Azure Reference Architecture

DEV / OPS

git push

Source Code Management

CI/CD

Azure Pipelines

container push → Container registry → container pull

helm upgrade

nginx 1...N

php-fpm 1...N

cronjob

fluentd

drupal namespace

Ingress Gateway 1...N

istio-system namespace

Azure Kubernetes Service (AKS)

Platform Services

Vault

Cert Manager

Istio / Kiali

Open Policy Agent

ElasticSearch Operator

Fluentd Operator

Velero

Prometheus Operator

Falco

Azure Load Balancer

Azure DNS

Clients

Content Delivery Network (CDN)

Firewall

1 or more Virtual Machines power the cluster.

VMs are configured by AKS.

Virtual Network

Managed Database Service

Azure Files Storage

Log Analytics

Infrastructure: https://github.com/canada-ca-terraform-modules/terraform-kubernetes-aks

Platform: https://github.com/canada-ca-terraform-modules/terraform-kubernetes-aks-platform

All application secrets are encrypted, dynamically rotated and fully audited thanks to Vault

Helm Chart: https://github.com/drupalwxt/helm-drupal

Open Policy Agent with policy enforcement from GateKeeper v3

Velero is leveraged for point in time backups of your application and PVC's

Istio is the chosen Service Mesh which enforces Mutual TLS across all services

Cert Manager is leveraged to automate the management and issuance of certs

Azure Key Vault
Cluster secrets are encrypted using a key stored in the Azure Key Vault.

Disks are also encrypted at rest.

Azure Active Directory
Provides user authentication for cluster management.

Monitoring
Internal cluster monitoring logging handled by ElasticSearch / Kibana.

Log Analytics
Fluentd can export any Kubernetes log to Azure Log Analytics.

Use **Azure DNS** to provide domain name resolution.

Use the **Azure Content Delivery Network (CDN)** to provide caching of static content and cacheable dynamic content.

Use the **Azure Firewall** to secure the Virtual Network.

Use the **Azure Kubernetes Service** to provide a managed Kubernetes cluster to run Drupal WxT. There can be multiple VMs backing the cluster.

Use an **Azure Load Balancer** to provide access to the Istio Ingress Gateway running on one or more Kubernetes nodes.

Use **Istio**, a service mesh, to provide: (a) mutual TLS between services in the cluster, (b) real-time observability and tracing, (c) canary / blue/green deployments, (d) advanced traffic routing.

Other **platform services**: ElasticSearch and Fluentd for logging, Prometheus + Grafana for monitoring.

Use **MySQL** from a Managed Database provided the cloud provider. Or, alternatively leverage the MySQL operator for in Cluster persistent storage.

Use **Azure File Storage (NFS)** for Drupal public and private files.

Prepared by:

William Hearn (william.hearn@canada.ca)
Zachary Seguin (zachary.seguin@canada.ca)