

10 dicembre 2021

# POWERCON2021

---

ICT  POWER.IT

# #POWERCON2021

Windows Server 2022, le novità sulla sicurezza  
e la gestione ibrida di Azure

Nicola Ferrini

*Trainer – Microsoft MVP*



/NicolaFerrini.it



@nicolaferrini

# Windows Server 2022

Run business critical workloads in Azure, on-premises and at the edge



Advanced multi-layered security



Hybrid capabilities with Azure



Flexible application platform



Azure innovation for Windows Server

# Secured-core server

Secure hardware, firmware and OS capabilities to help protect against threats



## Protect

at boot-up with hardware root of trust

- Trusted Platform Module 2.0
- Secure cryptographic capabilities to better protect sensitive keys and measurements



## Defend

against firmware level attack with validated system integrity

- Windows Defender System Guard to protect, maintain, and validate system integrity
- Dynamic root of trust of measurement (DRTM) to boot up securely and minimize firmware vulnerabilities



## Prevent

access to unverified code with Virtualization-based security

- Hypervisor protected code integrity (HVCI) protects from unverified code execution
- Virtualization-based security supports features like Credential Guard to protect enterprise domain credentials

- ### nic-srv2022
- #### Tools
- 
- Certificates
  - Containers
  - Devices
  - Events
  - Files & file sharing
  - Firewall
  - Installed apps
  - Local users & groups
  - Networks
  - Packet monitoring
  - Performance Monitor
  - PowerShell
  - Processes
  - Registry
  - Remote Desktop
  - Roles & features
  - Scheduled tasks
  - Security**
  - Services
  - Settings

## Security PREVIEW ⓘ

Summary Protection history **Secured-core**

[What is Secured-core server?](#)

Enable  Disable ↻

<input type="checkbox"/> Security Feature	Status
<b>Hypervisor Enforced Code Integrity (HVCI) ⓘ</b>	✔ On
<b>Boot DMA Protection ⓘ</b>	✔ On
<b>System Guard ⓘ</b>	✔ On
<b>Secure Boot ⓘ</b>	✔ On
<b>Virtualization-based Security (VBS) ⓘ</b>	✔ On
<b>Trusted Platform Module 2.0 (TPM 2.0) ⓘ</b>	✔ On

- Refine results
- System configuration
    - Integrated System
    - Validated node
  - Solution builder
    - Lenovo
    - Dell Technologies
    - DataON
    - See More
    - Purchase as a Service
    - Optimized for
    - CPU
    - GPU support
    - Storage
    - Feature support


**Microsoft strongly recommends choosing Integrated Systems**

Integrated Systems provide the best customer experience for Azure Stack HCI. They come with the operating system pre-installed on high quality, integrated hardware that is optimally configured for Azure Stack HCI and has completed Microsoft's clustered solution validation testing.

[Help me choose](#) | [Compare solutions](#) | [Clear All](#) | Search | Sort By

Secured-core Server    
 Showing 1-4 of 4 platforms with 13 solutions

**HPE DL380 Gen10 Plus**




**Hewlett Packard Enterprise**

2 to 16 nodes  
Intel® 3rd Gen Xeon® Scalable Processor

[4 solutions >](#)

**HPE DL325 Gen10 Plus v2**




**Hewlett Packard Enterprise**

2 to 16 nodes  
AMD 3rd Gen EPYC™

[3 solutions >](#)

**HPE DL360 Gen10 Plus**




**Hewlett Packard Enterprise**

2 to 16 nodes  
Intel® 3rd Gen Xeon® Scalable Processor

[3 solutions >](#)

**HPE DL385 Gen10 Plus v2**



**Hewlett Packard Enterprise**

2 to 16 nodes  
AMD 3rd Gen EPYC™

[3 solutions >](#)

# Network Protection



- INTERNET
- LIVE CHAT
- MEDIA
- PHOTOS
- VIDEOS
- MUSIC

# TLS 1.3 - More Secure

- Many of the major vulnerabilities in TLS 1.2 had to do with older cryptographic algorithms that were still supported
- TLS 1.3 drops support for vulnerable cryptographic algorithms



# TLS 1.3 - Faster

- TLS handshakes in TLS 1.3 only require one round trip instead of two, shortening the process by a few milliseconds
- When the client has connected to a website before, the TLS handshake will have zero round trips. This makes HTTPS connections faster, cutting down latency.

