1. 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.
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.

2. Thomas-Krenn.AG Storage Spaces Direct Systems

All the Azure Stack HCI solutions by Thomas-Krenn.AG 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.

- S2D Micro-Cluster Variants (includes TPM 2.0 module)
- S2D Series Variants (optional TPM 2.0 module)

3. Plan your Azure Stack HCI environment with S2D Micro-Cluster

- Micro-Cluster Basic is designed for up to 8 server VMs
- Micro-Cluster Advanced is designed for up to 16 server VMs
- Azure IoT Edge workloads run in containers, consuming 1 VM

(1) each VM planned with 4 vCPUs & 6GB vRAM. Custom-sized VMs are also supported

- Predefined Storage-Capacity available
  - 3TB Nested-Mirror (6TB Mirror)
  - 6TB Nested-Mirror (12TB Mirror)
  - 9TB Nested-Mirror (18TB Mirror)
  - 12TB Nested-Mirror (24TB Mirror)

(2) Nested two-way Mirror is highly recommended for 2-Node-S2D-Clusters

Please consider backup and restore times for large-capacity configurations. Most data protection solutions are not able to ingest and restore at speeds businesses expect.

4. Plan your Azure Stack HCI environment with S2D Series

- Maximum flexibility and scalability
- Up to 2x Intel Scalable CPU 2nd-generation each Node
- Up to 1 TB RAM each Node
- Up to 2x 100 GbE RDMA-Network each Node
- Individual calculated Storage-Capacity available
  - NVMe-Storage
  - SSD-Storage
  - HDD-Storage

(2) Nested two-way Mirror is highly recommended for 2-Node-S2D-Clusters

Please consider backup and restore times for large-capacity configurations. Most data protection solutions are not able to ingest and restore at speeds businesses expect.

5. Network and Switch Connectivity

1. RoCE/RDMA technology for Storage Spaces Direct Traffic. With RoCE there is additional DCB and PFC configuration required. Network devices have to support this capabilities.

2. iWarp/RDMA (recommended) technology for Storage Spaces Direct Storage Traffic. iWARP is “plug and play” and requires no additional network configuration. Existing 10GbE TCP/IP infrastructure is fully compatible.
3. Available as switch-connected or direct-attached solution\(^{(3)}\)
   - One single/standalone switch
   - Two redundant/stacked switches
   - Optional: Direct-attached for RDMA (storage/cluster) traffic

\(^{(3)}\) Thomas-Krenn.AG recommends a switched configuration. The switch helps the cluster determine whether loss of node connectivity is due to node or network failure, ensuring more predictable failover behavior.

6. Unboxing and first startup the S2D Micro-Cluster
   - Every S2D Micro-Cluster is shipped with Windows Server 2019 DC pre-installed.
   - All required firmware and drivers are pre-installed.
   - Use the getting started guide for provisioning the S2D Micro-Cluster

7. Configure VBS-Enabled Azure Stack HCI
   For details, refer to Step by Step guide to deploy Azure Stack HCI.
   In general, follow these simple steps:
   1. Customize hostnames
   2. Join your active directory domain, different deployment options available\(^{(4)}\)
      - Fully self-contained, virtualized domain controllers within the cluster itself.
        - Do not store DC VMs on cluster shared volumes, keep all VM files on storage local to each node.
        - Do not include DC VMs in cluster management: do not add them to cluster manager.
        - Run one DC on each node.
        - On each DC, configure the remote DC as primary DNS and itself as secondary DNS. This ensures all DNS records are live and current, even after booting up from a long time offline.
        - Domain controllers are redundant and highly available by design.
      - Dedicated physical domain controller, for example deployed on a Thomas-Krenn.AG LES
        - We recommend a second, virtual domain controller on the cluster itself. Follow the guidelines above.
   3. Prepare Witness for Cluster-Quorum
      - Azure Cloud Witness, when on-prem infrastructure is to be kept at a minimum.
      - SMB File Share or USB witness with write-access from all nodes for on premises based witness
   4. Configure network ports
      - Set up a Switch Embedded Teaming (SET) for Traffic-NICs
      - Set up RoCE / iWarp / RDMA for SMB-NICs
   5. Add Roles and Features for each node. IMPORTANT: Skip the Data-Center-Bridging role, if you are using iWARP.
   6. Setup Storage Spaces Direct
      - Setup Failover Clustering and enable a Witness
      - Enable Storage Spaces Direct
      - Create Volumes
   7. Enable virtualization-based protection of code integrity
   8. Install Windows Admin Center (WAC) (Download here)
   9. Install the Thomas-Krenn.AG Extension for S2D Micro-Cluster
      - Download from official Extension-Store in WAC
      - Name: Thomas-Krenn.AG | S2D Micro-Cluster

\(^{(4)}\) Both variants are officially supported. Thomas-Krenn.AG recommends the dedicated physical scenario.
8. From Windows Admin Center (WAC), set up Azure Security Center to add threat protection and quickly assess your security posture of your workloads.

9. Additionally, you can set up additional Azure hybrid services such as Backup, Monitoring, File Sync, Site Recovery, Point-to-Site VPN and Update Management in WAC. Use cases we recommend for trusted enterprise virtualization scenarios are:
   - Monitoring Hosts and VMs to gain insight into your infrastructure health using Azure Monitor.
   - Protect your mission-critical VM data off-prem using Azure Backup.
   - Add disaster recovery capabilities by automatically failing your on-prem cluster to Azure Site Recovery.
   - Deploy Azure File Sync to sync data between locations and even with mobile end users, as well as expand internal storage capacity when needed.

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.