capabilities that the solution must have in order to meet the needs that a given stakeholder has.
* **Software/Application** – Describes the capabilities and attributes that specific software and applications must have in order to meet the needs that a given stakeholder has.
* **Security** – Describes the ability to ensure appropriate confidentiality of information, the integrity of information stored in the system, the ability to verify whether actions were taken and by whom, and the ability to authenticate users.
* **Reliability** – Describes the ability of the system to recover from errors, uptime, or failures in the interfaces.
* **Performance** – Describes the time taken to perform activities, functions, and resource utilization levels.
* **Maintainability** - Describes the ability to change one component without affecting others, the ability to reuse components, whether the system can be effectively tested and problems can be properly diagnosed, the ease of making changes, and the ability to implement changes without causing unexpected failures.
* **Operations & Supportability** – Describes items needed for day-to-day execution of work. This will include new business & support processes, organizational changes, resource & staffing needs.
* **Legal & Compliance** - Describes the needs of governing authorities.
* **Interfaces** – Describes the ability and extent to which the system connects to internal and external systems or solutions.
  + 1. **Requirement Priority**

A priority is given to each requirement to ensure analysis, design, and implementation efforts focus on the most critical requirements. The priorities are defined to reach a common understanding with stakeholders on the importance they place on the delivery of each requirement. Requirement priorities are divided into four categories: Must, Should, Could, and Won’t.

Category descriptions are as follows:

* **Must** - Describes a requirement that must be satisfied in the final solution for the solution to be considered a success.
* **Should** - Represents a high-priority item that should be included in the solution if it is possible. This is often a critical requirement but one which can be satisfied in other ways if strictly necessary.
* **Could** - Describes a requirement, which is considered desirable but not necessary. This will be included if time and resources permit.
* **Won’t** - Represents a requirement that stakeholders have agreed will not be implemented in a given release but may be considered for the future.

## Reference Documents

The following documents were referenced in the creation of this document.

|  |  |
| --- | --- |
| **Artifact Name** | **Location** |
| Microsoft Azure Well-Architected Framework | https://docs.microsoft.com/en-us/azure/architecture/framework/ |
| Azure Advisor | https://docs.microsoft.com/en-us/azure/advisor/ |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| AKS | Azure Kubernetes Service |
| K8s | Kubernetes |
| ACR | Azure Container Registry |
| MCR | Microsoft Container Registry |
| System | Azure Kubernetes Service |
|  |  |
|  |  |

# Project Overview & Scope

## Project Overview & Business Statement

Randstad will provide Solution Architect(s) to work under the direction of ACME LLC Company to support the following activities [collectively referred to as the “Services”]:

* Provide AKS design, deployment, and tuning support
* Leverage best practices and expertise in the following, but not limited to:
  + Microsoft Azure Kubernetes Service (AKS)
  + Security ingress/egress of data
* Convene a project closure meeting, at the conclusion of services delivery, to ensure both parties agree that the services have been completed and that issues have been addressed.

**Owner Key:**

ACME LLC: Multiple Corporate IT Departments

RT: Randstad Technologies

RT-PM: Randstad Technologies Project Manager

RT-DR: Randstad Technologies Disaster Recovery Specialist

RT-SA: Randstad Technologies Strategy & Architecture

ACME LLC-PC: Production Control

ACME LLC-PS: Production Support

ACME LLC-SA: ACME LLC Solution Architect

ACME LLC-PM: ACME LLC Project Manager

ACME LLC-PA: ACME LLC Performance Architecture team

ACME LLC-EM: ACME LLC Enterprise Monitoring

ACME LLC-IPS: ACME LLC Information Protection Services

ACME LLC-NET: ACME LLC Network Services

ACME LLC-VDI: ACME LLC Desktop Technology team

ACME LLC-DCSS: ACME LLC Server team

ACME LLC-STORAGE: ACME LLC Storage Management team

ACME LLC-DBA: ACME LLC Database Administrators

ACME LLC-CM: ACME LLC Change Management

ACME LLC-WH: ACME LLC Web Hosting Team

## Scope

* + 1. **In Scope**

Describe functionality, processes, devices, products, services, etc. that are within the range of work for the project.