# SMB Encryption



### nic-srv2022

#### Tools

Search Tools

- Overview
- Azure hybrid center
- Azure Kubernetes Service
- Azure Backup
- Azure File Sync
- Azure Monitor
- Azure Security Center
- Certificates
- Devices
- Events
- Files & file sharing**
- Firewall
- Installed apps
- Local users & groups
- Networks
- Packet monitoring
- Performance Monitor
- PowerShell
- Settings

#### File shares

+ New share Edit share Remove share File server settings

Name	Path	UNC path	Offline files	SMB encryption	Current users	Special
<a href="#">ADMIN\$</a>	C:\Windows	\\Nic-SRV2022.W...	Manual	false	0	true
<a href="#">C\$</a>	C:\	\\Nic-SRV2022.W...	Manual	false	0	true

- Protects against Man in the Middle attacks
- More Secure
  - Windows Server 2022 & Windows 11 introduce AES-256-GCM and AES-256-CCM cryptographic suites for SMB 3.1.1 encryption
  - Windows will automatically negotiate this more advanced cipher method
- Flexible and Easy to Use:
  - Can be configured per share or entire file server
  - Can be mandated through Group Policy
  - Via PowerShell
  - One checkbox in Windows Admin Center

#### New file share

This shares the folder you select on the network using the SMB protocol.

Folder location \*

Share name \*

Share permissions

Name	Permission
Everyone	Full control

Offline files

Manual

Compress data

Enable SMB encryption



- ### nic-srv2022
- #### Tools
- Search Tools
- Overview
  - Azure hybrid center
  - Azure Kubernetes Service
  - Azure Backup
  - Azure File Sync
  - Azure Monitor
  - Azure Security Center
  - Certificates
  - Devices
  - Events
  - Files & file sharing
  - Firewall
  - Installed apps
  - Local users & groups
  - Networks
  - Packet monitoring
  - Performance Monitor
  - PowerShell
  - Settings

- ### Settings
- General
- File shares (SMB server)
  - Environment variables
  - Azure Arc for servers
  - Power configuration
  - Remote Desktop
  - Role-based Access Control

### File shares (SMB server)

These settings affect all file shares on this server that use the SMB protocol, overruling settings on individual shares.

#### General settings

- SMB 1 isn't installed
- SMB 1 removal ⓘ
  - Don't audit SMB 1 connections
  - Audit SMB 1 connections
- SMB signing ⓘ
  - Not required
  - Required
- SMB 3 encryption ⓘ
  - Not required
  - Required from clients that support it
  - Required from all clients (others are rejected)
- Disable SMB 3 compression ⓘ

Server wide SMB Encryption

#### File sharing across the internet with SMB over QUIC

Enable shares on this file server to be accessible across the internet — without using a VPN — by configuring the QUIC protocol. [Learn more](#)

