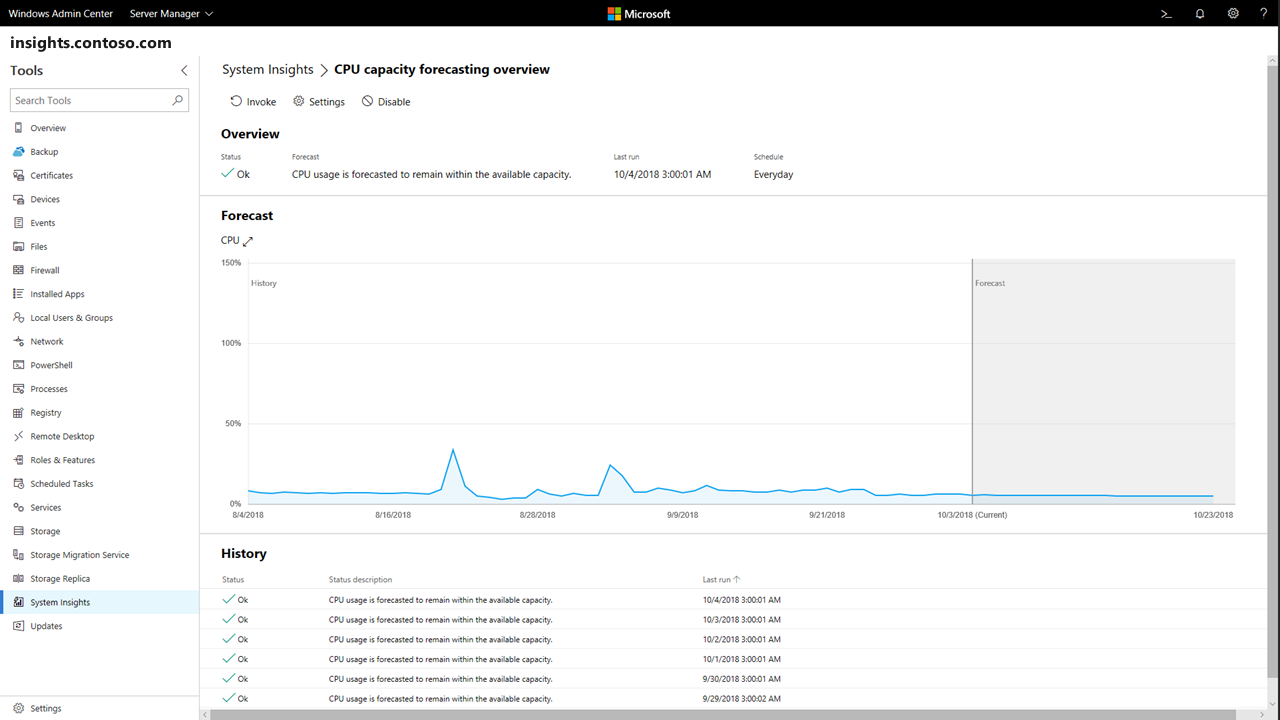
Windows Server 2019 is Microsoft’s latest foray into the enterprise computer server software field. There are many new features that show Microsoft’s commitment to push the limit on what is possible and what can be integrated together in order to bring seamless ease-of-use to its customers. Drawing on our experience with Windows Server 2012, we noticed quite a few differences that were interesting enough to warrant further discussion. These differences primarily fall into the categories of Azure Integration, Infrastructure, Security, and Application. This report will describe the main differences between Windows Server 2012 and 2019, but by no means is a comprehensive list, as there are too many differences to detail in the scope of this report.

