Azure VM Encryption at Host (Preview)

Date published: 2022-06-06
Date modified: 2024-12-04

Legal Notice

This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided ‘as is’ without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.

Contents

Legal Notice 2
Contents 3
Introduction 4
Limitations 4
Prerequisites 4
Enable encryption at host for an environment 5
Enable encryption at host for a Cloudera Data Hub cluster 8

Introduction

You can optionally enable encryption at host for Data Lake, FreeIPA, and Cloudera Data Hub clusters. Currently, you need to enable it individually for each Virtual Machine (VM) on Azure Portal.

As described in Azure documentation, when you enable encryption at host, the encryption starts on the VM host, where the data for your temporary disk, and OS and data disk caches are stored. After enabling encryption at host, all this data is encrypted at rest and flows encrypted to the Storage service, where it is persisted. Thus, encryption at host essentially encrypts your data from end to end.

Temporary disks and ephemeral OS disks are encrypted at rest with platform-managed keys when you enable end-to-end encryption. The OS and data disk caches are encrypted at rest with either customer-managed keys (CMK) or platform-managed keys, depending on the selected disk encryption type. For example, if a disk is encrypted with customer-managed keys, then the cache for the disk is encrypted with customer-managed keys, and if a disk is encrypted with platform-managed keys then the cache for the disk is encrypted with platform-managed keys.

Encryption at host does not use your VM's CPU and doesn't impact your VM's performance.

Related links
Encryption at host - End-to-end encryption for your VM data

Limitations

When using Azure VM encryption at host with Cloudera, the following limitations apply:

- Even if you wish to use the feature for a single subscription only, you need to enable encryption at host for all subscriptions within your Azure tenant.
- This feature can currently be configured individually for each Data Lake and FreeIPA node. Additionally, encryption at host for Data Hub nodes can be configured individually for each Cloudera Data Hub node. The configuration must be performed on the Azure Portal.

Prerequisites

Prior to enabling encryption at host in Cloudera, meet the following Azure prerequisites:

1. Enable encryption at host, as described in Use the Azure CLI to enable end-to-end encryption using encryption at host: Prerequisites in Azure documentation.
   Note: You need to enable this for each subscription within your Azure tenant.

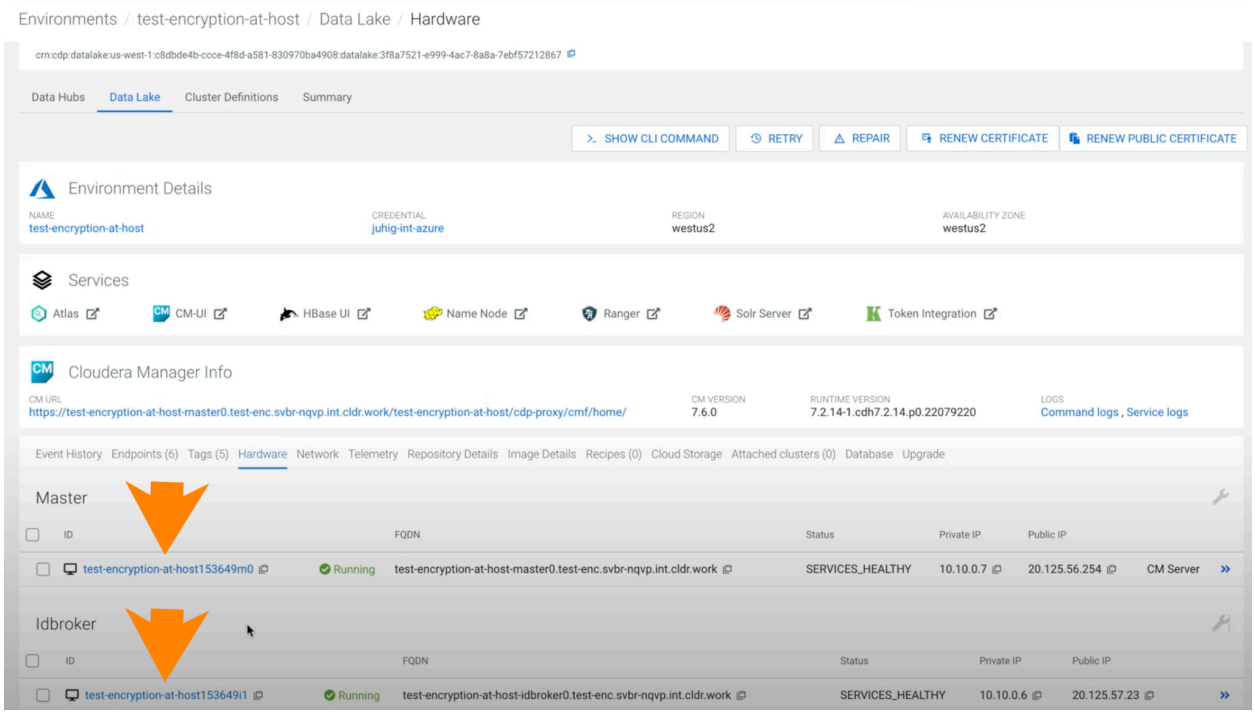
2. If you would like to use Azure disk encryption with a customer-managed key (CMK) along with encryption at host, meet the prerequisites mentioned in Customer managed encryption keys.

