Microsoft

AZURE STACK HCI: TRUSTED ENTERPRISE VIRTUALIZATION

Technical Use Cases
For Azure Stack HCI

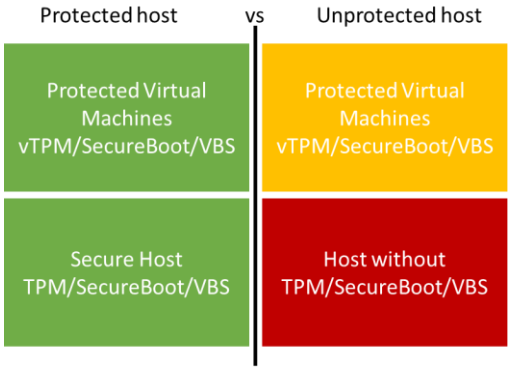
Branch office and edge | Virtual desktop infrastructure | High-performance Microsoft SQL Server | **Trusted enterprise virtualization** | Scale-out storage

Leverage your Azure Stack HCI investment to run workloads on a highly secure infrastructure by choosing the hardware designed for the Trusted enterprise virtualization scenario, with unparalleled levels of operating system security enabled with virtualization-based security (VBS) and hybrid cloud capabilities made easy through Windows Admin Center.
Below, you will find a how-to guide for building an infrastructure for the Trusted enterprise virtualization scenario on Azure Stack HCI that includes:

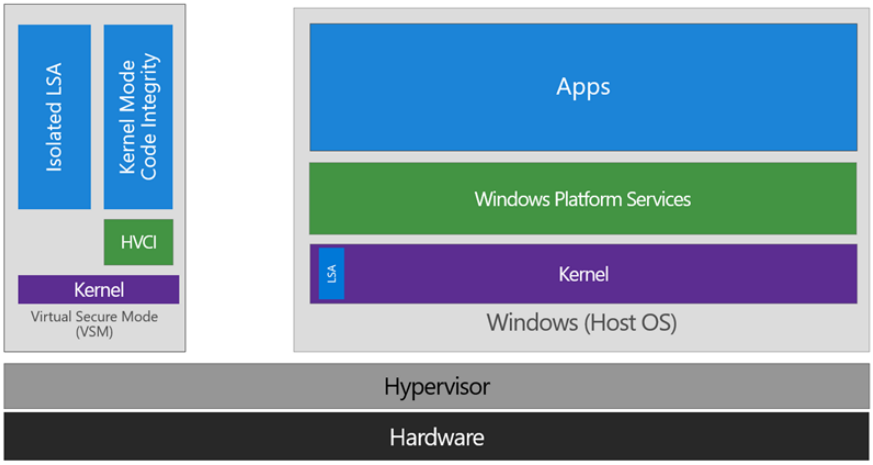
- Overview of Trusted enterprise virtualization scenario
- Step by step guidance of deploying VBS-enabled Azure Stack HCI and Azure Security Center via Windows Admin Center

Overview of Trusted enterprise virtualization scenario

Virtualization-based security (VBS) is a key component of the security investments in Azure Stack HCI to protect hosts and virtual machines from security threats.
For example, the Windows Server 2019 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems, and lists VBS and hypervisor-protected-code-integrity (HVCI) as general security requirements. It is imperative to use host hardware that is VBS and HVCI enabled, in order for the protected workloads on virtual machines to fulfil their security promise because protection of virtual machines is not guaranteed on a compromised host.



VBS uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system. Windows can use this "virtual secure mode" to host a number of security solutions, providing them with greatly increased protection from vulnerabilities in the operating system, and preventing the use of malicious exploits which attempt to defeat protections.VBS uses the Windows hypervisor to create this "virtual secure mode", and to enforce restrictions which protect vital system and operating system resources, or to protect security assets such as authenticated user credentials. With the increased protections offered by VBS, even if malware gains access to the operating system kernel, the possible exploits can be greatly limited and contained because the hypervisor can prevent the malware from executing code or accessing platform secrets.



QCT

One such example security solution is HVCI, which uses VBS to significantly strengthen code integrity policy enforcement. Kernel mode code integrity checks all kernel mode drivers and binaries before they're started and prevents unsigned drivers or system files from being loaded into system memory.

