TechTarget | SearchWindows Server

PRO+ Content

The Essential Guide to Windows Server 2016

In this guide

Introduction

Now that mainstream support for Windows Server 2008 has ended and Windows Server 2012 is getting up in years, more enterprises may want to consider jumping to Windows Server 2016, which is scheduled to be released in the third quarter of 2016.

Microsoft Windows Server 2016 includes several new features, including Nano Server -- a lightweight installation option that is 93% smaller than traditional Windows Server deployments -- and native container support. Windows Server 2016 also includes new software-defined storage options and improvements to Hyper-V.

Whether you're on the fence about upgrading or have already decided to deploy the new server operating system when it is officially released, this guide will highlight the most anticipated Windows Server 2016 features.

In this guide

What to know before you start

How to prepare for a Windows Server 2016 upgrade

While everything may run fine on the existing server platform, there may be benefits in Windows Server 2016 that make an upgrade more appealing. Migrating server operating systems isn't a light undertaking. Does your IT staff have the expertise -- or the time -- to handle this type of upgrade or should it be outsourced to consultants?

Why enterprises should consider Windows Server 2016

Microsoft Windows Server 2016 is in Technical Preview, meaning organizations are starting to tinker with it a bit. But soon, administrators will have to evaluate the new OS and even decide where, when and how to integrate Windows Server 2016 into their environments. And that's not an easy decision.

Most enterprises likely will take a conservative upgrade path: Wait for the first or second service pack before implementing an actual upgrade. But while admins

In this guide

wait for changes and bug fixes to level off, executives weigh the financial and technical implications of the upgrade. This decision can be broken down into three principal areas -- support, feature set and existing architectures.

What is the availability of support and its effect on corporate compliance?

No enterprise deploys major platforms without software support, but support lifecycles for Microsoft OSes are finite. Support is often a cornerstone of enterprise business continuance and regulatory compliance obligations. If you've been running older OSes that are facing end of life (EoL), a strategic upgrade to a new (supported) version may be the safest route.

For example, mainstream support for Windows Server 2003 ended in 2010 and extended support ended in July 2015. Mainstream support ended for Windows Server 2008 in January 2015; extended support should be available until January 2020. Even Windows Server 2012 R2 will face initial EoL by January 2018.

Will the business or end users benefit from the features slated for Windows Server 2016?

In this guide

Microsoft Windows Server 2016 promises several new features, including a pared-down Nano Server mode for cloud and container environments, support for Docker and native Hyper-V containers as well as rolling upgrades for Hyper-V and storage clusters. Other features include hot add/remove virtual memory and virtual network adapters, nested virtualization, a new version of PowerShell for improved system management, Linux secure boot, better security for VM encryption using BitLocker and cluster access to JBODs.

It's unlikely these new features alone would compel a company to upgrade to Windows Server 2016, but the impact of new features on compliance and new business opportunities might make early upgrades more attractive for some organizations.

How well will your existing servers support Windows Server 2016 technical requirements?

The actual requirements for Windows Server 2016 are fairly modest -- a 1.4 GHz processor, 512 MB of memory, 32 GB of disk space, and a 1 gigabit Ethernet adapter. These are the same basic requirements for Windows Server 2012 R2 -- and any current production-class server will provide far more than enough resources to support the new OS, along with an array of busy VMs.

In this guide

However, new features emerging with Windows Server 2016 can take advantage of network interface cards that support remote direct memory access, improve server security with trusted platform modules, handle SMB 3, and support comprehensive remote management. Therefore, older servers should run the new OS, but a server technology refresh may help improve capacity, performance and feature compatibility.

How to ensure a pain-free Windows Server 2016 upgrade

A Windows Server upgrade can pose serious risks -- errors, oversights, incompatibilities and other consequences can affect workload performance or disrupt key services. There are a few things to consider before planning a Windows Server 2016 upgrade.

An experienced and knowledgeable IT staff is the key to a smooth upgrade path. Have IT teams start working with Windows Server 2016 Technical Preview. This might include allocating funds to build or expand test setups; IT admins should also deploy current (or intended) servers and get better

In this guide

acquainted with Windows Server 2016 installation wizards. Get installation errors and hang-ups out of the way before moving anything into production.

And don't stop there. Use the test setup to deploy some workload VMs and see how current workloads perform under the new OS. Test out management tools and ensure admins can manage servers running Windows Server 2016 along with other OS versions. Incompatibilities will pop up; understand what needs to be patched or updated for proper compatibility, or what workarounds might be available.

All of this preparation takes time; however, Windows Server 2016 isn't slated for release to manufacturing until 2016. So it's good practice to start early. It may be 18 to 24 months before your upgrade plan is actually implemented in production. When you finally roll out a Windows Server 2016 upgrade, it will probably occur in phases -- upgrading servers in manageable groups rather than all at once.

Focus on what you actually intend to change. For example, new versions of workloads like SQL Server and Exchange Server are coming down the pike too. Don't plan to upgrade everything at the same time. Start with the new OS, and

leave the workload updates until the new OS deployments are stable. Work on new enterprise application deployments later as separate projects.

Decide who should perform a Windows Server 2016 upgrade

A new version of Windows Server is coming, so organizations should do what they can to get a head start on the upgrade process. Actual justifications and planning will vary dramatically and often depend on each organization's size and needs. But organizations must learn the product early and weigh costs and logistics involved in an upgrade in advance of Microsoft's promised Windows Server 2016 release.

But there are two spheres of discussion here. Should your IT staff master Windows 2016? And should your in-house IT staff have the sole task of installing or upgrading the enterprise to Windows 2016?

In this guide

There is no question that the IT staff should learn and master Windows Server 2016 along with any relevant systems management tools. Operating systems (OSes) form the foundation of any production environment. OSes include bare metal hypervisors such as VMware ESXi or Hyper-V, along with the OSes on legacy physical servers, OSes on all of your VMs and the OSes shared among container instances. Nothing runs without an OS, so it's critical that in-house IT staff is comfortable with installing, configuring, managing and troubleshooting OSes -- this eventually means Windows 2016.

But positioning an IT staff for Windows Server 2016 isn't free or easy. Learning requires initiative, resources, time and money. The initiative starts from the top -- usually from a CIO or an IT executive -- which outlines the mandate to prepare for a Windows Server 2016 upgrade. Management can facilitate most learning goals by providing a budget and the logistical latitude to set up a dedicated test lab for learning. Existing operating system knowledge is largely transferable, and staff can use technology previews now (and the actual release later) to practice working with Windows 2016 deployments, setups and configurations; they can even see how existing workloads integrate with the new OS. Take notes and share ideas. It's unlikely that an experienced IT staff should need

formal training for Windows 2016, but classroom-based training may eventually become available if it's needed.

Calling in the experts

Just because the in-house IT staff should master Windows Server 2016 doesn't necessarily mean that they're the best choice to implement the actual OS upgrade plan in 2016 or beyond. In-house IT staff will probably be adequate for small or midsize organizations with a smaller number of servers or workloads to upgrade.

Your IT staff has a lot to do. There are other pressing projects to work on and many daily fires to fight. Huge OS upgrade projects may be too time-consuming or disruptive for the in-house staff, even when done in smaller phases. Your in-house staff may just need to keep the shop open.

If the scope or complexity of a Windows Server 2016 upgrade is too burdensome for your IT staff, it may be necessary to hire new staff or seek help from qualified consultants or contractors.

Staffing up with temporary talent can mitigate some of that strain, but it might be more effective to engage local value-added resellers or consultants to help with

large OS upgrade projects. This allows several senior IT staff to manage the upgrade project and oversee the contractors who possess any additional expertise or workarounds that can be shared with the in-house staff. The expense of a knowledgeable contractor's engagement may prove less costly in terms of a faster, less disruptive OS upgrade process.

Windows Server 2016 backup challenges

The release of a new operating system (OS) often results in challenges for backup operators. Backing up the new OS, for instance, may require a new backup agent specifically designed to be compatible with it. In the case of Microsoft Windows Server 2016, which is scheduled for release sometime next year, data backup requirements and challenges may go far beyond the need for an updated agent. The new OS will include features that current backup applications may be ill-equipped to handle.

One of the biggest changes Microsoft is making in Windows Server 2016 is the introduction of Nano Server. However, Nano Server is also one of the two features with the potential to be the most problematic in regard to the backup requirements process.

In this guide

Nano Server will be a tiny, completely bare-bones way to deploy Microsoft Windows Server 2016. This concept isn't exactly new; Microsoft has long offered the option to deploy Windows Server in a lightweight Server Core configuration. Even so, a Nano Server deployment will be far smaller than a server core deployment. It will be so small that Nano Server won't include a user interface -- not even PowerShell.

Nano Server's small size -- about half a gigabyte in the current preview release -- and lack of a user interface limit its use. For now, Microsoft recommends that Nano Server be used to host Hyper-V, scale out file servers or run cloud applications.

While it will be possible to create backups of Nano Servers, they will require some planning. If a Nano Server is running as a VM, a virtualization-aware backup application with Windows Server 2016 support should be able to back it up. If a guest-level backup is required, the backup agent -- which must be Nano Server-compatible -- will need to be injected into the deployment image from which Nano Server is created. Nano Server can only be installed from a

Microsoft Windows containers

In this guide

Another Microsoft Windows Server 2016 feature with the potential to break an organization's backups is containers. Microsoft has not yet released a lot of information about containers, aside from the fact that Windows containers will essentially be Docker containers designed to work with Windows. And these containers will be useful to virtualize applications.

The problem with backing up Windows containers is that backup vendors may not initially offer a good solution for container backups. This will likely change over time, but early adopters will have to find a way to back up containers within the limits of their backup application's capabilities.

Although Docker has been around for a while, most backup vendors do not have Docker-specific capabilities baked into their software. Organizations running Docker on Linux servers commonly use scheduled scripts to back up Docker containers to a tar file. Once created, the tar file can be backed up just like any other file.

Windows as a Service architecture

It isn't just the Microsoft Windows Server 2016 feature set that has the potential to complicate backup requirements. Microsoft also plans to deliver Windows as

In this guide

a Service. So far, Microsoft has only talked about Windows as a Service with regard to the new Windows 10 OS. Even so, Microsoft has a long history of Windows desktop and Windows Server builds paralleling one another. As such, there is a strong possibility that Microsoft will extend the concept of Windows as a Service to Windows Server 2016.

For those unfamiliar with Windows as a Service, it refers to Microsoft's plan to deliver new features and capabilities to the Windows OS through updates, rather than requiring customers to purchase new versions of Windows every few years. If this approach is applied to Windows Server, backup operators will have to perform rigorous testing of new builds -- especially those that contain major changes or additions -- to ensure that updates do not cause problems.

Microsoft Windows Server 2016 has the potential to force organizations to rethink their backup strategy. Initially, it will probably only be the early adopters who have to deal with issues that stem from using backups in conjunction with new Windows Server features. But as the new features gain wider adoption, organizations will have to think about how their backups will be impacted.

In this guide

Windows Server 2016 Storage

Storage Spaces Direct adds functionality

Storage Spaces Direct, a new storage feature in Windows Server 2016, uses software to let administrators build highly available storages systems with local storage.

Get started with Storage Spaces Direct

Storage Spaces Direct is one of the most highly anticipated features being introduced in Windows Server 2016. Storage Spaces Direct builds onto the Windows Storage Spaces feature, allowing administrators to pool storage from servers in a cluster.

Windows failover clusters typically make use of a cluster shared volume (CSV). A CSV is a storage volume that is accessible to all of the nodes that make up the cluster. If a server hosting a clustered resource -- which Microsoft refers to

as a clustered role -- fails, then the workload can be seamlessly moved to another node within the cluster. This is possible because all the cluster nodes share a common CSV and therefore have access to the same files.

CSVs have been used for many years and are dependable, but they can be complicated and expensive to create. In large, enterprise-class organizations, CSVs tend to exist on storage area networks and are connected to the cluster nodes via Fibre Channel. Smaller organizations may opt to use iSCSI connectivity, which is generally less expensive to implement, but can be complicated to configure.

Storage Spaces Direct avoids need for CSV

This is where the Windows Server 2016 Storage Spaces Direct feature comes into play. Storage Spaces Direct is designed to allow failover clusters to be built around commodity storage without a CSV.

A CSV must be created on top of a supported shared storage architecture. In contrast, Storage Spaces Direct can use either Direct Attached Storage or locally connected JBOD storage.

In this guide

Storage Spaces Direct does not turn a cluster node's local storage into shared storage or make each cluster node a full mirror of the cluster storage. Administrators must create storage pools on each cluster node. These storage pools include the node's local storage. Once the pools are created, virtual disks are created on top of the storage pools. If a virtual disk uses a combination of SSD and HDD storage, then storage tiering can be enabled automatically for the virtual disk. These virtual disks are then made available as cluster storage.

The key difference with Storage Spaces Direct

The important thing to understand about this configuration is that the virtual disks are not simply being treated as virtual hard disk (VHD) files, but rather as a series of extents. An extent is a 1 GB segment of a virtual hard disk. As such, a 500 GB VHD is made up of 500 separate extents.

This is important because the VHD is not being mirrored to each cluster node; therefore, there isn't a dedicated copy of the VHD for each cluster node. That being the case, Storage Spaces Direct applies a technique called fault domain awareness to maintain the integrity and availability of the cluster storage.

In this guide

Fault domain awareness works by placing extents on the various cluster nodes in a manner to prevent data loss if the node -- or node storage -- fails. As an example, say a 500 GB VHD has been created on a four-node cluster.

There are a few different ways to structure the data, but one of the preferred methods involves creating a three-way mirror. When a three-way mirror is created, there are three copies of the data. Since there are four nodes in this particular cluster, not every node can have its own copy of the data. As such, Windows creates three separate copies of the 500 extents for a total of 1,500 different extents. These extents are scattered among the cluster nodes in a way that maximizes resiliency.

Storage Spaces Direct promises to drive down the cost of cluster storage, while simplifying the creation of failover clusters. You can find a more comprehensive introduction to the technology on TechNet.

In this guide

Notable features in Storage Spaces Direct

Microsoft introduced Storage Spaces Direct in Windows Server 2016 Technical Preview 2. This feature expands the use of local storage when configuring high availability (HA) storage systems.