Enable encryption at host for an environment

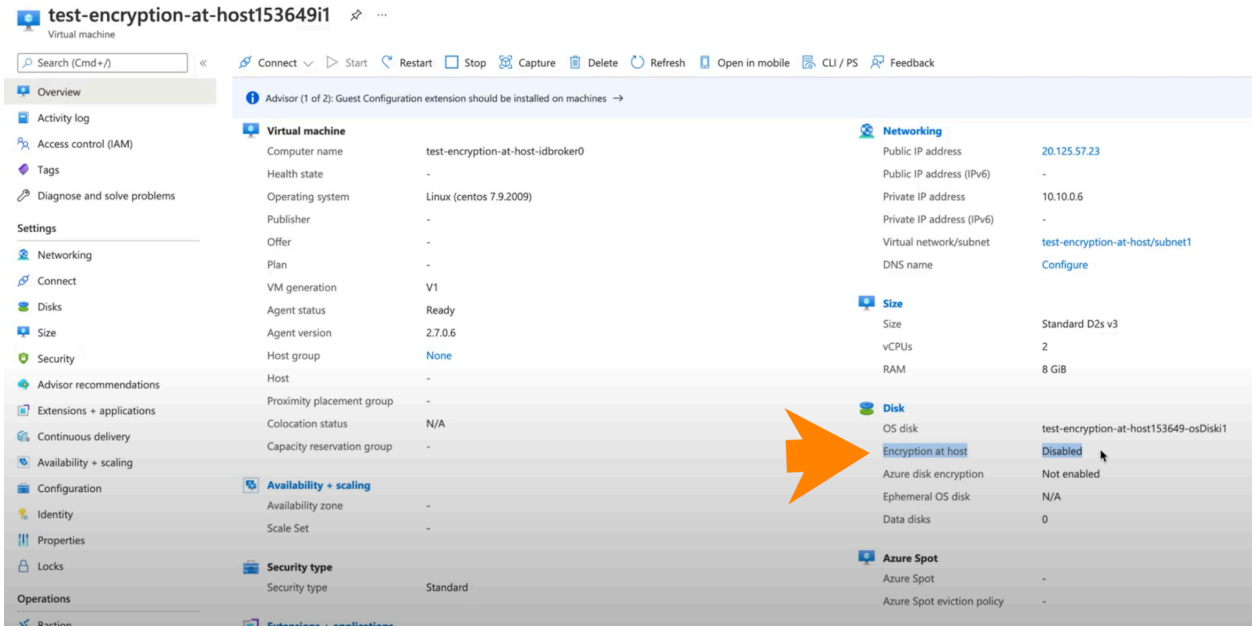
Use these steps to enable encryption at host for an existing Cloudera environment running on Azure. The steps involve manually enabling encryption at host for each Data Lake and FreeIPA VM via the Azure Portal.

