Configuring Azure AD workload identity on AKS

Let's configure the Azure AD workload identity feature on our AKS cluster so that our pods can later get access to our Azure Key Vault secrets.

In Play.Identity repo

1. Show the Azure docs page

2. Update the README:

Creating the Azure Managed Identity and granting it access to Key Vault secrets
```powershell
az identity create --resource-group $appname --name $namespace
$IDENTITY_CLIENT_ID=az identity show -g $appname -n $namespace --query clientId -otsv
az keyvault set-policy -n $appname --secret-permissions get list --spn $IDENTITY_CLIENT_ID
```

3. Run the commands

4. Show identity in Azure Portal

5. Show identity in Key Vault access policies

6. Add the service account to identity.yaml:

```
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations:
    azure.workload.identity/client-id: REPLACE_WITH_IDENTITY_CLIENT_ID
  labels:
    azure.workload.identity/use: "true"
  name: identity-serviceaccount
```

7. Update the pod template spec:

```
apiVersion: apps/v1
kind: Deployment
…
spec:
  …
  template:
    metadata:
      labels:
        app: identity
        azure.workload.identity/use: "true"
```

```
  spec:
    serviceAccountName: identity-serviceaccount
    containers:
  …
```

8. Deploy to kubernetes:

kubectl apply -f .\kubernetes\identity.yaml -n $namespace

9. Update the README (copy commands from the docs page):

Establish the federated identity credential
```powershell
$AKS_OIDC_ISSUER=az aks show -g $appname -n $appname --query oidcIssuerProfile.issuerUrl -otsv

az identity federated-credential create --name $namespace --identity-name $namespace --resource-group $appname --issuer $AKS_OIDC_ISSUER --subject "system:serviceaccount:${namespace}:${namespace}-serviceaccount"
```

10. Run the commands

11. Show the federated credentials configuration in the identity in Azure Portal

12. Commit and push
"Added steps to configure the workload identity and grant access to secrets"

In the next lesson you will verify that your Identity microservice pod can successfully read secrets from Key Vault via its associated Azure managed identity.