Azure AKS Deployment Requirement Document

1. Cluster Configuration

Cluster Name: clync-aks-cluster

Region: westeurope

2. Node Pools

2.1. System Node Pool

- Node Size: Standard_D2s_v3
- Node Count: 3
- Purpose: Run system pods and essential services like the Kubernetes API server, DNS, and system-level components.

2.2. Application Node Pool

- Node Size: Standard_DS3_v2
- Node Count: 5
- Purpose: Run the microservices and application workloads.
- Auto-scaling: Enabled
  - Min Count: 3
  - Max Count: 10

3. Network Configuration

Virtual Network (VNet):

- Address Space: 10.0.0.0/16
- Subnet: aks-subnet (10.0.0.0/24)

Network Policy: Azure

Network Plugin: Azure CNI

4. Storage

Managed Disks:

- Type: Standard_LRS
- Size: 100 GB
- Count: 10

5. Security

RBAC: Enabled

AAD Integration: Enabled

Network Security Groups (NSGs): Configured to restrict access to the cluster

Azure Policy: Applied for governance and compliance

Explanation of Azure AKS Deployment Requirements

1. Cluster Configuration

This section outlines the basic setup for the Azure Kubernetes Service (AKS) cluster.

- Cluster Name: `clync-aks-cluster` - This is the unique identifier for the AKS cluster within your Azure environment.

- Region: `westeurope` - Specifies the geographic location where the AKS cluster will be deployed. In this case, it's in the `westeurope` region, which influences latency, data residency, and compliance requirements.

2. Node Pools

2.1. System Node Pool

- Node Size: `Standard_D2s_v3` - The size (SKU) of the virtual machines used for this pool. `Standard_D2s_v3` offers a balanced combination of CPU, memory, and cost, suitable for system-related tasks.

- Node Count: `3` - The number of nodes in this pool. Three nodes ensure high availability and redundancy.

- Purpose: This pool runs essential Kubernetes components like the API server, DNS, and other system-level services that manage the cluster.

2.2. Application Node Pool

- Node Size: `Standard_DS3_v2` - The size chosen for application workloads. `Standard_DS3_v2` provides more resources, suitable for running your microservices.

- Node Count: `5` - Five nodes are allocated to run the application workloads, balancing performance and cost. Following are the services that run on these nodes:

i. Social
ii. Financial
iii. Flagship
iv. Admin APIs
v. Admin Portal Frontend

- Auto-scaling: `Enabled` - Automatically adjusts the number of nodes based on demand, optimizing resource usage.

- Min Count: `3` - The cluster will have at least 3 nodes and can scale up to 10 based on workload requirements.

3. Network Configuration

This section defines the networking setup for the AKS cluster.

- Virtual Network (VNet):

- Address Space: `10.0.0.0/16` - The address range allocated for the virtual network.

- Subnet: `aks-subnet (10.0.0.0/24)` - A smaller range within the VNet where the AKS nodes will reside.

- Network Policy: `Azure` - This defines the network rules and policies, like restricting or allowing traffic between pods.

- Network Plugin: `Azure CNI` - The plugin responsible for networking in the cluster. Azure CNI integrates directly with Azure networking, providing features like network security groups (NSGs) and virtual network integration.

4. Storage

This section outlines the storage resources needed by the AKS cluster.

- Managed Disks:

- Type: `Standard_LRS` - The disk type is set to Standard Locally Redundant Storage, providing cost-effective, durable storage.

- Size: `100 GB` - Each disk will have a capacity of 100 GB.

- Count: `10` - Ten managed disks will be provisioned for storing persistent data used by applications running in the cluster.

5. Security

Security configurations ensure the cluster is protected and complies with organizational policies.

- RBAC: `Enabled` - Role-Based Access Control (RBAC) restricts access to the Kubernetes API based on user roles.

- AAD Integration: `Enabled` - Azure Active Directory (AAD) integration allows users to authenticate using their Azure AD credentials, simplifying management and enhancing security.

- Network Security Groups (NSGs): Configured to control incoming and outgoing network traffic, ensuring only authorized communication with the cluster.

- Azure Policy: Policies are applied to enforce compliance and governance across the cluster, ensuring that it adheres to your organization’s standards.