Steps

1. In the Cloudera Management Console, select **Environments** and then click on the specific environment.
2. Make sure that your Cloudera environment is running.
3. Click on the **Data Lake** tab and then navigate to the **Hardware** tab. Here you can find the list of all Data Lake VMs organized into host groups:

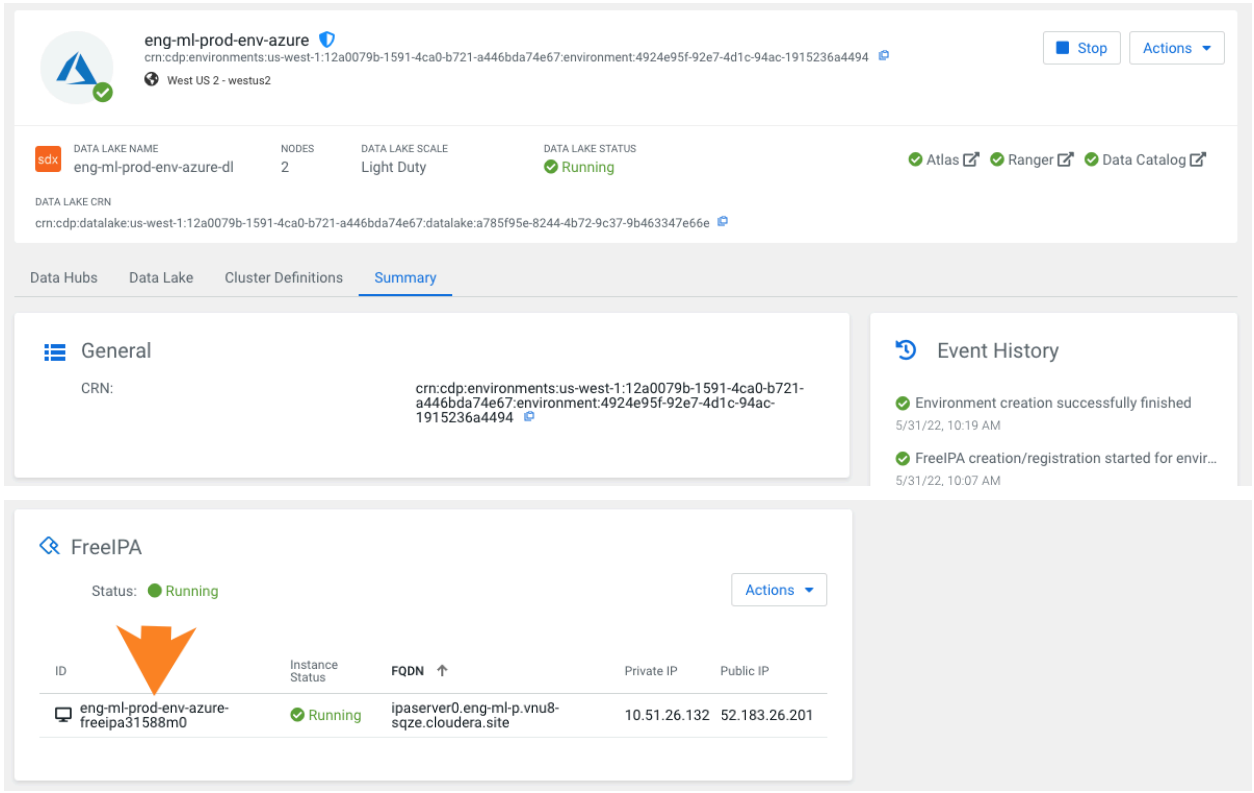


4. Click on each of the VM links and a new browser tab will open for each, redirecting you to the Azure Portal. You need to do this individually for each VM.
5. For each of the VMs, navigate to the **Disks** section in Azure Portal. It will show the “Encryption at Host” as “disabled”:



Leave the Azure Portal browser tabs open. You will need to get back to them shortly.