HVCI leverages VBS to run the code integrity service inside a virtual secure mode, providing stronger protections against kernel viruses and malware. The hypervisor, the most privileged level of system software, sets and enforces page permissions across all system memory. Pages are only made executable after code integrity checks inside the virtual secure mode have passed, and executable pages are not writable. That way, even if there are vulnerabilities like buffer overflow that allow malware to attempt to modify memory, code pages cannot be modified, and modified memory cannot be made executable.

How to deploy VBS and HVCI-enabled Azure Stack HCI

1. Hardware and OS configuration for Scale-out storage configurations

QCT QuantaGrid D52BM-2U

Scale:

- 2 to 4 nodes

Single Node Data:

- CPU: 20 - 40 cores (Intel)
- RAM: 192GB - 768GB
- Raw storage: 40TB to 160TB
- Storage type: DCPMM+HDD
- Network speed: Up to 25Gb

QCT QuantaGrid D52B-1U

Scale:

- 2 to 16 nodes

Single Node Data:

- CPU: 20 - 56 cores (Intel)
- RAM: 256GB - 768GB
- Raw storage: 12.8TB to 38.4TB
- Storage type: NVMe
- Network speed: Up to 25Gb

QCT QuantaGrid D52T-1ULH

Scale:

- 2 to 4 nodes

Single Node Data:

- CPU: 20 - 56 cores (Intel)
- RAM: 256GB - 384GB
- Raw storage: 32TB to 120TB
- Storage type: SSD+HDD
- Network speed: Up to 25Gb

QCT QuantaGrid D52BQ-All flash / Performance

Scale:
- 2 to 4 nodes

Single Node Data:
- CPU: 20 - 56 cores (Intel)
- RAM: 256GB - 768GB
- Raw storage: 2TB to 48TB
- Storage type: SSD
- Network speed: Up to 25Gb

QCT QuantaGrid D52BQ-Hybrid / Balanced

Scale:
- 2 to 4 nodes

Single Node Data:
- CPU: 20 - 56 cores (Intel)
- RAM: 256GB - 768GB
- Raw storage: 32TB to 80TB
- Storage type: SSD+HDD
- Network speed: Up to 25Gb

QCT QuantaPlex T21P-4U

Scale:
- 2 to 16 nodes

Single Node Data:
- CPU: 12 - 36 cores (Intel)
- RAM: 256GB - 512GB
- Raw storage: 80TB to 640TB
- Storage type: SSD + HDD
- Network speed: Up to 25Gb

2. Plan Hardware Deployment

All the Azure Stack HCI solutions by QCT are certified for the Hardware Assurance Additional Qualification, which tests for all the functionality needed for VBS. However, VBS and HVCI are not automatically enabled in Azure Stack HCI and Step 2 will guide you to enable them.
Please refer to QCT's solutions listed on Azure Stack HCI Catalog

3. Deploy VBS-Enabled Azure Stack HCI

- Deploy Azure Stack HCI

  Step by Step guide to deploy Azure Stack HCI (Microsoft Official Document)

  - Or you can follow ***QCT's detailed deployment guide below:***

  QCT Azure Stack HCI Deployment Guide for Scale-out Storage v.1.3

  1. Install Windows Server 2019 Datacenter
  2. Add roles and features
  3. Set up Failover Clustering and enable a Cluster Witness

4. Set up Storage Spaces Direct
5. Install Windows Admin Center (WAC) and add QCT's WAC extension.
6. Add Azure hybrid services to take advantage of Azure Security Center, Azure Monitor, Azure Backup, Azure File Sync, Azure Site Recover

- Enable virtualization-based protection of code integrity

Precautions

- Do not store Domain Controller (DC) VMs on Cluster Shared Volume, place the DC VM files on local storage of each node.
- Run one DC on each node.
- On each DC, configure the remote DC as the primary DNS and itself as the secondary DNS. This ensures all DNS records are up to date and synchronized, even after a reboot or undergoing a disconnection for a long period of time.
- DCs are redundant and highly available by design.
- DO NOT deploy ADDS on a dedicated physical DC, such as a QCT D52BQ-2U node.
- Must at least deploy a second, virtual DC on the cluster itself.

Resources

- Windows Server Security and Assurance
- Microsoft Security Compliance Toolkit
- Windows 10 Enterprise Security
- Top 10 ways to secure Office 365 and Microsoft 365 Business plans

Summary

With completion of the Azure Stack HCI Trusted enterprise virtualization deployment and the configuration of VBS / HVCI, you now have a platform with the highest security standards for protecting security sensitive workloads on both physical and virtual machines.