|  |  |
| --- | --- |
| **In-Scope Description** | **Source** |
| Deployment of Azure Kubernetes Service in an existing ACME LLC tenant/subscription to support the Big Data App Application/Container | SOW |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

* + 1. **Out of Scope**

Describe functionality, processes, devices, products, services, etc. that are outside the range of work for the project.

|  |  |
| --- | --- |
| **Out of Scope Description** | **Source** |
| CI/CD tools, integration, and any configuration outside of MS ARM templates and Helm charts provided by Big Data App. | RT |
|  |  |

# Non-Functional Requirements Infrastructure

* + 1. **Environment Landscape**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall leverage documented MS best practices and reference architectures as a starting point for the technical design | RT-SA | Must | RT |
| 2 | The system architecture and technical design shall focus on security and identify unmitigated risks | RT-SA | Must | RT |
| 3 | The system shall be designed in a manner to support a single workload (Big Data App Container) using vendor-provided sizing guidelines | RT-SA | Must | RT |
| 4 | The system shall have a development and a production environment | ACME LLC | Must | RT |
| 5 | The system shall have at least one ACR to store certified images for containers and workloads | RT-SA | Must | RT |
| 6 | All Host OS and Big Data App images must be stored in a ACR that the system will leverage | RT-SA | Must | RT |
|  |  |  |  |  |

* + 1. **Server**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Obtain final sizing estimates & recommendations from Big Data App | Big Data App | Must | RT |
| 2 | Big Data App Node Configuration - Qty: 1, vCPU: Standard\_E16d\_v4, 128GB, Big Data App Heap:16GB | Big Data App | Must | RT |
| 3 | Executor Node Configuration: Qty: 3, 128GB, Heap: 16GB | Big Data App | Must | RT |
| 4 | Zookeeper Node Configuration: Qty: 3, 8GB | Big Data App | Must | RT |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Operating System**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall use the Ubuntu 18.04.5 LTS image for the cluster host OS | Microsoft | Must | RT |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Data Storage**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Persistent storage shall be required for key components of the AKS system | Microsoft / K8s | Must | RT |
| 2 | Data Storage shall perform at a minimum of 100/MB sec | Big Data App | Must | RT |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Database**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Data/Database Reporting Services**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Data/Database Analysis & Integration**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Network**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The Big Data App workload shall have a load balancer | Big Data App | Must | RT |
| 2 | The system shall leverage an existing ‘hub and spoke’ topology for shared components, i.e. WAF and Azure Firewall | RT-SA | Must | ACME LLC |
| 3 | The system shall Deploy the AKS cluster into an existing Azure Virtual Network spoke. | RT-SA | Must | ACME LLC |

* + 1. **Peripherals**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

## 3.2 Software/Application

* + 1. **Version**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system can utilize Kubernetes 1.19 and higher (1.2.0) | Big Data App | Must | RT |
| 2 | The system shall leverage Azure AD ‘Premium’ for identity management and MFA enablement | RT | Should | ACME LLC |
| 3 | Big Data App Node Configuration - Qty: 1, vCPU: Standard\_E16d\_v4, 128GB, Big Data App Heap:16GB | Big Data App | Must | RT |
| 4 | Executor Node Configuration: Qty: 3, 128GB, Heap: 16GB | Big Data App | Must | RT |
| 5 | Zookeeper Node Configuration: Qty: 3, 8GB | Big Data App | Must | RT |
|  |  |  |  |  |