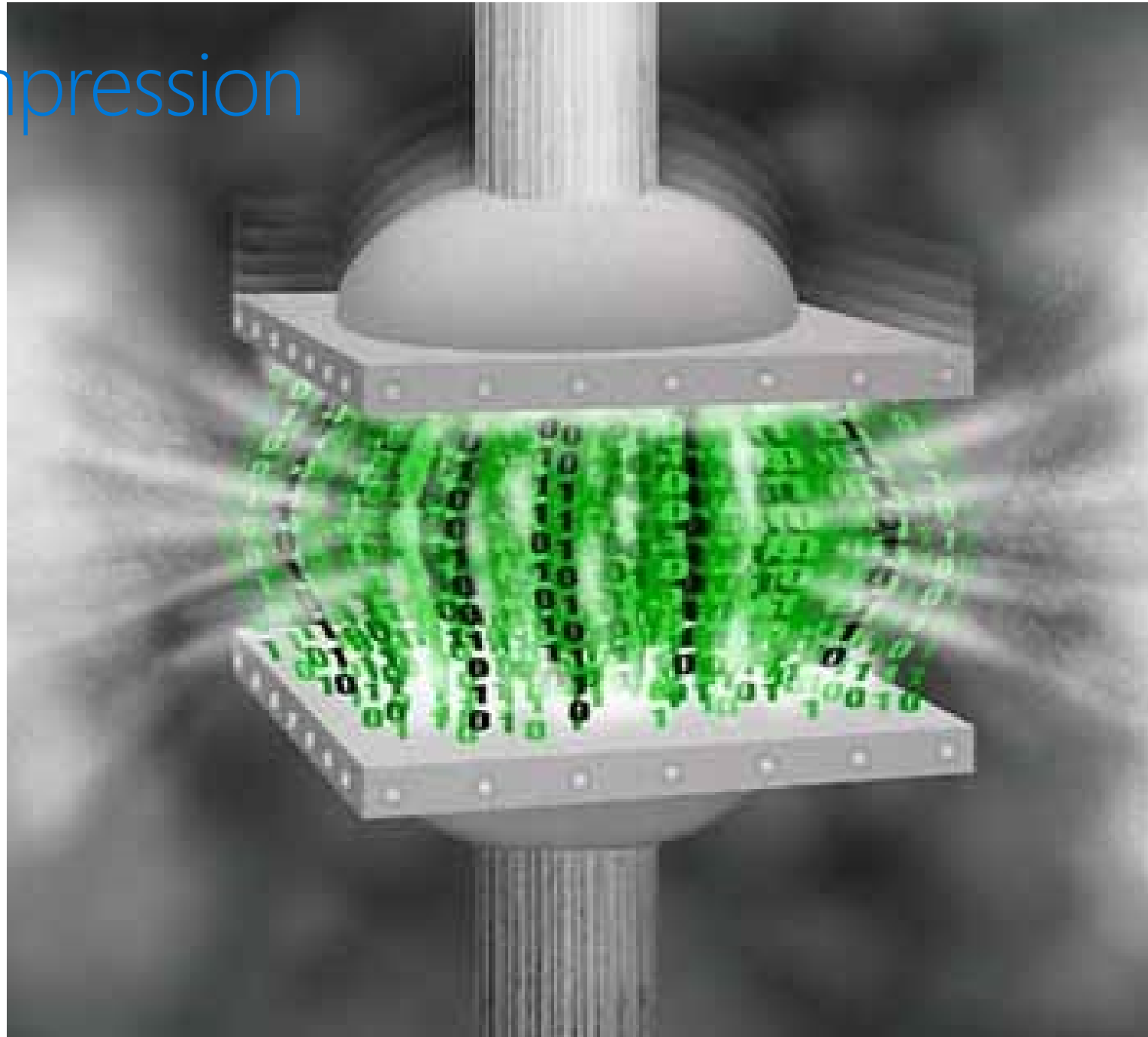
**i** SMB over QUIC is only supported on the Azure Edition of Windows Servers. You are not connected to an Azure Edition server.

**Save** **Discard changes**

# SMB Encryption & SMB Direct (RDMA)

- Windows Server 2022 and Windows 11 SMB Direct now supports encryption
- Previously, enabling SMB encryption disabled direct data placement, making RDMA performance as slow as TCP
- Now data is encrypted before placement resulting in security and performance while adding AES-128 and AES-256 protected packet privacy
- You can enable encryption using
  - Windows Admin Center
  - Set-SmbServerConfiguration
  - UNC Hardening group policy

# SMB Compression



- ### nic-srv2022
- #### Tools
- Search Tools
- Overview
  - Azure hybrid center
  - Azure Kubernetes Service
  - Azure Backup
  - Azure File Sync
  - Azure Monitor
  - Azure Security Center
  - Certificates
  - Devices
  - Events
  - Files & file sharing**
  - Firewall
  - Installed apps
  - Local users & groups
  - Networks
  - Packet monitoring
  - Performance Monitor
  - PowerShell
  - Settings

#### File shares

+ New share Edit share Remove share File server settings

Name	Path	UNC path	Offline files	SMB encryption	Current users	Special
<a href="#">ADMIN\$</a>	C:\Windows	\\Nic-SRV2022.W...	Manual	false	0	true
<a href="#">C\$</a>	C:\	\\Nic-SRV2022.W...	Manual	false	0	true

**Flexible and Easy to Use**  
Can be configured per share  
Can be mandated through Group Policy  
Via PowerShell  
One checkbox in Windows Admin Center

#### New file share

This shares the folder you select on the network using the SMB protocol.