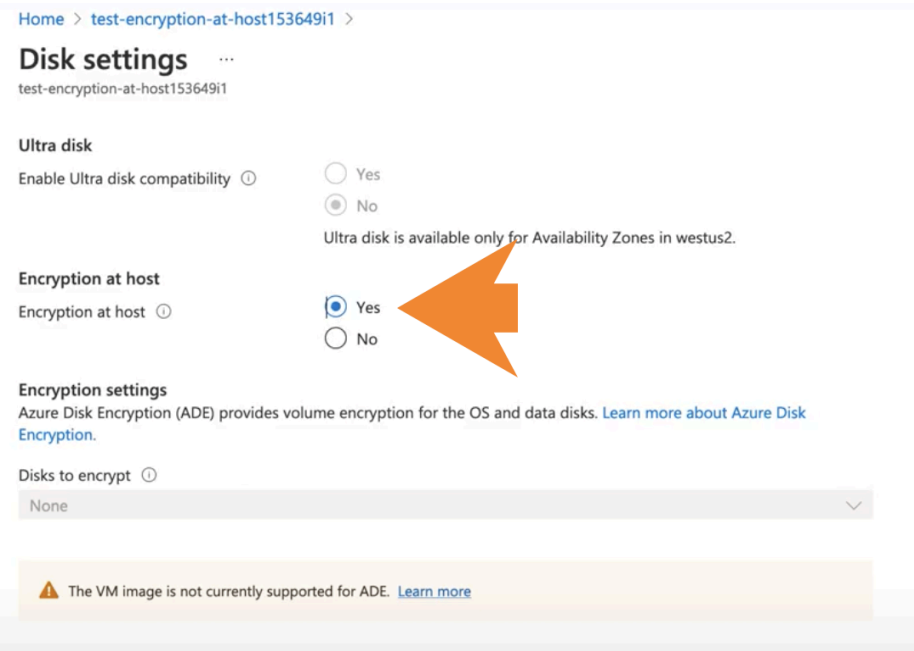
6. Navigate back to the Cloudera Management Console to repeat the same steps for FreeIPA VMs. To access FreeIPA VMs, navigate to environment details and click on the **Summary** tab. Next, scroll down to the **FreeIPA** tile. Here you can find the list of all FreeIPA VMs organized into host groups:



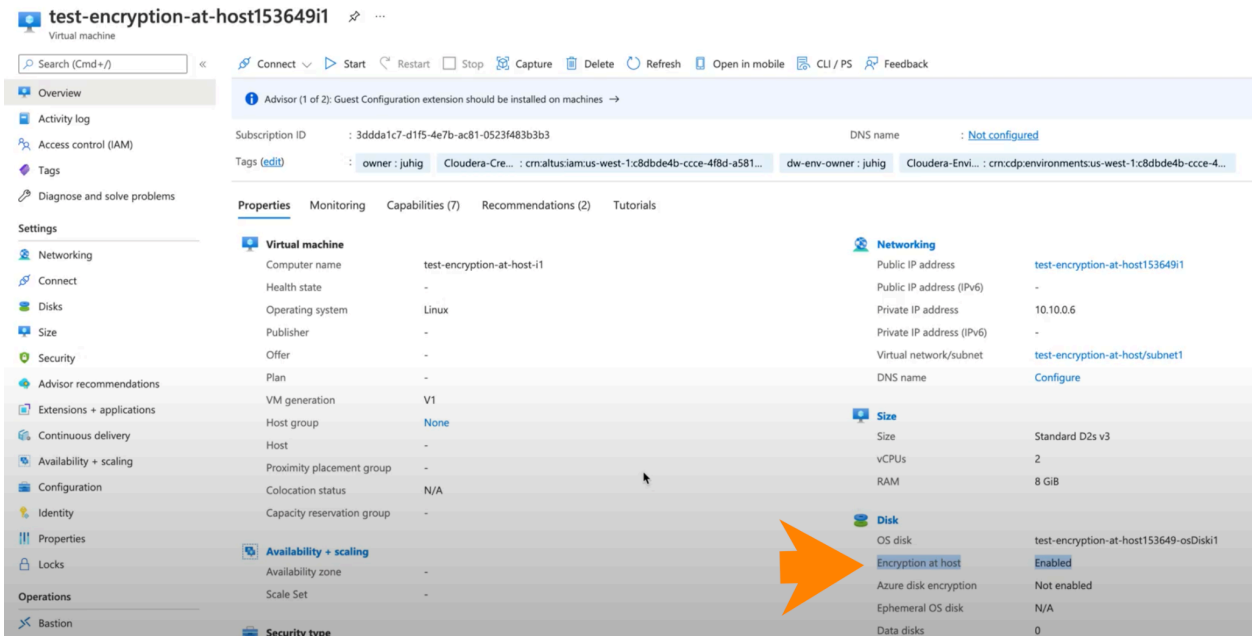
There is no link to Azure Portal, but you can copy the IDs of the VMs and search for them on Azure Portal. Just as you did for each Data Lake node, for each FreeIPA node,