* + 1. **Function/Component**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Azure Container Registry will be used for the container image registry. The cluster will access the registry through Azure Private Link. | RT-SA | Must | RT |
| 2 | AKS will be integrated with Azure Active Directory for role-based access control. | RT-SA | Must | RT |
| 3 | Azure Monitor will be used for logging, metrics, monitoring, and alerting to use the existing knowledge of Log Analytics. | RT-SA | Must | RT |
| 4 | Azure Key Vault will be used to store all secret information including SSL certificates. Key Vault data will be mounted by using Azure Key Vault with Secrets Store Container Storage Interface (CSI) driver. | RT-SA | Must | RT |
| 5 | Azure Key Vault will be used to store all secret information including SSL certificates. | RT-SA | Must | RT |
| 6 | Key Vault data will be mounted by using Azure Key Vault with Secrets Store Container Storage Interface (CSI) driver. | RT-SA | Must | RT |
| 7 | To make sure the workload is scaled properly, requests and limits will be enforced by assigning quotas for the Horizontal Pod Autoscaling (HPA). | RT-SA | Must | RT |
| 8 | AKS cluster autoscaler will be enabled so that additional nodes are automatically provisioned if pods can’t be scheduled. | RT-SA | Must | RT |
| 9 | Two node pools will be used in AKS. | Big Data App | Must | RT |
| 10 | The system node pool will be used for critical system pods. The second node pool will be used for the application workload. | Big Data App | Must | RT |
| 11 | The AKS system will have its own (ARM Template deployed) dedicated Key store | RT-SA | Must | RT |

* + 1. **Configuration**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | AKS deployment configuration shall be handled through the use of ARM templates | RT-SA | Must | RT |
| 2 | Big Data App container configuration shall be managed through the use of Helm charts | Big Data App | Must | ACME LLC |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Implementation**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Big Data App workload/container shall be stored in the ACR and deployed via Helm charts | RT-SA/Big Data App | Must | RT/Big Data App |
| 2 | The AKS system shall be initially implemented through the deployment of parameterized ARM templates | RT-SA | Must | RT/ACME LLC |

## Security

* + 1. **Authentication**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Use Azure Managed Identities with the Azure AKS Cluster | AKS Best Practice | Shall | RT |
| 2 | Do not use/configure AKS Cluster Service Principals | AKS Best Practice | Shall | RT |

* + 1. **Authorization**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Implement Azure RBAC for Kubernetes Authorization | AKS Best Practice | Shall | RT |
| 2 | The system shall have an Owner role on the AKS cluster and a Log Analytics contributor role to enable container monitoring | RT-SA | Must | RT |

* + 1. **Accounting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Setup Alerts within Azure Security Center (ASC) and Sentinel to alert on Azure resource changes and administrative account suspicious activities | AKS Best Practice |  | ACME LLC/RT |
| 2 | Set up Alerts to notify on attempts to use deactivated credentials | AKS Best Practice |  | ACME LLC/RT |
| 3 | Setup Azure AD Identity Protections with Sentinel for auditing and investigation needs | AKS Best Practice |  | ACME LLC/RT |
| 4 | The system shall require a Log Analytics Workspace | RT-SA | Must | RT |

* + 1. **Data Confidentiality**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system should use separate AKS environments with separate Azure Resource Groups (prod and dev resource groups) | AKS Best Practice | Shall | ACME LLC/RT |
| 2 | The system should use namespaces to separate Kubernetes with logical isolation | AKS Best Practice | Shall | ACME LLC/RT |
| 3 | The system should monitor all ingress and egress traffic to ensure encryption in transit for all sensitive information | AKS Best Practice | Shall | ACME LLC/RT |
| 4 | The system should encrypt data at rest on AKS clusters with Azure Storage Service Encryption (SSE) | AKS Best Practice | Shall | RT |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Access Controls**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system must secure access to the API server using authorized IP address ranges when creating the aks cluster using --api-server-authorize-ip-ranges parameter or via the Azure portal (Kubernetes, settings, networking, set authorized IP ranges) | AKS Best Practice | Must | RT |
| 2 | The system should secure access to the AKS cluster with Azure Conditional Access policies (Named locations only, AKS App Restrictions) | AKS Best Practice | May | RT/ACME LLC |
| 3 | The system should secure access to the AKS cluster with Azure AD Privileged Identity Management (PIM) for just-in-time access | AKS Best Practice | May | RT/ACME LLC |
| ~~4~~ | ~~The system should use a privileged access workstation (PAW) for all control plane/admin tasks~~ | ~~AKS Best Practice~~ | ~~Shall~~ | ~~RT~~ |
| ~~5~~ | ~~The system should integrate Azure Key Vault using FlexVolume drive to store and rotate credentials, storage keys, or certificates~~ | ~~AKS Best Practice~~ | ~~Shall~~ | ~~RT~~ |

