Cyber Shujaa

Cyber Shujaa

Cloud Security Specialist

Assignment 14 : AZ-500 Learning Path - Secure Compute

NAME: WELDON KIPKIRUI KENEI

CS NO: ADC-CSS02-25027

Introduction

In this assignment module, we will be equipped with the knowledge and skills needed to plan and implement advanced security measures for Azure compute resources, safeguarding applications and data against evolving security threats.

Plan and implement remote access to public endpoints, Azure Bastion and just-in-time (JIT) virtual machine (VM) access

The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly over TLS from the Azure portal or via the native client.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Azure Kubernetes Service

Azure Kubernetes Service (AKS) is a managed Kubernetes service that you can use to deploy and manage containerized applications. AKS reduces the complexity and operational overhead of managing Kubernetes by offloading much of that responsibility to Azure. AKS is an ideal platform for deploying and managing containerized applications that require high availability, scalability, and portability, and for deploying applications to multiple regions, using open-source tools, and integrating with existing DevOps tools.

Configure network isolation for Azure Kubernetes Service (AKS)

AKS allows flexibility in how you run multitenant clusters and isolate resources. A Kubernetes Namespace creates a logical isolation boundary. Other Kubernetes features and considerations for isolation and multi-tenancy include the following areas:

- Best practices for cluster isolation in Azure Kubernetes Service (AKS)
    - Design clusters for multi-tenancy
    - Scheduling
    - Networking
    - Authentication and authorization
    - Containers

- Logically isolated clusters
  With logical isolation, you can use a single AKS cluster for multiple workloads, teams, or environments. Kubernetes Namespaces form the logical isolation boundary for workloads and resources.

- Physically isolated clusters
  In this isolation model, teams or workloads are assigned their own AKS cluster. While physical isolation might look like the easiest way to isolate workloads or teams, it adds management and financial overhead.

Secure and monitor Azure Kubernetes Service

Microsoft Defender for Containers is a cloud-native solution to improve, monitor, and maintain the security of your containerized assets (Kubernetes clusters, Kubernetes nodes, Kubernetes workloads, container registries, container images and more), and their applications, across multi-cloud and on-premises environments.

Defender for Containers assists you with four core domains of container security:

- Security posture management
- Vulnerability assessment
- Run-time threat protection
- Deployment and monitoring

Configure authentication for Azure Kubernetes Service

As you deploy and maintain clusters in Azure Kubernetes Service (AKS), you implement ways to manage access to resources and services.

We achieve this through;

- Using Microsoft Entr ID
  Deploy AKS clusters with Microsoft Entra integration. Using Microsoft Entra ID centralizes the identity management layer. Any change in user account or group status is automatically updated in access to the AKS cluster.
- Use Kubernetes role-based access control (Kubernetes RBAC)
  Define user or group permissions to cluster resources with Kubernetes RBAC. Create roles and bindings that assign the least amount of permissions required. Integrate with Microsoft Entra ID to automatically update any user status or group membership change and keep access to cluster resources current.

- Use Azure RBAC

Use Azure RBAC to define the minimum required user and group permissions to AKS resources in one or more subscriptions.

- Use pod-managed identities
  Don't use fixed credentials within pods or container images, as they are at risk of exposure or abuse. Instead, use pod identities to automatically request access using Microsoft Entra ID.

Configure security for Azure Container Instances (ACIs)

Azure Monitor provides insight into the compute resources used by your container instances. This resource usage data helps you determine the best resource settings for your container groups. Azure Monitor also provides metrics that track network activity in your container instances.

These metrics are available for both a container group and individual containers. By default, they are aggregated as averages.

