

Azure VM Encryption at Host (Preview)

Date published: 2022-06-06

Date modified: 2024-12-04

Legal Notice

© Cloudera Inc. 2022. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms.

Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners. Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

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

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.

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.

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.

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:

Environments / test-encryption-at-host / Data Lake / Hardware

cm:cdp.datalake.us-west-1:c8dbde4b-ccce-4f8d-a581-830970ba4908:datalake:3f8a7521-e999-4ac7-8a8a-7ebf57212867

Data Hubs Data Lake Cluster Definitions Summary

SHOW CLI COMMAND RETRY REPAIR RENEW CERTIFICATE RENEW PUBLIC CERTIFICATE

Environment Details

NAME: test-encryption-at-host CREDENTIAL: juhig-int-azure REGION: westus2 AVAILABILITY ZONE: westus2

Services

Atlas CM-UI HBase UI Name Node Ranger Solr Server Token Integration

Cloudera Manager Info

CM URL: https://test-encryption-at-host-master0.test-enc.svbr-nqvp.int.cldr.work/test-encryption-at-host/cdp-proxy/cm/ / CM VERSION: 7.6.0 RUNTIME VERSION: 7.2.14-1.cdh7.2.14.p0.22079220 LOGS: Command logs, Service logs

Event History Endpoints (6) Tags (5) Hardware Network Telemetry Repository Details Image Details Recipes (0) Cloud Storage Attached clusters (0) Database Upgrade

Master

ID	FQDN	Status	Private IP	Public IP
test-encryption-at-host153649m0	test-encryption-at-host-master0.test-enc.svbr-nqvp.int.cldr.work	Running	10.10.0.7	20.125.56.254

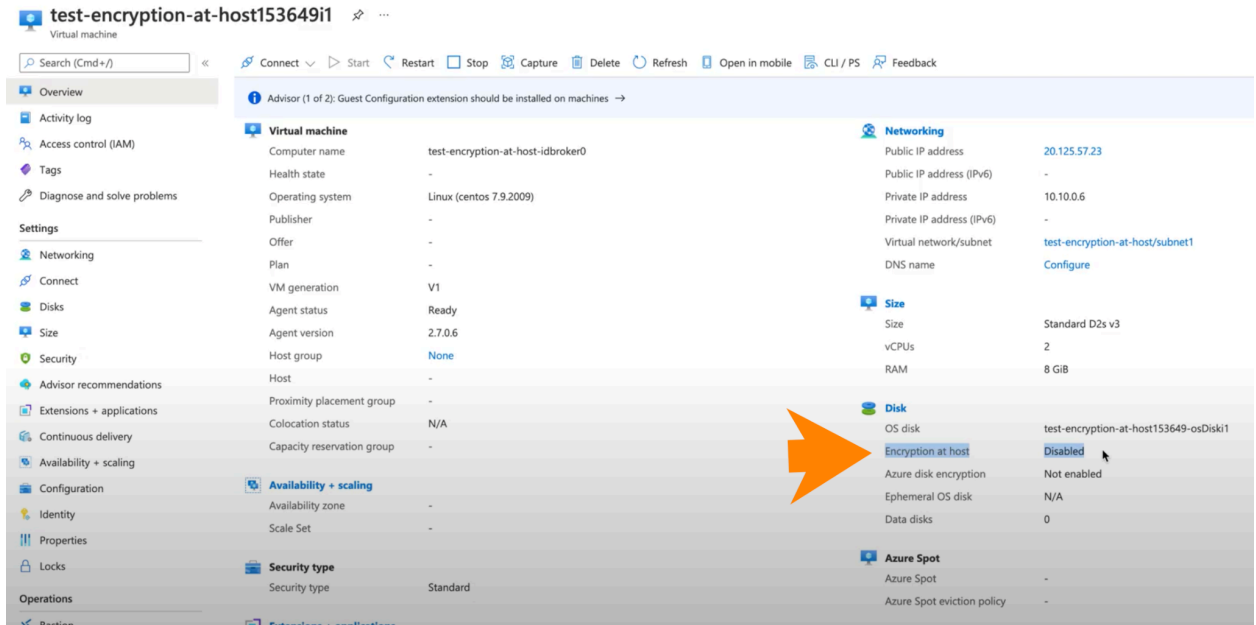
Idbroker

ID	FQDN	Status	Private IP	Public IP
test-encryption-at-host153649i1	test-encryption-at-host-idbroker0.test-enc.svbr-nqvp.int.cldr.work	Running	10.10.0.6	20.125.57.23

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”:

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.

