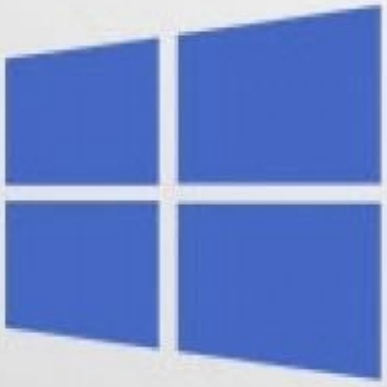
Windows Server 2022

New Roadmap
Fewer Editions
More Security



Windows Server 2022
New Roadmap, fewer editions, more security

Table of content

Introduction

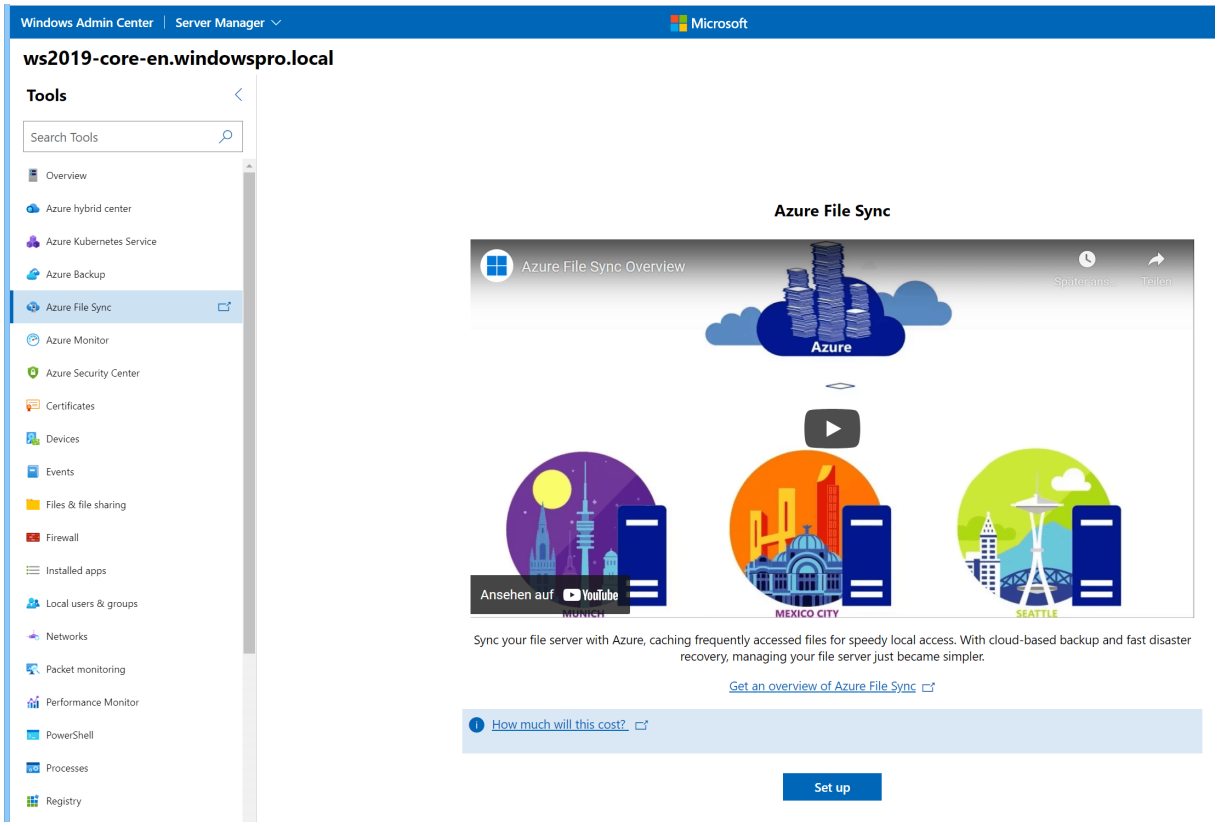
For more than 20 years, Windows Server has been Microsoft's on-prem platform for delivering IT infrastructure and applications. Companies have become accustomed to receiving an upgrade every three to four years, and with it, the latest server technologies. However, version 2022 shows that this legacy is coming to an end.

Windows Server has developed into a leading virtualization platform since version 2008, thanks to the integrated hypervisor. There have also been major advances in remote desktop services and, since Server 2016, in the features to provide hyperconverged infrastructures.

Cloud as Microsoft's highest priority

Microsoft's strategic focus on the cloud is having a massive impact on the role and importance of Windows Server. On the one hand, Microsoft is pushing companies to stop providing traditional workloads, such as Exchange or SharePoint on-prem, but to subscribe to Office 365 services instead.

On the other hand, the manufacturer has noticeably slowed down the innovation rate since version 2016, so that Server 2022 only received a modest number of new features. The functional level for Active Directory has even remained at the same version since 2016.



In the Admin Center, local Windows servers can be quickly integrated with Azure cloud services

A number of innovations in the operating system and in tools such as the Admin Center are aimed at setting up hybrid environments. For example, Windows Server 2022 can be managed out of the box via Azure Arc and connected to various cloud services, such as backup or monitoring.

In-house competition

Windows Server is now competing with Azure Stack HCI, which many users don't have on their radar yet. Microsoft is positioning it as the preferred OS for bare metal installations, currently only for hyperconverged clusters, but in the future also for individual servers.

To make Azure Stack HCI more attractive, it gets exclusive new features that are withheld from Windows Server.

If traditional storage arrays are to be replaced by a hyperconverged infrastructure based on Microsoft technology, it can be done with Windows Server 2022. However, the manufacturer's roadmap shows that future innovations are largely cut off, and its management is limited to relatively primitive tools.

As the competition grew for Windows Server, Microsoft started to reduce the number of editions for the OS. The semiannual channel has been dropped, and frequent feature updates are only available for Azure Stack HCI. The free Hyper-V Server has also fallen by the wayside, and the Essentials edition has been reduced to a pure license without its own features.

Gradual loss of relevance

Companies will therefore have to say goodbye to the automatic upgrade of Windows Server every few years to get the latest infrastructure services.

Increasingly, innovations are being reserved for the cloud, as proven by the rapid development of modern authentication methods in Azure AD, while traditional Active Directory stagnates.

However, if companies continue to provide services in their own data center via Windows Server, they will soon be faced with the decision between this OS and Azure Stack HCI for bare metal systems.

As development continues, Windows Server will increasingly fall behind when it comes to new features. Today, the vast majority of OS instances no longer run directly on the hardware, but inside virtual machines. Windows Server will increasingly be reduced to this function as a guest OS due to Microsoft's focus on Azure Stack HCI. There, it provides infrastructure services such as Active Directory, DNS, DHCP, or file and print services, which Microsoft already refers to as legacy services.

Azure Stack HCI versus Windows Server

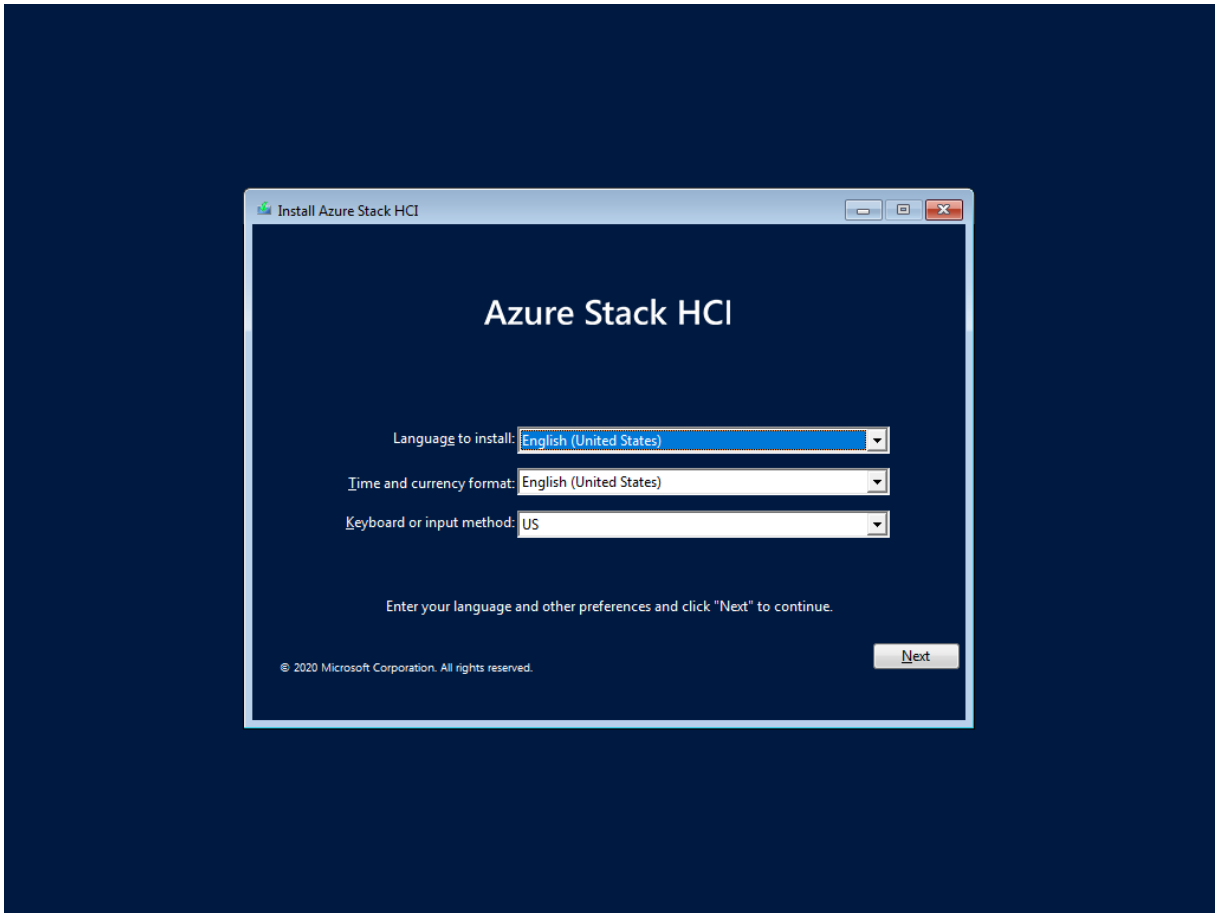
Microsoft introduced Storage Spaces Direct with Windows Server 2016. Since then, the OS has included all the components to set up a hyper-converged infrastructure. Based on the same technologies, the company announced Azure Stack HCI two years ago. What are the differences between the two solutions?

Storage Spaces Direct (S2D) is a virtual storage technology that pools the cluster nodes' local drives. This then serves as highly available storage for virtual machines. The Hyper-V cluster thus provides compute resources, (virtual) networks, and storage.

The same also applies to Azure Stack HCI, which stands for *Azure Stack hyperconverged infrastructure*. It essentially combines the same building blocks as Windows Server 2019 to set up hyperconverged systems.

Azure Stack OS for hosts only

It includes an operating system based on Windows Server, which, however, is sold under the name *Azure Stack HCI*. It is limited to the role of a host OS and may only be installed on bare metal, not in virtual machines.