For example, Storage Spaces Direct supports the use of low-cost, low-performance, high-capacity devices such as SATA disks and solid-state devices -- such as solid-state drives (SSD) and serial storage architectures -- attached through the PCI Express bus -- an approach now dubbed nonvolatile memory express (NVMe) or the nonvolatile memory host controller interface specification. SATA and NVMe-based devices were not supported with earlier Storage Spaces clusters and shared disks.

From a practical standpoint, administrators can use Storage Spaces Direct to configure HA storage using the disks available in each clustered server and JBOD arrays connected to single servers. The idea is to remove the expense and complexity involved to create a serial-attached SCSI (SAS) disk fabric and allow much higher storage performance with nonvolatile memory devices and much cheaper high-volume storage with SATA disks. Storage Spaces Direct opens up the potential for HA tiered storage and the application of software-defined storage in the enterprise.

Administrators who plan to experiment with Storage Spaces Direct should keep some current caveats and limitations in mind. For example, Storage Spaces

Direct should be deployed and managed through Windows PowerShell rather than through Server Manager or Failover Cluster Manager, though final release and future versions of Storage Spaces Direct may be manageable through other platforms.

In addition, Storage Spaces Direct does not currently handle disks connected through multiple paths -- disk fabrics -- nor does it support the Multipath I/O software stack. Lab environments with such multipath configurations may need to be simplified before deploying Storage Spaces Direct.

There is no finalized hardware compatibility list, so Storage Spaces Direct is not guaranteed to work with any specific combinations of SAS, SATA or SSD disks, host bus adapters or remote DMA-based network adapters. Compatibility and performance issues can arise with some combinations of hardware, firmware and software.

Windows Server 2016 features focus on cloud

As the world of IT evolves from the traditional client-server model, so has the next iteration of Windows Server. Due out some time in the second half of this year, Windows Server 2016 will come equipped to reflect these changing times.

In this guide

Some Windows Server 2016 features include support for containers, tighter integration with Microsoft's Azure cloud service and more security for Hyper-V virtual machines.

While a move to the cloud and microservices may not be on the immediate roadmap for most organizations, Microsoft is laying the groundwork for what it considers to be an eventuality for companies that want to reduce capital expenditures by using Microsoft's infrastructure to handle their workloads.

John Joyner works for managed services provider ClearPointe as the company's director of product development. Because ClearPointe's monitoring stack is based on Microsoft Azure and Systems Center, Joyner has been working with the technical previews of Windows Server 2016 to see what the future holds for Windows Server administrators. In this podcast, Joyner talks about some of the more intriguing Windows Server 2016 features.

(This transcript has been edited for clarity and brevity.)

SearchWindowsServer: What are the top innovations that you've seen in Windows Server 2016?

In this guide

Joyner: I'm going to lead with Storage Spaces Direct [which] is the software-defined storage technology, the latest evolution of it. Microsoft introduced Storage Spaces with Window Server 2012, and the ability to transcend the need for a SAN -- a storage area network -- and dedicated storage networking hardware. Basically, Storage Spaces moved the SAN controller function into Windows software and allowed you to use inexpensive disk enclosures, populated by what we called JBOD or disks that are not in a sophisticated fault-tolerant array, but are rather presented to the operating system as individual discs. And in the array-type technology, the [disk] striping, and the fault tolerance, that's done by Windows now rather than relying on an external appliance.

Microsoft identified storage and SANs and associated SAN infrastructure as being the most costly single component in data center [capital expenditure]. Microsoft research [says] approximately 60% of a new data center cost is directly attributed to storage and storage area networking. Microsoft released Storage Spaces as a way out of this cost issue by eliminating the need for the separate SAN infrastructure. Storage Spaces leverages the less expensive passive disc enclosures, the less expensive JBOD discs running on essentially less expensive commodity hardware rather than the more pricey proprietary hardware; and thereby giving you high performance at significantly reduced cost. Through converge networking which is running your storage and your data over the same 10 [Gigabit Ethernet] or 40 [Gigabit Ethernet] pipe, again that's

how we eliminate the need for the separate Fibre Channel or the iSCSI networks.

The difference between Storage Spaces in Windows Server 2012 and Storage Spaces Direct in Server 2016 is that in 2012, each enclosure still required its own redundant serial attached SCSI connectors to each scaled out file server node. There was a bit of a scaling limitation because you could only fit so many dual channel SAS [host bus adapters] in a server. That limited how many enclosures you could connect to. Microsoft has eliminated that bottleneck or that scaling constraint by not requiring a direct SAS connection anymore.

Are four hosts required to use Storage Spaces Direct?

I don't have that specific information about four hosts. I haven't heard that specifically. It may be necessary to deploy a certain number of hosts to have the highest level of redundancy possible. For example, you can deploy Storage Spaces with the enclosures. You have to have three enclosures to have enclosure awareness. Two nodes aren't enough of a vote to make a decision. You have to have three and so that's a limitation. You can run Storage Spaces on one or two enclosures. But to have the ability to lose an entire enclosure and keep running, you need three. In terms of how many nodes and enclosures you need, there probably is an optimum spot that provides the highest level or redundancy. But there's probably ways to deploy it with fewer components if you can accept slightly reduced redundancy.

In this guide

The next strategic thing is what's called the shielded VM and the guarded fabric feature. This is a solution Microsoft has come up with, a very high-security virtualization solution for the hosting and the financial services communities. There's a product that Microsoft competitor VMware has; it's part of their vSphere Suite that's often called the host-based firewall. VMware wraps a protective layer around each virtual machine to prevent a hostile virtual machine from overtaking the host. This is a common feature that's implemented in the PCI, the payment card industry. Your credit card and financial and banking industry frequently has implemented this solution from VMware as providing the highest level of workload isolation in a data center for the extremely, extremely sensitive financial transactions.

Microsoft has developed an alternative technology [that assumes] the worst case that the host is already compromised. How can we protect the guests from a hostile host? We can't protect the guest from being shut down, right? We can't prevent maybe denial of service and mischief. But we can prevent data loss and data theft. The shielded VM solution leverages the Microsoft's proven BitLocker technology with the Trusted Platform Module (TPM) in the Hyper-V host, and the guarded fabric solution which virtualizes those TPMs. When you create a shielded VM, the VM is encrypted at rest and in production with the virtual trusted computing module assigned to that virtual machine.

This allows the highly security-conscious [hosting company] or enterprise customer to deploy an absolutely forward-looking, leading-edge, high-security

In this guide

solution at far less cost than using competing technology. To use the VMware solution … you have to use VMware, and you have to use a storage technology supported by VMware, such as Fibre Channel or iSCSI. With the Microsoft solution, we're using Storage Spaces. We don't need the expensive SAN architecture. And we also don't need the third-party product.

Does encrypting the virtual machine have any impact on performance?

It's a small impact. For example, reading a compressed file or an encrypted file includes some overhead. I don't have exact numbers but it's usually in the 5% to 15% category. It's not really significant for planning. It's not a significant slowdown at all.

What were some of the other Windows Server 2016 features worth noting?

The adoption of containers and new technologies that depend on containers. Containers come from the open source world, particularly the product known as Docker. In a Docker configuration, you write a configuration, you author a configuration document that describes your service or application in terms of its resource requirements. So much storage, so much networking, so much compute. This definition of your service has been deployed to a container. And then appropriate resources, compute, storage, and networking are assembled and delivered just in time to create that resource. This is a radically different way of deploying services, that we're not standing up a server and then deploying an app in a server. We're deploying an entire service all at once. The

In this guide

networking, the firewall, the security, the apps, the database, all deployed as a single configuration.

When we write our application to a Docker or a container-type specification, we can then move the entire application, all of its parts to any other Docker compliant cloud. The concept is that you can write an application once, and then move it to another private cloud or to a hosted cloud or a partner cloud, whatever makes the most sense for you economically, feature-wise in your market and industry. Using containers evolves us away from the service-based way of deploying services to a more holistic method.

There are two specific sub-technologies that complement containers. One is called Nano Server. Nano Server is Microsoft's concept to provide on-demand compute that is highly elastic and very inexpensive to manage. Nano Servers are highly stripped down compute kernels of Window server. Think of them as Window Server Core, but even to the next level of stripping down in function. Because a Nano Server is not made to be treated like a pet and given a lot of love and attention over many years of its lifecycle. A Nano Server is meant to be treated more like cattle. It's meant to be herded and handled by quantity and with no special attachment to any one particular instance of Nano Server. They are ephemeral compute resources.

A third and final thing I'll throw out there is DSC, Desired State Configuration, which is another PowerShell-derived technology from Jeffrey Snover, the lead architect for Windows. Jeffrey's vision is that the Desired State Configuration

service, which is a Web service, enables automatic configuration of servers that -- either through push or pull technology -- are aware of the DSC server. So you would define your application through DSC, and then when you deployed Nano Servers to fulfill that application, those Nano Servers would wake up and pull their configuration details from DSC and say, 'Oh, I'm going to be a web server. Oh, I'm going to be a file server; here are my file shares' All of these are contained in the DSC document, the reference, the Desired State Configuration reference. Tthen we just point that DSC definition to a container.

Through this technology, Microsoft is addressing another major cost of the data center, and that's design and deployment. We're significantly reducing the storage cost by going to Storage Spaces Direct. We're also significantly reducing or even eliminating the design and deployment costs, because when we have an application that is authored to run in the container and uses Nano Servers and Desired State Configuration, there's no mental challenge to performing the deployment. All of the mental work is done in creating that definition.

What are the differences with Windows containers and Hyper-V containers?

There's not much difference. The standard is Docker. It's an open source standard that defines how to deploy services to containers. Microsoft's goal is to make things not proprietary, and make them open and empower the customer to decide where they want to run their workloads. If they can run them most

In this guide

effectively and cost efficiently on premises, or in a partner cloud, or in the Microsoft cloud, they want to empower you to do that and not be constrained technically. It made them all run technically the same. You can decide where to host it based on other business factors like cost, proximity, etc.

How different is management in Windows Server 2016?

I think the most marked change or development for administrators from a management point of view is that a lot of stuff is now moving to Azure. Azure is becoming the destination for the new services. Systems Center components may be enabled. They may be adapted. They may be superseded by the cloud features. But more and more activities and services are requiring investment and familiarity and use of Azure tools. This is a good thing because Microsoft is not throwing things willy-nilly into the cloud. They are onboarding services based on what they call user voice, which is their actual metric-based feedback from customers around the world on what enterprises need first in a priority.

As those are addressed, Azure is releasing the answers to those business [requests]. Every few months, a significant new service [or] significant new management service is becoming available in Azure. An example would be Azure Automation, which is the ability to take remediation steps based on scripting from an Azure alert. Using the Microsoft [Operations Management Suite] product, we can monitor the performance of a server just like we can with Operations Manager.

In this guide

In Operations Manager, if we want to perform a task based on an alert; for example, an alert says a router is malfunctioning. We may have an automatic test to restart that router before we escalate any further tickets. In Operations Manager, that sort of remediation can be built into a management pack. It can be enabled as a task in the System Center Operations Manager console. In the new Azure-based world, there are now Azure automation hooks that can allow an Azure alert to kick off an Azure Automation for remediation. And so, instead of being confined to your on-premises tools, you now have a globally available, high-performing tool that you can write your automation to that isn't dependent on a particular server or business location. From the administrator point of view, more and more is rolling up to the cloud and that's probably the biggest news on the management side.

In this guide

Windows 2016 virtualization

The debut of containers and Hyper-V updates

Containers are the next progression of virtualization -- isolated environments where applications and services can run without affecting the system and vice versa. Windows Server 2016 will also feature significant security developments to Hyper-V.

Secure Hyper-V VMs with Host Guardian

One perennial problem for IT is keeping data safe from prying eyes. How can an organization keep sensitive data confidential if the IT department has access to the data? Over the years, enterprise IT has tried to solve this problem, including compartmentalized access and variations of role-based access control.

In this guide

Concerns over these types of privacy issues are getting more attention as organizations contemplate cloud usage; how can they guarantee data privacy when that data resides in a public cloud?

To that end, Microsoft developed a new feature for Windows Server 2016 Hyper-V called Host Guardian. Host Guardian is a server role that is designed to provide virtual machine (VM) privacy at the hypervisor level. Host Guardian uses a combination of three different features to provide this privacy.

Host Guardian uses layers for Hyper-V security

The first of these features is virtual hard disk encryption. For quite some time Microsoft provided the ability to encrypt physical hard disks through BitLocker. Host Guardian encrypts virtual hard disks associated with Hyper-V VMs by enabling BitLocker within the guest operating system. Just as BitLocker uses a physical server's trusted platform module (TPM) chip, a BitLocker encrypted VM will be able to use a virtual TPM chip.

A second Host Guardian capability is something that Microsoft has referred to as encryption in flight. VMs are not static. A Hyper-V VM can be live-migrated

from one host server to another. The Host Guardian service can be used to encrypt the VM during the migration.

The third capability is that Host Guardian blocks access to a VM's memory. This should prevent attacks that use host level memory extractions to access VM data.

Microsoft hopes Host Guardian will spur use of cloud VMs

Although these mechanisms can protect a Hyper-V VM from an administrator's prying eyes, it would be short-sighted to think of Host Guardian as just a hypervisor-level privacy mechanism. Microsoft has stated it has designed Windows Server 2016 to be a cloud-first operating system. Even though Host Guardian is able to ensure privacy for VMs running in an organization's own data center, it is also designed to provide privacy for VMs running in public clouds.

When you consider Microsoft's goal of providing privacy for cloud-based VMs, it becomes apparent why Microsoft chose to design Host Guardian to include all these security capabilities. Microsoft needed a way to guarantee VM-level privacy without interfering with cloud level or data center level operations.

In this guide

Regardless of where a VM physically runs, there are certain tasks an administrator needs to do to keep the environment healthy. For instance, the administrator needs the ability to live migrate the VM on an as needed basis. The administrator also needs to be able to create backups of the VM. Microsoft designed Host Guardian with such tasks in mind, ensuring VM privacy, without being intrusive.

Protection comes at a price

Host Guardian can be used in one of two ways. When an administrator sets up Host Guardian, she must choose an attestation mode. The attestation mode can be hardware based or administrator based; it cannot be both.

