Imagen que contiene agua, hombre, vuelo, sostener

Descripción generada automáticamente

**Lab 09: Microsoft Defender for Cloud**

**Student lab manual**

**Lab scenario**

You have been asked to create a proof of concept of Microsoft Defender for Cloud-based environment. Specifically, you want to:

* Configure Microsoft Defender for Cloud to monitor a virtual machine.
* Review Microsoft Defender for Cloud recommendations for the virtual machine.
* Implement recommendations for guest configuration and Just-in-time VM access.
* Review how the Secure Score can be used to determine progress toward creating a more secure infrastructure.

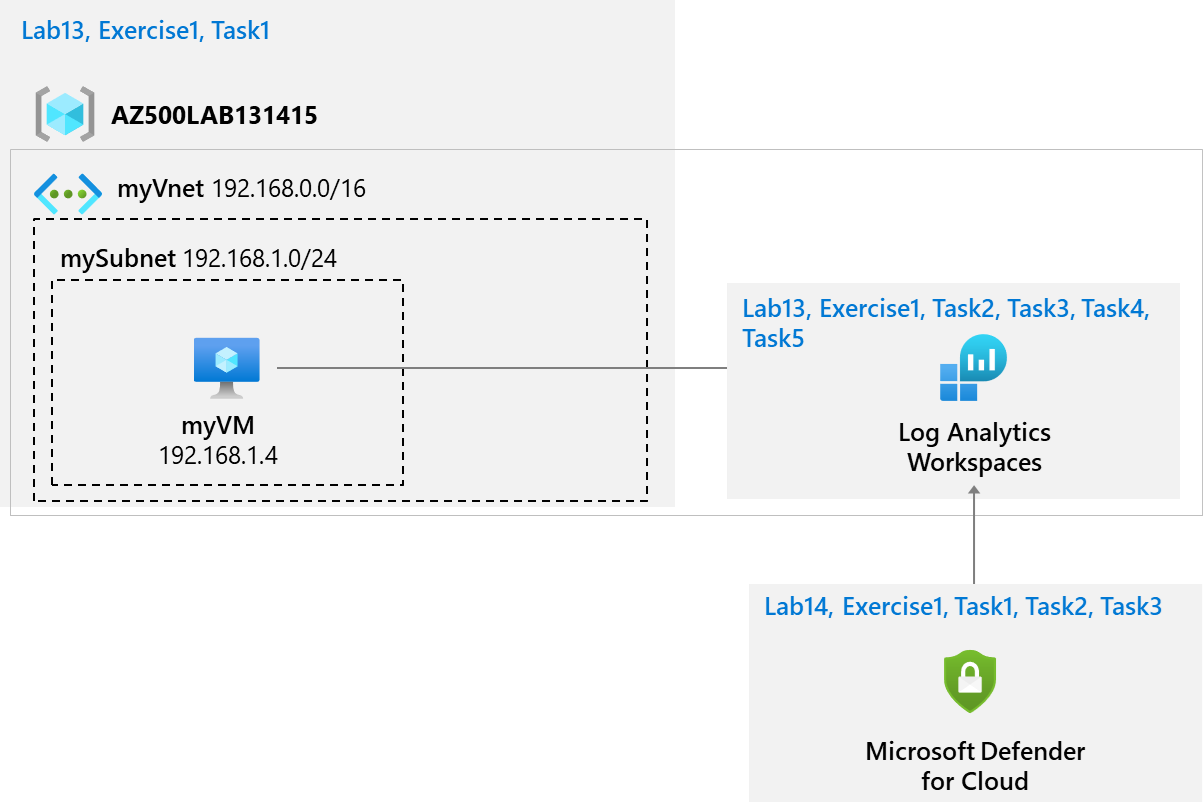
For all the resources in this lab, we are using the **East US** region. Verify with your instructor this is the region to use for class.

**Lab objectives**

In this lab, you will complete the following exercise:

* Exercise 1: Implement Microsoft Defender for Cloud

**Microsoft Defender for Cloud diagram**

[](https://private-user-images.githubusercontent.com/91347931/274952862-c31055cc-de95-41f6-adef-f09d756a68eb.png?jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..vGujGsHjzBha3hTbkDfR26HSQl5ccVJqeX8bRTaBnmc)

**Instructions**

**Exercise 1: Implement Microsoft Defender for Cloud**

In this exercise, you will complete the following tasks:

* Task 1: Configure Microsoft Defender for Cloud
* Task 2: Review the Microsoft Defender for Cloud recommendations
* Task 3: Implement the Microsoft Defender for Cloud recommendation to enable Just-in-time VM Access

**Task 1: Configure Microsoft Defender for Cloud**

In this task, you will on-board and configure Microsoft Defender for Cloud.

