AZURE STACK HCI: BRANCH OFFICE AND EDGE

Leverage your Azure Stack HCI investment to run key virtual applications and workloads in a highly available, resilient fashion on hardware designed for branch office and edge scenarios with industry-leading support for 2 node configurations including: Nested resiliency, Cloud or USB thumb drive cluster witness, and browser-based administration via Windows Admin Center.

Below, you will find a how-to guide for Azure Stack HCI branch office and edge configurations that includes:

- Plan and deploy Thomas-Krenn.AG hardware and OS/tools to support Azure Stack HCI branch office and edge scenarios
- Step by step guide to enable branch office and edge support with Azure IoT Edge and cloud-driven container management

1. Thomas-Krenn.AG Storage Spaces Direct Systems
   - **S2D Micro-Cluster Variants**
   - **S2D Series Variants**

2. Plan your Azure Stack HCI environment with **S2D Micro-Cluster**
   - Micro-Cluster Basic is designed for up to 8 server VMs\(^1\)
   - Micro-Cluster Advanced is designed for up to 16 server VMs\(^1\)
   - Azure IoT Edge workloads run in containers, consuming 1 VM\(^1\)

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

   - Predefined Storage-Capacity available\(^2\)
     - 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.

3. Plan your Azure Stack HCI environment with **S2D Series**
   - Maximum flexibility and scaleability
   - Up to 2x Intel Scalable CPU 2\(^{nd}\)-generation each Node
   - Up to 1 TB RAM each Node
   - Up to 2x 100 GbE RDMA-Network each Node
   - Individual calculated Storage-Capacity available\(^2\)
     - 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.
4. 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
      - 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.

5. 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

6. Configure 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
      - 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. Install Windows Admin Center (WAC) (Download here)
   8. 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.
7. From Windows Admin Center (WAC), Set up Azure Monitor to gain insight into your application, network and server health of your Azure Stack HCI Branch office and edge solution.
   1. Unless you have one, create an Azure tenant and add a subscription
   2. Connect your Cluster to Azure using WAC’s step-by-step wizard
   3. Enable Azure Monitor to collect data from your S2D-Cluster
   4. Configure Azure Alerts for immediate, actionable notifications when needed.
   To get started, we suggest these basic thresholds:
   - Logical Disk $\rightarrow >80\%$ Used Space
   - Processor $\rightarrow >90\%$ Processor Time average over 1 hour
   - Memory $\rightarrow <1000$ Pages/sec average over 1 hour

8. Additionally, you can set up additional Azure hybrid services such as Backup, File Sync, Site Recovery, Point-to-Site VPN, Update Management, and Security Center in WAC.
   Use cases we recommend for Branch Office and Edge scenarios are:
   - 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.

9. Enable Modern, containerized application support for Azure IoT Edge:
   Once your Azure Stack HCI Branch office and edge setup is complete, follow the steps below to enable your environment to support modern Container-based application development and IoT data processing by deploying a VM running Azure IoT Edge.

What is Azure IoT Edge?

- Open source software from Microsoft
- Runs on Windows or Linux
- Built to run “on the edge” for near-real time responses
- Secured by software and hardware mechanisms
- Available AI Toolkit
  [https://github.com/Azure/ai-toolkit-iot-edge](https://github.com/Azure/ai-toolkit-iot-edge)

…combines AI, cloud and edge computing to containerize cloud workloads—such as Azure Cognitive Services, Machine Learning, Stream Analytics, and Functions—and run them locally on devices from a Raspberry Pi to an industrial gateway or converged edge server and manages edge applications / devices with Azure IoT Hub.

© 2020 Thomas-Krenn.AG
How do I deploy Azure IoT Edge on Azure Stack HCI?

1. **Create a VM on your Azure Stack HCI using Windows Admin Center**
   (For supported OS versions, VM types, processor architectures and system requirements, click [here](#))

2. **Create an Azure IoT Hub in the Azure Portal**

3. **Register an IoT Edge device** in the Azure Portal
   (The IoT Edge “device” is the Windows or Linux VM running on your Azure Stack HCI installation)

4. **Install and start the IoT Edge runtime** on the VM you created in step 1
   (You will need the device string created in step 4 above to connect the runtime to your Azure IoT Hub)

5. **Deploy a module to IoT Edge**
   (Pre-built modules can be sourced and deployed from the [IoT Edge Modules section of the Azure Marketplace](#))

**NOTE:** In addition to gathering and processing IoT data from IoT sensors, Azure IoT Edge can also be utilized to deploy Containers with general purpose usage capabilities. Adding Azure IoT Edge to your Azure Stack HCI Branch office and edge deployments modernizes your environment to support [CI/CD pipeline](#) application deployment framework. Your DevOps personnel can deploy and iterate on Containerized applications that IT builds and supports via traditional VM management processes and tools.

**Summary**

With completion of the Azure Stack HCI Branch office and edge deployment and the installation and configuration of Azure IoT Edge, you now have a platform capable of running complex, highly available business workloads in VMs as well as containers for Branch office and edge deployments.