navigate to the **Disks** section in Azure Portal. It will show the “Encryption at Host” as “disabled”. Again, leave the Azure Portal browser tabs open. You will need to get back to them shortly.

7. Navigate back to the Cloudera Management Console and stop the environment by clicking the **Stop** button in the top right corner in environment details. If you need detailed instructions, see Stop and restart an environment.
8. Once the environment has been successfully stopped, navigate back to the Azure Portal browser tabs opened earlier.
9. In Azure Portal, perform this for each VM of the Data Lake and for each VM of FreeIPA:
    a. Navigate to the **Disks** section.
    b. Within the Disks tab, navigate to the **Additional settings** section.
    c. Select “Yes” for the **“Encryption at Host”** setting:



    d. Click on **Save**.
    e. Once the update is complete, you will see a message stating “Updated virtual machine”.
10. Before proceeding, ensure that you have performed the above steps for all Data Lake VMs and for all FreeIPA VMs.
11. Navigate back to the browser tab with the Cloudera Management Console and restart the environment by clicking the **Start** button in the top right corner in environment details. If you need detailed instructions, see Stop and restart an environment.
12. Once the environment has been successfully restarted, find the **Hardware** section in the **Data Lake** tab, just like you did earlier, and click on each of the Data Lake VM links. A new browser tab will open for each, redirecting you to the Azure Portal. For each of these VMs, navigate to the **Disks** section in Azure Portal. It will show the “Encryption at Host” as “enabled”:



Next, confirm the same for all FreeIPA VMs in the **Summary** tab > **FreeIPA** tile.

Enable encryption at host for a Cloudera Data Hub cluster

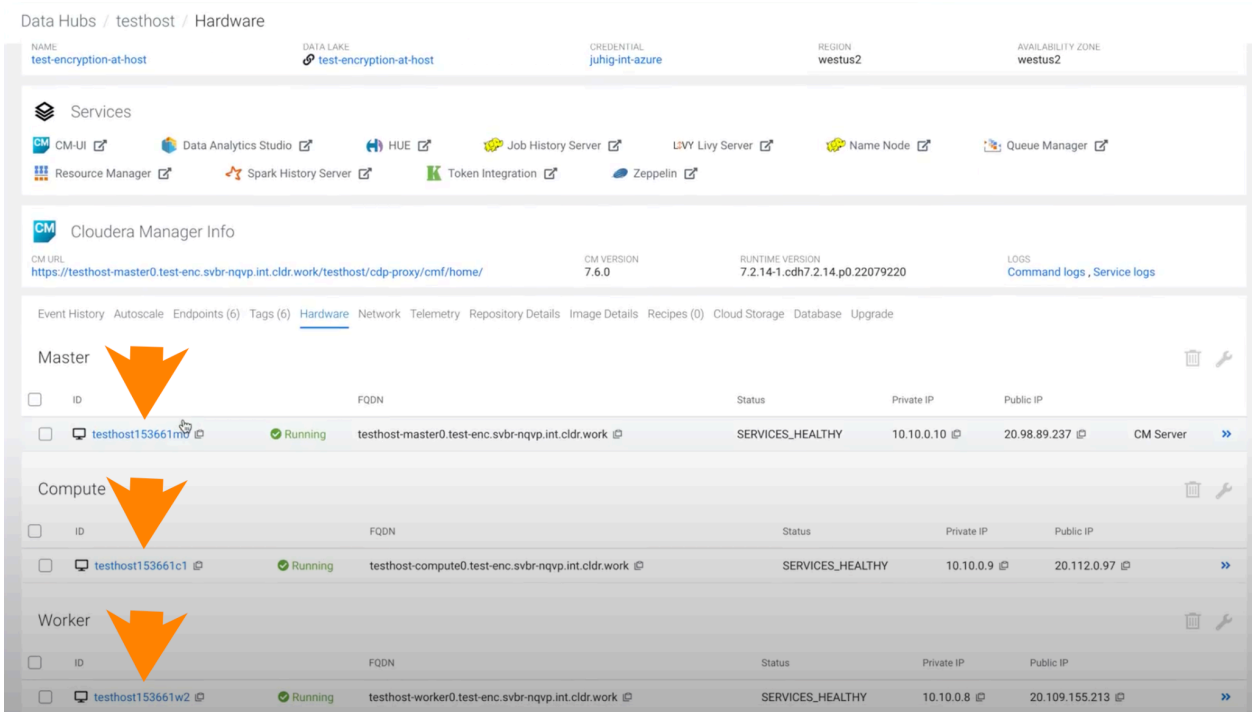
Use these steps to enable encryption at host for an existing Cloudera Data Hub running on Azure. The steps involve manually enabling encryption at host for each Cloudera Data Hub VM via the Azure Portal.