Hardware-based attestation is geared toward public hosting environments. Hardware-based attestation is the more complex type of attestation to configure but also provides the greatest privacy assurance because the trust is rooted in hardware. Hardware-based attestation requires the hardware to be equipped with TPM 2.0 chips and Unified Extensible Firmware Interface 2.3.1 or higher.

In this guide

Admin-based attestation is more suitable for enterprise IT. It is less complex to configure than hardware-based attestation, but it depends on a trusted Active Directory environment.

The Host Guardian role can be used to ensure privacy for VM owners. However, this privacy comes at a cost. The encryption process will undoubtedly add a degree of overhead to Hyper-V hosts. The shielding of VMs may also make certain types of upgrades or disaster recovery operations more difficult. It is also worth noting that not every VM can be shielded by Host Guardian. If a VM is to be shielded, it must be running Windows Server 2012 or Windows 8 or higher. Likewise, some of the Microsoft documentation indicates that only generation 2 VMs are supported.

Hyper-V 2016 at a glance

Microsoft introduced several new features in Windows Server 2012 and Windows Server 2012 R2 Hyper-V, making the number of additions to Windows Server 2016 Hyper-V seem modest. Still, there are a number of noteworthy Hyper-V features in the latest version, including shielded VMs, improved

In this guide

storage resiliency, changes to PowerShell, and production checkpoints. Here's a rundown of what Hyper-V features to expect.

Production checkpoints

Checkpoints, which were previously referred to as snapshots, have existed in Hyper-V since its inception. They allow administrators to roll back a virtual machine (VM) to an earlier point in time without having to restore a backup. The problem with using checkpoints is that they didn't work very well with application servers. If used improperly, a Hyper-V checkpoint can corrupt databases and can severely damage applications.

Production checkpoints function in much the same way, except they use the power of the Volume Shadow Copy Services. When you create or apply a checkpoint, the process works similar to creating or restoring a backup, allowing admins to avoid various corruption issues often associated with the use of checkpoints. Production checkpoints will be enabled by default in Windows Server 2016 Hyper-V; however, it will also be possible to revert to the old checkpoint model if necessary.

Shielded VMs

The basic idea behind shielded VMs is that a fabric can now be designated as the owner of a VM. Therefore, the VM cannot be moved to another fabric nor will it function in another. Shielded VMs are encrypted to prevent unauthorized

access to VM contents. This encryption can be achieved through the use of BitLocker. The new version of Hyper-V will support virtual TPM, which allows a VM to be BitLocker-encrypted.

Storage resiliency

In previous versions of Hyper-V, the momentary loss of storage connectivity could cause a VM to fail. Even though admins could use failover clustering to fail a VM over to another cluster node, that still requires storage connectivity. And sometimes a failover is overkill.

For example, in a Hyper-V deployment in which a number of cluster nodes are connected to an iSCSI target, the iSCSI target will suffer from low bandwidth and intermittent connection failures will become common during periods of peak activity. A crash would occur every time a VM lost connectivity for more than a minute.

The storage resiliency feature is designed to detect momentary loss of connectivity to VM storage and pause the VM until storage connectivity is re-established. But performing a cluster-level failover is still an option.

PowerShell Direct

PowerShell can run scripts or cmdlets on remote Windows Servers in several ways. The best-known method involves using the Invoke-Command cmdlet. An administrator would enter the Invoke-Command cmdlet, followed by the –

ComputerName parameter, the credentials for the remote machine, and the command that they wanted to run.

With previous versions of Hyper-V, it was possible to use the Invoke-Command cmdlet to run a command on a Hyper-V VM. To do so, however, the target VM needed network connectivity.

In Windows Server 2012 R2, admins have the ability to copy files into a VM -- even if no network connectivity exists. The file copy process could make use of the VMBus in the absence of network connectivity. In Windows Server 2016, the PowerShell Direct feature builds on this concept.

Windows Server 2016 will allow administrators to remotely run PowerShell cmdlets or scripts on a VM, even if the VM is not connected to the network. The process uses the power of the VMBus and the Invoke-Command cmdlet. This means replacing the cmdlet's ComputerName parameter with the VMName parameter.

How to protect Hyper-V containers

The benefits of container technology -- lightweight resource demands, faster deployment, vast scalability -- have attracted significant attention from the IT

In this guide

industry. But the most popular container engine, a Linux-based platform from Docker, struggles to address important security issues.

The problem with Docker security stems from a lack of isolation between container instances. In the simplest terms, every container shares the same host OS kernel, libraries and binaries. If a malware attack or other security event is able to break out of a container and access the root OS, it is possible to compromise the underlying OS and affect every container running on it. A container can already talk to the host kernel when it runs, and Linux doesn't namespace major kernel subsystems or devices to separate or protect them. This means if you can communicate with the kernel or devices, it's possible to compromise the whole system.

While Docker promises future security improvements, there are some tactics that protect Hyper-V container.

1. Restrict containers to workloads that you know and trust from trusted parties -- avoid random workloads, such as interesting tools or other "stuff" you find on the Internet.

In this guide

2. Test and apply Linux patches and security updates diligently. Trusted OS support like the kind supported by Red Hat Enterprise Linux can help to find and fix vulnerabilities.

3. Run containers as non-root whenever possible, and drop root privileges as soon as you can. No matter what, always consider root privileges in a container to be the same as root privileges outside of the container.

Hyper-V containers in Windows Server 2016 use Hyper-V to first create a VM for isolation. Once a VM is available, Linux can be installed as the OS and an engine such as Docker can run to support containers. This is a form of nested virtualization. If the container and underlying Linux OS is compromised, the entire security event should remain contained within the Hyper-V VM.

While the concept of containers has existed for years, the Docker engine spawned a renewed interest in this technology. Microsoft hopes its Windows Server 2016 will move containers from Linux deployments to Windows environments by supporting native containers and nested virtualization.

Windows Server 2016 also promises streamlined management and improved isolation for container instances, helping organizations embrace and expand

container deployment. IT staff should soon be able to experiment with Hyper-V containers in Technology Preview versions of the OS and make plans for container adoption under Windows and Docker.

Nested virtualization supports Windows containers

In 2016, one term you will hear more of is Hyper-V nested virtualization. Not just because it's a new feature coming in Hyper-V Server 2016, but also because of the implications it has on another technology that is becoming more popular.

In virtualization, a hypervisor runs atop the physical hardware and virtual machines (VMs) run on top of that hypervisor. Nested virtualization allows a VM to host another VM. For a long time -- at least in the Windows Server and Hyper-V world -- just this type of virtualization was possible.

But now in Windows Server 2016 Hyper-V, the server role can run in a VM to host other Hyper-V VMs, adding that second -- or nested -- layer of virtualization. Nested virtualization has been supported within other hypervisors for a long time, namely VMware. Adding this feature to Windows Server 2016

does not represent a technological breakthrough, but rather a tightening of the feature gap between other virtualization offerings and Hyper-V Server 2016.

Nested virtualization has a few benefits. Organizations can more easily deploy complex networking and server infrastructure testing and demonstration environments to keep the production network from being used for operational experiments. Also, training environments have an even better way of simulating production deployments because a VM hosting the simulation or test can deploy guest VMs within itself.

Hyper-V nested virtualization paves way for containers

The top benefit to Hyper-V nested virtualization is support for containers, which have become quite popular over recent months. Containers present a new take on VMs with less overhead and more flexibility to develop and deploy applications.

Containers are a new type of VM that in some ways have less isolation than a traditional VM. Resources that are common to all the containers running on a host are shared -- operating system files, directories and running services. This allows for greater efficiency; if you're running three different containers on a host

that all run the same version of Windows Server as guests, you only need one copy of the Windows directory. This sharing reduces overhead and makes containers more lightweight. You have more headroom per server to run containers as opposed to running traditional VMs, which are more isolated and do not share anything and tend to have much more duplication.

What containers mean for administrators

Containers benefit the Windows administrator in several ways. Perhaps most prominently, containers provide a mental framework around which developers can come closer to the actual operation of the code. This means developers can not only code an entire application but also build a custom version of the environments the code requires to run. Developers build container images which are then shipped over to administrators. Containers are run essentially as they are -- as guests on that host -- and updates can be handled quickly and easily in the same way. Each of these container images might even work on a very small part of the overall application, which componentizes the application and makes it easier to work in a microservices-oriented environment.

From an elevated perspective, working with containers increases the accountability for developers to write good code that works exactly within their

environment. Using containers decreases the friction between operations and IT -- with their pristine server environments -- and developers who expect certain configurations but often lacked the ability or the rationale to change production environments to fit those expectations. Administrators spend less time figuring out if code is not working based on the server configurations and more time managing the overall infrastructure and platform.

How to manage containers

Microsoft's container management story has centered on using Docker's application program interfaces (APIs) and other tools. Windows Server containers are part of the overarching Docker open source project, and Windows Server containers are generally thought to be the functional equivalent of a Docker container. Once Windows Server 2016 is released, one could anticipate that Docker tools and utilities would manage Windows Server containers. For now, there is a collection of PowerShell commands for this, but clearly more work will be done in this area.

So how does Docker fit into this? Docker provides a "management layer" of APIs and engines to control containers that have quickly become an industry standard. Docker is open source and widely used. The Docker Hub, available

for use by anyone, is a true marketplace style repository of applications that run within Docker-style containers.

VMware has a wide lead on supporting containers. It has a well thought out offering called vSphere Integrated Containers that also works alongside Docker. These tools are available and much more mature than Microsoft's tools at this point; however, they only work with Linux containers.

What's the difference between Hyper-V and Windows Server containers?

Containers are one of the most significant new features in Windows Server 2016. They are also among the most confusing, for two reasons. First, although containers have existed in the open-source world for quite some time, they are a new concept to Windows. Second, Microsoft is simultaneously introducing two different types of containers: Windows Server Containers and Hyper-V Containers.

In this guide

To understand how containers work, you need a basic understanding of server virtualization. Containers are not the same thing as virtual machines (VMs), but they are a form of virtualization.

More powerful servers made virtualization possible

At one time, server hardware was relatively modest in its capabilities. Workloads needed dedicated hardware to run. Over time, server hardware became far more powerful; many applications consume only a small fraction of the resources that a modern server can deliver. Server virtualization was introduced to make better use of the hardware by allowing multiple workloads to run simultaneously within VMs. These VMs acted as isolation boundaries, with each virtual machine having its own dedicated operating system, virtual hard disk, memory allocation, etc.

Over time, the pendulum began to swing in the other direction. Whereas VMs were originally created to improve hardware utilization, users began spinning up so many VMs that the hardware once again became the limiting factor. A physical server can only host so many workloads before resources run out.

In this guide

As server virtualization matured, hypervisor vendors looked for ways to increase the number of VMs that a physical server could accommodate. These vendors introduced features such as thinly provisioned virtual hard disks and memory overcommitment. Containers can be thought of as being similar to these types of features because they can help a server to accommodate additional workloads.

Containers trim virtualization bulk

This raises the question of how virtual servers and containers differ from one another. A virtual server is designed to be self-contained with its own operating system, applications and hardware resources. If a problem occurs inside of a VM, that problem would not affect other VMs because the virtual server acts as an isolation boundary.

The problem with VMs is they are larger than they really need to be. Think of an application server, for example. That application server contains the application and a dedicated operating system. This operating system consumes storage space, memory, CPU cycles and other hardware resources. While this might not be an issue for hosts with a small number of VMs, imagine if a host had to run a

large number of VMs and all of those VMs were running the same operating system.

Containers seek to solve this size issue by using a single operating system instance that all the containers share. A container is similar to a virtualized application in that it stores the application's binaries and configuration files, but only stores operating system components the application modifies, such as registry entries or application specific drivers.

Why Microsoft offers container choices

Why is Microsoft introducing Windows Server Containers and Hyper-V Containers? There are a number of different answers to this question, but most come down to trust.

When Windows Server Containers are used, the containers leverage the host operating system. This might be OK for running trusted applications, but it would not be desirable for running an untrusted application. Hyper-V Containers provide an extra isolation boundary where each container has its own copy of the operating system binaries. The only real difference between a Hyper-V

Container and a Hyper-V VM is that Hyper-V Containers can be managed by Docker, while Hyper-V VMs cannot.

Containers are a mechanism for improving efficiency through the sharing of operating system binaries. Not only does this approach improve host capacity, it also makes patch management easier because there are fewer operating systems to patch.

What are Windows containers?

Containers have gained enormous popularity in the last year, providing highly scalable, lightweight virtualization for software components and complete applications. Despite the potential benefits, container technology has been largely Linux-based and focused on major platforms such as Docker. This has slowed container adoption in Windows environments, with administrators relying instead on familiar hypervisors and full-fledged VMs under Hyper-V.

This is poised to change with the impending release of Windows Server 2016, which promises support for Docker containers along with support for new

In this guide

Hyper-V containers. Let's take a closer look at the container support anticipated for Windows Server 2016.

Conventional Windows virtualization installs a hypervisor such as Hyper-V that abstracts the software from the underlying hardware. Once a hypervisor is running, an administrator can create individual, fully functional VMs -- each with its own operating system, application and other components. This allows almost any OS version and workload to operate simultaneously on the same system and then migrate across systems without regard for the underlying servers or data center infrastructure.

Containers provide an alternative approach to virtualization; first installing a host OS on a server, then installing a container layer or engine, and then compartmentalizing workloads into virtual container spaces. Each container shares the common OS kernel, libraries and binaries. This enables containers to eliminate resources wasted by redundant OSes that would be needed for traditional VMs. The result is lightweight virtualization that allows greater consolidation and cross-platform mobility than traditional hypervisor-based virtualization.

Windows Server 2016 should support two forms of container technology:

In this guide

1. Docker containers through nested virtualization where Hyper-V would create a VM running a Linux OS, and then Docker would be installed atop the Linux OS to support Linux containers.

2. Windows Server 2016 is expected to directly support containers as either a direct container -- a Windows Server container -- or under Hyper-V as a Hyper-V container.

With Windows Server containers, the Docker engine will be able to create and support Windows containers directly on Windows Server; each container can share a common toolbox of Windows processes. Hyper-V containers more closely resemble nested virtualization in which Hyper-V first creates a VM and then the Docker engine creates a Windows container within the Hyper-V environment.

This might seem like a distinction without a difference, but the decision to invoke Hyper-V for containers can enhance isolation and improve security. Because containers share the common OS kernel and processes, if a container is compromised, malware in one container might pass to the underlying OS and potentially affect other containers. Hyper-V isolates containers and prevents

activity in one container from passing back to the OS and affecting other containers.

As Windows Server 2016 evolves to support several container approaches, the issue of container management is also attracting serious attention. Tools such as Docker Machine can create Docker hosts in cloud facilities such as Microsoft Azure, on laptops and within data center servers. Docker Machine can then install and configure the Docker client, and can start, stop, restart, upgrade and configure Docker in Linux and Windows environments. A common tool will simplify container creation and management, helping organizations better use resource space and save management time.

New Hyper-V features in Windows Server 2016

Over the last few years, we have seen massive improvements in Hyper-V. Windows Server 2012 R2 introduced a number of important Hyper-V features, and the upcoming Window Server 2016 release boasts even more, as well as improvements to preexisting features. Listed below are some of the new Hyper-V features offered in the latest installation of Windows Server.

In this guide

Change in VM configuration file: This is the first time Microsoft has changed the format of the VM configuration file. Currently, VM configuration files use an XML-based file that has been changed to a binary format. The new VM configuration file will use the .VMCX file format. The reason for this change is to provide better control over XML-based configuration files; you could easily edit an XML file in an editor like Notepad and make unintended VM configuration changes that could lead to downtime for production VMs.

Nested virtualization: Although you could easily run a Hyper-V role inside a VM with some minor tweaking to the virtualization software, Windows Server 2016 adds nested functionality by default. This allows users to easily run Hyper-V roles inside VMs that are running on a Windows Server 2016 Hyper-V host. In order to use the nested virtualization feature, you must be running Windows Server 2016 or Windows 10 as the guest OS.

Add/remove virtual network interface card or memory on the fly: The ability to hot add and remove virtual network cards and memory reduces the downtime for line-of-business applications. Windows Server 2016 will provide the ability to hot add and remove virtual network cards to Generation 2 VMs and the ability to hot add and remove memory to both Generation 1 and Generation 2 VMs. There is no need to enable the Dynamic Memory feature for a VM before adjusting memory for a running VM.

Linux Secure Boot: Earlier versions of Hyper-V lacked a Secure Boot option for Linux VMs. Windows Server 2016 provides the ability to configure a variety

In this guide

of Linux distributions to use the Secure Boot feature which, in turn, enables organizations to host Linux virtualized workloads on Hyper-V and operate them securely.

PowerShell Direct: As its name suggests, PowerShell Direct can be used to run PowerShell commands interactively against local VMs running on a Windows Server 2016 Hyper-V host. This eliminates the need for a working network connection or firewall changes in order to execute PowerShell commands from a Hyper-V host against local VMs. In order to use this feature, the VMs must be running Windows Server 2016 or Windows 10 as a guest on Windows Server 2016 Hyper-V hosts.

In addition to the new Hyper-V features shown above, Windows Server 2016 will also provide the ability to update Hyper-V Integration Services through Windows Update. This enables Storage Quality of Service for scale-out file servers and bypasses the Hyper-V parent partition by enabling VMs direct access to PCI-based devices, which helps reduce the overall CPU cycles on a Hyper-V host.

In this guide

How are Hyper-V and Windows Server licensed?

In November 2015, Microsoft announced a significant change to Windows Server 2016 and Hyper-V licensing models. This change, slated to go into effect during the third quarter of 2016, marks a shift by Microsoft from a per-processor to a per-core licensing model for Windows Server 2016 Standard and Datacenter Editions. Unlike other reported improvements to Windows Server, such as the introduction of Windows Containers and updates to Nano Server, the move to per-core licensing poses more challenges than potential benefits to customers.

Experts agree that this change further complicates Microsoft's already convoluted licensing scheme, forcing customers to calculate how many cores are run for each server in order to ensure that each are properly licensed, lest they be audited by Microsoft. Others fear that the change may drive up costs for customers utilizing core-dense servers and older servers with multiple processors and a low core count. More pricing and licensing information for Windows Server 2016 and Hyper-V are scheduled to be released in the first quarter of 2016, and nothing yet is set in stone.

In this guide

While it's important to stay apprised of potential licensing changes, there are also strategies and tips you can use to help save money on Hyper-V licensing today. Check out these quick links to get a better understanding of the implications for licensing in virtual environments and of potential ways to budget licensing costs.

Calculating Windows Server 2012 and Hyper-V licensing

While virtualization makes server deployment quick and simple, it can also land users in hot water, as the rapid deployment and shuffling process can lead to server license violations. In order to avoid such violations, it's vital that users understand and utilize the many types of licenses within their virtualized data center. This can be achieved by first understanding the distinction between licenses for physical and virtual servers: Though similar in many respects, virtual server environments require a greater number of licenses, potentially increasing costs. As a result, software vendors have made a concerted effort to develop virtualization-aware licenses to keep expenses low; Microsoft's policy for Windows Server 2012 is one such example of virtualization-aware licensing.

Additionally, it is essential that users know the effect of VM migrations on licensing requirements. This is further compounded by the relationships

In this guide

between Windows Server software and the hardware it runs on, but fear not -- Microsoft offers certain exceptions to their hardware/software licensing policy in the form of a 90-day restriction. By taking advantage of Microsoft's 90-day policy and educating themselves fully, Windows Server customers can easily avoid Hyper-V licensing pitfalls.

How to avoid high prices on Windows Server licensing

Software licensing is an unfortunate reality in IT, one that is made more difficult by the introduction of virtualization. Thanks to the presence of multiple guests on top of a single hardware platform, virtualization increases the number of required software licenses, in turn creating new licensing complexity. With the cost of traditional license models going into the hundreds of thousands, it's crucial that system admins be savvy about licensing and look for ways to cut costs without cutting corners. In his Windows Server licensing guide, virtualization expert Brian Kirsch offers tips and techniques, such as selecting multiple virtual CPUs or multiple vCores per vCPU, to reduce licensing costs for Windows Server 2012.

Understanding the licensing implications of free Hyper-V

In this guide

One of the most important things to consider when choosing between Microsoft's standalone Hyper-V Server and Windows Server 2012 R2 with Hyper-V is the cost of licensing. Much of Hyper-V Server's appeal lies in its cost efficiency -- Hyper-V Server is available to download for free, and offers many of the same capabilities as Windows Server 2012 R2 Hyper-V without the cost. That said, there are still significant advantages to paying for a Windows Server license fee. In this article, Microsoft MVP Brien Posey weighs the pros and cons of both installations of Hyper-V, and figures out which is the better financial investment for you.

Is the free Hyper-V Server really worth it?

As previously mentioned Microsoft Hyper-V Server 2012 R2 is available for free and features many of the same functions as Windows Server 2012 R2 Hyper-V, which has made it popular in the world of virtualization. However, "free" sometimes comes with literal and figurative costs: Though certainly less expensive than its licensed counterpart, the free Hyper-V Server installation comes with a host of limitations putting VMs and workloads at risk.

Without essential software, such as a GUI or technical support from Microsoft, Hyper-V Server offers few protections in the event of an outage, jeopardizing

In this guide

the hard work of system admins. While Hyper-V might initially appeal to small businesses who cannot afford the licensing fee for Windows Server, the potential cost of lost time and work has many hesitating to deploy Hyper-V Server outside of a lab environment.

Building a free Hyper-V Server failover cluster

Once thought to be impossible, there is now a way to build a fault-tolerant Hyper-V deployment and Brien Posey's here to show us how. The process isn't exactly simple -- it requires an understanding of failover clustering and PowerShell -- but it is manageable and, if done correctly, boasts numerous benefits. Though Windows Server still boasts certain advantages over the free Hyper-V Server, the ability to create high availability with Hyper-V Server makes it a viable option to those looking to save money on licensing fees while using a program that's efficient and reliable.

In this guide

How containers affect application virtualization and management

Containers aren't just an alternative means of virtualizing applications -- they're also changing the way applications are built, deployed and maintained. Traditional application workloads tend to be monolithic where all of the code, components and services that compose them are developed, deployed and installed together as a single complete package.

Containers are an ideal complement to cloud computing and DevOps environments, where virtual instances must spin up quickly -- often in large quantities -- and then scale down again as computing loads or needs change. Operating system vendors such as Microsoft are quietly recognizing that massive, complex platforms like traditional Windows Servers aren't necessarily the best fit for dedicated container or cloud computing environments, which would benefit from small, lightweight OSes that start or restart faster, use fewer computing resources and require less disruptive patching.

Containers also divide complex applications into constituent components, and then install each component (such as a Web server or database) into a separate container. The containers can be linked together to form the complete application. This is the concept of microservices, where each component can then be updated or patched without affecting other related containers.

In this guide

A microservices-based application architecture also enables greater functional scalability. When a traditional workload reaches its practical performance limits, an entirely new iteration of the application (and all of its components) would need to be deployed -- along with a complete suite of computing resources. By placing related application components into containers, it becomes a simple matter to spin up more containers that address the bottleneck. For example, if a microservices-based application finds that the Web server container becomes a performance bottleneck, it's easy to deploy additional Web server containers to scale up that functionality. This allows scalability using minimal computing resources

Microsoft's Nano Server version of Windows Server 2016 addresses these needs. Nano Server focuses on running containers and is reported to be only about 5% the size of a complete OS deployment. It saves computing resources by removing the GUI, 32-bit support, remote desktop support, Microsoft Windows Installer and other ancillary services that remote cloud infrastructures just don't need. Nano Server is managed through PowerShell and Windows Management Instrumentation.

In this guide

Microsoft goes small

Nano Server in Windows Server 2016

Nano Server is a lightweight installation that is 93% smaller than a traditional Windows Server deployment. Despite its small size, Nano Server offers big benefits to enterprises. This section will break down the benefits of Nano Server, how to deploy it and what it means for Windows Server.

In this guide

Why Nano Server matters for businesses

Microsoft Nano Server, part of the forthcoming Windows Server 2016 release, is a new type of Windows Server deployment that is designed to provide the smallest footprint possible. Like any new Windows Server feature, administrators must consider whether it is appropriate for the organization, and if so, how to best use it.

Nano Server is similar to Server Core in that it lacks a GUI interface, but beyond that, there are several major differences between the two deployments. Nano Server also lacks the Win32 APIs the graphical environment requires. Many of these APIs still exist in Server Core deployments because they allow command prompt windows and similar items to be displayed. In contrast, Microsoft stripped support for MSI application packages or for 32-bit applications in Nano Server. Nano Server is so lightweight that it does not have a local interface, nor does it support local logins.

A whittled down version of Windows Server

In this guide

Microsoft made Nano Server so basic, so what can we do with it? After all, stripping away the vast majority of the feature set from Windows Server greatly reduces the server's capabilities.

Microsoft detailed four specific roles for use on Nano Server: DNS, DHCP server, Hyper-V and scale-out file servers. Since Windows Server 2016 is the first version of Windows Server to support the use of Nano Server, it seems likely Microsoft will support a very limited number of roles at first, and then add support for additional uses as Nano Server matures. Microsoft took a similar approach to Azure. For example, Microsoft did not initially support running Exchange Server on Azure virtual machines (VMs), which now it does.

It is easy to take a somewhat cynical view of these limited Nano Server roles. After all, services such as DNS and DHCP are already lightweight and do not generally consume many resources. As such, it's easy to question whether there is any real benefit to move these services off traditional VMs and into Nano Server.

Where Microsoft Nano Server can help

In this guide

Microsoft said there are three main areas where businesses will benefit from using Nano Server: security, availability and scalability. From a security perspective, Nano Server has an attack surface that is about 93% smaller than a Server Core deployment. Because Microsoft has removed so much of the code, the company estimates there will be about 92% fewer critical security bulletins released for Nano server.

The small code base affects server availability. Because so much of the legacy code is gone, patch management becomes easier and less intrusive. Microsoft estimates there will be 80% fewer reboots required in the patch management process.

Lastly, Microsoft said Nano Server will provide significant scalability. Nano Server has a small footprint, and this, combined with the types of roles Microsoft envisions, means Nano Server should consume fewer system resources. This feature will allow IT to develop higher levels of virtual server density. According to some estimates, a single Hyper-V host may be able to accommodate 1,000 or more virtualized Nano servers.

In this guide

How to deploy Nano Server

Windows Server 2016 features Nano Server, an extremely minimalistic Windows Server deployment that's smaller than Server Core but more difficult to install. Currently, administrators don't have an option to deploy Nano Server from Windows Setup. So, how do you deploy Windows Nano Server -- without an option in Windows Setup? Let's take a look.

The Windows Server 2016 preview 2 installation media contains a folder called "Nano Server" that contains a Windows Image file. This WIM file must be converted into a bootable virtual hard disk.

Microsoft provides a script on its website called Convert-WndowsImage.ps1 and this PowerShell script is designed to convert a Windows image file into a virtual hard disk. That may make it seem as though deploying Nano Server is a somewhat simple process; however, the devil is in the details.

If you convert the WIM file to a virtual hard disk file, that virtual hard disk won't be bootable. The easiest way around this problem is to run the script on a Windows 8.1 machine; the script does not currently work on Windows 10. The parameters you must include are:

In this guide

WIN -- The path to and name of the .WIM file

VHD -- The path to and name of the virtual hard disk that you are creating

DiskType -- A fixed disk type is preferable

VHD Format -- VHD or VHDX

SizeBytes -- The virtual disk size -- 2GB should be enough

Edition -- This parameter must be set to 1

Running the Convert-WindowsImage.ps1 script with the specified parameters will create a bootable virtual hard disk. However, Windows Nano Server won't do anything if you stop there. The Windows Server 2016 preview 2 installation media contains a number of packages that need to be injected into the image.

To do this, mount the virtual hard disk and then use the Add-WindowsPackage PowerShell cmdlet to add the contents of each package to your virtual hard disk. However, the Add-WindowsPackage cmdlet is based on DISM; the Windows 8.1 version of DISM won't work with Windows Server 2016. Therefore,

In this guide

it's best to copy your virtual hard disk to a Windows 10 machine and perform the package injection there.

While the virtual hard disk is mounted, you will need to create a Windows installer answer file (unattend.xml) because Windows Server 2016 Nano Server does not include a user interface -- not even PowerShell. Without an answer file, there is no way to provide Setup with an administrator password. The Windows installer answer file should be exactly the same as any other answer file you would use when deploying a sysprepped image.

The last step is to dismount the virtual hard disk and connect it to a Hyper-V VM. But be careful: Compatibility problems have been noted between Windows Nano Server and Generation 2 VMs. I recommend creating a Generation 1 VM.

When you boot the VM, a Windows logo will appear and you'll have to wait for the process to complete. Windows has to install itself before it is ready to use. The process is complete when you see a solid black screen.

In this guide

What does Nano Server mean for Windows Server?

With the buzz surrounding the Windows 10 release to manufacturing and general availability, you may have missed an important out–of-band Windows Server announcement. It was totally reworked to be smaller, faster, more nimble and more secure. This version is Windows Nano Server, and it's an important development.

We first heard about Windows Nano Server in early 2015 when Microsoft distinguished engineer and lead architect Jeffrey Snover discussed it in a blog post. Windows Nano Server is a lighter version of Windows Server designed to run exclusively in cloud and container scenarios.

It strips out the graphical user interface stack, desktop and interactive application compatibility, as well as the entire 32-bit compatibility layer -- it will only run 64-bit applications. Nano Server doesn't support installing applications through Microsoft Installer technology, which further erodes traditional application support.

The benefits of this lobotomy of the traditional Windows Server product are legion:

- The installed size of an entire Windows Nano Server instance can be up to 93% smaller than traditional Windows Server setups.

In this guide

- Reboots because of security patches and other sorts of configuration administration tasks are cut down by 80%.
- In an analysis of security patches, Microsoft was able to demonstrate that 92% fewer critical patches would apply to a production Nano Server deployment than a traditional Windows Server instance.
- The time required for a preboot execution environment to boot and install Nano Server over the network reduces from 19 minutes to three minutes.

Nano Server supports runtimes for C#, Java, Node.js, Python and more, so it makes for a compact, lightweight and robust Web server and Web application role. It also supports Hyper-V and scale out file server clusters, meaning you could have lots of these small Nano Server instances provide file server support on a fault tolerant basis; it would also be at a significantly lower cost than you can do so today because of the traditional Windows Server resource requirements in that role. You can program against it directly using Visual Studio, which is great for your development team to roll out a new application complete with a preinstalled operating system, such as Docker or other container options. You can also manage Nano Server instances with System Center, PowerShell remoting and the old-fashioned Windows Management Instrumentation. Most of your existing remote management tools will still work, but interactive ones and those requiring an agent to be installed on the system won't function with Nano Server.

In this guide

Why is Windows Nano Server important?

I think Windows Nano Server is the biggest thing to happen to Windows Server, or maybe even the entire Windows platform itself, since Active Directory. Active Directory's introduction in Windows 2000 cemented a move away from the 16-bit kernels of Windows 3.1, Windows 95 and Windows 98 while ushering in the NT codebase as the one from which Windows would be built -- we still use that today. It improved the Windows platform's usability and stability, so much so that I don't think computing would be where it is today if Microsoft hadn't made that move.

Nano Server signals a similar sea change for Windows. It's a break with the past -- the complete elimination of interactive applications and 32-bit application compatibility -- and solves problems that can make Windows insecure and unreliable. A clean departure from the albatross of robust backward compatibility allows Nano Server to really get compact and rugged. It makes Nano Server instances extremely portable, executable anywhere -- from a local Hyper-V host to a server closet -- and makes having an "OS appliance" a reality.

Think about the pure scalability of this option. Microsoft has frequently put up to 1,000 Windows Nano Server instances on a single host. For Web hosts and others who always look to compartmentalize and consolidate, stacking hundreds of virtual machines on one host is a dream come true. Your scale out file server clusters can happen with a few thousand dollars' worth of hardware

and your existing storage area network, not with thousands of dollars of machines equipped to run the full Windows Server version. Your developers can package up their own applications complete with a well-tuned, customized, fully set up Web environment and make it part of their installable package, fully realizing the promise of the DevOps movement while eliminating a lot of back and forth between the developers and the IT team to get configurations tweaked and "just so."

Windows Nano Server is a hugely important development. Watch for its general availability alongside Windows Server 2016 early next year. While it might not be totally practical for you right now, it will be soon.

How Nano Server is changing containers

In anticipation of the upcoming Windows Server 2016 release, Microsoft has been educating customers on the virtues of Nano Server. Microsoft Nano Server is a new type of Windows Server deployment that will allow IT pros to create tiny, single purpose, Windows Server deployments. Regardless of whether your organization intends to use Nano Server, Server Core, a Windows Server deployment with a full GUI, or some combination of the three, it is still possible to take a cue from Nano Server. The goal of Microsoft Nano Server is

to minimize the operating system footprint. However, minimizing your server footprint is a good idea, even if you do not plan to use Microsoft Nano Server.

Less code means less risk

So why should IT professionals reduce the Windows Server deployment size? One commonly cited reason is it improves security by shrinking the server's attack surface. There is an old rule of computing that states as the code base grows, so does the chance of adding a security vulnerability. In short, increasing the amount of code running on a server gives the bad guys more to work with. It is theoretically easier for a hacker to compromise a server running a large, complex set of code than a server running an extremely minimal code base. The more complex system contains more potential points of entry for the hacker.

Fewer running resources can boost speed

Another reason organizations should reduce the server footprint is to reduce costs while also improving performance. Reducing the server's footprint means eliminating anything that isn't necessary. This might mean shutting down unneeded OS services, disabling unwanted OS components or even uninstalling management tools -- assuming those tools can be run elsewhere. These and other actions generally cause the server to consume less memory and CPU time. The server may also consume less storage space, and might even generate fewer requests for storage IOPS. As a result, the server's

In this guide

performance may increase because the available hardware resources are not being wasted by running unnecessary code.

In virtualized environments, this more efficient use of hardware resources translates directly into cost savings. Reducing a virtual machine's (VM) resource consumption increases a host server's potential VM density.

A smaller Windows Server deployment can reduce issues

Another benefit to reducing the size of a Windows Server deployment is that doing so may allow you to compartmentalize functionality, which provides a number of different benefits of its own. The goal behind compartmentalizing server functionality is to make it so each of your servers performs one very specific task. This means running a single application on each server, and separating out dependencies wherever possible. System Center Virtual Machine Manager, for instance, has a dependency on SQL Server. In smaller organizations, it is possible to run SQL Server and VMM on the same server. Compartmentalizing the application however, would mean running SQL Server on one VM and VMM on another.

Compartmentalizing workloads in this way may increase the number of VMs that exist within an organization. Even so, there are advantages to using single purpose VMs.

In this guide

Because each VM performs a very specific function, it becomes easier to troubleshoot problems. Not only should it be relatively easy to figure out which VM is causing a particular issue, but running a single application or a single module on each VM eliminates any possibility that two applications are conflicting with one another inside of the VM.

You may also find that running one specific workload on each VM improves the overall availability. A single purpose VM that is running a minimal code base is going to theoretically require fewer patches than a server that is running multiple applications. This should translate directly into fewer required reboots.

Running one workload per VM can make it easier to perform future upgrades. It is much easier to predict the outcome of an upgrade to a server that is running a single, well-defined workload than to anticipate what might happen if you attempt to upgrade a server that is running multiple workloads. Even if your organization is already running one workload per VM, minimizing a VM's footprint by disabling or uninstalling unnecessary components will help to ensure the success of future upgrades, because there will be fewer potential points of failure.

In this guide

Admins anticipate containers, Nano Server in Windows Server 2016

Microsoft generated quite a bit of fanfare for its moves in the consumer space following the release of Windows 10 and its renewed push toward establishing itself as a hardware vendor with the Surface Pro 4 tablet, Surface Book and Microsoft Band. In the enterprise space, the company also drew enthusiasm for the number of Windows Server 2016 features it added with each ensuing technical preview.

For administrators, the biggest news in the software space was how Microsoft was going small with the next version of Windows Server to help businesses even further maximize their resources beyond traditional virtualization. Microsoft released three technical previews of Windows Server 2016, refining and adding features with each consequent release. The company unveiled Nano Server in the second technical preview, offering a barebones version of Windows Server for hosting containers and Hyper-V virtual machines. The third technical preview debuted support for Windows Server containers to fit more virtualized applications on a host. Microsoft also delivered Hyper-V containers in technical preview 4 of Windows Server 2016, wrapping up containers inside a virtual machine for added security.

We asked our SearchWindowsServer contributors to tell us what they were anticipating the most from Microsoft in 2016 and why.

In this guide

Adam Bertram

It's almost 2016 and Windows administrators should be excited for a ton of new features coming from Microsoft in the server space. I've decided to focus on a few items that have garnered lots of attention. If Windows Server 2016 RTM is anything like the technical previews, administrators should prepare now to dedicate some serious time to exploring everything in the server OS.

Nano Server

I see Nano Server, the brainchild of technical fellow Jeffery Snover, as the most important new operating system coming in 2016. Enterprises are struggling with VM sprawl. They are wasting precious resources to host these VMs that are sometimes only running at 10% utilization or less. Microsoft introduced Nano Server in April 2015 to provide enterprises with a server that's fast; small; and, due to its minimalistic nature, secure. Microsoft built Nano Server without a GUI to strip out gigabytes of unnecessary artifacts to make it 93% smaller than Windows Server with a GUI. Microsoft claims Nano Server will reduce reboots by 80% and result in 92% fewer critical bulletins.

Containers

With the meteoric rise of container darling Docker, containers were a hot topic in 2015 and show no signs of slowing down for 2016. Although Linux containers have been around since 2008, it wasn't until 2015 that Docker made them cool.

In this guide

As an answer to containers, Microsoft has released Hyper-V and Windows Server containers -- and provides Docker support in Windows Server 2016. I'm looking forward to seeing where Microsoft-supported containers go in 2016.

Nested virtualization

Have you ever needed to virtualize a Hyper-V host? I have! I am a trainer and use demo environments with virtualized servers every day, but building a lab to demonstrate concepts of a Hyper-V host meant we had to pull together some physical hardware. This is no more. Using "meta" virtualization we can virtualize a Hyper-V hypervisor through nested virtualization!

PowerShell Direct

When you've got dozens -- or hundreds -- of Hyper-V VMs to deploy, sending commands to them without a network connection used to be a pain. Now, with PowerShell Direct in Windows Server 2016, Microsoft removed that limitation. PowerShell Direct provides a simple way to manage Hyper-V VMs through a powerful new parameter to the PSSession cmdlets called VMName. No network stack needed.

Brien Posey

The thing I am looking forward to the most from Microsoft in 2016 is the Windows 10 Phone. Some of the next generation Windows Phones will be able to function as a PC replacement, running Windows 10 universal apps and

In this guide

supporting keyboard, monitor and mouse connectivity. These phones will essentially be the same as having a PC in your pocket.

On the server side, I am most looking forward to the next version of Hyper-V called Hyper-V 2016. The next version of Hyper-V will have a number of improvements to an already excellent hypervisor. One of the new features that I am most excited about is discreet device assignment. This feature maps a PCI device to a specific VM, giving the VM ownership of that device. This could lead to the virtualization of servers that had special hardware requirements that prevented them from being virtualized.

Microsoft is also going to make it possible to add or remove network adapters and memory while a virtual machine is running, allowing administrators to reconfigure VMs without needing to reboot. The ability to hot add or remove network adapters will be supported for generation 2 virtual machines running Windows or Linux. Hot adding or removing memory will be supported for both generation 1 and generation 2 virtual machines.

Another feature that I am excited about is updates to the Hyper-V integration services will be delivered through Windows Update. Currently, it's a pain to update the Hyper-V integration services for VMs that are running a guest operating system that does not match the host operating system. Delivering Hyper-V integration services updates through Windows Update will ensure the integration services remain up to date, and VMs are able to fully utilize the hypervisor's capabilities.

In this guide

Trevor Pott

I think the biggest thing to look forward to in Windows Server 2016 is containers. Containers are a big hit with developers, and this might spread to Windows if Microsoft manages everything right. In turn, this could help drive adoption of Azure; however, I honestly think Microsoft's moves to disconnect legal liability in its European operations from its U.S. headquarters will have a much greater impact on cloud uptake than any Windows Server 2016 features. Americans can't understand it, but privacy and data sovereignty actually mean something in the rest of the world.

Storage replica might be interesting, but it might also be too little, too late. Storage replica is really of interest to an organization that wants to roll its own small hyper-converged clusters. Multiple players are offering hyper-converged solutions for Hyper-V today, so the relevance is disputable. It's a nice to-have, however.

Hewlett Packard Enterprise's "Azure in a can" hyper-converged offering is probably more important than any feature of Windows Server itself, as it brings Microsoft's hybrid cloud solution to the masses. Microsoft's cloud tools have been horribly unfriendly to install, administer and use, but this Azure product just might be usable. That's a huge step forward and will make Microsoft a real threat in 2016.

In this guide

Hyper-V hot-add of NIC and memory are also very important. This brings critically needed feature parity to Microsoft's offering and finally allows it to catch up to VMware for serving tier 0 and tier 1 applications. This will let Microsoft start challenging VMware for critical application hosting.

What I believe won't be a huge deal is Nano Server. So far, Windows Core hasn't seen huge uptake, and neither has Hyper-V Server. Windows administrators still use full-fat GUI installs to do everything, even if it is "just" a Hyper-V server.

Microsoft wants to wean administrators from RDPing into servers, but doesn't understand that many administrators don't want to be tied into the client/server lock-step. They need to be able to manage servers remotely from older versions of the Windows client operating system, which Microsoft does not allow.

Ed Tittel

There's quite a bit of buzz building around a Remote Desktop Universal Windows Platform (UWP) app. This tool will let Windows Phone users access their Windows 10 PC desktops through the Continuum feature. Sounds pretty slick and handy, right?

It's supposed to be ready in a Windows Server Technical Preview sometime very late in 2015 or early in 2016 for Windows 10 Mobile. Given where we're at

in the build cycle for Windows 10, that probably means some preview build in the short term and inclusion in the next "big" set of cumulative updates.

I see it as a trend to put smart devices and smartphones on the front lines of computing everywhere. The excellent remote access and remote control environment called TeamViewer already makes this possible, and it also already supports iOS and Android. Except for the small percentage of phone users who've stuck it out with Windows-based hardware and software, that future is pretty much already here.

Manage Windows Server 2016

Keep the server OS running smoothly

This section of the guide will walk you through how to manage Windows Server 2016 using features such as rolling cluster upgrades and PowerShell Direct.

In this guide

Rolling cluster upgrades reduce downtime

Mission critical workloads running in a Windows Server environment are almost always clustered. The workload might be running on top of a clustered Hyper-V deployment, a hardware-based failover cluster or even a guest cluster. All of these commonly used forms of clustering are based on the Failover Clustering Service.

Failover clustering has always presented a special challenge with regard to operating system (OS) upgrades. Failover clusters prevent a mission-critical workload from going offline during a hardware failure. Even so, the process of upgrading cluster nodes -- the Windows servers that make up the cluster -- to a newer Windows version has typically resulted in some downtime for the clustered workloads. Some administrators will build a new cluster and migrate workloads instead, but this approach requires extra hardware resources and comes with its own challenges. This is where rolling upgrades come in.

In Windows Server 2016, rolling cluster upgrade support will make it possible to upgrade existing Windows Server clusters to Windows Server 2016 without downtime.

Functionally, cluster OS rolling upgrades are very similar to Active Directory upgrades. Imagine an organization has an Active Directory forest based on domain controllers running Windows Server 2008 R2 and wants to upgrade its domain controllers to Windows Server 2012 R2. This upgrade does not require

taking the Active Directory offline or rebuilding it from scratch. Instead, Microsoft makes it possible to blend the old with the new.

An administrator would upgrade Active Directory by upgrading one domain controller at a time to the new OS, perhaps also adding a few new domain controllers in the process. This workflow keeps the Active Directory functional throughout the entire upgrade because there is never more than one domain controller offline at a time.

It is possible to upgrade Active Directory this way because the new Windows Server OS -- in this case, Windows Server 2012 R2 -- is backward compatible with the existing OS, Windows Server 2008 R2. Once all the domain controllers have been upgraded, the Active Directory is technically running on Windows Server 2012 R2, but still behaves as if it is running on Windows Server 2008 R2. This is due to the use of functional levels. Functional levels essentially tell the domain controllers to act as if they were running a specific OS. If all the domain controllers were running Windows Server 2012 R2, but the domain and forest functional levels were set to Windows Server 2008 R2, then Active Directory would behave as if it were running on Windows Server 2008 R2 servers. None of the new features that were introduced after Windows Server 2008 R2 would be used, and it would continue to be possible to join Windows Server 2008 R2 domain controllers to the domain. Active Directory only behaves as though it is running on Windows Server 2012 R2 after the administrator raises the functional level.

In this guide

Microsoft applies this approach to cluster upgrades in Windows Server 2016. Microsoft allows administrators to upgrade cluster nodes one by one, until all of the nodes are running the new OS. Even up to this point, the upgrade process is reversible. If the administrator decides to back away from using Windows Server 2016, they can revert to previously used OS.

The upgrade becomes permanent if the administrator raises the cluster functional level. Just as the forest functional level and the domain functional level settings determine the behavior of supported OSes for domain controllers, the cluster functional level tells Windows whether the cluster should behave as a native Windows Server 2016 cluster or as a legacy Windows Server cluster.

Currently, there are a number of restrictions and limitations to rolling cluster upgrades that may change when Windows Server 2016 is officially released. Some of the more significant restrictions include:

- The cluster being upgraded must be running Windows Server 2012 R2.
- In-place upgrades of cluster nodes are not supported. A clean installation of Windows Server 2016 is required.
- All cluster level management actions, including adding nodes to the cluster, must be performed using the Windows Server 2016 management tools.

Microsoft recommends that you avoid reconfiguring storage or adding storage to a mixed-mode cluster because of lingering compatibility issues.

In this guide

Essential security improvements in Windows Server 2016

Windows Server 2016 is almost here. The preview, dubbed the Windows Server Technical Preview, is available now with the final release slated for early next 2016. Regardless of your current plans for Windows 2016, it's good to think about how these changes and improvements could affect security for enterprise setups.

Whenever Microsoft releases a new operating system (OS), think about how the company addresses security differently and how the new OS can be broken. Beginning with Windows Server 2008 R2, the server OS has continued to be resilient out of the box. But there are five forthcoming security changes for Windows 2016 that will interest enterprise Windows Server admins and security professionals.

Windows Server 2016 security changes

2. There's a strong authentication option through Microsoft Passport that relies on public and private key pairs in Azure, onsite public key management and

In this guide

Trusted Platform Module chips on the endpoints. There are also additional improvements for Active Directory Federation Services and Azure Active Directory involving Lightweight Directory Access Protocol, access control policies and single sign-on.

3. A feature called Just Enough Administration -- a PowerShell tool introduced in 2014 -- will also be available. JEA gives admins the option to place more granular restrictions on specific tasks to help ward off "Snowden" types of situations.
4. Windows Server 2016 supports HTTP/2 via Internet Information Server 10.0, which includes denial of service protection and includes features such as header compression, protocol block sizes and flow control. This won't fix underlying application layer flaws, such as SQL injection and weak login mechanisms, but it's a necessary step for successful Web protection.
5. Windows Defender is installed and enabled out of the box, even in the non-graphical user interface (GUI) version of the OS. I often see servers with no antimalware protection and the negative consequences.
6. The telnet server is not included. Microsoft realized that people will still use an inherently vulnerable service because that's what they know and it's there. Given how prevalent telnet is across most network environments I see today, I

In this guide

suspect the service and its flaws won't go away anytime soon. But at least Microsoft is doing its part to help fix the fixable issues.

There are also a number of resiliency benefits outside of security in Windows Server 2016. These involve features for disaster recovery, VMs, network interface card fault tolerance and storage Quality of Service nearly all organizations and use cases can benefit from. These features in Windows 2016 won't make your network environment inherently compliant or secure, but they'll certainly provide you with another leg up on achieving those goals.

Now that you have an idea about the security changes in Windows Server 2016, begin thinking about how current and future projects may benefit from using these features. I've only seen rare instances of Windows Server 2012 usage in the enterprise. Perhaps the stigma of the Metro GUI is passing and Windows 2016 will be the next big thing. Or, it may provide a good upgrade path for many Windows 2003 Server installations that still exist.

In this guide

Why Microsoft hasn't gotten rid of the GUI

One of the most significant features that is slated to be released as a part of Windows Server 2016 is Nano Server. Nano Server is a new Windows Server deployment model that is far smaller than even the most modest Server Core deployment.

To create such a small operating system, Microsoft eliminated any component that was not essential to the server's functionality. This included the Windows Server GUI. Although Nano Server contains a very lightweight text interface, it is primarily used to modify network and firewall settings. The interface is similar to the one that VMware provides with its hypervisors.

For several years now, Microsoft has been telling its customers that Server Core is the preferred Windows Server deployment type. Server Core marked a radical departure from a traditional GUI interface, and the upcoming Nano Server will abandon the GUI altogether. In the technical previews of Windows Server 2016, the preferred deployment method does not install the GUI by default.

If Microsoft is encouraging customers to deploy operating systems with either a light GUI interface, or no GUI at all, it seems fair to consider why Microsoft continues to produce a GUI interface for Windows Server. To the best of my knowledge, Microsoft has not made an official statement why it continues to

allow GUI-based deployments, but I believe there are at least three major reasons.

The demand is still there

The first reason why Microsoft continues to include a GUI is customers still want it. Sure, there are IT pros who prefer using the command line and enjoy creating elaborate PowerShell scripts, but there are still countless administrators who prefer to point and click their way through a task. This isn't surprising when you consider Windows Server has had a GUI since its debut more than 20 years ago.

Administrators have gotten used to using a GUI, and therefore the GUI interface remains the preferred management tool for many.

Consider the backlash Microsoft received when it made the decision to omit the Start menu from Windows 8. A lot of users were angry and frustrated -- all over a single menu. Now imagine if Microsoft decided to abandon the GUI altogether.

Admittedly, it was mostly end users who were upset over the absence of the Windows 8 Start menu, and Windows Server is geared toward IT pros. Even so, the Windows 8 incident demonstrates how passionate some people can be about the interface.

For the sake of accessibility

In this guide

A second reason why I feel Microsoft has chosen to keep the Windows Server GUI around for the time being is because the management tools have to run somewhere. It's likely that Microsoft will move the administrative tools such as Active Directory Users and Computers and Server Manager out of the server OS and onto either a Web interface or onto a desktop operating system. For now, being able to access the management tools from the server console is a convenience feature, especially for smaller shops.

The GUI is still a necessity

Finally, I think the number one reason why Microsoft continues to include a GUI with Windows Server is because most applications require it. The vast majority of the server side applications that I have installed over the years could not be installed without a GUI.

In Windows Server 2012, Microsoft gave us the ability to remove the GUI. One of the reasons why Microsoft chose to add this functionality is while many applications can be run without a GUI, they cannot be installed without one. The removable GUI makes it possible to install an application and then remove the server's GUI once the application is up and running.

Eventually, the Windows Server GUI will go away, but that day is most likely not to be for many years. Microsoft acknowledges there are both administrators and applications that rely on the GUI, so they are giving customers the ability to run

In this guide

Windows Server without a GUI, but are not taking the GUI away from those who wish to use it.

How administrators can prepare for Docker containers

Recent developments from Microsoft must have most traditional Windows systems administrators wondering how much heterogeneousness they can take on before systems -- and IT personnel -- are stretched beyond their limits. Windows Docker containers are coming, Linux virtual machines run on the Azure cloud platform, the forthcoming Nano Server has no GUI and requires PowerShell proficiency -- the client-server architecture is slowly crumbling away.

Where Linux and open source software were once considered a bane to the company, Microsoft has embraced new technologies that make application development and cloud computing more attractive to its customers. Demands for higher efficiency have spurred Microsoft to include support for containers in Windows Server 2016, due in the second half of 2016. Containers promise higher utilization of resources and faster application development -- but what does it mean for the average Windows systems administrator? Has the management portion of containers developed sufficiently to give IT the necessary tools to handle these workloads?

In this guide

We asked the SearchWindowsServer advisory board members for their thoughts on what Windows Docker containers will mean to IT administrators who have to contend with this new way of virtualizing applications.

Brien Posey

Containers represent a new and more efficient way to run applications. Virtual servers gained massive popularity because they allowed multiple workloads to run on a single server, but were terribly inefficient because each virtual machine (VM) had its own dedicated operating system (OS). Containers help to improve efficiency by allowing OS components -- and in some cases, application components -- to be shared by multiple containerized applications. This sharing occurs without compromising the isolation boundary that exists between containers.

Initially, the biggest challenge for Windows administrators will be the learning curve. Containers require administrators to think of applications, OSes and VMs in a new way. There are almost certainly going to be challenges associated with the transition to containers as a result of unfamiliarity with the technology. For example, administrators may have to rethink their approach to backups, troubleshooting problems and even workload scalability.

In this guide

Once Windows shops get past the initial learning curve, the biggest challenge with containerization is going to be management. Although tools exist for managing Windows containers, it is going to take some time before the tools fully mature.

Some have predicted that containers will eventually replace server virtualization. I don't think the hypervisor is going to go away any time soon, but its role may change. Eventually hypervisors will probably be more widely used as container hosts than VM hosts.

Trevor Pott

Containers could mean many things for the average Windows administrator. It really depends on how Microsoft licenses everything.

Done right, containers would be a replacement for how applications are installed in Windows. Instead of scattering libraries and data about the OS, everything -- literally every single file and registry entry -- required by an application would be restricted to that application's container. Installing an application would be as simple as copying over the container and registering it. Uninstalling will be as simple as deregistering the container and deleting it. This is important because

In this guide

installing applications in Windows has traditionally made them almost inseparable from the OS. Developers don't follow Microsoft's guidelines, and Microsoft's guidelines change all the time. Communication between containerized applications is also done through traditional networking instead of the internal message bus of the OS. This means it can be firewalled, inspected and otherwise have security applied at an inter-application level.

Lots of people think PowerShell is all you need. I suspect it's fine for them, but the overwhelming majority of Windows admins work for small businesses and prefer the GUI. Unless and until there's a much better UI available than Microsoft has proven capable of producing in the past several years, adoption will be restricted to those who love the command line and scripts.

For now, containers are a convenient means of packaging applications for organizations that have their own in-house development teams making in-house applications. They may be useful to a handful of hyperscale operations teams, but I do not see those kinds of organizations using anything from Microsoft. It doesn't make economic sense.

What is important to remember is that containers are emphatically not a replacement for virtualization. Anyone who says so doesn't understand

containers. Containers are a means of packaging applications. Hypervisors are a means of packaging OSes. There is a huge difference.

When I package an OS, I am wrapping up a complete environment. All libraries, kernel version, configuration, monitoring, network configuration and so on. OSes have a lot of moving parts. Tweak any one and you can greatly affect how an application works.

Containers can have some -- but not many -- network elements to themselves. They can have some -- but not all -- libraries relevant to an application packaged. They don't have the kernel of the OS packaged and many other environmental variables also remain set at the OS level.

If you have 10,000 applications that all need the same operating environment then by all means run 10,000 containers on the same OS. If, however, you have 10,000 applications that need eight different environments to run in, go run eight different VMs and sort your applications into containers on the relevant OS.

Despite Microsoft's best efforts, no data center is homogenous. Organizations run varied configurations even when running the same version of a given OS, and almost all organizations run multiple OSes. This means that different

In this guide

environments are normal and will be for the foreseeable future. Hypervisors are thus not going anywhere.

But containers allow easier packaging of applications. So the sane way to wrap this all up -- from an operations standpoint, at least -- is to deploy applications into containers that run on OSes that live in VMs. Where applications can share an OS configuration they are deployed in a container to the VM which contains that configuration. The end result is perhaps not the most efficient possible data center, but easily the most manageable compromise between theoretical perfect efficiency and real world ease of use for administrators.