1. Sign-in to the Azure portal **https://portal.azure.com/**.

**Note**: Sign in to the Azure portal using an account that has the Owner or Contributor role in the Azure subscription you are using for this lab.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. In the Azure portal, in the **Search resources, services, and docs** text box at the top of the Azure portal page, type **Microsoft Defender for Cloud** and press the **Enter** key.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. In the left navigation panel, click **Getting started**. On the **Microsoft Defender for Cloud | Getting started** blade, click **Upgrade**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **Microsoft Defender for Cloud | Getting started** blade, in the Install agents tab, scroll down and click **Install agents**.

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

1. On the **Microsoft Defender for Cloud | Getting started** blade, on the **Upgrade** tab >> scroll down until the **Select workspaces with enhanced security features** section is visible >> turn on the **Microsoft Defender plan** by selecting your Log Analytics Workspace, then click the large Blue Upgrade button.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

**Note**: Review all the features that are available as part of Microsoft Defender plans.

1. Navigate to **Microsoft Defender for Cloud** and, in the left navigation panel under the Management section, click **Environment Settings**.
2. On the **Microsoft Defender for Cloud | Environment settings** blade, scroll down, expand until your subscription appears and click the relevant subscription.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **Settings | Defender plans** blade, select **Enable all plans** and, if needed, click **Save**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Navigate back to the **Microsoft Defender for Cloud | Environment settings** blade, expand until your subscription appears, and click the entry representing the Log Analytics workspace you created in the previous lab.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. On the **Settings | Defender plans** blade, ensure that all options are "On". If needed, click **Enable all plans** and then click **Save**.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Select **Data collection** from the **Settings | Defender plans** blade. Click **All Events** and **Save**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Task 2: Review the Microsoft Defender for Cloud recommendation**

In this task, you will review the Microsoft Defender for Cloud recommendations.

1. In the Azure portal, navigate back to the **Microsoft Defender for Cloud | Overview** blade.
2. On the **Microsoft Defender for Cloud | Overview** blade, review the **Secure Score** tile.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Note**: Record the current score if it is available.

1. Navigate back to the **Microsoft Defender for Cloud | Overview** blade, click **Assessed resources**.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

1. On the **Inventory** blade, click the **myVM** entry.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

**Note**: You might have to wait a few minutes and refresh the browser page for the entry to appear.

1. On the **Resource health** blade, on the **Recommendations** tab, review the list of recommendations for **myVM**.

Una captura de pantalla de una computadora

Descripción generada automáticamente

**Task 3: Implement the Microsoft Defender for Cloud recommendation to enable Just-in-time VM Access**

In this task, you will implement the Microsoft Defender for Cloud recommendation to enable Just-in-time VM Access on the virtual machine.

1. In the Azure portal, navigate back to the **Microsoft Defender for Cloud | Overview** blade and click **Workload protections** under **Cloud Security** in the left navigation panel.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **Microsoft Defender for Cloud | Workload protections** blade, scroll down to the **Advanced protection** section and click the **Just-in-time VM access** tile.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. On the **Just-in-time VM access** blade, under the **Virtual machines** section, select **Not Configured** and then select the checkbox for the **myVM** entry.

**Note**: You might have to wait a few minutes, refresh the browser page and select **Not Configured** again for the entry to appear.

1. Click the **Enable JIT on 1 VM** option on the far right of the **Virtual machines** section.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

1. On the **JIT VM access configuration** blade, on the far right of the row referencing the port **22**, click the ellipsis button and then click **Delete**.

Texto

Descripción generada automáticamente con confianza media

1. On the **JIT VM access configuration** blade, click **Save**.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**COMPROBACIÓN**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Note**: Monitor the progress of configuration by clicking on the **Notifications** icon in the toolbar and viewing the **Notifications** blade.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

**Note**: It can take some time for the implementation of recommendations in this lab to be reflected by Secure Score. Periodically check the Secure Score to determine the impact of implementing these features.

Results: You have on-boarded Microsoft Defender for Cloud and implemented virtual machine recommendations.