Before you begin

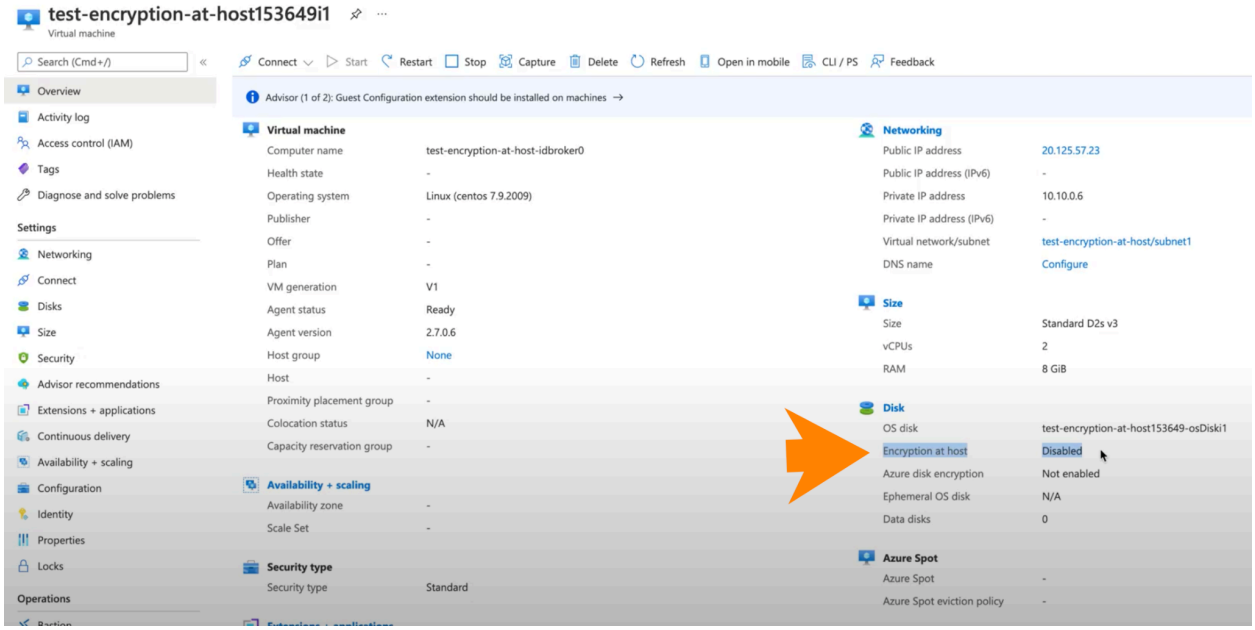
Not all Azure VM types support encryption at host. In order to use encryption at host, when creating your Data Hub, select VM types that support encryption at host for each Data Hub host group. VM types can be selected per host group during Cloudera Data Hub creation in **Advanced Options > Hardware and Storage**. To find which VM types support encryption at host, follow the steps in Finding supported VM sizes**.**

