**Set 2: Setting-up Azure Kubernetes Cluster**

For the implementation of the Infrastructure, I will use an azure Traffic Manager (has health check and can direct traffic to a standby DR site when needed) to direct traffic to a Public IP Address and to an Azure Application Gateway. I will also implement OWASP 3.1 and rewrite HTTP headers and URL as additional protection. Then, the Application gateway will pass the connection to the Azure Kubernetes Service. I will use an Ingress Controller (like Traefik) as reverse proxy. This means all connections coming to AKS (Azure Kubernetes Service) cluster will be HTTPS while HTTP is used within the AKS cluster’s pods or services. The AKS Cluster, Application Gateway and IP address are placed in a public facing virtual network which is not joined to any corporate network. Then, azure container registry will be used for our container registry and azure devops pipeline will handle the building of codes when there are changes. We will also utilize Helm charts to deploy our containers to the AKS cluster. We can also use terraform to orchestrate our azure resources such as the AKS cluster, Virtual Network, Application gateway and Azure container registry. We just have to add a service connection in azure devops pipeline that has permission to modify resources in our subscription or resource group.

Then a separate Azure Virtual Network is created for **internal-assets**. This azure Vnet is private and has no internet access. We typically join this private Vnet into the corporate internal network if we have one. Then, we will create a Vnet peering between the public facing Vnet above and the private Vnet so we can have communication between our resources.

Monitoring, it is important to have proper readinesProbe and/or livenessProbe in our Pods that check the needed connection between the AKS pods and internal-assets resources. As a sample. <https://company.cluster/weatherforecast/healthcheck/> will return either 200 if all check are successful and return any other result if not. We can then create log alerts for such errors. AKS has Container insights which can monitor stdout or stderr and send these to Log analytics workspace. We can then create Log alerts for these types of logs.

Please review Se2-InfrastructureDiagram.png file that is also included in the list of files in this directory. Thanks.

Sources: <https://learn.microsoft.com/en-us/azure/azure-monitor/containers/kubernetes-monitoring-enable?tabs=cli#enable-container-insights>