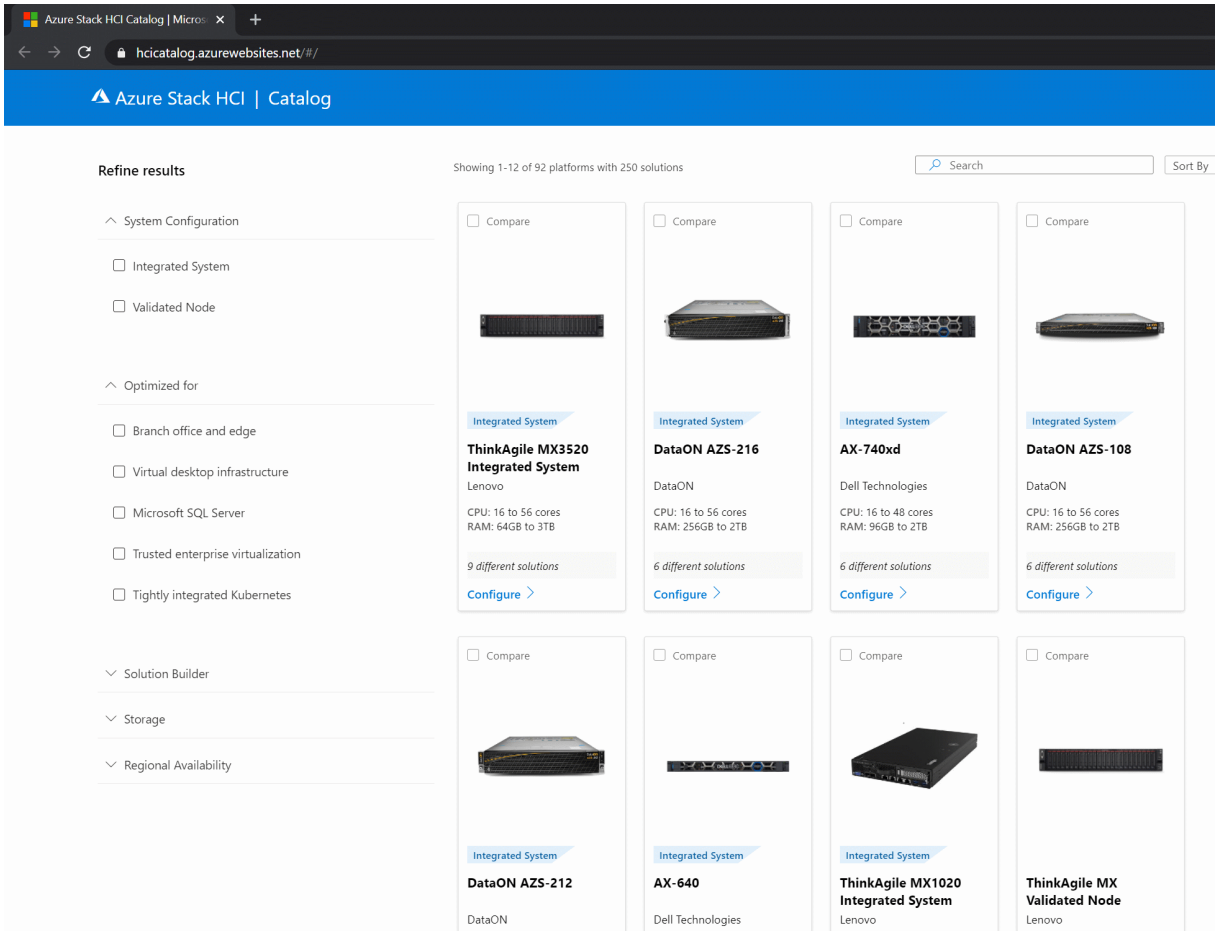


Azure Stack HCI is based on a customized Windows Server Core

Accordingly, it only has the roles that it needs for this task; first and foremost, it includes Hyper-V, the cluster service, and S2D. It also doesn't offer a desktop experience, so it is ultimately something in the middle between the free Hyper-V server and Server Core.

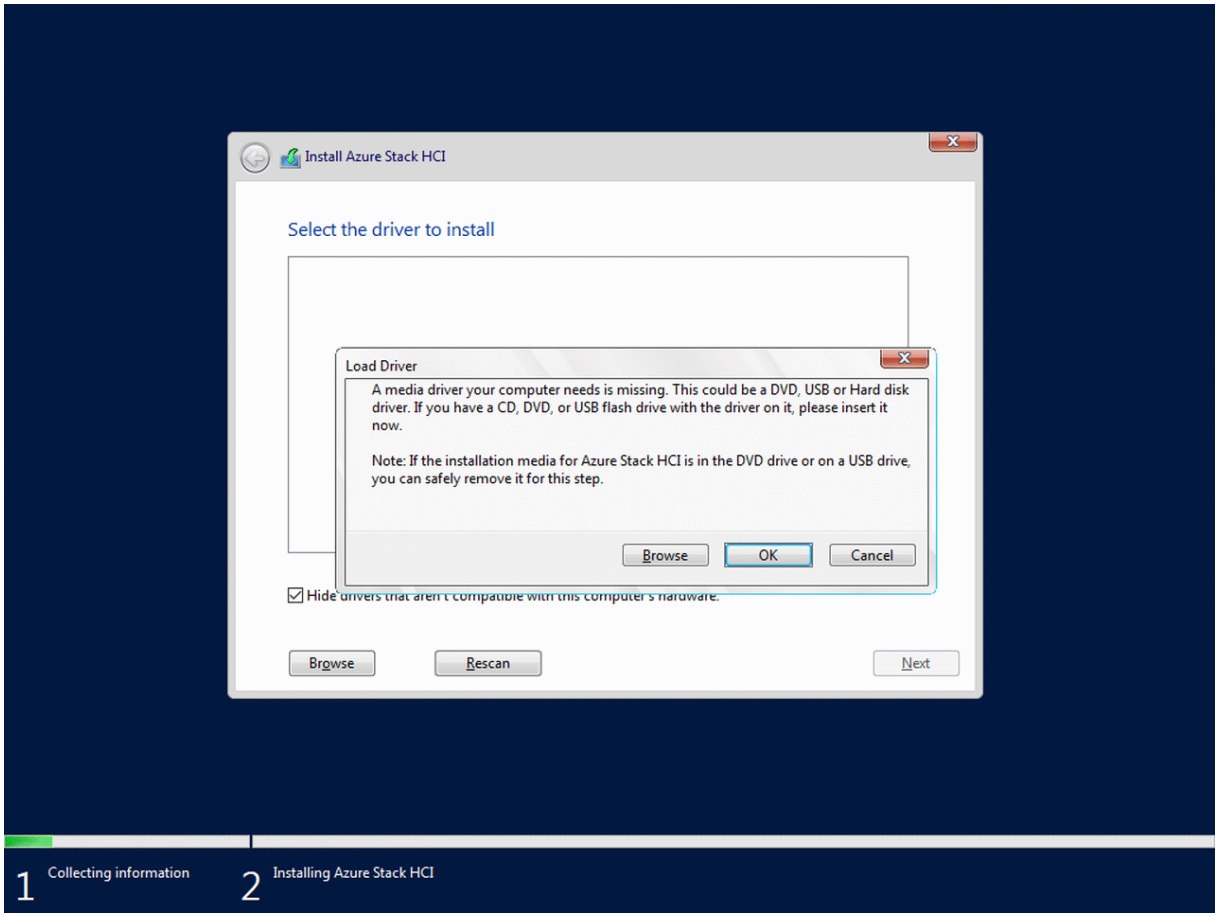
Own certification program

A key difference from Windows Server is that the hardware is subject to more stringent requirements, and the "Certified for Windows Server 2019" logo isn't enough. Systems that pass Microsoft's validation can be found in the Azure Stack HCI Catalog.



The Azure Stack HCI Catalog contains a number of certified complete systems

The fact that Azure Stack HCI only supports a few hand-picked components out of the box is evident, for example, when you want to install the operating system in a VMware Workstation VM for evaluation. There is no driver on the installation medium for the virtual SCSI controllers and NICs that are most commonly used there, whereas Windows Server can be set up in this context without any problems.



The Azure Stack HCI driver set is limited to a relatively small number of supported components

With the restriction on a manageable number of components and certified complete systems, Microsoft is now pursuing an approach similar to that of VMware or Nutanix for hyperconverged systems. Since HCI clusters must consist of largely identical computers, an inferior driver would have far-reaching consequences for the entire infrastructure and a number of applications.

Windows Server cost advantage

The licensing conditions for Azure Stack HCI are also similar to those of the competition. The operating system can only be used as a host OS and has to be purchased via a subscription billed to the Azure account. This currently costs 10 USD per compute core per month; hence, for example, a dual CPU machine with 16 cores would add up to 1920 USD per year.

Windows Server Datacenter Edition, on the other hand, contains all the components required for setting up a hyperconverged infrastructure in the host OS and authorizes the operating system to run in an unlimited number of VMs.

Therefore, it is often difficult for IT departments to justify spending additional money on pure infrastructure, for example, by deploying VMware vSphere. The finance and controlling department can then argue that similar functions are already included in Windows Server, whose datacenter license is required for the VMs anyway.

This conflict now also arises in the decision to buy Azure Stack HCI because there is usually no way around an additional Windows Server Datacenter for the VMs.

Features exclusive to Azure Stack HCI

It is easy to predict that Microsoft will prefer this variant and equip it with exclusive features. This includes, for example, that Azure Stack HCI continuously receives new features, while the LTSC version of Windows Server only gets an update about every three years.

You could also get the short update cycles through Windows Server in the semiannual channel (SAC), but Microsoft doesn't recommend it for infrastructure services, such as running virtual machines.

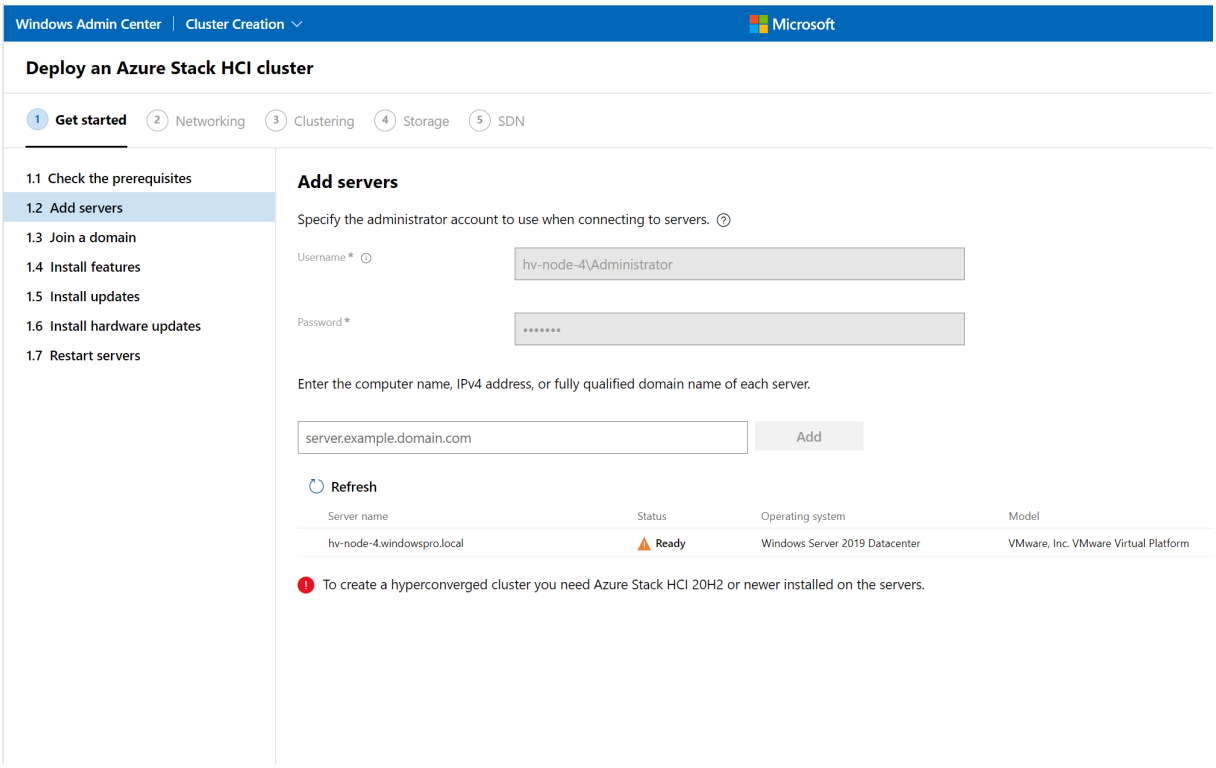
The features currently reserved for Azure Stack HCI include the ability to set up a stretched cluster across two sites for disaster recovery, built-in driver and firmware updates, and significantly faster S2D resync, such as when disks need to be replaced.