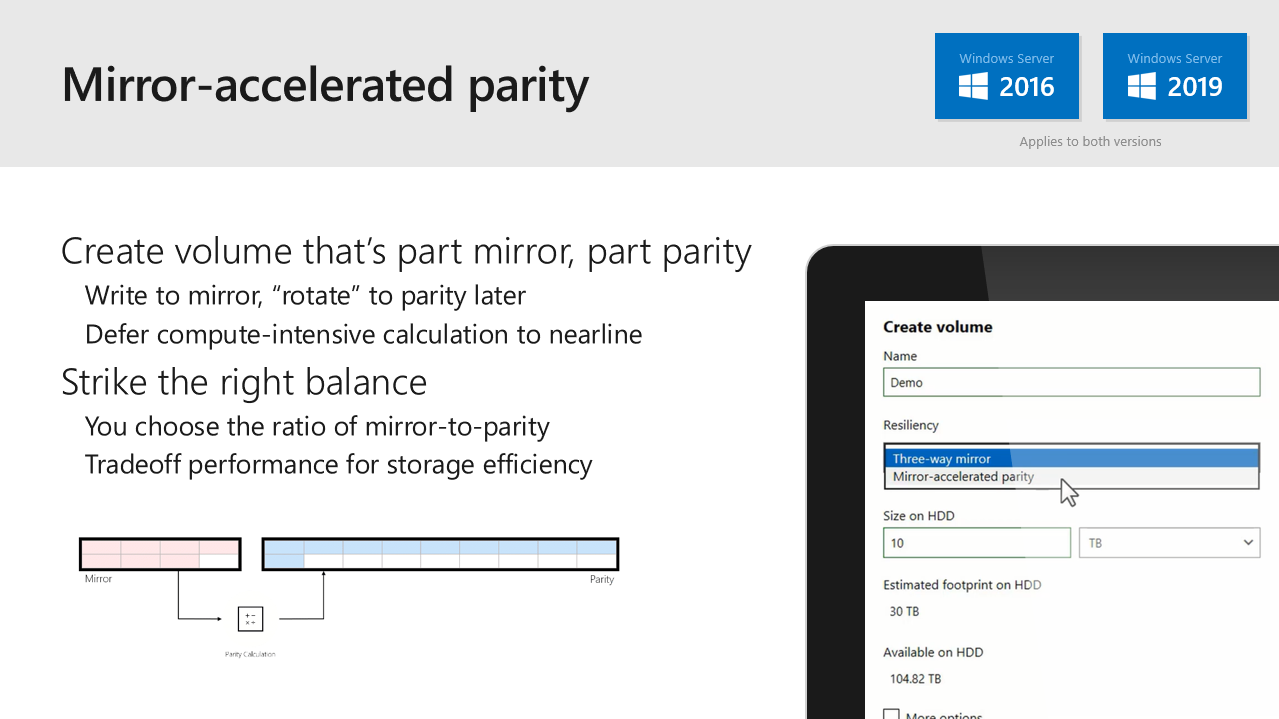
The first category is Azure Integration. Microsoft’s Azure Services are cloud-based SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), and IaaS (Infrastructure-as-a-Service) that include more than 600 different cloud-based services. Windows Server 2019 has been setup to provide seamless integration with Azure services. Starting with the initial setup of WS2019, the new features ease the path into configuring the new software. First, the Storage Migration Feature deals with the transfer of data from legacy systems to WS2019 and Azure. Second, Azure Network Adapter connects to Azure virtual networks and allows for an easy setup of a point-to-point VPN to the Azure services. WS2019 can also join Azure Active Directory, allowing WS2019 accounts to be used for Azure cloud authentication.

Just as, if not more important than the initial setup of an operating system is the monitoring capabilities to ensure that the service is reliable and secure. WS2019 brings System Insights, which allows for not only monitoring and analytics, but actually predictive analytics. This allows WS2019 to predict problems that might come up in the future, allowing the business to adapt and fix the problems before they occur. This is a big improvement, as it generally easier, cheaper, and better to proactively avoid problems rather than reactively fix them. As many businesses are moving toward cloud-based services, it is vital to integrate local services into cloud services to provide greater benefits to the business customer.



-Shows System Insights CPU Capacity Forecast. Taken from <https://docs.microsoft.com/en-us/windows-server/manage/system-insights/overview>

The second category of differences between Windows Server 2012 and 2019 is the area of Infrastructure Features. The first is Storage Spaces, which was introduced on WS2012. This allows for virtualization of storage drives, bringing the ability to create virtual volumes out of a storage pool of disks. WS2019 steps that up by introducing Enhanced Storage Spaces Direct (S2D) which allows for up to 4PB (petabyte) of storage in a storage pool and 64TB (terabyte) of storage per volume, which is a staggering increase over WS2012’s 480TB total storage pool capacity. This is immense storage capability, which is needed in today’s data-driven enterprise computing market. This is linked with Storage Health Monitoring, which allows continuous monitoring, maintenance, and logging of the Storage Spaces to help prevent lost data and downtime. Storage Quality of Service (QoS) uses configurable policies to set up and monitor storage I/O minimums and maximums in order to ensure consistent performance to all VMs. Mirror-Accelerated Parity creates volumes that are part mirrored (for speed) and part parity (for data redundancy). Data written to such a volume will first be mirrored to increase write performance by 2x. The data is then moved at a later time to the parity part of the volume to help protect against data loss.

