AZURE CLOUD (ENGLISH)

4. forduló

MSCI

A kategória támogatója: MSCI

Ismertető a feladatlaphoz

Közeleg az 5. forduló, figyelj az időpontokra!

Használd a naptárat:

Vagy figyeld kategóriánként az időpontokat (íme egy MINTA, hol találod):

Beágyazott rendszerek (C)

● 3. FORDULÓ

A lezárult fordulókban eddig megszerzett pontok:
[redacted]

BOSCH
Invented for life

Fordulók

Forduló	Pontok, időtartam	Feladat megoldható	Státusz
7. forduló	23 pont 25:00	2023.11.28. 20:00-tól 2023.11.28. 20:35-ig	Feladatlap
6. forduló	23 pont 30:00	2023.11.21. 20:00-tól 2023.11.21. 20:40-ig	Feladatlap
5. forduló	28 pont 25:00	2023.11.14. 20:00-tól 2023.11.14. 20:35-ig	Feladatlap

Amennyiben olyan kategóriában játszol, ahol van csatolmány, de hibába ütközöl a letöltésnél, ott valószínűleg a vírusirtó korlátoz, annak ideiglenes kikapcsolása megoldhatja a problémát. (Körülbelül minden 3000. letöltésnél fordul ez elő.)

Jó versenyzést kívánunk!

Your task is to create an Azure Kubernetes Service (AKS) deployment based on a blueprint coming from Security Architects, with the following constrains:

The nodes needs to be deployed on a VNET, which is peered to a regional Virtual Hub.

All Internet bound egress traffic must leave your estate through centrally managed perimeter Azure Firewalls. These are standard firewalls sitting in another spoke VNET of the VHUB.

The KubeAPI only needs to be reachable internally.

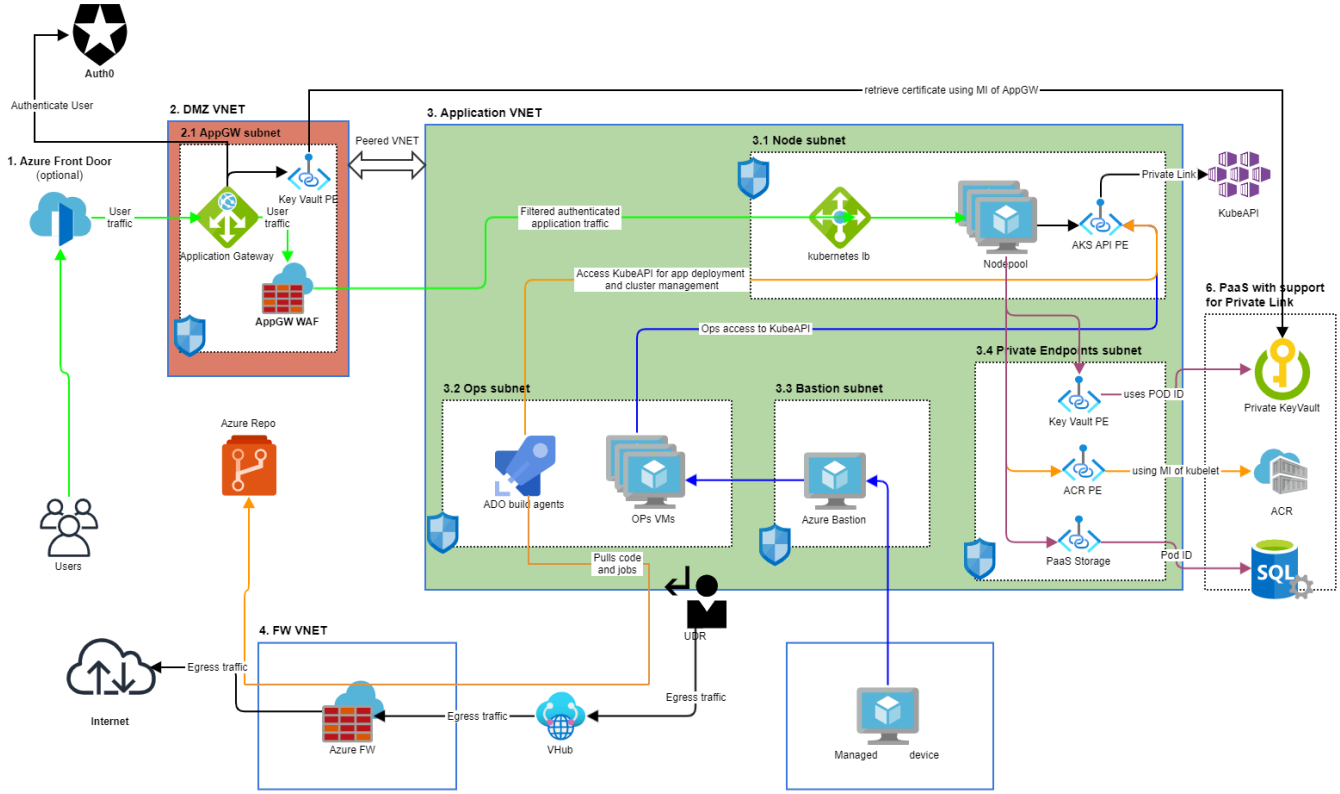
The Cluster must be accessible from the internet for clients, through an Application Gateway with Web Application Firewall (WAF) deployed, which support Custom Rules and the BotManager Ruleset.

