Microsoft Azure

AKS Cluster Guide

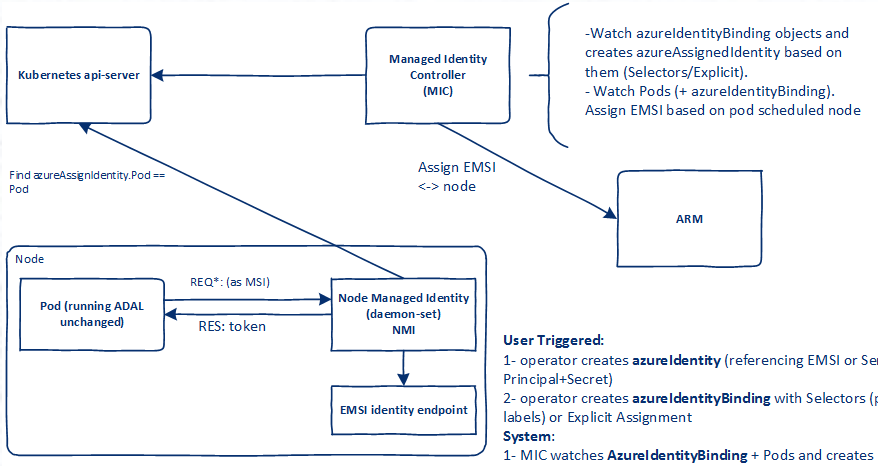
Setup AAD Pod Identity Configuration in AKS

AAD Pod Identity Project

AAD Pod Identity enables Kubernetes applications to access cloud resources securely with Azure Active Directory (AAD).

Using Kubernetes primitives, administrators configure identities and bindings to match pods. Then without any code modifications, your containerized applications can leverage any resource in the cloud that depends on AAD as an identity provider.

Design Concept



User Triggered:
1- operator creates **azureIdentity** (referencing EMSI or Service Principal+Secret)
2- operator creates **azureIdentityBinding** with Selectors (pods labels) or Explicit Assignment
System:
1- MIC watches **AzureIdentityBinding** + Pods and creates **azureAssignedIdentity**
2- MIC watches pods and assign MSI to nodes where are they are scheduled.
Token Acquisition:
1- pod uses ADAL (as-is) to acquire token for MSI
2- call is picked up by NMI. NMI uses source ip to resolve pod-name. NMI uses pod-name to find which identity assigned to it
3- NMI calls node's EMSI endpoint (or use SP/Secret) to acquire token on behalf of pod.

** Uses SPIFFE assigned identity (instead of source IP) once available*

Deploy aad-pod-identity

Use `kube-system` namespace

Deploy `aad-pod-identity` components to an RBAC-enabled cluster:

```
kubectl apply -f https://raw.githubusercontent.com/Azure/aad-pod-identity/master/deploy/infra/deployment-rbac.yaml

# For AKS clusters, deploy the MIC and AKS add-on exception by running -
kubectl apply -f https://raw.githubusercontent.com/Azure/aad-pod-identity/master/deploy/infra/mic-exception.yaml
```

Setup Environment variables

```
# resource group that is not MS_ prefixed
$rg="aks-cluster-rg"
$podId="aks-identity"

# cluster name
$name="a-aks"
```

Create Managed Identity (user-assigned identity)

```
# Create Identity
az identity create -g $rg -n $podId -o json

# Assign Role
# use this value for aadpodidentity.yaml clientId value
$clientId = az aks show -g $rg -n $name --query servicePrincipalProfile.clientId -o tsv
# use this value for aadpodidentity-binding.yaml resourceId
$resourceId = az identity show -g $rg -n $podId --query "id" --output tsv
az role assignment create --role "Managed Identity Operator" --assignee $clientId --scope $resourceId
```

[Role Assignment]

Create AzureIdentity with

aadpodidentity.yaml

```
    echo $clientId
    echo $resourceId
```

```yaml
apiVersion: "aadpodidentity.k8s.io/v1"
kind: AzureIdentity
metadata:
  name: [$podId]
spec:
  type: 0   #user assigned MS or type:1 Service Principal
  # az identity show -g $rg -n $podId --query "id" --output tsv
  resourceID: /subscriptions/2092a2b8-c72d-4127-98ff-3c16161d9721/resourcegroups/$rg/providers/Microsoft.ManagedIdentity/userAssignedIdentities/$podId
  # az identity show -g $rg -n $podId --query clientId -otsv
  clientID: e977848a-d9d5-4666-aeb2-6bbfb79f118c
```

Run: `kubectl apply -f aadpodidentity.yaml`

Create AzureIdentityBinding with `aadpodidentity-binding.yaml`

```
apiVersion: "aadpodidentity.k8s.io/v1"
kind: AzureIdentityBinding
metadata:
  name: $podId-binding
spec:
  azureIdentity: $podId
  selector: $podId_access
```

Run: `kubectl apply -f aadpodidentity-binding.yaml`

Check install

1. `kubectl get azureidentities -o yaml` or
   `kubectl describe azureidentity`
2. `kubectl get azureidentitybindings -o yaml` or
   `kubectl describe azureidentitybinding`

Using MSI with Deployment

```
spec:
  template:
    metadata:
      labels:
        # $podId_access
       aadpodidbinding: "<value of Selector in AzureIdentityBinding>"
```

Configure Azure Vault MSI Access

- Configure Managed Identity has `Reader` role on Azure Key Vault resource

```
$vault="v1"
$vaultId = az keyvault show --name $vault --query "id" --output tsv
$msiClientId = az identity show -g $rg -n $podId --query "clientId" --output tsv

# assign role
az role assignment create --role "Reader" --assignee $msiClientId --scope $vaultId

# allow read for secrets
az keyvault set-policy -n $vault --secret-permissions get list --spn $msiClientId
```

Questions 😆?