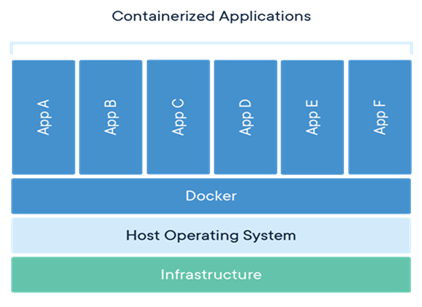


-Taken from <https://blogs.technet.microsoft.com/filecab/2018/06/27/windows-server-summit-recap/>

There are several other features provided by WS2019 that help with keeping your system running smoothly. Unified Management is a browser-based remote management interface that can define and control network configuration and allow for network monitoring. The system kernel can be ‘soft-rebooted’, allowing for a much faster hardware reboot time. A network controller feature brings automated configuration, management, monitoring, and troubleshooting to the virtualized networks in your system. A Software Load Balancer (SLB) provides cloud-optimized load-balancing to your networks, which will help alleviate data slowdowns and losses during heavy traffic periods. Two different virtual networks in the same datacenter can be ‘peered’ together, which will allow faster data transfer without having to go through a gateway. Distributed firewalls and network segmentation can break up networks and allow for increased security between network segments. Precision Time Protocol (PTP) enables all network devices to incorporate latency into the network timing measurements, allowing for a much more accurate time result than using Network Time Protocol (NTP). Similarly, Low Extra Delay Background Transfer (LEDBAT) will allow for the use of the entire network bandwidth when possible for moving data while automatically scaling back and using less bandwidth when users and applications are in use. Leap Second functionality gives the ability to add periodic 1-second intervals to UTC time in order to keep up with the slowing of the Earth’s rotation. Control Flow Guard helps protect against memory corruption attacks. For clusters of machines running WS2019, the cluster hardening feature can bypass the requirement of using Active Directory if needed. Keeping a business-grade network and data storage system running smoothly is extremely important, and relies on many different tools to configure, monitor, and fix problems as quickly and efficiently as possible to avoid costly work stoppages and data loss.

The third category of differences we found between Windows Server 2012 and 2019 is in the area of security. While a business would, of course, not want to rely solely on security features available in an operating system, there are a few new features of WS2019 that stand out as providing greatly increased security in the enterprise setting. Windows Defender Advanced Threat Protection (ATP) has been enhanced, bringing new host-intrusion-prevention tools for prevention as well as attack detection and zero-day exploit monitoring. Virtual Machines are now shielded, which helps to prevent from attacks as well as administrative accounts that have been compromised. This shielding also allows for greatly increased threat resistance. VM-to-VM data traffic can now be encrypted even within subnets to allow for secure communications. VM Connect allows for a secure console connection to configure and interact with shielded VMs. Device Guard is a code integrity protocol that helps ensure that programs are authorized to run. Finally, Credential Guard secures credential information by using virtualization-based security to stop advanced persistent threats on the network as well as preventing credentials from being stolen by malware or compromised administrator accounts. This Credential Guard also works in Remote Desktop Protocol situations to provide single-sign-on logins. Keeping data secure is paramount in today’s data-driven businesses. Providing for attack threat detection and monitoring ensures that enterprise systems will remain as trouble free as is possible.

Finally, the last category of differences is the features that work with applications directly. Azure Service Fabric for Windows Server gives the ability to create a multi-machine, multi-platform cloud-based computing cluster in your own infrastructure. This allows you to create your own cloud-based service which can be private or public as you wish. The non-GUI Server Core and Nano Server versions of WS2019 are in their own containers, thus reducing download times. Server Core also now has Features On Demand (FOD) which include many of the features from the full desktop version without adding any of the GUI functionality. Containers result in keeping applications separated so that they won’t affect each other.



-Shows Application Container organization. Taken from https://www.altaro.com/msp-dojo/containers-for-msps-part-1/

Windows Server containers create isolation, allowing for applications to be re-configured and changed without affecting any other applications or the system as a whole. Isolation of the Hyper-V hypervisor by using application containers means that the host operating system cannot be affected by any other running container/VM.

Some of the most exciting new features work with Linux systems. Linux containers allow administrators to manage both Windows and Linux applications in the same environment, reducing overhead. Windows Subsystem for Linux (WSL) allow software developers and admins to use Linux tools along with Windows Command Prompt and Powershell. Integrating Linux configuration and monitoring into the Windows Server environment will bring a whole new way of managing cross-platform enterprise environments and the introduction of application containers supports increased security and system robustness.

Microsoft has brought a lot of advanced features to the market with the introduction of Windows Server 2019. Increases in available tools in the areas of infrastructure, security, and applications show that Microsoft is committed to the enterprise server market. In addition, vastly increased integration with Azure cloud services show that Microsoft is looking to the future by bringing cloud-based services increasingly within reach of businesses. We believe that Windows Server 2019 will fulfill an important role in the near future as more and more business of all sizes are looking to cloud-based services to fulfill their needs.