Folder location \*

Share name \*

Share permissions

Name	Permission	
Everyone	Full control	X

Offline files

Manual

Compress data

Enable SMB encryption

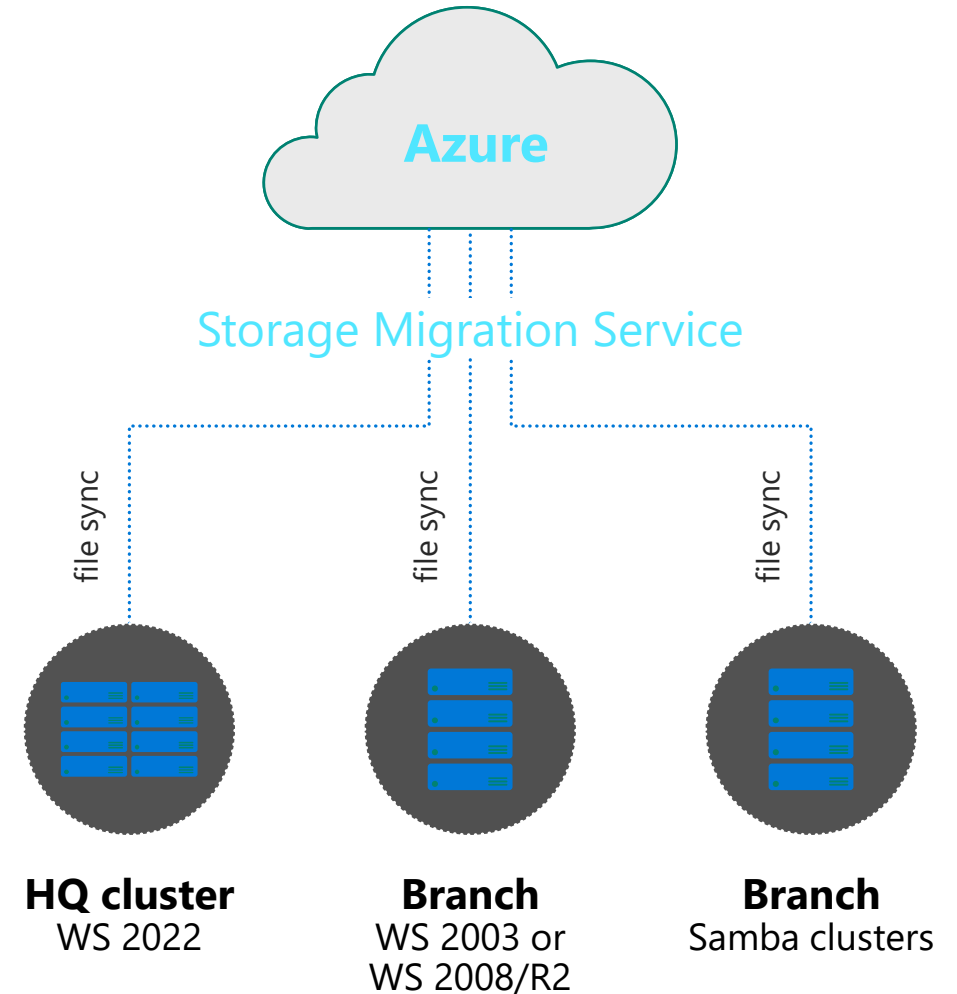


# Storage Migration Service

With Windows Server 2022

## Modernize your File Server and Future Proof On-Prem Storage Costs

- SMS will:
  - Automatically use Azure File Sync
  - Sync your data into Azure Files for bottomless storage
  - Migrate all your data to a modern Windows Server
- On-premises File Server is a hot cache