* + 1. **Identity and Access Controls**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | AKS local accounts will be disabled/removed after successful AKS cluster deployment (all environments) | RT-SA | Must | RT |
| 2 | The system shall use a secure store for sensitive information | RT-SA | Must | RT |

* + 1. **Single-Sign-On (SSO)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Okta SSO shall be used for workload authentication to Big Data App | ACME LLC | Shall | ACME LLC |
|  |  |  |  |  |

* + 1. **Domain/Directory**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall use AKS-managed Azure AD integration | AKS Best Practice | Must | RT |
| 2 | The system shall use OKTA multi-factor authentication for all Azure AD-based access (already existing) | AKS Best Practice | Must | ACME LLC/RT |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Network Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall minimize direct exposure to Azure resources to the public internet | RT-SA | Must | RT |
| 2 | All web applications shall require a web application firewall (WAF or similar technology, i.e. NGINX) service to help govern HTTP traffic flows | RT-SA | Must | RT |
| 3 | The system shall expose all web services through SSL and aim for end-to-end encryption, as much as possible. (Edge termination of SSL/TLS at AKS cluster perimeter is an option) | RT-SA/Big Data App | Must | RT |
| 4 | The system shall leverage IP restrictions to the system API | RT-SA | Must | RT |
| 5 | Azure Network Policy will be enabled for use, even though there's a single workload in one line of business. | RT-SA | Must | RT |
| 6 | The system will access the registry through Azure Private Link. | RT-SA | Must | RT |
| 7 | TLS/SSL shall be used | RT-SA | Must | RT |
| 8 | TLS/SSL shall be used for Big Data App Flight (ODBC/JDBC) | ACME LLC | Shall | ACME LLC/Big Data App |

* + 1. **Vulnerability Management**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Use Azure Security Center to scan AKS instances including Container Registries for vulnerabilities | AKS Best Practice | Must | ACME LLC/RT |
| 2 | Implement Azure Defender for AKS | AKS Best Practice | Should | ACME LLC/RT |
| 3 | Implement a process to ensure Big Data App remains patched for the duration of the cluster lifetime | AKS Best Practice | Must | ACME LLC/Big Data App/RT |
| 4 | The system design & approach can minimize the attack surface | AKS Best Practice | Must | RT/ACME LLC Security |
| 5 | The system design & approach can implement a Layered Defense | AKS Best Practice | Should | ACME LLC/RT |
|  |  |  |  |  |

## Reliability

* + 1. **Availability**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall utilize availability sets for VMs | RT-SA | Must | RT |
| 2 | The AKS control plane, nodes, and pods shall be highly available and all components will be fault-tolerant | RT-SA | Shall | ACME LLC |
| 3 | The AKS system shall have no documented availability requirements and will be deemed ‘best effort’ | RT-SA | Shall | ACME LLC |
|  |  |  |  |  |

* + 1. **Accuracy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Disaster Recovery**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Regularly maintained backups should be maintained along with recovery validation supporting ACME LLC disaster recovery efforts | RT-SA | Shall | ACME LLC/RT |
| 2 | The AKS system shall leverage existing Azure technologies, services, and ACME LLC procedures to provide a ‘Best Effort’ recovery in the event of a disaster. | RT-SA | Shall | ACME LLC |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Failure Management**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall ‘self-heal’ and spawn new nodes and pods upon detected failures | RT-SA | Must | RT |
| 2 | The AKS system will ‘self-manage’ and resolve Node and POD failures | RT-SA | Shall | ACME LLC |

