

Azure Confidential Computing

This is a feature that allows you to isolate sensitive data when it is being processed in the cloud.

This feature is available for your virtual machines. In Confidential computing , a part of the CPU's hardware is reserved for the portion of code and data in your application. This portion is known as an enclave.

There is a special series of virtual machines which support confidential computing. This is the DCsv2-Series

<https://docs.microsoft.com/en-us/azure/virtual-machines/dcv2-series>

These series of virtual machines are built on Intel SGX technology for hardware-based enclaves.

To actually ensure that your code or application runs inside the enclave, you will have to program it accordingly.

For this you need to use two open-source frameworks

a) Open Enclave Software Development Kit

<https://github.com/openenclave/openenclave>

·b)Confidential Consortium Framework

<https://github.com/Microsoft/CCF>

Azure Dedicated Hosts

This service provides physical servers to host virtual machines. The physical server is dedicate to the Azure subscription.

The benefits of Azure Dedicated Hosts is that no other virtual machines from any other customers would be placed on the physical server.

You can also control the maintenance events that are initiated on the Azure platform.

Here the users are charged per dedicated host. This is irrespective of the number of virtual machines running on the physical server

For more information on Azure Dedicated Hosts , you can visit the URL -

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/dedicated-hosts>