Local Accounts must be disabled by default.

AKS must be fully Azure-AD Integrated.

AKS needs to use Kubenet to deploy pods, in order to preserve IPs on the routed network.

AKS Node's Disks must be encrypted.



1. feladat 1 pont

Which resources must be pre-existing in your subscription, so you can successfully deploy your AKS?

Válaszok

- [ ] The Control Plane User Managed Identity.
- [ ] An Azure Route Table associated with your AKS subnet.
- [ ] The subnet where your nodes will be deployed.
- [ ] The Azure Scale Set resource.
- [ ] The Azure Load Balancer used as your ingress controller.

2. feladat 2 pont

Your estate managing it's Azure DNS Zones in a central subscription with fallback option to OnPrem DNS servers.

Your context user only have the DNS Zone Contributor RBAC Role provided for those DNS Zones.

An Azure Policy denies the creation of DNS Zones in any spoke subscription.

What is the easiest and most secure way to register your KubeAPI private endpoint in your DNS?

Válasz

- Register the endpoint on your OnPrem DNS servers.
- Register the endpoint on Microsoft Public DNS Register.
- Ask for exempt from your security team, and get the Network Contributor RBAC Role for your context user on the central subscription, then connect your cluster to the central DNS Zones.
- Ask for exempt from your security team, and allow the creation of DNS Zones on the spoke subscription, and let AKS creates and manage the DNS Zone.

3. feladat 1 pont

You need to set up an Azure DevOps release pipeline for your cluster's deployments. You need to use kubelogin in a non-interactive way to be able to connect to your KubeAPI.

The context user of this pipeline must have the following ClusterRoleBinding definition:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: kubelogin-role-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
  - apiGroup: rbac.authorization.k8s.io
    kind: User
    name: 00000000-0000-0000-0000-000000000000 #object_id of the identity
```

Which would be the best option for you?

Válasz

- Create an User Managed Identity, which you provide the ClusterRoleBinding manually with an admin account, once the AKS resource exists.
- Create a Service Principal and add it to an AAD Security Group, then use that group with the aad-admin-group-object-ids property in your AKS deployment.

Create an Service Principal, which you provide the ClusterRoleBinding manually with an admin account, once the AKS resource exists.

4. feladat 2 pont

You are writing a terraform module to handle the AKS deployment.

You have an input variable container_registry_ids with type list(string), and you need to provide AcrPull RBAC Role, so your cluster able to pull images from the Azure Container Registry.

Which hcl code would you use in order to complete this task?

Válasz

```
resource "azurerm_role_assignment" "aks_cluster_role_acr" {
  scope                = azurerm_kubernetes_cluster.aks_cluster.id
  role_definition_name = "AcrPull"
  principal_id         = var.control_plane_identity.principal_id
}
```

```
resource "azurerm_role_assignment" "aks_cluster_role_acr" {
  for_each             = { for idx, principal_id in var.container_registry_ids
  scope                = each.value
  role_definition_name = "AcrPull"
  principal_id         = azurerm_kubernetes_cluster.aks_cluster.kubelet_identi
}
```

```
resource "azurerm_role_assignment" "aks_cluster_role_acr" {
  for_each             = { for idx, principal_id in var.container_registry_ids
  scope                = each.value
  role_definition_name = "AcrPull"
  principal_id         = var.control_plane_identity.principal_id
}
```

5. feladat 3 pont

Which Azure AD RBAC Roles do you need to assign to your Control Plane Identity, so all required cluster operation is functioning?

Válaszok

- [ ] "Network Contributor" on the AKS Subnet.
- [ ] "Monitoring Metrics Publisher" on the AKS Resource.
- [ ] "Contributor" on the Azure Route Table.
- [ ] "Managed Identity Operator" on the AKS Resource.
- [ ] "AcrPull" on the Azure Container Registry Resource.
- [ ] "Reader" on the Azure Disk Encryption Set used to encrypt the node's disks.

6. feladat 1 pont

Which SKU Tier you need to use for your Application Gateway?

Válasz

- ( ) **Standard**
- ( ) **Standard_v2**
- ( ) **WAF**
- ( ) **WAF_v2**

Megoldások beküldése