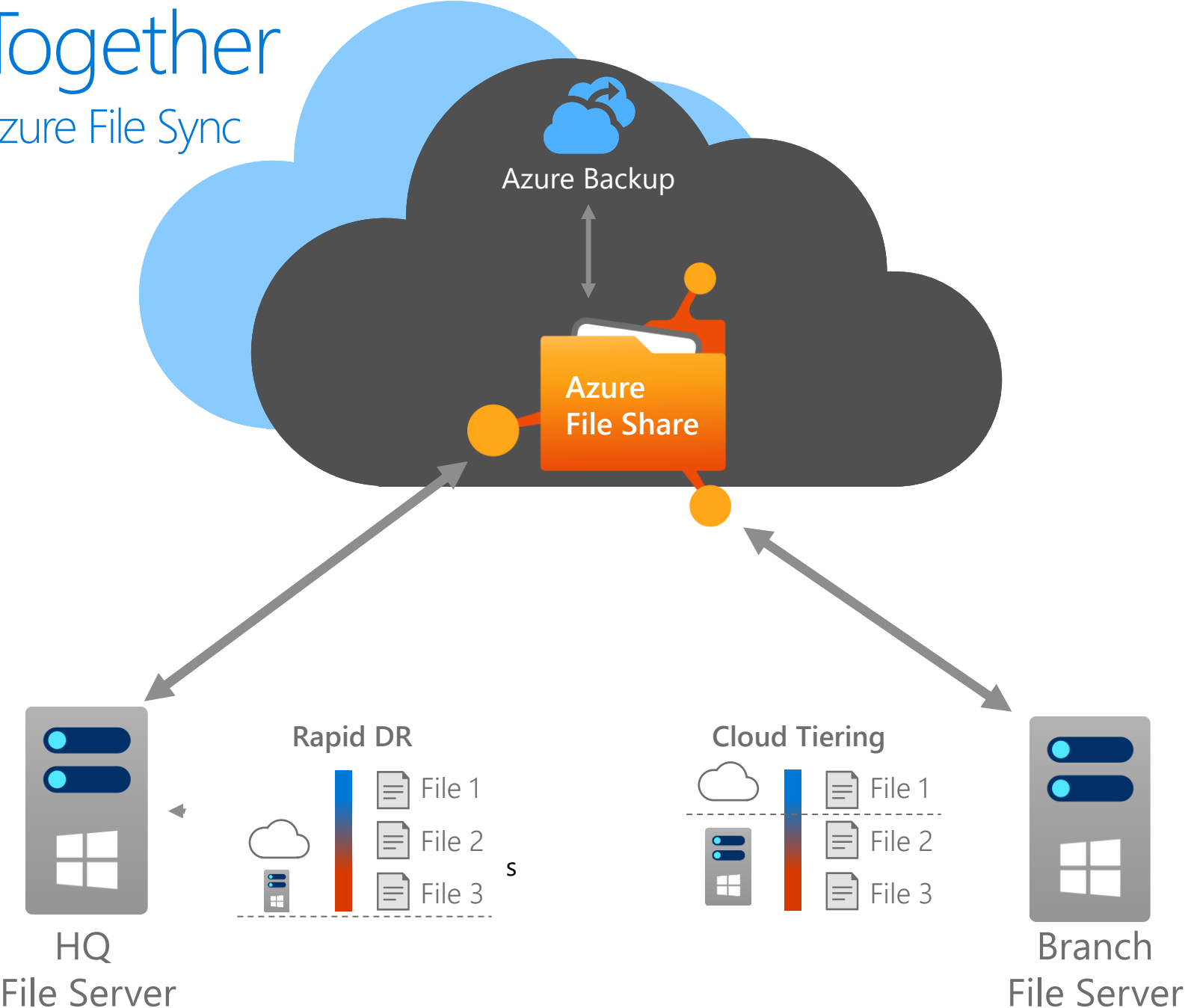




# File Storage Better Together

Windows Server 2022 File Server & Azure File Sync

- Multi-site Sync
- Cloud Tiering
- Cloud Backup
- Disaster Recovery



# Windows Server & SQL Server

Capability	Windows Server 2012/2012 R2 Standard and Datacenter	Windows Server 2016/2019 Standard and Datacenter	Windows Server 2022 Standard and Datacenter
<b>Physical (Host) Memory Support</b>	Up to 4 TB per physical server	Up to 24 TB per physical server	<b>Up to 48 TB per physical server</b>
<b>Physical (Host) Logical Processor Support</b>	Up to 320 LPs	Up to 512 LPs	<b>Up to 2048 LPs</b>

# Windows Server 2022 Hyper-V

Support for Nested  
Virtualization with AMD  
EPYC/Ryzen



# Windows Server 2022 Containers



# Windows Server 2022 Containers

Nano Server Containers

Server Core Containers

# 5 Year

Container Support

- gMSA without domain joined hosts
- Virtualized Time Zone
- CRI-containerd and HCS integration
- Tigera Calico for Windows
- Scalability improvements for overlay networking
- Containerization tooling on Windows Admin Center
- DSR routing for overlay and I2bridge networks
- YAML authoring for AKS and AKS-HCI deployment
- Smaller base container image size
- IPv6 Support for Windows Containers
- Multisubnet support for Kubernetes worker nodes
- Azure Migrate App Containerization