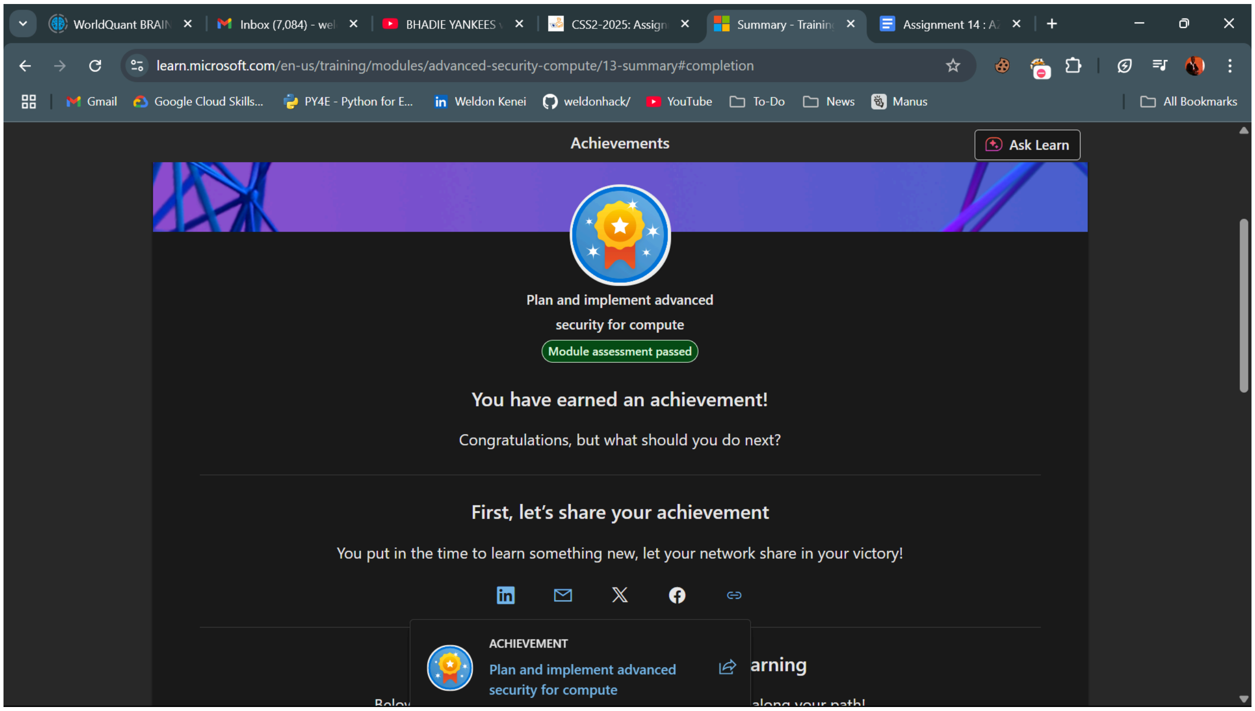
- CPU Usage measured in millicores.
- One millicore is 1/1000th of a CPU core, so 500 millicores represents usage of 0.5 CPU core.
- Memory Usage in bytes.
- Network bytes received per second.
- Network bytes transmitted per second.

Manage access to Azure Container Registry (ACR)

The Azure Container Registry service supports a set of built-in Azure roles that provide different levels of permissions to an Azure container registry. Use Azure role-based access control (Azure RBAC) to assign specific permissions to users, service principals, or other identities that need to interact with a registry, for example, to pull or push container images. You can also define custom roles with fine-grained permissions to a registry for different operations.

Conclusion

In conclusion, we have learned how to plan and implement advanced security measures for Azure compute resources, including enabling secure remote access using Azure Bastion and just-in-time (JIT) VM access, configuring network isolation for Azure Kubernetes Service (AKS), securing and monitoring AKS clusters, configuring authentication and security monitoring for container instances and apps, managing access to Azure Container Registry (ACR), implementing disk encryption strategies such as Azure Disk Encryption (ADE) and confidential disk encryption, and providing recommendations for securing Azure API Management.
https://learn.microsoft.com/api/achievements/share/en-us/weldonkenei-6817/FMPCAH9X?sharingId=1C66F93EC0530812



Achievements

Plan and implement advanced security for compute

Module assessment passed

You have earned an achievement!

Congratulations, but what should you do next?

First, let's share your achievement

You put in the time to learn something new, let your network share in your victory!

ACHIEVEMENT

Plan and implement advanced security for compute

arning

Belov along your path!