


Features removed or no longer developed starting with Windows Server 2019

Article • 11/28/2022

Each release of Windows Server adds new features and functionality; we also occasionally remove features and functionality, usually because we've added a better option. Here are the details about the features and functionalities that we removed in Windows Server 2019.

Tip

- You can get early access to Windows Server builds by joining the [Windows Insider program](#)  - this is a great way to test feature changes.



The list is subject to change and might not include every affected feature or functionality.

Features we've removed in this release

We're removing the following features and functionalities from the installed product image in Windows Server 2019. Applications or code that depend on these features won't function in this release unless you use an alternate method.

 Expand table

Feature	Explanation
Business Scanning, also called Distributed Scan Management (DSM)	We're removing this secure scanning and scanner management capability - there are no devices that support this feature.
Print components - now optional component for Server Core installations	In previous releases of Windows Server, the print components were disabled by default in the Server Core installation option. We changed that in Windows Server 2016, enabling them by default. In Windows Server 2019, those print components are once again disabled by default for Server Core. If you need to enable the print components, you can do so by running the <code>Install-WindowsFeature Print-Server</code> cmdlet.

Feature	Explanation
Remote Desktop Connection Broker and Remote Desktop Virtualization Host in a Server Core installation	<p>Most Remote Desktop Services deployments have these roles co-located with the Remote Desktop Session Host (RDSH), which requires Server with Desktop Experience. To be consistent with RDSH, we're changing these roles to also require Server with Desktop Experience. These RDS roles are no longer available for use in a Server Core installation. If you need to deploy these roles as part of your Remote Desktop infrastructure, you can install them on Windows Server with Desktop Experience.</p> <p>These roles are also included in the Desktop Experience installation option of Windows Server 2019.</p>
RemoteFX 3D Video Adapter (vGPU)	We're developing new graphics acceleration options for virtualized environments. You can also use Discrete Device Assignment (DDA) as an alternative.
Nano Server installation option	Nano Server isn't available as an installable host operating system. Instead, Nano Server is available as a container operating system. To learn more about Nano Server as a container, see Windows Container Base Images .
Server Message Block (SMB) version 1	Starting with this release, Server Message Block (SMB) version 1 is no longer installed by default. For details, see SMBv1 isn't installed by default in Windows 10 version 1709, Windows Server version 1709 and later versions
File Replication Service 	File Replication Services, introduced in Windows Server 2003 R2, has been replaced by DFS Replication. You need to migrate any domain controllers that use FRS for the sysvol folder to DFS Replication  .
Hyper-V Network Virtualization (HNV)	Network Virtualization is now included in Windows Server as part of the Software Defined Networking (SDN) solution. The SDN solution also includes the Network Controller, Software Load Balancing, User-Defined Routing, and Access Control Lists.


Features we're no longer developing

We're no longer actively developing these features and may remove them from a future update. Some features have been replaced with other features or functionality, while others are now available from different sources.

 Expand table

Feature	Explanation
Key Storage Drive in Hyper-V	We're no longer working on the Key Storage Drive feature in Hyper-V. If you're using generation 1 virtual machines (VMs), check out Generation 1 VM Virtualization Security for information about options going forward. If you're creating new VMs, use Generation 2 virtual machines with TPM devices for a more secure solution.
Trusted Platform Module (TPM) management console	The information previously available in the TPM management console is now available on the Device security page in the Windows Defender Security Center .
Host Guardian Service Active Directory attestation mode	We're no longer developing Host Guardian Service Active Directory attestation mode, instead we've added a new attestation mode, host key attestation . Host key attestation is simpler and equally as compatible as Active Directory based attestation. This new mode provides equivalent functionality with a setup experience, simpler management and fewer infrastructure dependencies than the Active Directory attestation. Host key attestation has no extra hardware requirements beyond what Active Directory attestation required, so all existing systems will remain compatible with the new mode. For more information, see Deploy guarded hosts for more information about your attestation options.
OneSync service	The OneSync service synchronizes data for the Mail, Calendar, and People apps. We've added a sync engine to the Outlook app that provides the same synchronization.
Remote Differential Compression API support	Remote Differential Compression API support enabled synchronizing data with a remote source using compression technologies, which minimized the amount of data sent across the network.
WFP lightweight filter switch extension	The WFP lightweight filter switch extension enables developers to build simple network packet filtering extensions for the Hyper-V virtual switch . You can achieve the same functionality by creating a full filtering extension. As such, we'll be removing this extension in the future.
IIS 6 Management compatibility	<p>Specific features being considered for replacement are:</p> <ul style="list-style-type: none"> • IIS 6 Metabase Compatibility (Web-Metabase) • IIS 6 Management Console (Web-Lgcy-Mgmt-Console) • IIS 6 Scripting Tools (Web-Lgcy-Scripting) • IIS 6 WMI Compatibility (Web-WMI) <p>IIS 6 Metabase Compatibility acts as an emulation layer between IIS 6-based metabase scripts and the file-based configuration used by IIS 7 or newer versions. You should start migrating management scripts to target IIS file-based configuration directly, by using tools such as the <code>Microsoft.Web.Administration</code> namespace.</p>

Feature	Explanation
	You should also start migration from IIS 6.0 or earlier versions, and move to the latest version of IIS, which is always available in the most recent release of Windows Server.
IIS Digest Authentication	This authentication method is planned for replacement. Instead, you should start using other authentication methods such as Client Certificate Mapping (see Configuring One-to-One Client Certificate Mappings) or Windows Authentication (see Application Settings).
Internet Storage Name Service (iSNS)	The Server Message Block (SMB) feature offers essentially the same functionality with more features. See Server Message Block Overview for background information on this feature.
RSA/AES Encryption for IIS	This encryption method is being considered for replacement because the superior Cryptography API: Next Generation (CNG) method is already available. To learn more about CNG encryption, see About CNG .
Windows PowerShell 2.0	This early version of Windows PowerShell has been superseded by several more recent versions. For the best features and performance, migrate to Windows PowerShell 5.0 or later. See PowerShell Documentation for plenty of information.
IPv4/6 Transition Technologies (6to4, ISATAP, and Direct Tunnels)	6to4 has been disabled by default since Windows 10, version 1607 (the Anniversary Update), ISATAP has been disabled by default since Windows 10, version 1703 (the Creators Update), and Direct Tunnels has always been disabled by default. Use native IPv6 support instead.
MultiPoint Services	We're no longer developing the MultiPoint Services role as part of Windows Server. MultiPoint Connector services are available through Feature on Demand for both Windows Server and Windows 10. You can use Remote Desktop Services , in particular the Remote Desktop Services Session Host, to provide RDP connectivity.
Offline symbol packages (Debug symbol MSIs)	We're no longer making the symbol packages available as a downloadable MSI. Instead, the Microsoft Symbol Server is moving to be an Azure-based symbol store . If you need the Windows symbols, connect to the Microsoft Symbol Server to cache your symbols locally or use a manifest file with SymChk.exe on a computer with internet access.
Software Restriction Policies in Group Policy	Instead of using the Software Restriction Policies through Group Policy, you can use AppLocker or Windows Defender Application Control . You can use AppLocker and Windows Defender Application Control to manage which apps users can access and what code can run in the kernel.
Storage Spaces in a Shared configuration using a SAS fabric	Deploy Storage Spaces Direct instead. Storage Spaces Direct supports the use of HLK-certified SAS enclosures, but in a non-shared configuration, as described in the Storage Spaces Direct hardware requirements .

Feature	Explanation
Windows Server Essentials Experience	We're no longer developing the Essentials Experience role for the Windows Server Standard or Windows Server Datacenter SKUs. If you need an easy-to-use server solution for small-to-medium businesses, check out our new Microsoft 365 for business  solution, or use Windows Server 2016 Essentials .