WAC workflow for Azure Stack HCI only

In addition to the operating system, which includes S2D, the Windows Admin Center (WAC) is also part of the Azure Stack HCI package. The Cluster Manager contains a wizard for setting up a hyperconverged cluster that covers the entire workflow.

Microsoft partners who offer certified complete systems for Azure Stack HCI are required to preinstall the operating system. This is sufficient as a starting point to configure the HCI cluster with the WAC.

Although there are no fundamental technical differences between Azure Stack HCI and Windows Server with S2D, the WAC wizard refuses to configure a hyperconverged cluster based on Windows Server 2019.



The wizard in WAC's Cluster Manager sets up hyperconverged clusters based on Azure Stack HCI only

Accordingly, admins still have to rely on a mix of failover cluster managers and PowerShell for this task, which requires some manual work. If they also deploy a custom-built system, they must check the Windows Server Catalog for each component to see if it is suitable for S2D.

Overall, with the implementation of Azure Stack HCI, Microsoft is following a course that VMware, Nutanix, and smaller providers like StarWind have been following for some time: partners provide certified systems that are largely standardized and can be delivered to the customer as turnkey appliances if required.

The classic Windows model, where users or partners implement solutions on site based on very heterogeneous hardware, will be obsolete for HCI in the foreseeable future.

Comparison of editions and features

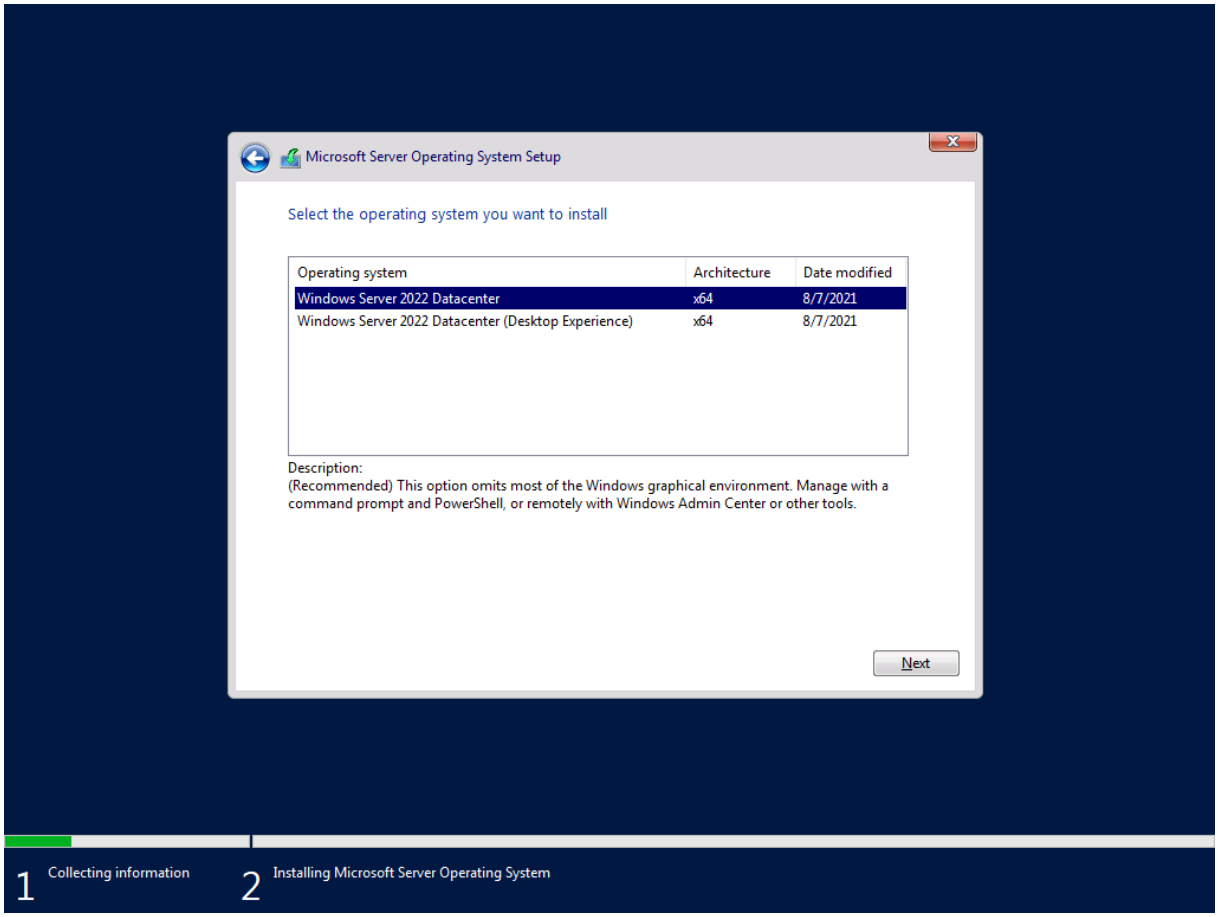
Windows Server 2022 will be available in two main editions: *Standard* and *Datacenter*. In addition, Microsoft will introduce a new edition for Azure. Windows Server Essentials will no longer be a separate SKU, and there is a new OS for hyperconverged systems.

In every edition, the name of Windows Server 2022 will change because the suffix "LTSC" has been dropped by Microsoft. This acronym stands for *Long-Term Service Channel* and helped to differentiate this version of the operating system from the *Semi-Annual Channel* (SAC).

Like its predecessors in the LTSC, Windows Server 2022 will receive 10 years of support. As usual, this period is divided into five years of mainstream support and five years of extended support.

Desktop versus Core

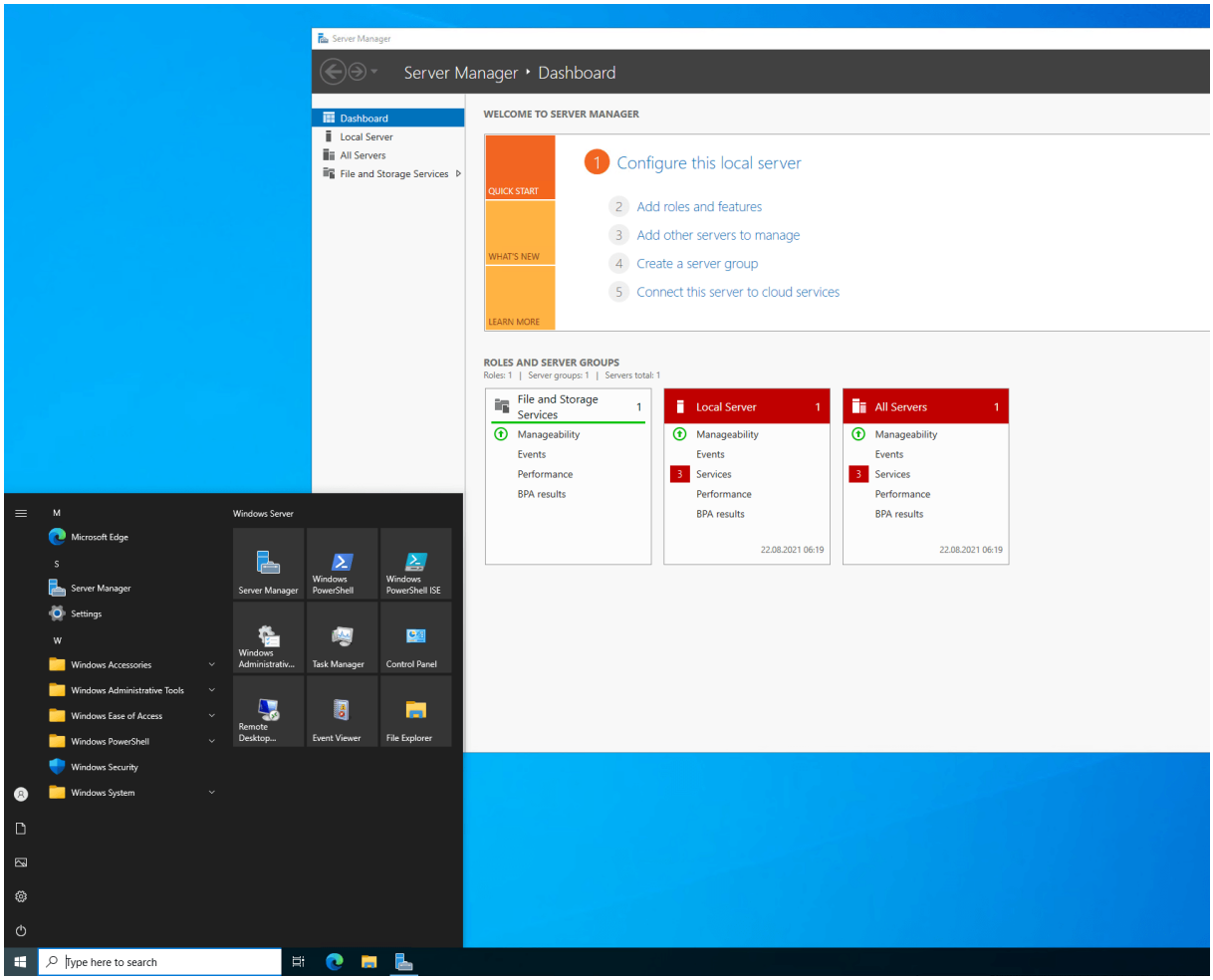
The two installation options, Desktop Experience and Server Core, also remain unchanged. Microsoft recommends using the slim version without the GUI for most infrastructure services; it is also the default in the setup.



Server Core is the default installation option in the Windows Server 2022 setup.

To achieve better compatibility with GUI tools for system administration, you can add Core App Compatibility as a feature on demand in Server 2022.

The installation of the Desktop Experience is primarily intended for RD Session Hosts. Its desktop shows that Windows Server 2022 is not a counterpart to Windows 11 but to Windows 10 21H2, and thus still includes the old Start menu.



Windows Server 2022 offers the familiar Windows 10 desktop.

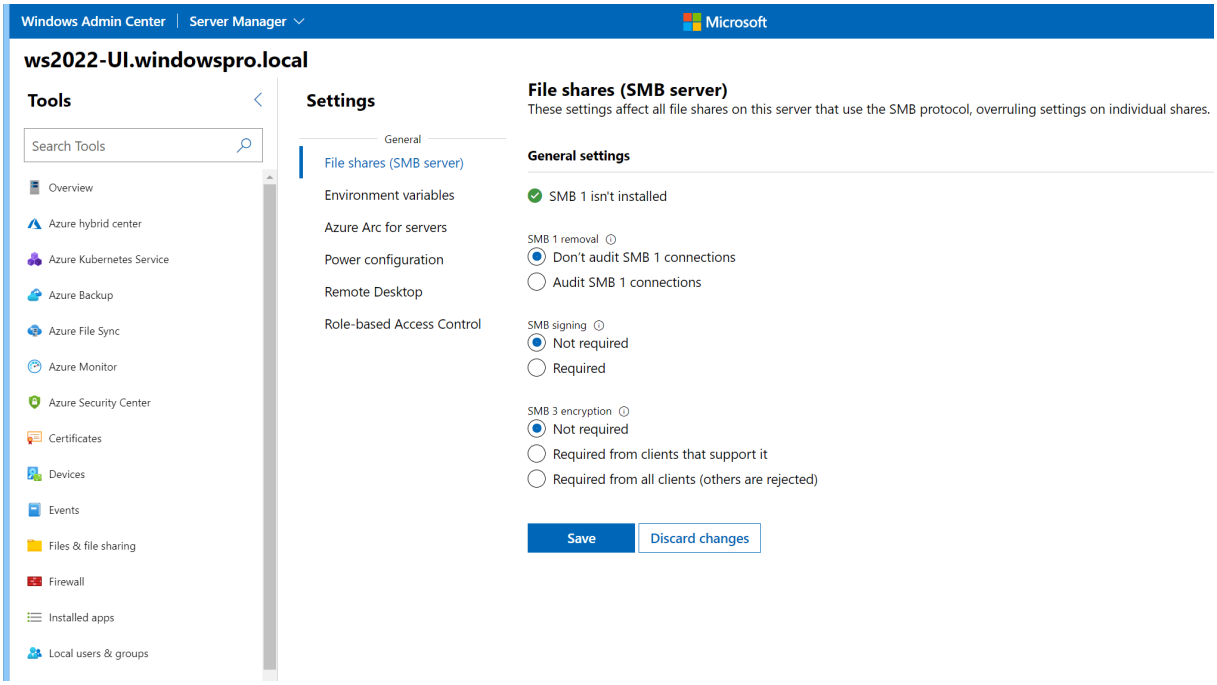
Three editions for Server 2022

Since version 2012, Microsoft has offered the Server OS in two main editions, which differ primarily in terms of virtualization rights. Since Server 2016, however, the Datacenter Edition has received exclusive features that are missing in the standard edition. These include Shielded VMs, Storage Replica, and software-defined storage with Storage Spaces Direct.

This difference remains in the 2022 version, where the Standard Edition is limited to two virtual instances and only includes a stripped-down version of Storage Replica (limited to one partnership with a maximum of 2 TB volumes).

The two editions are now joined by a third, called *Windows Server 2022 Datacenter: Azure Edition*. As the name suggests, this is intended only for running in the Microsoft cloud and on Azure Stack HCI.

It has two exclusive features in its debut, which are not available on-prem, at least not for the time being. These are hotpatching, which allows for installing updates without rebooting the computer, and SMB over QUIC as an alternative to VPNs.



In the SMB settings of the Admin Center, the section on SMB over QUIC is missing when connecting to an on-prem server 2022.

The Azure edition is otherwise functionally identical to the Datacenter Edition, even if some features don't seem to offer much benefit in an Azure VM. This applies to Storage Spaces Direct, for example, and SMB Direct and SMB over RDMA are not supported in Azure VMs anyway.

Essentials Edition is no longer a separate product

For Windows Server 2019, Microsoft still offered the Essentials edition, which is aimed at small businesses with a maximum of 25 users. In this version, however, Microsoft removed special functions, such as the dashboard, client backup, and *access anywhere*.

At the same time, the manufacturer stripped out the *Windows Server Essentials Experience* role in the main editions. This is also missing in the Standard and Datacenter editions of Server 2022.

Despite expectations, the smallest version of Windows Server will be available again in the 2022 version. However, it is no longer a product on its own; rather, it is a Standard Edition with an alternative license.

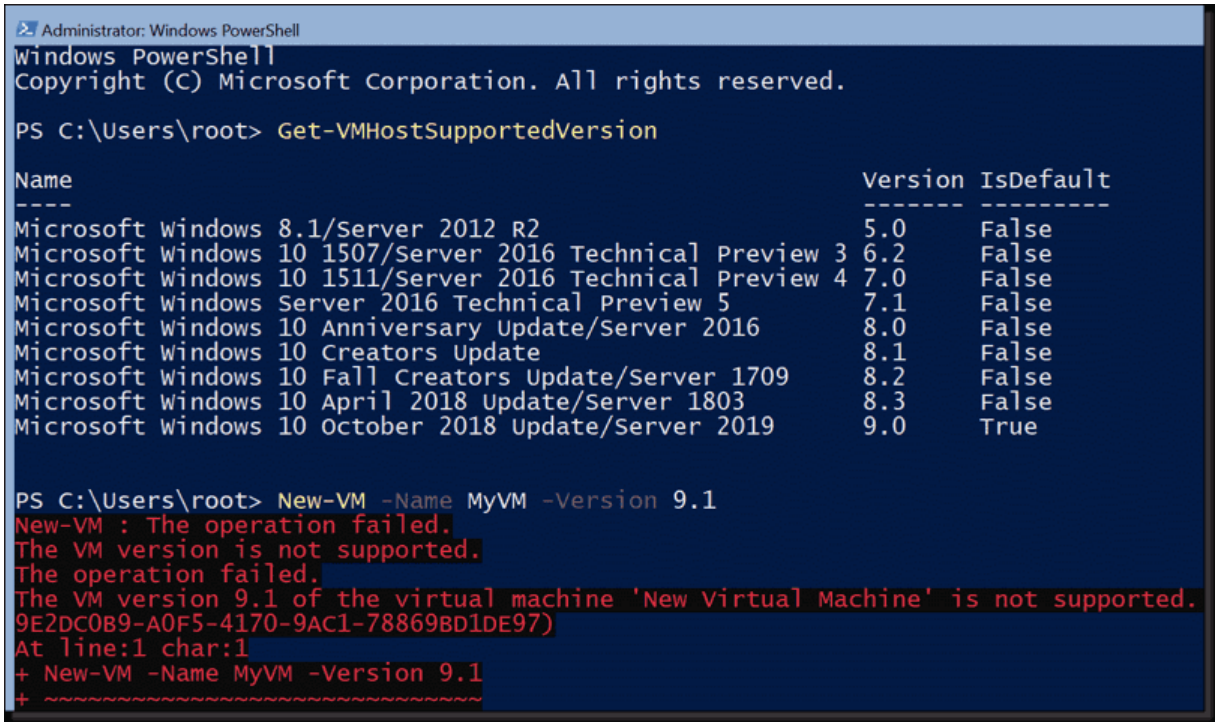
As before, this includes a number of restrictions, for example, a maximum of 25 users and 50 devices. In addition, Server 2022 limits the Essentials Edition to one CPU with a maximum of 10 cores.

No free Hyper-V Server 2022

Until now, with each new version of Windows Server LTSC, Microsoft released a corresponding version of the free Hyper-V Server. However, this will no longer be the case with Windows Server 2022. Instead, Microsoft now directs users to Azure Stack HCI.

The free Hyper-V server is a slimmed-down server core that can run the Hyper-V role and offers a few other infrastructure functions, such as clustering or storage connectivity.

The license is limited to a bare metal installation and does not include rights to run Windows Server in the VMs.



Hyper-V Server 2019 supports VM Configuration Version 9.0 at most

Due to the license terms, Hyper-V Server is primarily suited for running Linux in VMs, such as for firewalls, web servers, or management tools. Another main application is desktop virtualization, where Windows 10 runs as a guest OS in virtual machines.

The vendor recommends switching to Azure Stack HCI instead. Unlike the free hypervisor, it also includes features for provisioning software-defined storage, i.e., primarily Storage Spaces Direct. And unlike Hyper-V Server, this OS is not free, but requires a subscription that costs $10 per CPU core per month.

Another difference from the free hypervisor is that Azure Stack HCI cannot be used to set up standalone hosts. Rather, it requires a cluster with at least two nodes.

Azure Stack HCI as successor for Windows Server SAC

Besides Windows Server LTSC with 10 years of support, there were also semi-annual updates of the operating system since version 1709. However, before the release of Server 2022, Microsoft announced the end of the Semi-annual Channel SAC.

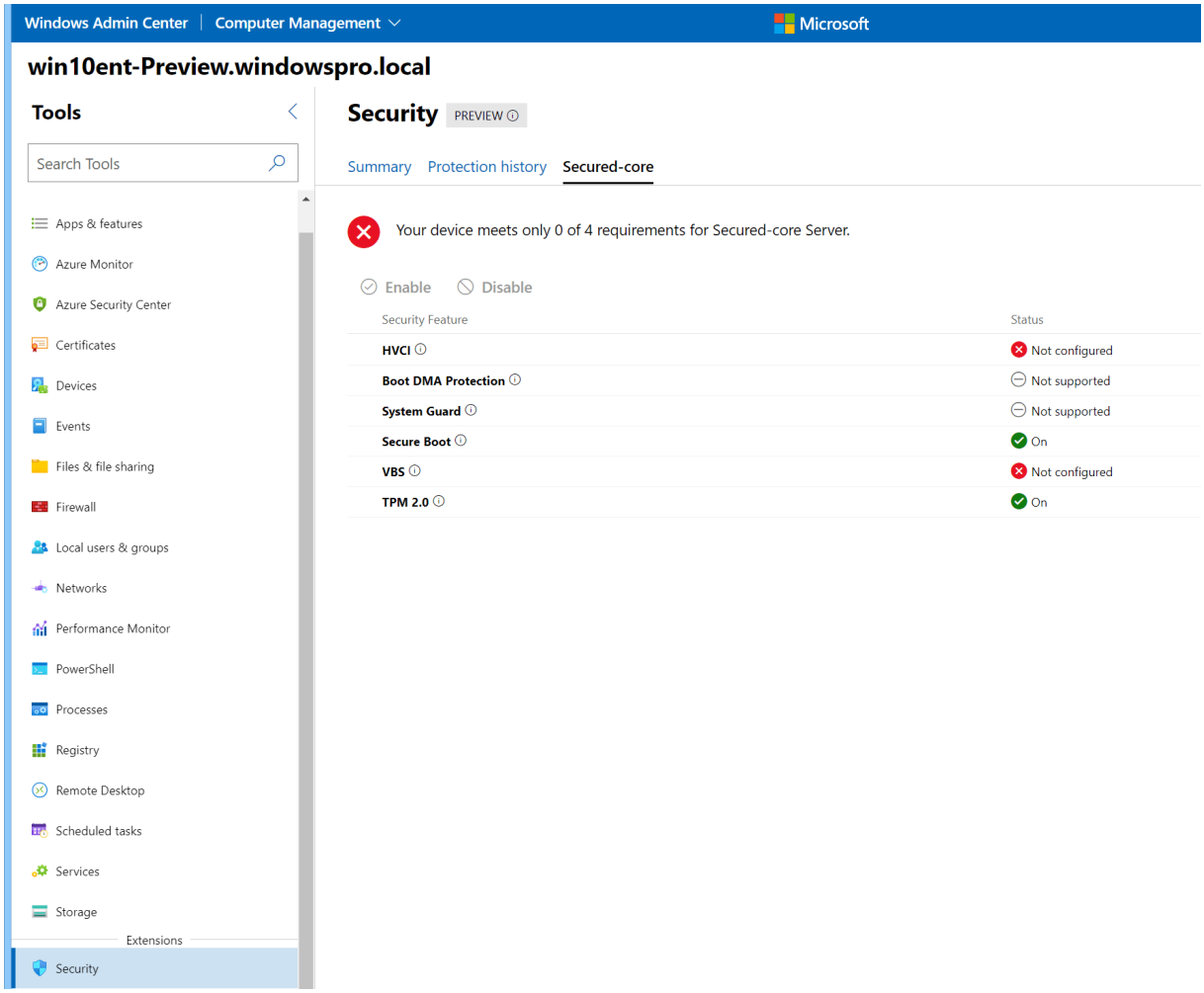
With version 1803, Microsoft repositioned the SAC versions as a container hosts only and discouraged its use for infrastructure services, even though most of the roles needed for that purpose remained on board.

SAC's role as a container host will now be taken over by Azure Stack HCI. This does not come as a complete surprise, because the manufacturer already announced the porting of the Azure Kubernetes service to this OS last fall.

The container feature is also present in Windows Server 2022, but orchestrating containers using Kubernetes is only possible after manually setting up a corresponding infrastructure. In contrast, Windows Admin Center supports the deployment of Kubernetes clusters on Azure Stack HCI since version 2103.2.

The most important new features

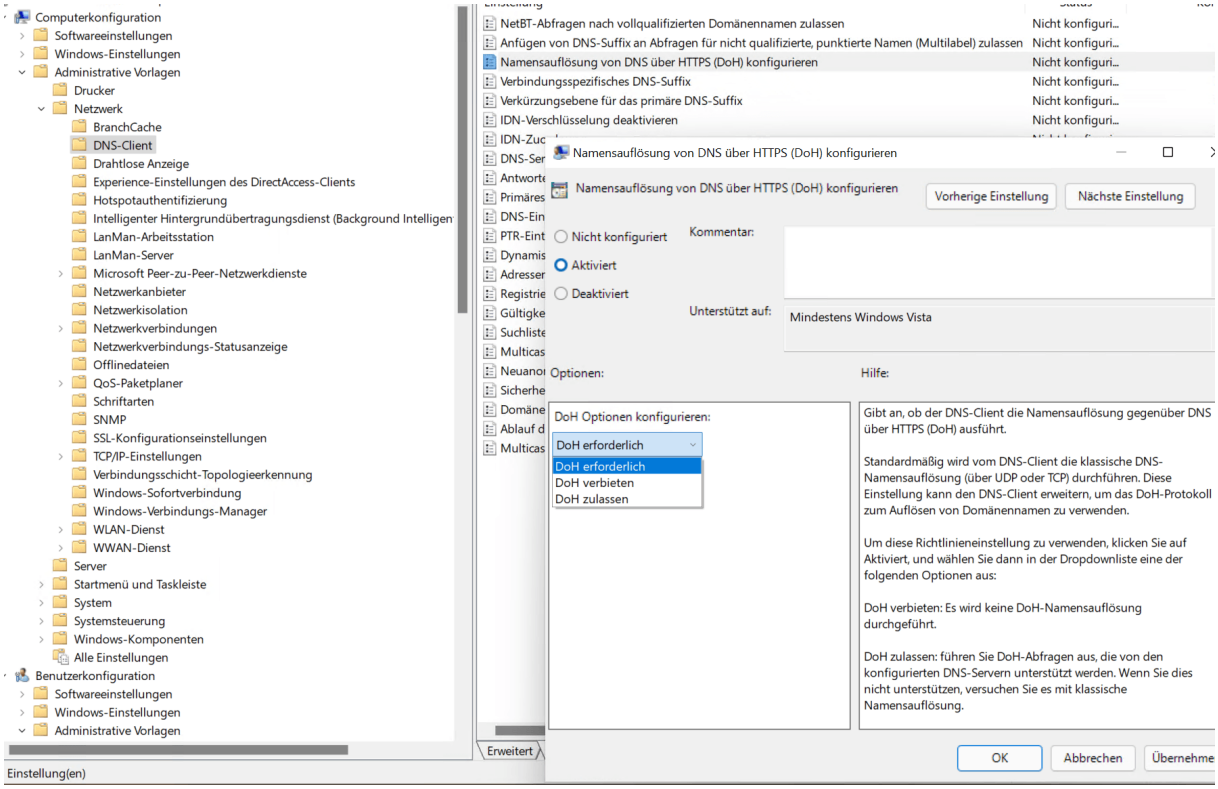
In the preview phase, Microsoft particularly emphasized the new features for improving security. These implement the concept of Secured-core Server, which is based on a combination of hardware (TPM), firmware, and drivers. The related features can be configured in the Windows Admin Center (WAC).



The functions that Microsoft combines for Secured-core Server can be configured via the WAC

As a further innovation, the manufacturer announced that HTTPS and TLS 1.3 would be enabled by default. Also, part of the new OS is Secure DNS (DNS over HTTPS), which will be included in Windows 10 21H2 and Windows 11 as well.

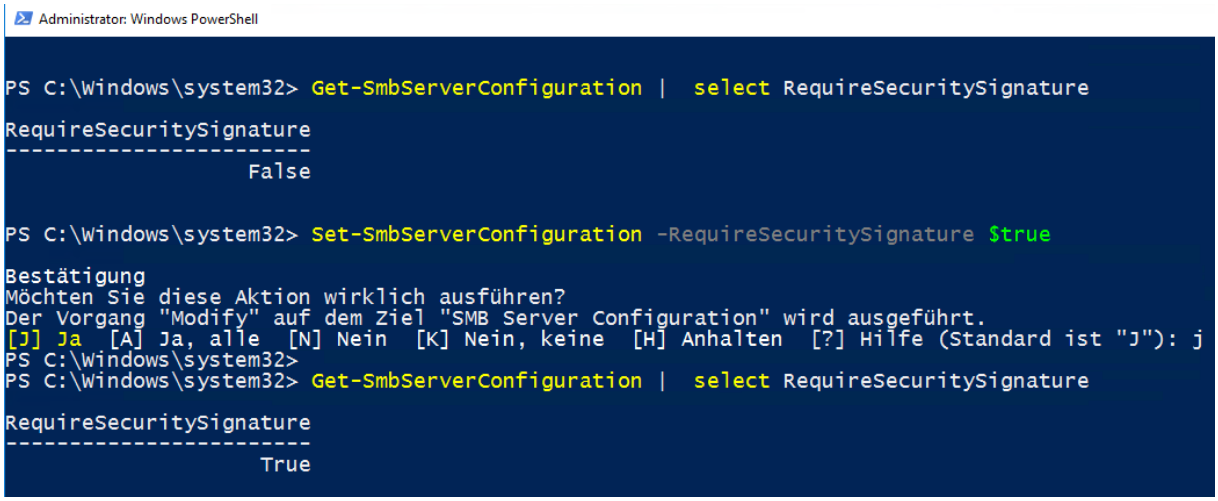
The current group policy templates already ship with a setting to configure the feature.



Group policy for the configuration of DNS over HTTPS

Enhancements to Server Message Block

Server 2022 also improves signing and encryption for the SMB protocol, where two more secure algorithms are now available (AES-256-GCM and AES-256-CCM). AES-128 will still be supported for backward compatibility.

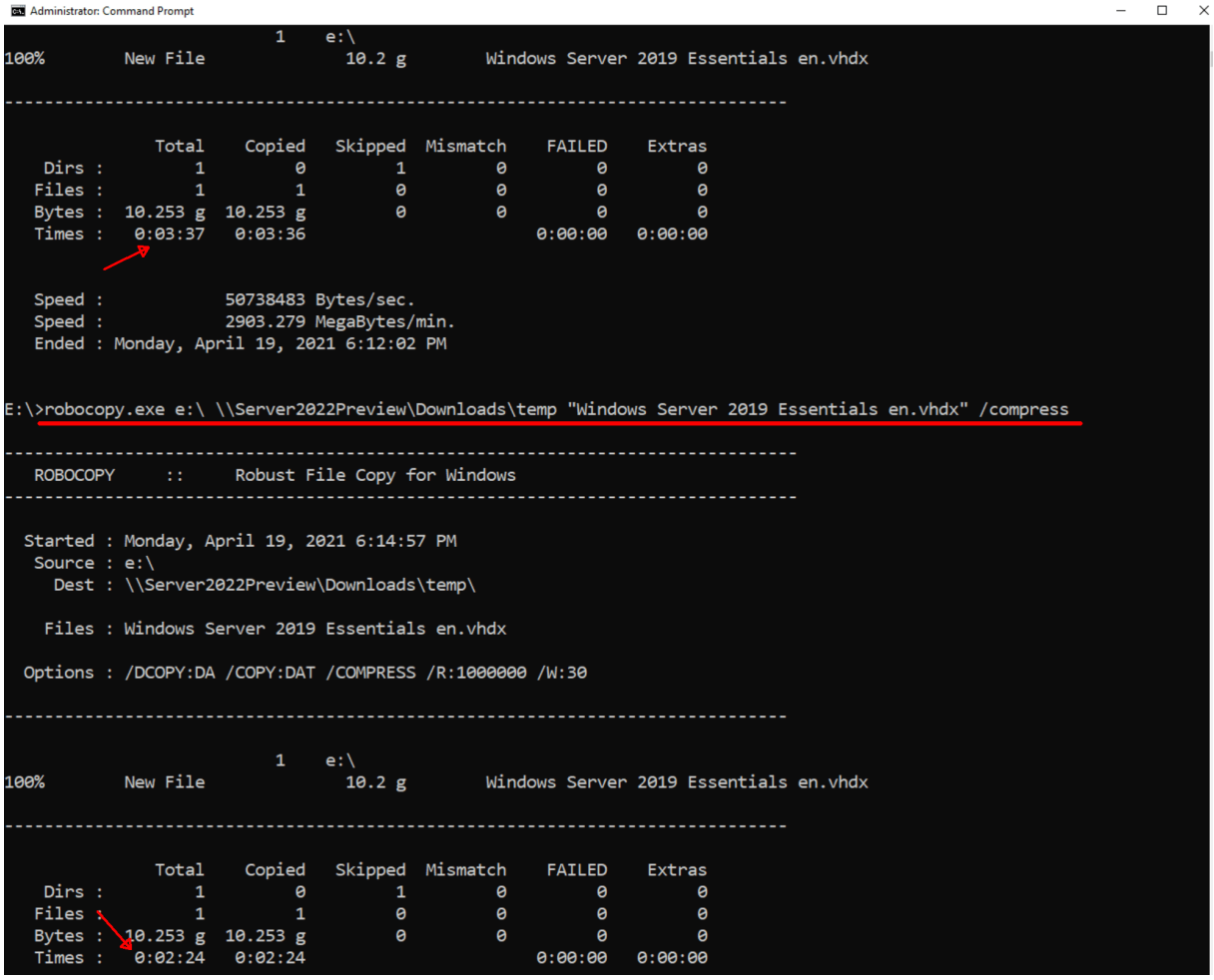


Signatures for SMB connections can now be generated using the AES-256 algorithms

In addition, SMB encryption and signing can be configured separately for communication between the nodes of a cluster ("east–west"). This affects both Cluster Shared Volumes (CSV) and Storage Spaces Direct.

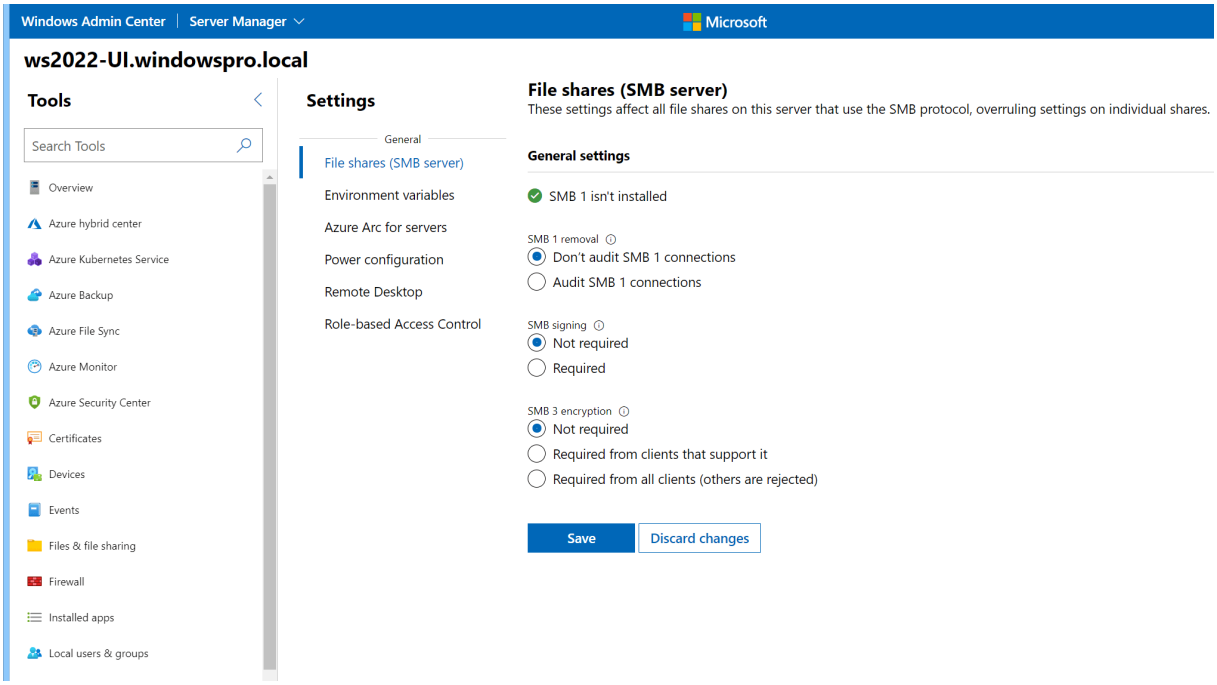
These security features are now also compatible with SMB Direct, whereas in previous versions of Windows Server, they caused performance degradation with RDMA NICs.

Another new feature is the ability to compress SMB traffic. In Windows 10, since release 20H2, SMB compression could be enabled for xcopy and robocopy with separate switches for these programs. In Server 2022, this feature can now be enabled for file shares in general via either the Windows Admin Center or PowerShell.



SMB compression is no longer limited to xcopy and robocopy in Server 2022

Another new feature for accessing file shares is support for SMB over QUIC. The QUIC protocol can be used as an alternative to TCP, and in combination with TLS 1.3, it can also be used to replace VPNs. However, this feature is only available in Windows Server 2022 Datacenter: Azure Edition.



The SMB configuration section of Windows Admin Center doesn't contain settings for SMB over QUIC when connected to Server 2022 Datacenter

Strangely, the call to *Get-SmbServerConfiguration* returns the value $true for the property EnableSMBQUIC, even in the Datacenter Edition.

With hotpatching, Microsoft reserves another interesting new feature for Azure. It allows updates to be applied without having to restart the server. Windows Server 2022 uses the Azure service *Automanage* for this.

In addition to new options for hybrid configurations (such as managing on-prem servers via Azure Arc) and expanded support for containers, Windows Server 2022 also offers some progress that is more in line with the conventional use of the system.

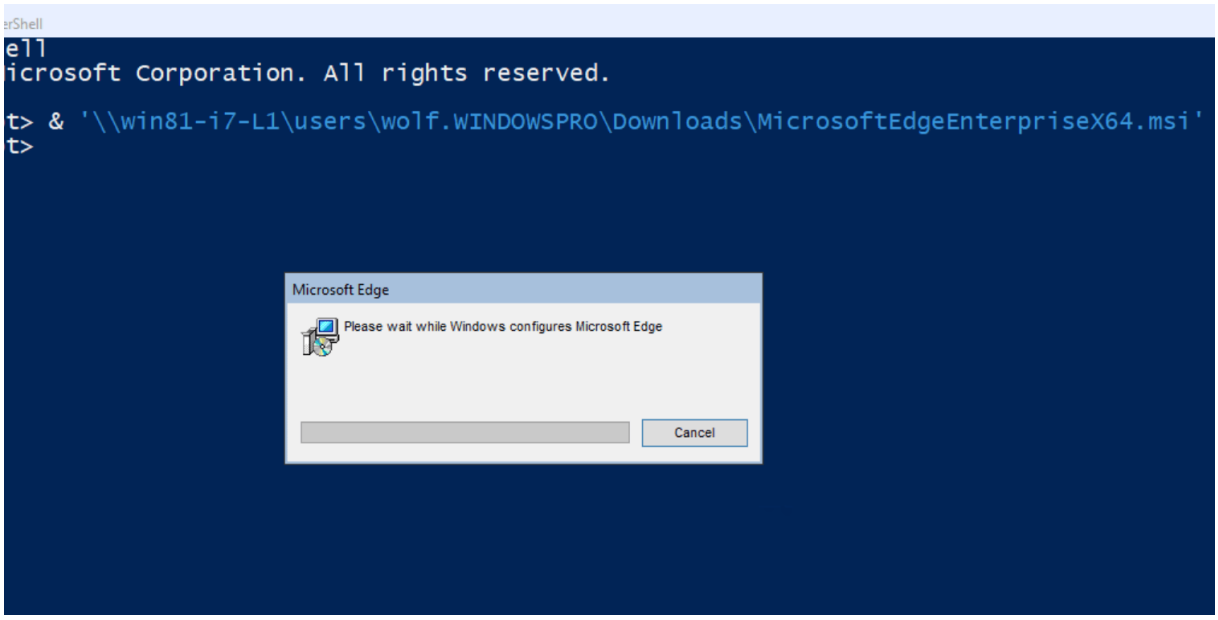
Nested virtualization for AMD

This includes support for nested virtualization on AMD processors, which has been available for Intel CPUs since Windows Server 2016.

In terms of CPU support, version 2022 can also take advantage of Intel Ice Lake processors. On this platform, it can address up to 48 TB of RAM and provide up to 2048 logical processor cores.

Edge is included in Server Core

With the end of support for Internet Explorer on June 15, 2022, Microsoft Edge will replace the outdated browser on the server as well. Edge is thus included in Server 2022 and can also be used with the Server Core installation option. This configuration has already been supported, but there were some hurdles for manual installation.



Microsoft supported the installation of Edge under Server 2019 Core, and now the browser is included with 2022

Improvement for Storage Spaces Direct

For running hyperconverged infrastructures, all future innovations will go into Azure Stack HCI; however, Windows Server will continue to benefit from improvements to existing features.

This is now reflected in Server 2022, which still lacks advanced features such as stretched clusters, but has been given a new repair option for Storage Spaces Direct ("Adjustable Storage Repair Speed"). Admins can use this to control how many resources they want to allocate for repairing data copies or active workloads.

Other storage innovations

While Storage Spaces Direct combines the local storage of the cluster nodes into a storage pool, Storage Spaces only manages the drives of a single server. This feature also received an update in Windows Server 2022. It now offers storage tiering, which can use fast media, such as SSDs or NVMe, for caching.

Finally, in Server 2022, Microsoft has extended the Storage Migration Service introduced with the 2019 release. It was originally intended to move file shares from legacy systems to a newer Windows Server. It now supports failover clusters, Samba servers, and NetApp FAS as sources, and it also migrates local users and groups.

Overall, Windows Server 2022 does not introduce any new roles or features, but it does improve a number of existing functions and protocols. Some of the new features will benefit server security.

Unfortunately, the on-prem server is deprived of improvements in genuine OS features such as hotpatching or SMB over QUIC. To get them, you have to run Server 2022 in Azure.

Secured Core

Microsoft has implemented the security concept Secured Core in Windows Server 2022 and Azure Stack HCI. It is intended not only to protect the boot process but also to thwart attacks on vital system components. Some features, such as HVCI or DMA protection, must be explicitly activated first.

Secured Core combines hardware, firmware, and OS features to ensure the integrity of the system during startup and runtime. The hardware requirements include a CPU with activated virtualization extensions (Intel VT, AMD-V), UEFI with Secure Boot, and TPM 2.0.

All modern servers should easily meet these requirements, especially if they have been certified for Azure Stack HCI or Windows Server. The hardware acts as root-of-trust, with the TPM storing the keys needed to verify all components during the system startup.

The Secured Core security concept is based on features of hardware, firmware, and software

During the early boot phase, the firmware's secure boot routine ensures that a legitimate boot loader is used and not a rootkit or bootkit.

System Guard monitors the boot process

However, in the next phase, Windows does not rely on UEFI integrity, but rather uses System Guard (comprising Secure Launch and System Management Mode (SMM) Protection) to ensure that the system is in a trustworthy state.

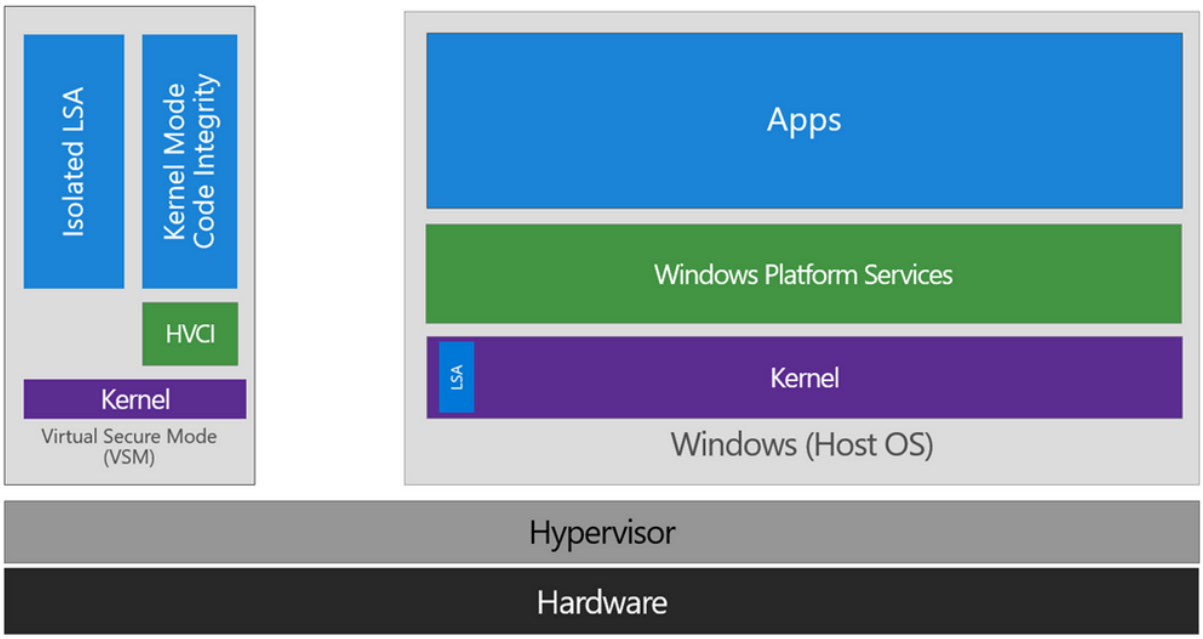
Another mechanism is Kernel DMA Protection, which is intended to prevent attackers from gaining access to the computer's RAM via external PCI devices and thus stealing passwords or injecting malware.

Devices whose drivers are not compatible with DMA remapping are prevented from direct memory access by default until an authorized user is logged onto the system.

HVCI as a VBS feature

Finally, Secured Core relies on virtualization-based security (VBS), which uses the hypervisor to isolate critical functions from the rest of the operating system, thus protecting them from malware infection.

VBS runs a separate secure kernel at a higher trust level than the actual Windows system kernel. Therefore, the OS kernel and user-mode processes cannot access the protected functions and data directly.



VBS uses a kernel shielded by the hypervisor to protect critical OS functions

One VBS feature is hypervisor-protected code integrity (HVCI). It monitors kernel code and only allows it to be executed if it has been verified as legitimate. Without it, malware in the context of the kernel would have access to all of the PC's memory. HVCI requires compatible drivers, and their suitability can be checked using the DGReadiness tool.

Configuring Secured Core

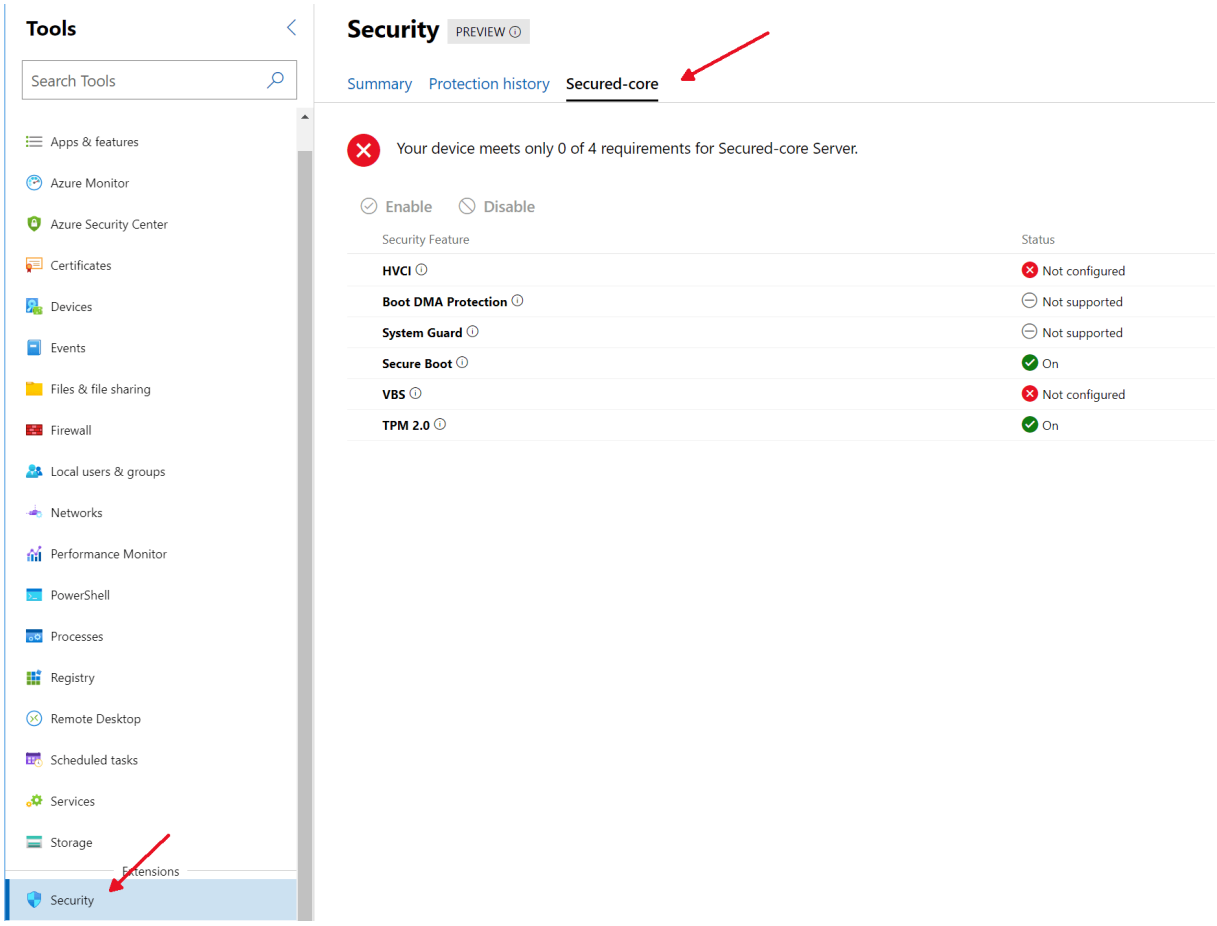
Some components need to be present in the system, such as the aforementioned TPM 2.0, the UEFI firmware, or a modern processor. Features such as Secure Boot are already enabled by default on most machines, as are CPU extensions for virtualization.

If you want to quickly find out if Secure Boot is enabled, execute the following command in a PowerShell session using elevated privileges:

```
Confirm-SecureBootUEFI
```

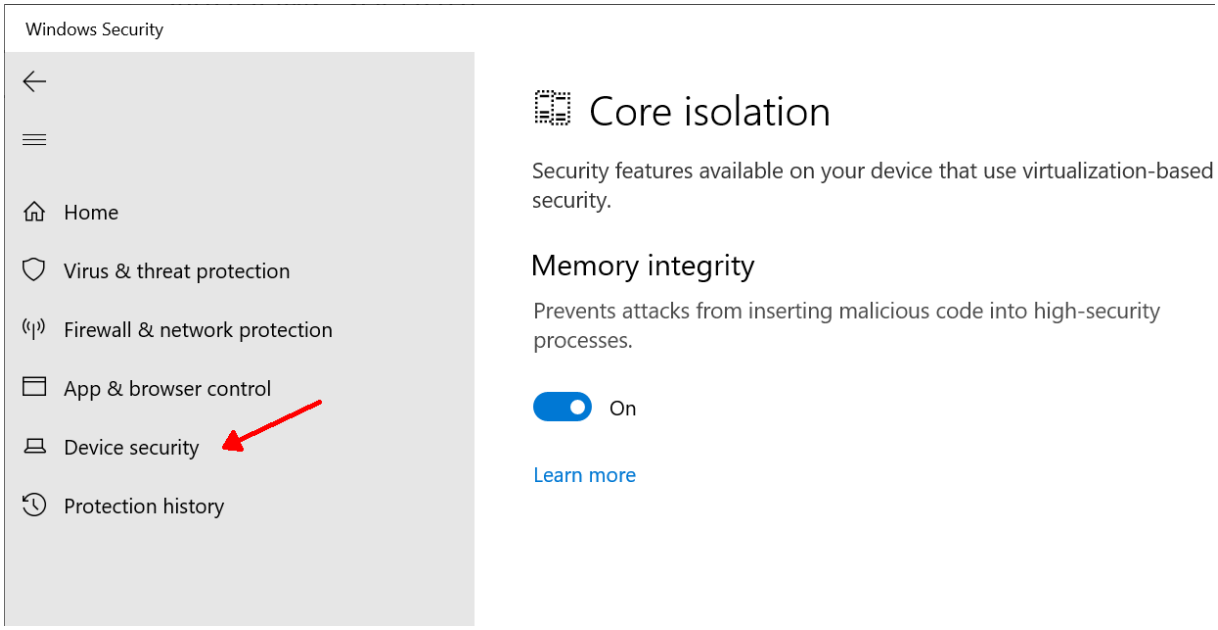
Information about the virtualization extensions can be found in the Task Manager under *Performance* or via msinfo32.exe.

The Windows Admin Center (WAC) can be used to check the status of all Secured Core components at a glance. The *Security* extension has its own tab for this purpose.



Overview of the status of Secured Core in Windows Admin Center

You can enable HVCI via the app settings under *Device security*; Secure Boot is configured in the UEFI settings anyway. The WAC also allows changing the status of the VBS-based features.



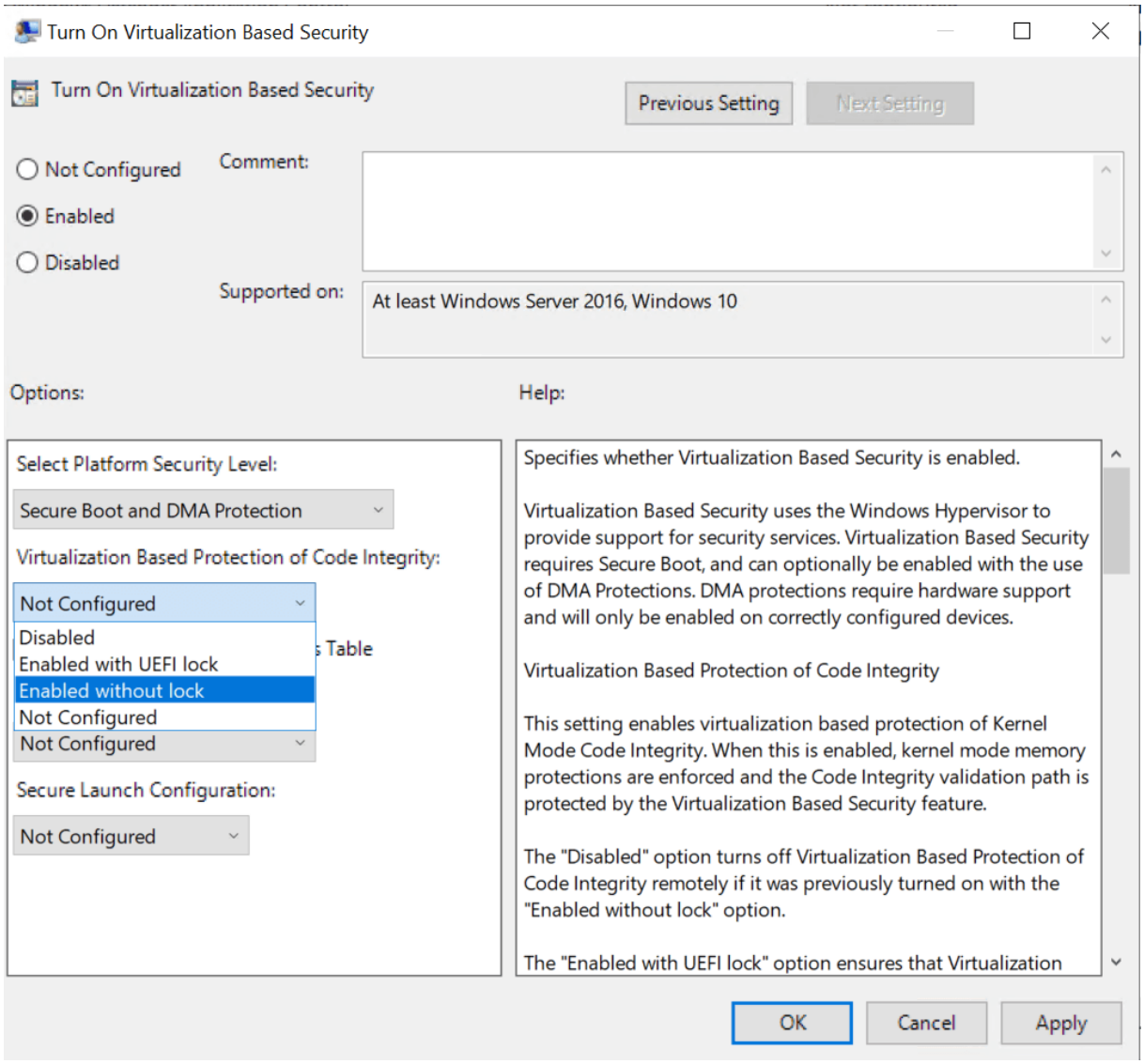
Interactive configuration of HVCI in the Settings app

Controlling VBS via Group Policies

Since Secured Core is not just a concept of Windows Server, but is also present in the client OS, group policies will be the preferred tool to centrally manage the relevant security functions.

The main setting for this can be found under *Computer Configuration > Policies > Administrative Templates > System > Device Guard* and is called *Turn On Virtualization Based Security*.

When enabled, four options can be configured via dropdown menus. The first of these is Secure Boot, which can be supplemented with DMA protection on compatible PCs.