# Windows Server 2022 Nano Server

docker hub  [Explore](#) [Pricing](#) [Sign In](#) [Sign Up](#)

Explore > Verified Publishers > Nano Server >



## Nano Server

By **Microsoft**

The official Nano Server base image for containers

↓ 500M+

- Container
- x86-64
- Base Images

Windows Server 2022 Nano Server  
<100 MB

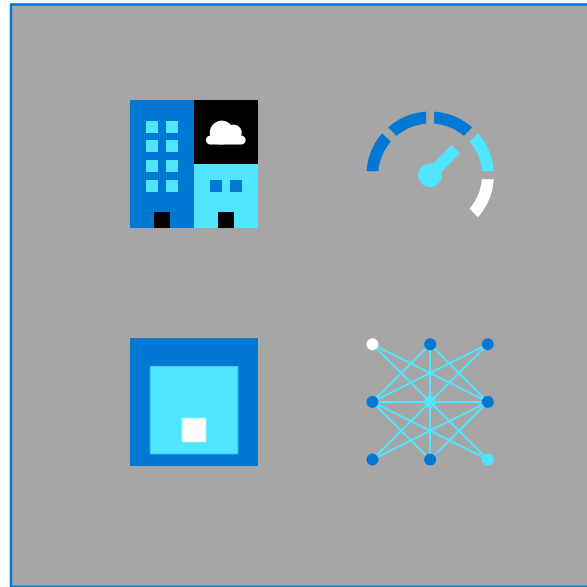
```
docker pull mcr.microsoft.com/windows/nanoserver
```

[https://hub.docker.com/\\_/microsoft-windows-nanoserver](https://hub.docker.com/_/microsoft-windows-nanoserver)

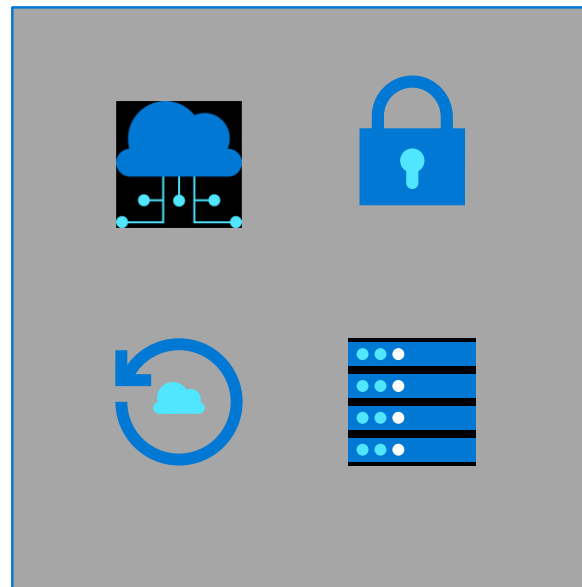
# Windows Server 2022 Datacenter: Azure Edition



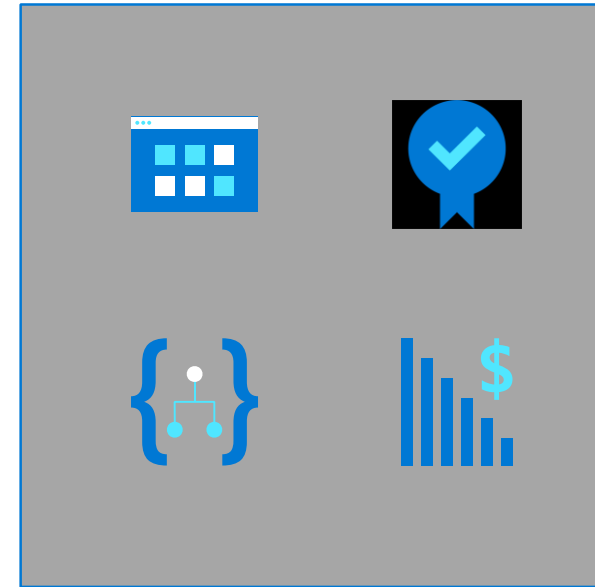
# Windows Server 2022 Datacenter: Azure Edition