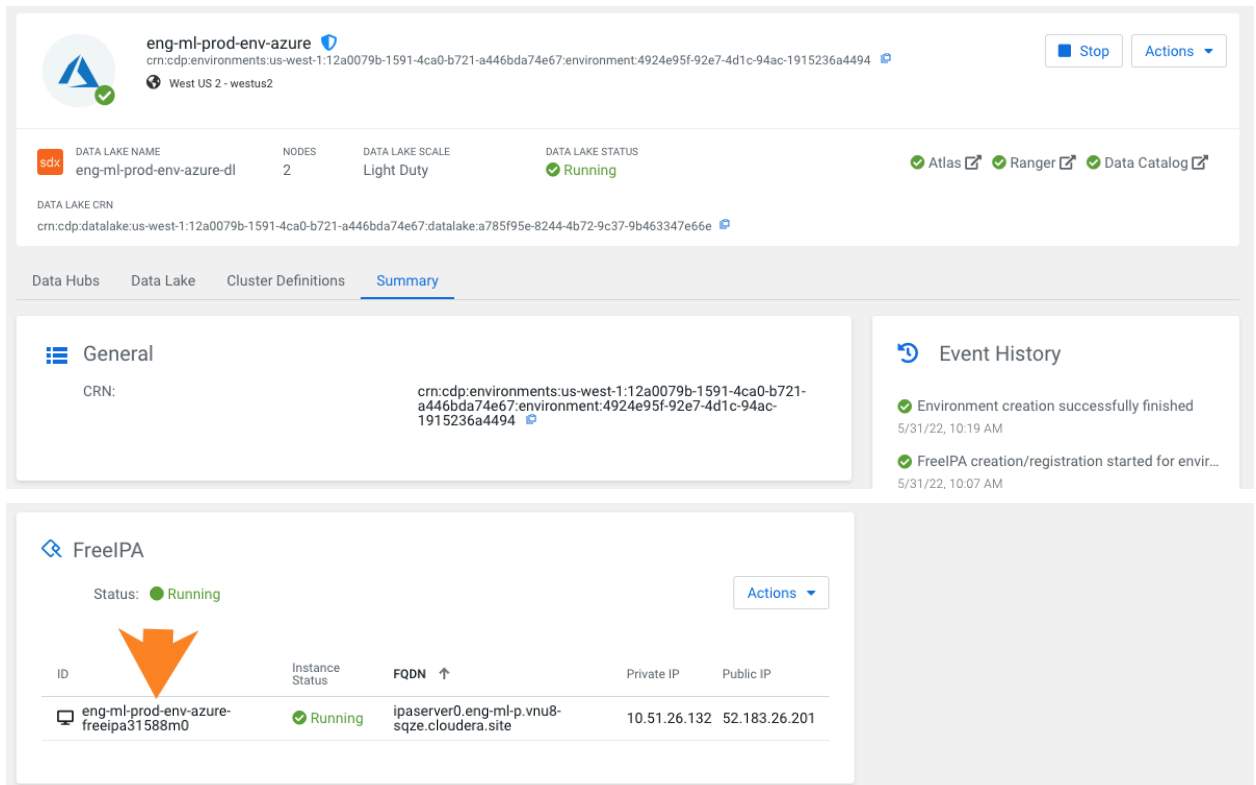
CLUDERA TECHNICAL PREVIEW DOCUMENTATION



The screenshot shows the Azure Portal interface for a virtual machine. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Security, Advisor recommendations, Extensions + applications, Continuous delivery, Availability + scaling, Configuration, Identity, Properties, Locks, and Operations. The main area displays the VM configuration for 'test-encryption-at-host153649i1'. Under the 'Disk' section, the 'Encryption at host' option is highlighted with a red arrow and is currently set to '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:



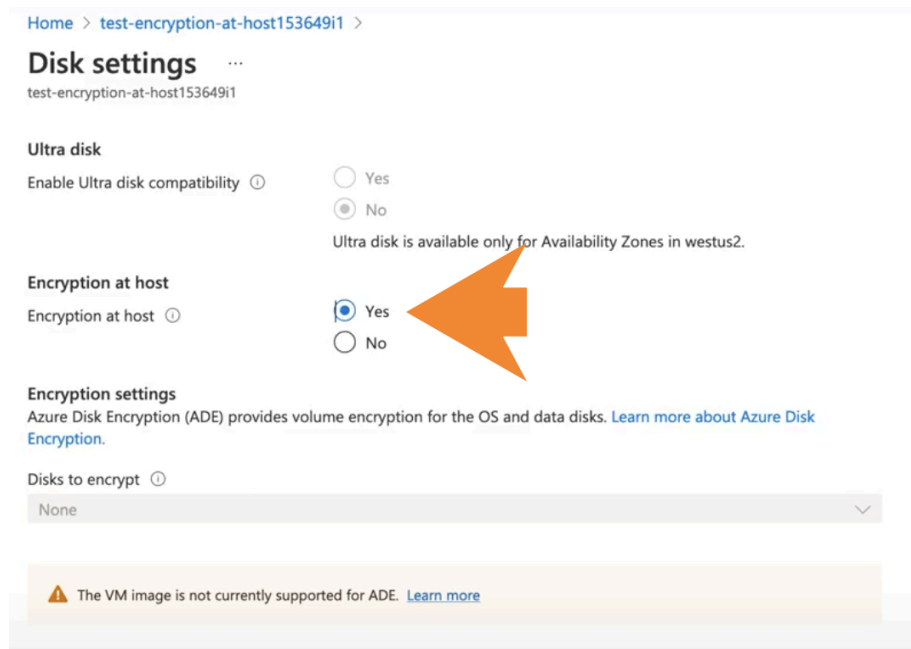
The screenshot shows the Cloudera Management Console interface. The top section displays the environment 'eng-m1-prod-env-azure' with a 'Stop' button and an 'Actions' dropdown. Below this, there are tabs for 'Data Hubs', 'Data Lake', 'Cluster Definitions', and 'Summary'. The 'Summary' tab is selected, showing a 'General' section with the CRN and an 'Event History' section with two events. The 'FreeIPA' tile is highlighted with a red arrow, showing a list of VMs with columns for ID, Instance Status, FQDN, Private IP, and Public IP.

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,

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.

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”:

The screenshot shows the Azure Portal interface for a virtual machine. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Security, Advisor recommendations, Extensions + applications, Continuous delivery, Availability + scaling, Configuration, Identity, Properties, Locks, Operations, and Bastion. The main area displays the 'test-encryption-at-host153649i1' VM details. Under the 'Properties' tab, the 'Virtual machine' section shows details like Computer name, Health state, Operating system, Publisher, Offer, Plan, VM generation, Host group, Host, Proximity placement group, Colocation status, and Capacity reservation group. The 'Availability + scaling' section shows Availability zone and Scale Set. The 'Disk' section shows OS disk, Encryption at host (set to 'Not enabled'), Azure disk encryption, Ephemeral OS disk, and Data disks. An orange arrow points to the 'Encryption at host' setting.

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:

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.

CLOUDERA TECHNICAL PREVIEW DOCUMENTATION

Data Hubs / testhost / Hardware

NAME: test-encryption-at-host DATA LAKE: test-encryption-at-host CREDENTIAL: juhig-int-azure REGION: westus2 AVAILABILITY_ZONE: westus2

Services

- CM-UI
- Data Analytics Studio
- HUE
- Job History Server
- LIVY Livy Server
- Name Node
- Queue Manager
- Resource Manager
- Spark History Server
- Token Integration
- Zeppelin

Cloudera Manager Info

CM URL: https://testhost-master0.test-enc.svbr-nqvp.int.cldr.work/testhost/cdp-proxy/cm/home/ CM VERSION: 7.6.0 RUNTIME VERSION: 7.2.14-1.cdh7.2.14.p0.22079220 LOGS: Command logs, Service logs

Event History Autoscale Endpoints (6) Tags (6) Hardware Network Telemetry Repository Details Image Details Recipes (0) Cloud Storage Database Upgrade

Master

ID	FQDN	Status	Private IP	Public IP
testhost153661m0	testhost-master0.test-enc.svbr-nqvp.int.cldr.work	SERVICES_HEALTHY	10.10.0.10	20.98.89.237

Compute

ID	FQDN	Status	Private IP	Public IP
testhost153661c1	testhost-compute0.test-enc.svbr-nqvp.int.cldr.work	SERVICES_HEALTHY	10.10.0.9	20.112.0.97

Worker

ID	FQDN	Status	Private IP	Public IP
testhost153661w2	testhost-worker0.test-enc.svbr-nqvp.int.cldr.work	SERVICES_HEALTHY	10.10.0.8	20.109.155.213

- 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.
- For each of the VMs, navigate to the **Disks** section in Azure Portal. It will show the “Encryption at Host” as “disabled”:

test-encryption-at-host153649i1

Virtual machine

Search (Cmd+/) Connect Start Restart Stop Capture Delete Refresh Open in mobile CLI / PS Feedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks
- Operations

Virtual machine

Computer name: test-encryption-at-host-idbroker0

Health state: -

Operating system: Linux (centos 7.9.2009)