Steps

1. In the Cloudera Management Console, select **Data Hubs**, and click on the specific Data Hub.
2. Make sure that your Cloudera Data Hub cluster is running.
3. In **Data Hub details**, navigate to the **Hardware** tab. Here you can find the list of all Cloudera Data Hub VMs organized into host groups:

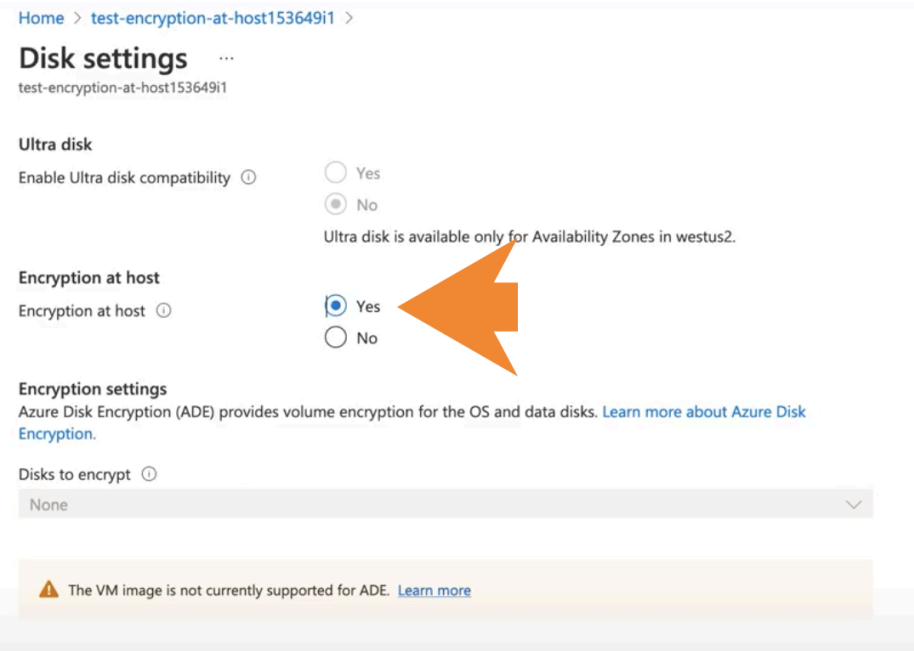


4. Click on each VM link and a new browser tab will open for each, redirecting you to the Azure Portal. You need to do this individually for each VM.
5. For each of the VMs, navigate to the **Disks** section in Azure Portal. It will show the “Encryption at Host” as “disabled”:



6. Leave the Azure Portal browser tabs open. You will need to get back to them shortly.
7. Navigate back to the browser tab with the Cloudera Management Console and restart the Cloudera Data Hub cluster by clicking the **Stop** button in the top right corner in environment details. If you need detailed instructions, see Stop a cluster.

8. Once the Cloudera Data Hub cluster has been successfully stopped, navigate back to the Azure Portal browser tabs opened earlier.
9. In Azure Portal, perform the following for each Cloudera Data Hub VM:
    a. Navigate to the **Disks** section.
    b. Within the Disks tab, navigate to the **Additional settings** section.
    c. Select “Yes” for the **“Encryption at Host”** setting:



    d. Click on **Save**.
    e. Once the update is complete, you will see a message stating “Updated virtual machine”.
10. Before proceeding, ensure that you have performed the above steps for all Data Hub VMs.
11. Navigate back to the browser tab with the Cloudera Management Console and restart the Cloudera Data Hub cluster by clicking the **Start** button in the top right corner. If you need detailed instructions, see Restart a cluster.
12. Once the environment has been successfully restarted, find the **Hardware** section in the **Data Hub details**, just like you did earlier, and click on each of the Cloudera Data Hub VM links.. A new browser tab will open for each, redirecting you to the Azure Portal. For each of these VMs, navigate to the **Disks** section in Azure Portal. It will show the “Encryption at Host” as “enabled”: