Top 10 security improvements in Windows Server 2019

This new version of Windows Server provides some significant security updates compared to the Windows Server 2016 version, including ransomware monitoring tools and other malware.

This new version of Windows Server provides a number of significant security enhancements over the Windows Server 2016 version, including tools for monitoring ransomware and other malware, and to monitor localized attacks. exploited.

Windows Server 2019 'joined' Windows 10 1809 through the addition of some extremely useful Windows security enhancements for Server administrators. Windows Server 2019 with the Desktop Experience option is the next Long-Term Servicing Branch (LTSB) release of the Windows server line. For those who are uncomfortable working on servers without GUI (user interface), this will be the version of Windows Server that should be chosen as the basis for Remote Desktop Servers and Exchange 2019.

Those who are familiar with Windows Server 2016 will find it very familiar to Windows Server 2019. But not only that, some security enhancements also make Windows Server 2019 a preferred choice. Here are the most important improvements to security features or administrative features that will make security-related tasks simpler.

10 security improvements in Windows Server 2019

1. Upgrade in place
2. Security fixes
3. .NET updates
4. Advanced Threat Protection (ATP)
5. Windows Defender ATP Exploit Guard
6. Improved security of Software-defined networking
7. Improvements to shielded VM
8. Linux support
9. Improved HTTP / 2
10. Congestion control

Upgrade in place

Unlike the Windows 10 platform, you need a license to upgrade from Windows Server 2016 to Windows Server 2019. The in-place upgrade feature is fully supported to migrate from Windows Server 2016 to Windows Server

2019 except Essentials The role is no longer included in Windows Server 2019.

Security fixes

Windows Server 2019 and Server have the Desktop Experience option that also receives security fixes such as Windows Server 2016. But it doesn't receive periodic feature releases every half year that Windows 10 desktops receive. Instead, it receives monthly security fixes. Also released in October, Windows Server Core, an option that does not have a graphical interface and receives scheduled updates every six months. You should pair the Server Core with the new Windows Admin Center to manage the servers.

.NET updates

Along with Windows 10 1809, Windows Server 2019 will receive its .NET updates as a separate package that can be installed or removed independently from the Windows operating system. As noted on the .NET blog, it gives users more flexibility in installing .NET Framework updates and allows Microsoft to better meet the critical needs of customers with fixes. NET Framework is independent. You can select, then check and install standalone .NET updates to ensure compatibility with Exchange 2019 or another enterprise application stream.

Advanced Threat Protection (ATP)

Another new feature is Advanced Threat Protection - ATP, which originally appeared on Windows 10 and is currently being ported to the Windows Server platform. With the addition of an Azure Security Center license, users now have the ability to monitor attackers and actions to extend the scope of attacks on the server. Extensive attacks and the use of PowerShell to access the system are monitored and recorded for later analysis.

Windows Defender ATP Exploit Guard

Those who have deployed Windows 10 are probably familiar with the security improvements that Windows Defender ATP brings to the operating system. On Windows Server 2019, server intrusion prevention has been added to the server. The task of Windows Defender Exploit Guard is to 'lock' the device to combat a variety of vector attacks.

1. **Attack Surface Reduction (ASR)** is a series of control actions to prevent malware from entering your computer, by blocking suspicious malicious files (specially crafted Office files are specially created). , scripts, scope extensions, ransomware and threats via email.
2. **Network protection** adds endpoint protection, avoiding web-based threats by blocking any process of sending data from devices to servers or untrusted IP addresses via Windows Defender SmartScreen.
3. **Ransomware protection** is provided by Access Folder Access, a tool to protect sensitive data from ransomware software by blocking unreliable processes accessing your protected folders use. This can be edited and adjusted to add the folders that users want to protect.
4. **Exploit Protection** is a set of actions that minimize the exploitation of vulnerabilities, which can be configured to protect your system and applications. This replaces the Enhanced Mitigation Experience Toolkit (EMET), which is no longer used.
5. **Code Integrity policy** released in Windows Server 2016 is difficult to implement, so Windows Defender Application Control now includes default Code Integrity, allowing applications like SQL Server to block known executable files.

Improved security of Software-defined networking

In Windows Server 2019, Software-defined networking has been improved to create firewall records with the same classification format as Azure Network Watcher. The Hyper-V server creates logs that can then be analyzed with many tools to support log file formats. Windows Server 2019 integrates the ability to lock Windows Server 2016 virtual network security by automatically applying Access Control Lists - access control lists (ACLs) to virtual machines (VMs) connected to virtual subnets and other Other structures. Windows Server 2019 allows you to restrict access by adding ACLs to the appropriate subnet. With Windows Server 2019, you can use virtual network encryption to prevent theft and data fraud while data is being forwarded.

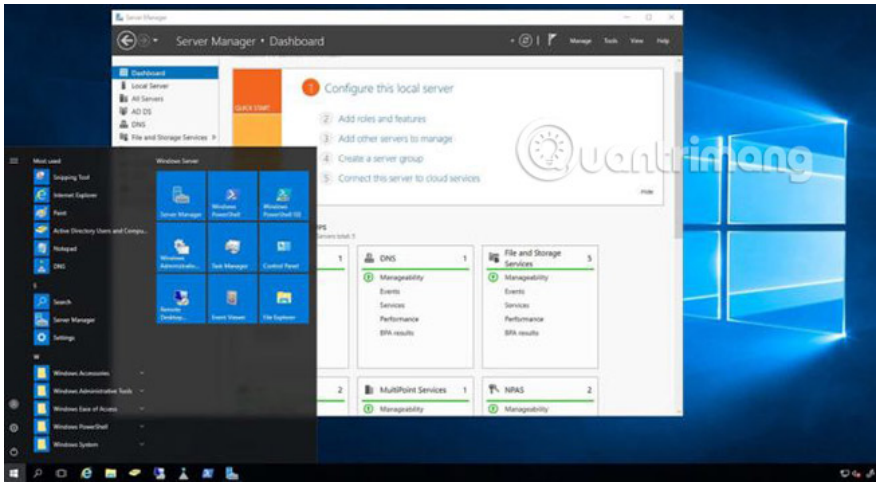
Improvements to shielded VM

When setting up secure branch offices using the shielded VMs (protected virtual machines), you can ensure that you do not lose access to Host Guardian Service by setting up a Host Guardian Service for backup and processing. offline level. This ensures you can set up a second URL group as a backup for the Hyper-V server to try if the main Host Guardian Service is inaccessible.

Windows Server 2019 adds support for VMConnect Enhanced Session mode and PowerShell Direct to help troubleshoot protected virtual machines more easily. These features are automatically activated when a virtual machine is protected on a Hyper-V server running Windows Server 2019 or Windows Server version 1803 or later (Windows Server 2019 with the Desktop Experience option or Windows Server Core).

Linux support

In Azure, Linux is the most used platform. Windows Server 2019 fully supports Ubuntu, Red Hat Enterprise Linux and SUSE Linux Enterprise Server inside protected virtual machines. Microsoft is developing it towards a Linux protection tool, not a competitor. Recently, Microsoft joined Open Invention Network (OIN), a community dedicated to protecting Linux and other open source software programs from patent-related risks. By participating in this project, Microsoft has allowed the Linux community to use 60,000 free patents without the risk of litigation.



Improved HTTP / 2

Included in Windows Server 2019 are improvements that make a website faster and safer. HTTP / 2 is a big improvement over existing HTTP technologies. Improvements include better server-side encoders, which help minimize automatic connection problems. It is also easier to deploy these new applications in a user environment.

HTTP / 2 shares a single TCP connection with multiple requests to the same site. During this sharing or multiplexing process, only the first request generates the necessary interactions to establish the connection. The following requests immediately send HTTP data to request that no connection be established.

Domains designed for HTTP / 1.1 are not without benefits. Connection synchronization is added to minimize sharding (sharding is a process of storing data records across multiple devices to meet data incremental requirements), and is enabled on both Edge and HTTP servers. For consolidation, stored subdomains will end up sharing a single TCP connection if their certificate is appropriate. Without this synchronization setting, sites like 1.bing.com and 2.bing.com will require separate TCP connections.

Windows Server 2019 automatically works to fix connection errors. HTTP / 2 requires at least version 1.2 of TLS while listing lower cipher suites. This results in broken connections. On current servers, until the encoder is

repaired, the connection will not work properly. Some changes in Windows Server 2019 ensure reconnection will be made.

As mentioned, here are the steps that Microsoft takes in Windows Server 2019 to fix the problem:

Fail mode occurs when the default SSL encoder in Windows Server 2016 is changed incorrectly. If any encoder is blocked by HTTP / 2 or appears before HTTP / 2-enabled encoders, Firefox and Chrome will disconnect (allowed, but not recommended by HTTP / 2) . Chrome shows:

```
ERR_SPDY_INADEQUATE_TRANSPORT_SECURITY
```

Firefox displays:

```
NS_ERROR_NET_INADEQUATE_SECURITY
```

Although the proper arrangement of SSL encoders (guaranteed by the default order in Windows) can avoid this problem, in Windows Server 2019, the robustness of the password negotiation mechanism is not possible. rearrangement of SSL encoders has been improved. Of course, this list must still include HTTP / 2-enabled encoders, but they do not necessarily appear at the beginning of any blacklist.

This reduces the complexity of HTTP / 2 deployment, enabling customers to more easily reap its benefits, including advanced encoders required by HTTP / 2.

Congestion control

Finally, Windows Server 2019 includes support for New-Reno, Compound TCP, Cubic and LEDBAT congestion control tools (Cubic is the new default option). Cubic is suitable for high bandwidth and high latency links, while standard TCP does this very badly.

All these changes have been added to provide more and more options for server and web administrators to ensure security, as well as secure data storage and distribution.

See more:

1. Discover new features in Windows Server 2019
2. Implement these tasks first when transferring data to Windows Server 2019
3. 10 new features in Windows Server 2012