These settings can be used to configure three features for Secured Core

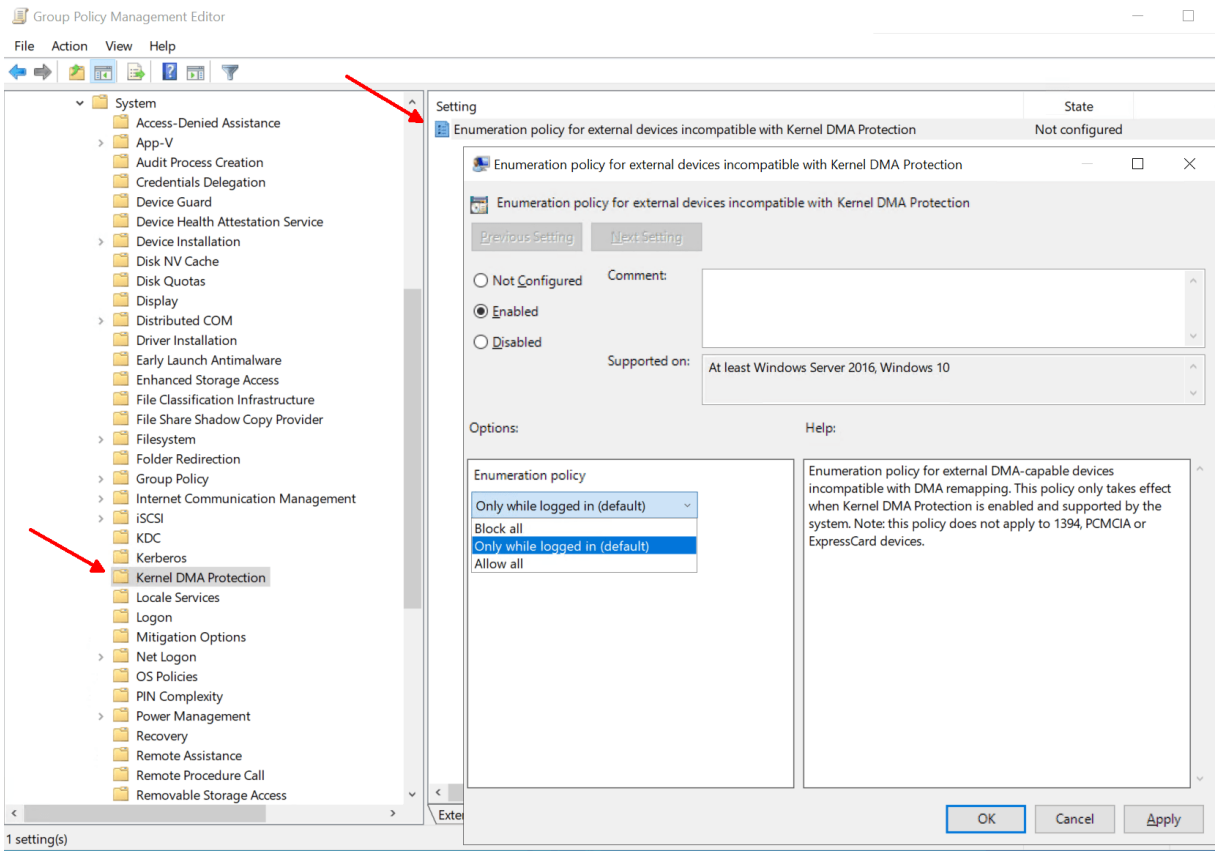
Another menu is used to configure HVCI, for which four options are available. *Disabled* deactivates code integrity, even if it was enabled interactively via the *Settings* app. On the other hand, *Not Configured* retains the current state as it is.

Enabled with UEFI lock causes the setting to be permanently stored in the firmware and cannot be removed by resetting the group policy. Rather, it must be physically removed from each PC. *Enabled without lock*, on the other hand, allows the setting to be changed via GPO.

Activating *Secure Launch Configuration* activates the System Guard function.

Another group policy can be used to customize DMA protection. By default, it blocks, for example, the connection of Thunderbolt devices that are not compatible with DMA remapping if no user is logged on or the screen is locked.

Under *Computer Configuration > Policies > Administrative Templates > System > Kernel DMA Protection*, you can change this default behavior to generally block or unblock these devices.



Define the behavior of DMA protection for devices that do not support DMA remapping

Secured Core in a VM

If you apply the described settings to a virtual machine, you can use VBS in general and HVCI in particular. The prerequisite for this, however, is that nested virtualization has been activated for the VM; otherwise, the hypervisor in the guest OS is not available.

System Guard and Boot DMA Protection, however, cannot be used. The WAC identifies both as *not supported*. For Secure Boot, you need UEFI, which is available only in a generation 2 VM.

The security settings of a VM can be queried in PowerShell with

Get-VMSecurity -VMName "Name-of-VM"

It will also display a parameter called *Virtualization¬Based¬Security¬OptOut*, which you can set to $true with Set-VMSecurity in case of compatibility problems. These occur, for example, when you try to connect a virtual Fibre Channel adapter.

Migration to Windows Server 2022: WSMT versus in-place updates

When organizations decide to move services in one Windows Server version to a newer Windows Server version, there are a few options. Businesses can perform an in-place upgrade of the current server to a more recent Windows Server version. There are also options for migrating roles and

services from one server to a newer server. The **Windows Server Migration Tools (WSMT)** serve this purpose.

Windows Server Migration Tools have been around quite a while. It is a Windows feature that provides access to specialized PowerShell cmdlets allowing automated migration of certain roles between a legacy server and a newer Windows Server operating system.

The Windows Server Migration Tools can migrate specific settings, including:

- Roles
- Features
- Shares
- Operating system configurations

The process to use Windows Server Migration Tools is generally the following:

1. Install WSMT on the destination server (the server that is the target of the roles, features, etc)
2. Copy the WSMT files to the source server
3. Export the roles, features, etc. from the source server to a destination folder
4. Import the roles, features, etc. to the destination server

Limitations of WSMT

While in concept, the Windows Server Migration Tools provide great functionality, in practice, it is limited in the scope of roles, features, settings, and other data that can be migrated from a legacy server to a destination. Note the following compatible roles, features, settings, and data:

Roles

- Active Directory Domain Services
- DNS
- DHCP Server
- File Services
- Print Services

Features

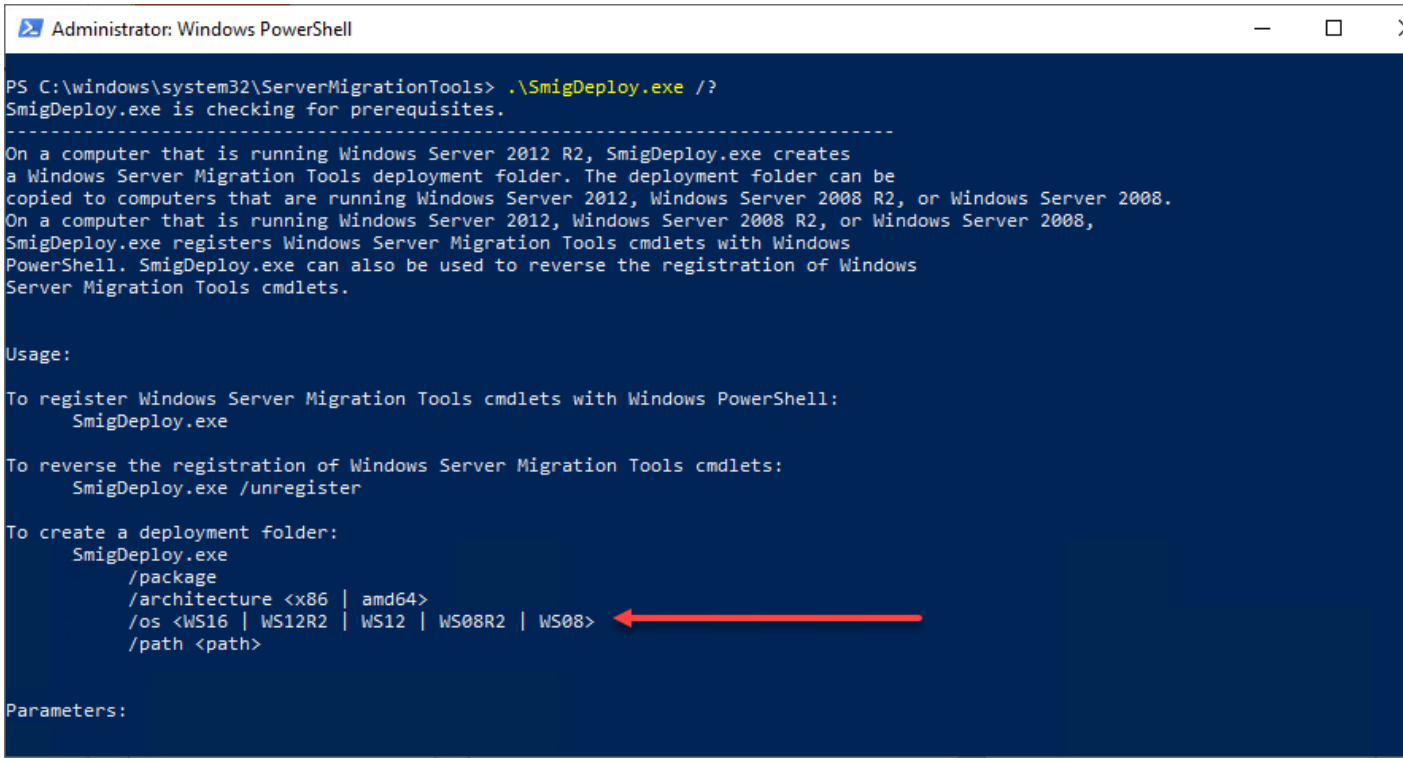
- BranchCache

Settings and Data

- Data and Shares
- IP Configuration
- Local Users and Groups

Additionally, if you look at the documentation for Windows Server Migration Tools, it is quite dated. It details scenarios of migrating roles and services up to Windows Server 2012 R2, which is now end of life. However, if you look in Windows Server 2022, the Windows Server Migration Tools feature is still available for installation.

The /OS switch which allows copying over the migration tools to a specific OS does have a switch that includes Windows Server 2016, so it is reasonable to assume it supports OS'es up to Windows Server 2016 as a source.



Supported operating systems to deploy the source SMIG files

Windows Server Migration Tools are still valid for specific roles, services, data, and configurations and can be a path to migrate the specific roles and services listed above. Just be aware of the potential for unsupported scenarios and buggy behavior that can be seen between different OS versions.

In-place upgrade vs. Windows Server Migration Tools

As mentioned at the outset, running an in-place upgrade is another common way to bring legacy servers up to current Windows Server versions. However, there can be challenges with in-place upgrades as well. These can include:

- **Hardware compatibility issues** – The hardware may not be compatible with the latest Windows Server versions
- **Driver issues** – Tying in closely with hardware compatibility, drivers can create issues during in-place upgrades
- **Unsupported software** – Legacy software that cannot be migrated to newer OS's can prevent an in-place upgrade
- **Multiple steps to arrive at the target Windows Server version** – The further back the source Windows Server OS is, the more likely it will be you will have to take multiple steps to get to the latest version. For instance, you cannot go directly from Windows Server 2008 R2 to Windows Server 2022. You have to go from Windows Server 2008 R2 to Windows Server 2012 R2 and then from Windows Server 2012 R2 to Windows Server 2022.
- **Time and maintenance windows** – The in-place upgrade could take a significant amount of time. Moving individual services and roles off a server can be more timely and, in many cases, works better.

Conclusion

This comparison is certainly going to be one that will be a different answer for different businesses depending on many factors. These factors include the roles and services needing to be migrated, the

difference in Windows Server versions between the source and destination servers (how many versions between), and compatibility.

Windows Server Migration Tools may work out well for some who need to migrate the specific supported roles and features. However, using modern Windows Server tooling may be better, such as the new Storage Migration Service that can migrate an entire legacy file server from Windows Server 2003 and grab permissions, users, shares, and assume identity.

Conclusion

As before, many companies will switch to version 2022 as part of the normal lifecycle of Windows Server. With the approaching end of support for Windows Server 2012 (R2) on October 10, 2023, a major replacement of existing systems is on the horizon.

There is not much to be said in favor of an early upgrade to Windows Server 2022 due to limited innovations. The most important argument for it would be the increased security of the new OS, especially due to the features that Microsoft subsumes under the name Secured Core.

Microsoft obviously envisions a future for Windows Server as an operating system for virtual machines only. There, it provides its well-known services and serves as a runtime environment for traditional applications.

The actual infrastructure is provided by Azure Stack HCI, for which companies must pay separately via a subscription. Hence, it will benefit from most of the innovations.

Those running Windows Server 2016 or 2019 today have few reasons to switch to version 2022 anytime soon. Rather, organizations in this situation should take time to observe the further roadmap of Windows Server.