Michael Stump

Microsoft's embrace of containers and Linux has many traditional Windows Server administrators scratching their heads, and for good reason.

For the last three years, we've heard that containers will take over data centers and clouds, while legacy technologies, such as x86 virtualization, will become the mainframe of the 21st century. That means no matter which hypervisor you choose to build your software defined data center, your world is about to turn

In this guide

upside down. VMware and Microsoft were quick to position their hypervisors as the ideal platform for your business' containers.

In October of 2014, Microsoft partnered with Docker to bring the most talked-about container system to the Windows platform. Then, Microsoft announced Hyper-V containers and Nano Server. Azure entered the mix with the ability to deploy Docker-managed VMs from the Azure Marketplace. Suddenly, it seemed as if Microsoft was "betting the company" on containers, and cloud-native applications were the new first-class citizens of the IT world.

Meanwhile, many enterprise customers were happily plugging along, worrying about things such as the upcoming end-of-life of Windows Server 2003, developing a cloud strategy and ignoring containers completely. And for good reason: enterprise customers with significant investments in data center facilities -- both physical and virtual infrastructure -- weren't looking for faster ways to spin up an Exchange server, for example. Containers solve a problem that most businesses don't have today.

To Microsoft's credit, it's not trying to solve today's problem. It's trying to become the preferred platform for solving tomorrow's problem, and that's laudable. And the introduction of support for solutions like Windows Docker and

In this guide

Nano Server does not telegraph the end of the old ways. Windows administrators will be able to use Server Manager -- or even Computer Management in the familiar Microsoft Management Console metaphor -- for the foreseeable future. In fact, it's possible that with Windows Server 2016, administrators and developers can peacefully coexist: admins can gleefully review event logs and deploy patches, while developers can command temporal legions of tiny VMs.

Containers will eventually make it to the enterprise, due in part to Microsoft's aggressive promotion of the technology as a core feature of future Windows Server releases. But for now, at least, containers are too bleeding edge for customers who are n-1 -- or n-2 or n-3 -- on OS releases.

Tim Warner

The concept of Docker containers usually makes Windows systems administrators nervous, especially those who have no prior experience with Linux and free, open source software. However, on further inspection, containerization bears many similarities to application virtualization.

In this guide

For example, many Windows systems administrators use tools such as Microsoft App-V, Citrix XenApp, or VMware ThinApp to package and distribute individual applications along with their dependencies.

Consider a business that recently upgraded all users to Windows 10, only to find out that the core line of business Web application doesn't work with the Microsoft Edge browser. Whoops. Application virtualization means administrators can distribute virtualized instances of, say, Internet Explorer 8 to users who can now use completely incompatible applications on their desktops.

Thus, with Docker containers we have the same idea: the ability to rapidly deploy isolated applications. Microsoft is taking this concept even further by including Windows Docker containers in the upcoming Windows Server 2016 OS.

Whereas Linux-based containers are used almost exclusively by application developers who need to quickly build and tear down development environments, in Windows Server 2016 we can use containers to rapidly release containerized -- that is, isolated -- Windows Server 2016 instances.

In this guide

The Windows Server containers are much more lightweight and agile than full Hyper-V or VMware VMs. Consider Nano Server -- the skeletal Windows Server installation option that has an installed disk footprint of little more than 650 MB -- to see where Microsoft is headed: a future where data centers host servers with the thinnest possible OS/hypervisor layers, deploying equally micro-VMs or containers.

The Nano Server option is particularly interesting. When you stand up a physical host and install Nano Server -- including the Hyper-V Server and container packages -- you have an even thinner hypervisor layer than ESXi. In turn, this Nano Server Hyper-V host can manage thick VMs -- when business needs require that option -- and thin Windows Server containers for alternative business requirements.

In short, it seems to me that any Windows systems administrator who wants to stay relevant should already be working hard to master Windows PowerShell, Docker containerization and DevOps methodology. Technology moves fast, and it's too easy to get left behind.

In this guide

How to use PowerShell Direct

Hyper-V administrators rely on remote management tools, such as Remote Desk Protocol or Virtual Machine Connect, if they need to execute PowerShell commands inside a Hyper-V VM. Although you can use the PowerShell Remoting feature to connect to a VM running on a Hyper-V host and execute commands remotely, this requires a working network connection, open network ports between the source and destination, and a series of PowerShell remote commands.

Windows Server 2016 Hyper-V hosts will help Hyper-V administrators solve common VM management problems. Starting with Windows Server 2016, you will be able to interact with VMs running on a Windows Server 2016 Hyper-V host in an easier, more reliable way. Before Windows Server 2016, a network connection and a modifying firewall configuration were necessary to run PowerShell commands inside a VM. Using the PowerShell Direct feature of Windows Server 2016, you can execute Windows PowerShell commands inside a VM from the Hyper-V host operating system (OS) without any network connection or modifying the organizational security policies.

There are a few prerequisites for using the PowerShell Direct feature. First, VMs and the Hyper-V host must be running Windows 10 or Windows Server 2016. Next, you must make sure that you are logged on to the Windows Server 2016

In this guide

Hyper-V host using Hyper-V administrator. All VMs must run on the "local" Hyper-V host and, finally, PowerShell must be installed in the VM.

It is important to note that PowerShell Direct is enabled by default on Windows Server 2016 Hyper-V hosts. The hypervisor code in Windows Server 2016 has been modified to include the PowerShell Direct feature, while the Hyper-V parent partition implements a PowerShell Direct component that runs under the VMMS.exe process. PowerShell Direct uses VMBUS communication channel to communicate with the VMs running on the local Hyper-V host.

There are two ways to run PowerShell commands using the PowerShell Direct feature. For the first method, you must begin by entering the following command:

```
Enter-PSSession –VMName <VMName>
```

This command allows you to create a PowerShell interactive session against the VM name specified in the –VMName parameter. After running this command, you can use the Get-Service command or run any other PowerShell command. When finished, run the Exit-PSSession command.

When you implement the above series of PowerShell commands on a Hyper-V host, the PowerShell cmdlet (Get-Service) is executed inside the VM and the output is shown in the PowerShell window of the Hyper-V host. The second method involves using an Invoke-Command cmdlet to allow you to run a

PowerShell command or a script against the VM specified in the –VMName parameter. Here is an example of using the Invoke-Command cmdlet:

Invoke-Command –VMName TestVM –FilePath C:\VMScripts\Script1.PS1

Invoke-Command –VMName TestVM –ScriptBlock { Get-Process }

At present, the PowerShell Direct feature isn't supported on VMs running on the remote Hyper-V host; the VMs must be running locally. It is also worth mentioning that the PowerShell Direct feature only works for VMs running Windows 10 and later OSes.

Stay up to date

Keep Windows Server 2016 news

This section will look at different Windows Server 2016 news stories.

In this guide

How Azure Stack integrates the cloud and data center

CHICAGO – Hoping to bolster its cloud strategies on a number of fronts, Microsoft debuted a sweeping set of products and services spanning Azure, Office 365 as well as upcoming versions of Windows Server and desktop.

What captured the attention of many of Microsoft Ignite 2015's 23,000 attendees here this week was Azure Stack, which is intended to deliver both infrastructure as a service and platform as a service to large data centers. This allows IT professionals to blend enterprise-class legacy applications, such as Exchange, SharePoint and SQL Server, with modern distributed applications and services that can all be managed from a single location.

The new offering, which works with the recently released Azure Resource Manager, helps IT administrators deliver more consistent application deployments when they are provisioned to the Azure public cloud or Azure Stack based in a data center. This allows users to write an application once and deploy them later, company officials said.

Users here who grapple with issues involving the melding of old and new enterprise applications were heartened by the news, but want more technical details.

In this guide

"I have to think this is an ideal solution for those with heavy investments in Microsoft legacy apps and platforms," said Jeff Haggerty, an IT administrator with a bank in Evanston, Ill. "But how they manage this combination [of legacy and modern applications] is what I am waiting to see."

In essence, Azure Stack is a meld of Windows Server 2016 Azure Service Fabric and Azure Pack, the latter a selected set of Azure features normally available to large enterprises. Besides combining Windows Server and Azure features, Azure Stack includes an improved Azure portal and Azure Resource Providers.

Azure Stack is the functional equivalent of OpenStack for Windows, according to Carl Brooks, an analyst with 451 Research, based in New York. It makes a Windows server look like Azure through a combination of several existing features, including Azure Pack and Azure Service Fabric, which is the "secret sauce that makes Azure scalable and manageable across more than one data center," he said.

The strategy is similar to VMware's attempts to have a seamless transition between on-premises servers and vCloud Air, Brooks said. Microsoft's goal is to be the default external service provider with Azure functioning as the server, hypervisor, orchestrator and interface.

This makes Azure more open -- with the caveat that you must buy Windows Server.

In this guide

Azure Stack vs. OpenStack?

Microsoft is so entrenched in data centers worldwide that Azure Stack – a name that is not-so-coincidentally close to OpenStack – should have a massive worldwide audience for IT departments transitioning to cloud, Brooks said.

Azure Stack could directly compete with OpenStack as a private cloud distribution, particularly for those that feel the open-source technology is immature or requires too much work to install and operate, Brooks said.

Windows Server users are typically behind the curve on implementing the latest version, but in a couple years Azure should become one of the standard flavors of compute and orchestration that people put in their own data centers, he said.

"By the end of 2016 it will fundamentally have changed the conversation about how to provision private cloud or how to do a tech refresh," Brooks said. "Potential customers for this are literally every IT department in the world."

Azure Stack is built on the same code as Azure, and will include a software-defined network controller and Storage Spaces Direct that will both sync and automatically failover, Microsoft said.

In this guide

The offering features shielded VMs and guarded hosts that deliver "zero-trust" software-defined security to private clouds that allows companies to more securely segment organizations and workloads, according to Brad Anderson, a Microsoft corporate vice president. It also is capable of monitoring access and administration rights.

"Users are working in a rapidly expanding world today which is good for collaboration, but that comes with an increasing risk," Anderson said. "You have to strike a balance with the right amount of empowerment with security and this is what we are think this product can achieve."

Another strategically important tool introduced here was the Microsoft Operations Management Suite, a hybrid management tool that handles corporate workloads whether they run on Azure, Amazon Web Services, Windows Server, Linux, VMware, or OpenStack.

Azure Stack provides an 'easy button' for on-premises private cloud deployments, but another important addition is Operations Management Suite, a SaaS-based delivery of log analytics, site recovery, and orchestration to support

a hybrid model, according to Mary Johnston Turner, an analyst with IDC in Framingham, Mass.

"They're really committing to providing customers a spectrum of on-premises and public cloud solutions that will interwork very closely because they're based on the same code," Turner said.

Previously, putting together a private cloud with Microsoft involved bringing together a couple different tools, and Azure Stack could fill the needs of enterprises that want to deploy private clouds but need an easier and more efficient way to do it, Turner said.

Azure Stack is expected to be available in late summer, according to the company.

More Microsoft software updates for business, IT

Microsoft also introduced a broadly distributed public preview Office 2016 that features real-time co-authoring to Office desktop applications – a feature found in Google Docs. The ability to view changes made to text in real-time better allows teams of people working together to stay up to date with each other as they create documents.

In this guide

Microsoft also launched Windows Update for Business, a service for Windows Pro and Windows Enterprise devices that delivers the latest Windows security protection and Windows features.

Also entering technical preview today is System Center Configuration Manager for Windows 10. The new offering has tools to deploy, update, manage and secure Windows 10 and integrates with Windows Update for Business.

Microsoft next week plans to release service packs for existing Configuration Manager 2012 and 2012 R2, as well as an update to Microsoft Intune that allows it to support Windows 10. The company also said it plans to deliver Exchange Server 2016 in preview later this year.

Second Windows Server 2016 technical preview excludes containers

CHICAGO - Microsoft released the second technical preview of Windows Server 2016 this week, but noticeably absent was the much anticipated Windows Server Containers and Hyper-V Container technologies.

In this guide

Given the strategic importance of the new container technologies to Microsoft, as well as its promise to give users more flexible ways to deploy Windows Server in a more bare bones version, some eager users here at the company's Ignite conference were a bit disappointed.

"It's clear now that containers are real and will have an impact on things like operating systems and other Microsoft products, [but] it would be nice to get my hands on it [Windows Server 2016 preview] sooner than later so I can know what I'll be dealing with for clients," said one senior technical administrator with a Chicago-based systems integrator. "[Microsoft will] likely have some tricky things to work through to make sure it works correctly with the rest of Windows Server," he said.

Windows Server Containers and Hyper-V will be included in the next Windows Server 2016 preview, due this summer, company officials said.

A Chicago-based IT consultant to financial services companies here at Ignite said Microsoft fell behind in developing Windows Server 2016 because the decision to include container technologies came late in the development cycle.

"They had hoped to get Windows Server out by 2015 but it has taken some time to integrate the [container] support in there," he said.

The container technologies are the most important change to the operating system in a long time, said Jeffrey Snover, lead architect for Windows Server,

In this guide

during a technical session. He described container technologies as a "deep refactoring" of the product "with a cloud emphasis."

The built-in container technology ultimately will heavily influence the way all versions of Windows Server are architected. The first version will be tightly focused on cloud infrastructure and born in the cloud applications, Snover said.

This first version will become the foundation of Windows Server with a range of different and more complex components or capabilities built on top of it, he said.

Besides the container technology, other new capabilities in Windows Server 2016 include support for rolling upgrades for Hyper-V and Storage clusters which, according to Snover, better enable VMs to continue operating even if the compute-cluster fabric fails. It also will have Storage Replica, which is a synchronous storage replication for both backup and disaster recovery.

The finished version of Windows Server 2016 will not ship until sometime in 2016, although Microsoft officials did not say whether that would be early or late next year.

Accompanying Windows Server 2016, Microsoft also showed off the second technical preview of System Center 2016. The latest release features enhanced Linux management capabilities, most notable Desired State Configuration support, as well as SSH support and better LAMP stack monitoring. The offering

also contains new monitoring capabilities for Azure, Office 365, SQL Server and Exchange.