Latest hybrid  
and compute  
features



Runs on Azure  
cloud & Azure  
Stack HCI 21H2



Best Windows  
Server VM with  
Automanage



# Windows Server 2022 Datacenter: Azure Edition



**Hotpatch with Azure Automanage (Preview)**



**SMB over QUIC**

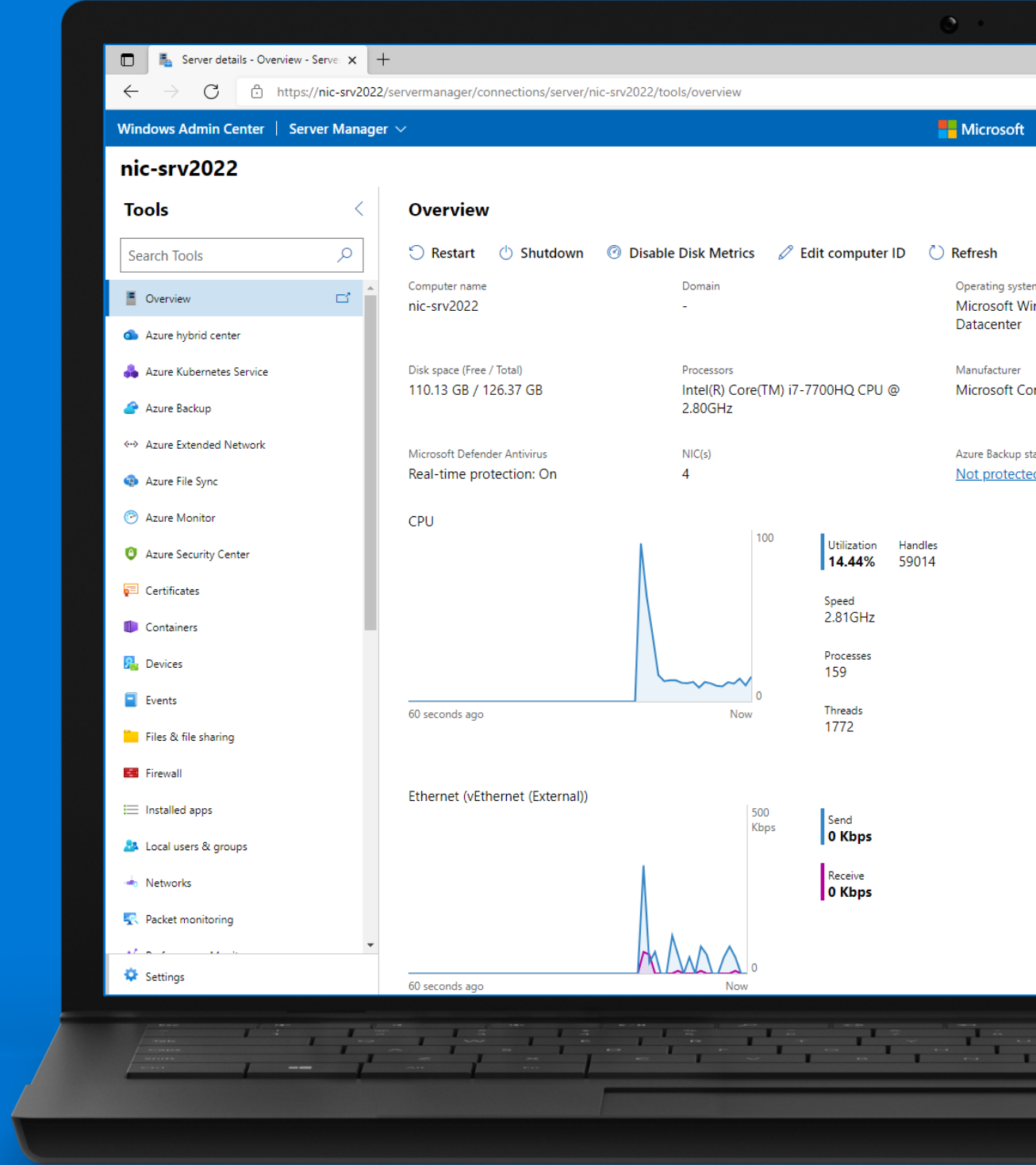


**Azure Extended Networking**

[Disponibili Windows Server 2022: Azure Edition \(general availability\), hotpatch \(preview\), automanage \(preview\) e configuration management \(preview\) in Microsoft Azure - ICT Power](#)

# DEMO

## TITOLO DEMO



# Grazie

Nicola Ferrini

*MCT – Microsoft MVP*



/NicolaFerrini.it



@nicolaferrini