Publisher: -

Offer: -

Plan: -

VM generation: V1

Agent status: Ready

Agent version: 2.7.0.6

Host group: None

Host: -

Proximity placement group: -

Colocation status: N/A

Capacity reservation group: -

Availability + scaling

Availability zone: -

Scale Set: -

Security type

Security type: Standard

Networking

Public IP address: 20.125.57.23

Public IP address (IPv6): -

Private IP address: 10.10.0.6

Private IP address (IPv6): -

Virtual network/subnet: test-encryption-at-host/subnet1

DNS name: Configure

Size

Size: Standard D2s v3

vCPUs: 2

RAM: 8 GiB

Disks

OS disk: test-encryption-at-host153649-osDisk1

Encryption at host: Disabled

Azure disk encryption: Not enabled

Ephemeral OS disk: N/A

Data disks: 0

Azure Spot

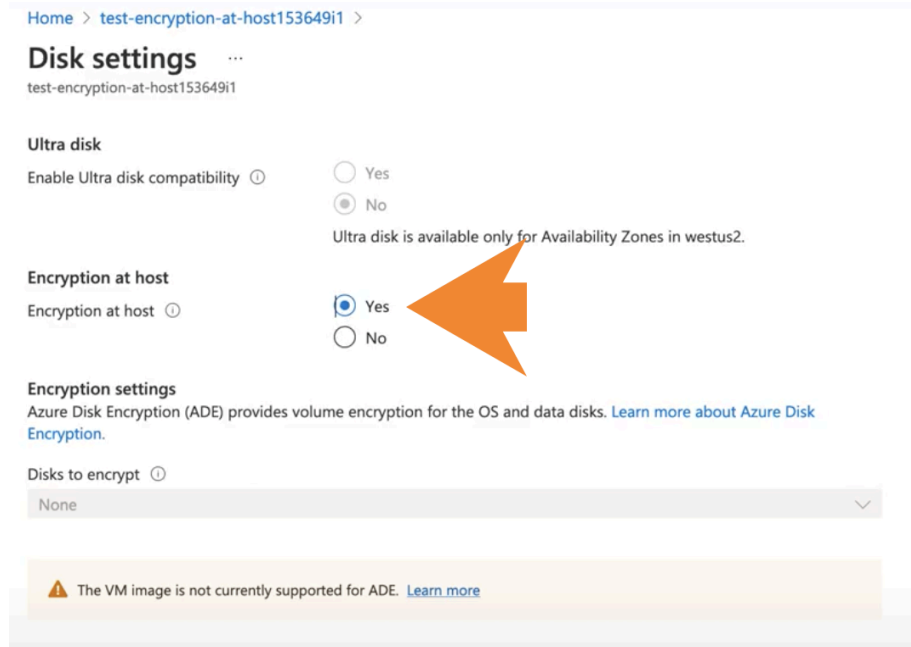
Azure Spot: -

Azure Spot eviction policy: -

- Leave the Azure Portal browser tabs open. You will need to get back to them shortly.
- 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](#).

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.

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”:

CLOUDERA TECHNICAL PREVIEW DOCUMENTATION

test-encryption-at-host153649i1

Virtual machine

Search (Cmd + /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
- Networking
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks
- Operations
- Bastion

Connect Start Restart Stop Capture Delete Refresh Open in mobile CLI / PS Feedback

Advisor (1 of 2): Guest Configuration extension should be installed on machines →

Subscription ID : 3ddda1c7-d1f5-4e7b-ac81-0523f483b3b3 DNS name : Not configured

Tags (edit) : owner : juhig Cloudera-Cre... : cmaatusiamus-west-1:c8dbde4b-ccce-4f8d-a581... dw-env-owner : juhig Cloudera-Envi... : cm.cdp.environmentus-west-1:c8dbde4b-ccce-4...

Properties Monitoring Capabilities (7) Recommendations (2) Tutorials

Virtual machine

Computer name	test-encryption-at-host-1
Health state	-
Operating system	Linux
Publisher	-
Offer	-
Plan	-
VM generation	V1
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

Availability + scaling

Availability zone	-
Scale Set	-

Security type

Networking

Public IP address	test-encryption-at-host153649i1
Public IP address (IPv6)	-
Private IP address	10.10.0.6
Private IP address (IPv6)	-
Virtual network/subnet	test-encryption-at-host/subnet1
DNS name	Configure

Size

Size	Standard D2s v3
vCPUs	2
RAM	8 GiB

Disk

OS disk	test-encryption-at-host153649-osDisk1
Encryption at host	Enabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

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.