**Recovery**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall leverage standard Azure technologies and procedures for recovering PaaS/IaaS services & devices | RT-SA | Shall | ACME LLC/RT |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Failover / High Availability**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | All system components shall be fault-tolerant | RT-SA | Must | RT |
| 2 | The Big Data App workload/container shall be fault-tolerant and highly available | RT-SA | Must | RT |

* + 1. **Scalability**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall enable autoscaling and Automatically scale to handle the demands of expected traffic patterns | RT-SA | Must | RT |
| 2 | The system shall Allow granular scaling per workload and independent scaling between different partitions in the workload | RT-SA | Must | RT |
| 3 | The AKS system shall scale horizontally through the use of the AKS auto-scale capability | RT-SA | Shall | ACME LLC |
| 4 | The AKS system overall scaling ‘max ceiling’ for cloud resources shall be limited by Big Data App licensing | RT-SA | Shall | ACME LLC |

* + 1. **Service Levels**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The Big Data App workload will be ‘right sized’ (scenario-based or stress-tested) to define a minimum service level that is deemed acceptable by ACME LLC | ACME LLC | Shall | Big Data App/ACME LLC |
|  |  |  |  |  |

## Performance

* + 1. **Response Times**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| ~~1~~ | ~~Requirements to be defined by ACME LLC~~ |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Throughput**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Volumes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Maintainability

* + 1. **Archiving**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Backups**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Cluster resources, configurations, and persistent volume data must be backed up using an automated system | AKS Best Practice | Must | ACME LLC/RT |
| 2 | A periodic restore of data shall be completed to validate data restoration | AKS Best Practice | Shall | ACME LLC/Big Data App |
| 3 | The system shall ensure the protection of backups and keys by enabling soft-delete and other resilient mechanisms | AKS Best Practice | Shall | ACME LLC/Big Data App |

* + 1. **Data Integrity**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Release Upgrade Management and control**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall be upgraded at a minimum of once a year to stay on a supported version of Kubernetes | Microsoft | Shall | ACME LLC |
|  |  |  |  |  |

* + 1. **Documentation and Help Systems**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Operational Recovery**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Data Refreshes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Governance**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

## Operations & Supportability

* + 1. **Service Levels**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **System Support & Staffing**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Deployments, Migrations, and Release Management**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The ACME LLC Enterprise Analytics/DS team shall leverage ARM templates to deploy the system | RT-SA | Must | RT |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **System Administration**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Troubleshooting**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Environment Access**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | SSH access to the jump box shall be provided by Azure Bastion | AKS Reference Architecture | Must | RT |
| 2 | A jump box within the same VNET as the system shall be used for Kubernetes management | AKS Reference Architecture | Must | RT |
| ~~3~~ | ~~Azure privileged identity management (PIM), shall be used to secure just in time (JIT) access requirements and establish a least privileged model for accessing the Kubernetes control plane~~ | ~~AKS Reference Architecture~~ | ~~Shall~~ | ~~RT~~ |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Monitoring**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | The system shall Emit telemetry metrics to get insights into the performance and scaling operations. Integration with Azure Monitor is preferred. | RT-SA | Must | RT |
| 2 | The system shall monitor service principles for service access and application-level access. | RT-SA | Must | RT/ACME LLC |
|  |  |  |  |  |
|  |  |  |  |  |

## Legal & Compliance

* + 1. **Legal**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Regulatory**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Audit**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **Privacy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
| 1 | Certain portions of the data contained in the ‘data source’ for Big Data App have been deemed ‘sensitive’. Existing control measures will be leveraged to restrict access to sensitive data. | ACME LLC | Should | ACME LLC |
|  |  |  |  |  |

* + 1. **External**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

## Interfaces

* + 1. **Internal**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* + 1. **External**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Requirement** | **Source** | **Priority** | **Owner** |
|  |  |  |  |  |
|  |  |  |  |  |

# Signoff & Approval

## Peer Review

|  |  |  |
| --- | --- | --- |
| **Reviewed By** | **Version Reviewed** | **Date** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Approvals

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_