Like Windows Server 2016, the finished version of System Center 2016 will ship sometime in calendar year 2016. However, the System Center Configuration Manager piece of the tools suite will ship in 2015 because of its support for Windows 10. Windows 10 is still due to ship in July, company officials said.

Docker containers may start hitting primary storage

Since their inception two years ago, Docker open source containers have been used mostly in application development and testing environments. How long before Docker containers are routinely deployed in primary storage is tough to forecast, but experts see a parallel to VMware, which gradually added features for creating, provisioning and managing storage to its server virtualization software.

"The key to Docker from a storage perspective is you really need a storage system that provides a lot of capabilities," said George Crump, president of IT analyst firm Storage Switzerland. "Like VMware in the early days, the storage aspects of Docker are pretty rudimentary. There's a dash-V parameter that allows you to mount images from a storage volume, but that's about all it does."

In this guide

Crump said VMware has "already ploughed the field" for Docker to make its way into primary storage systems, although it may be a slow process.

"My expectation is that Docker initially will be used in storage environments where you have a lot of the same instances. Say you're rolling out 80 Oracle or SQL Server apps. The efficiency and capacity should be high because you're not recreating all the operating systems within those apps," Crump said.

Docker storage similar, yet different, from VM storage

Docker is open source software for packaging a Linux application and its dependencies with a shared operating system. The buzz surrounding Docker storage containers thus far has exceeded widespread enterprise adoption of the technology.

But Crump and other industry observers say it's more a matter of when, not if, containers become a complement to virtual machine storage.

Docker Inc. commercialized the open source Docker container, but competitors are emerging, including Docker partner turned rival CoreOS with its Rocket container runtime engine. Google also last year unveiled Google Container Engine based on its Kubernetes open source container cluster management framework.

In this guide

EMC, Asigra, Catalogic and Zadara are among storage vendors to roll out product support for Docker containers. Microsoft said it plans to support Docker beginning with the rollout of Windows Server 2016.

Rob "Bubba" Hines, vice president of IT at Asheville, NC-based Signature Tech Studio, said his company runs thousands of jobs a day in Docker containers on Amazon Web Services. He said he is looking forward to taking advantage of Zadara's Docker support inside its Virtual Private Storage Array (VPSA), which Signature Tech uses as its main storage platform. But that will be a gradual process.

"Dockers have impacted the way we think about our architecture and infrastructure, but as far as our storage goes, a Docker instance is like any kind of virtual machine," Hines said. "It can access Zadara. Initially we'll run a handful of Docker containers inside the VPSA. I don't know if I'm ready to move hundreds or thousands into the VPSA, but maybe that's where we'll end up."

Docker containers bear similarity to virtual machines (VMs), but are also distinctly different.

"The biggest difference between VMs and containers is granularity," said Greg Schulz, founder of the StorageIO Group. "I could run five or 10 different VMs on a physical machine. With a container, I could run hundreds, if not thousands of lightweight instances simultaneously. Each container doesn't need to have its

own full-blown operating system, libraries and everything else associated with running a server."

Docker lacks native storage features for data protection such as replication and snapshots.

Docker containers don't natively provide persistent storage

Lack of data persistence and portability is also holding back containers from full-blown use in shared storage, Schulz said.

"You can move containers around, but here's the catch: Where is the data? You need to use a container that's configured for persistent storage," Schulz said.

Newcomer Portworx is trying to tackle that problem. Portworx has designed PWX software for scale-out block storage in Docker volumes, but it will not be available before 2016. Portworx CEO Murli Thirumale said PWX would enable containerized applications and their associated data to be ported between on-premises and cloud storage.

"We're managing the storage by attaching via graph drivers, not as an externally mounted storage," Thirumale said. "We're native to Docker and have the ability to retain whatever file system the Docker container uses. We keep that data while we mount and provide access to a block storage layer below that. The idea is that we're letting that container have access to a block of storage as it's moved from node to node."

In this guide

PWX is designed to run on x86 servers and Amazon Elastic Compute Cloud Instances, and it will consist of a block storage layer overlaid with orchestration and scheduling of container-level snapshots.

Portworx' debut comes on the heels of a partnership this month by EMC and ClusterHQ. EMC used ClusterHQ's Flocker software to develop pluggable drivers for Docker shared storage on its XtremIO and ScaleIO storage. The Flocker agent lets users move containerized applications and their data across a cluster of servers.

"Moving a storage volume from one container to another on the same server is mildly but not terribly interesting. A lot more valuable is being able to move a container from one physical server to another physical server and have its data go with it," ClusterHQ CEO Mark Davis said.

Container storage is new twist on familiar idea

Crump said companies provisioning storage for Hadoop clusters will notice similarities to Docker.

"Hadoop started with everything being local storage, and over time shared storage has become the preferred way to configure a Hadoop cluster. Docker is much the same way in that most implementations are using local storage. But as your Docker environment starts to scale, you'll want isolated containers that have the ability to communicate with each other," Crump said.

In this guide

Docker terminology may seem arcane to storage admins, but the concept is similar to creating a logical bucket of storage in Amazon Web Services or firing up database instances for Oracle applications, Schulz said.

"The simplest way for storage administrator to think about Docker is that it's just another application that needs storage," he said. "They need to provision storage for containerized apps, just as they do for the hypervisor, a bare-metal server or database backups."

Changes to Windows Server 2016 licensing

Microsoft's attempts to steer customers toward hybrid-cloud use on its Azure platform as part of a new Windows Server 2016 licensing model may not work as the company expects, according to at least one licensing expert.

That's in addition to what IT pros and attorneys who deal in licensing cases agree is likely to happen: many users will pay more for Windows Server licensing when Microsoft shifts billing from a per-processor basis to per-core later this year. The new billing model will be part of Windows Server 2016

Datacenter and Standard Edition when it enters general availability, which Microsoft says will happen in the third quarter of 2016.

n addition to the per-core billing, Windows Server client access licenses will still be required for every user or device accessing a server, according to the company.

"Somebody at Microsoft is probably rubbing their hands together at the opportunity to increase revenue through non-channel sources," said C. Christopher Barnett, a senior associate attorney at Scott and Scott, LLP in Southlake, Texas, who deals with software licensing cases.

If Windows Server 2016 was sold in a different marketplace, the move could cause users to explore other options. However, given the current landscape of choices in the data center where Windows Server is so familiar to IT pros and holds a commanding market share, the latest licensing change likely won't push users away from the upcoming server operating system, Barnett said.

"Microsoft knows there is elasticity with its Windows Server relationship with customers that allows it to push and push and push without breaking the relationship," he said.

Barnett's forecast for higher costs is based, in part, on his experience when a similar shift occurred with SQL Server 2012, where he saw costs rise after a change to per-core licensing.

In this guide

In addition to increasing costs for many users, the new billing model also is more complex, according to Barnett. Users will need to make sure they properly count the cores they are using to avoid a larger bill in the future. Each processor will need to be licensed with a minimum of eight cores, and each physical server will need to be licensed with a minimum of 16 cores, according to Microsoft. Licenses for servers with eight cores or less per processor will be same price as the Windows Server 2012 R2 two-processor license price, according to Microsoft.

The list price will increase by about 50% to license the same size servers with the same number of processors and cores. For example, a four-processor server with 12 cores per processor will go from $1,754 with Windows Server 2012 R2 Standard to $2,631 with Windows Server 2016 Standard under the new licensing scenario. Under the same scenario for Windows Server Datacenter, licensing costs would go from $12,236 for 2012 R2 to $18,354 for 2016, according to Paul DeGroot, principal consultant at Pica Communications in Camano Island, Wash.

"This is not good news for companies that run big data centers," Barnett said. "I don't believe it is something that will be warmly received by Microsoft customers once they start getting their hands dirty."

Enterprises are "soft targets" for more revenue, according to Carl Brooks, an analyst with 451 Research in New York. Microsoft's shift toward consumption-based billing aims to put data center and cloud billing on the same page, Brooks

In this guide

said, and recognizes where the company sees its growth opportunity: with providers.

In the past year, Window Server licensing revenue has been up 7% from service providers, while on-premises licensing fees have dropped 2% in the same time, according to Brooks.

For Microsoft customers with software assurance, the new licensing model will not affect them until renewal time, according to Microsoft. But the company acknowledges "there may be an increase in the cost of software assurance relative to the increase in processing power."

Microsoft has argued the new billing model offers greater value, including sessions in Azure, its cloud computing service.

The move to change the licensing of Datacenter and Standard editions from processors to physical cores "aligns licensing of private and public cloud to a consistent currency of cores and simplifies licensing across multi-cloud environments," according to the company's Windows Server 2016 Pricing and Licensing FAQ.

This follows the October 2015 addition of an "Azure benefit" for customers with Windows Server licenses with software assurance, allowing them to upload Windows images to Azure and pay just compute rates.

That reflects Microsoft's intent to move more users to Azure, and convert software assurance customers from a support and maintenance model to a hybrid cloud model, Barnett said.

What's best for end users?

Although Microsoft says this licensing change encourages users to move from their own data center to Azure, the new licensing fee structure makes it more attractive for Datacenter edition users to stay put. For companies that want to use Azure, they should purchase those cloud licenses separately, according to DeGroot.

In the cloud, both editions offer the same right -- two VMs on up to eight cores each or one on up to 16 cores. But on-premises, the Standard edition allows just two VMs while the Datacenter edition allows unlimited VMs, which makes it the best option for most enterprises, according to DeGroot.

In this case, transferring Datacenter edition licenses to the cloud will offer no additional benefit.

"I would optimize on-prem and I would not move those licenses to the cloud," said DeGroot.

The idea behind hybrid cloud is to move workloads between on-premises and the cloud, but DeGroot sees the new Window Server 2016 licensing model encouraging what he calls a "binary" treatment of workloads.

In this guide

"The whole notion that I will move a workload from on-prem to the cloud is killed by what happens when I move to the cloud," he said.

For many Windows Server customers, the new licensing model introduces a new set of questions and challenges.

"It is difficult for Microsoft to transition users to a new version of Windows Server; there is a lot of Windows Server 2003 out there," and transitioning to a new version will be a major disruption, according to Christian Perry, principal analyst and practice manager at Technology Business Research in Hampton, N.H. "[Add to that] a new pricing model that users might not perceive as beneficial to their bottom line. You are bringing in new issues where there are already unresolved issues."

Hewlett Packard Enterprise's Moonshot is an example of a product that has had some challenges because the licensing is done by core, Perry said.

"If users are [accustomed] to licensing on a per-box basis, they might not be willing to turn on cores. That can impact performance, and then you have virtualization issues -- a whole range of things are impacted across the data center," according to Perry. The move to Windows Server 2016, he predicts, will likely be "a sluggish rollout at best" this year.

In this guide

Docker and Azure CTO discuss containers

Docker burst onto the scene as a way to manage Linux containers, but over the past year the company behind the open-source project has also been working with Microsoft to incorporate those capabilities onto Windows. The two sides are partnering on full integration of Docker into the next version of Windows Server, with Windows Server Containers and Hyper-V Containers, expected out some time in 2016.

Docker co-founder and CTO Solomon Hykes and Microsoft Azure CTO Mark Russinovich talked to SearchWindowsServer to provide an update on the partnership. In Part 1 of this report, the pair also discuss the challenges of moving Docker to Windows and the crowded field of offerings for container orchestration.

What can you tell us about how the partnership between Microsoft and Docker is coming along?

Hykes: What we started out doing with Docker was really focused on helping developers build new kinds of applications. We call them distributed applications, and they span many machines, run anywhere in the cloud -- online 24/7. There's this new paradigm and we found a real deficit of tools available for developers to build that. We started out leveraging Linux containers and focusing on one specific aspect of these applications, and over time we got more demand for expanding the scope of those tools so that a developer

looking at the platform they're using can have some sort of common tooling across all of it. Pretty quickly when you try to meet that demand you run into the obvious situation that you need to support Windows to really allow developers to cover the entirety of their platforms.

It's very, very common for enterprises in particular to have some aspect of their applications running on Linux servers and some aspects running in Windows. It made a lot of sense for us to try and make Docker's tooling and the developer experience of Docker available on both platforms, and that was really the starting point of the partnership with Microsoft.

There is a full-time team at Microsoft collaborating with the open-source community basically porting all of Docker's tooling to Windows on top of the new container primitives available in the future Windows Server. Once that new version is out, we'll have reached that point where using native Docker tooling you can actually build distributed applications across both Linux and Windows. That's something we're really excited about.

Should customers expect some challenges moving between the two environments?

Hykes: I do expect a few bumps in the road, from a technical point of view as we roll this out. There's going to be a schedule of experimental releases and beta, etc., but the key is that the bar is not nearly as high as with traditional virtualization.

In this guide

We don't actually need to take any particular component and make it magically work in both Windows and Linux. The key here with distributed applications is that some of the components will only work in Windows and some of the components will only work on Linux and that's OK because the application is the sum of all those components. Instead of focusing our efforts on trying to make Windows look like Linux and Linux look like Windows -- which would be impossibly hard -- the approach we're taking is to make the strong suits of each platform visible to the developers and let them choose, but making it much easier because they have common tools.

Russinovich: What we've done in Windows Server is implement the same fundamental primitives comparable to what Linux Docker containers are built on, and then work with Docker to make sure all of the Docker APIs work against the primitives using plug-ins we write with them as well as the open-source community. You can take a Docker client, for example, and point it at a Windows host and deploy Docker containers using the same APIs, same commands you would use as if you pointed it a Linux host and deployed a Linux container.

Are there any concerns about Docker containers eating into Windows Server or Hyper-V sales?

Russinovich: Containers are really powerful tooling, as is creating microservice-based applications. It's something we embrace, even internally at Microsoft. Docker is a fantastic tool for making deployment and management of those

applications much more efficient, so I don't think there's a concern. It's more like let's get this technology out there so developers can take advantage of it on Windows as quickly as we can.

Unlike some of its competitors, Microsoft has opted against developing its own tools for container orchestration. Can we expect anything from Azure in terms of orchestration or will it remain more agnostic about incorporating whichever tool the developer wants to use?

Russinovich: At this point, we're embracing many of the orchestration engines, [Google] Kubernetes being one of them, and there are several others like Mesos and Swarm, for deployment on top of Azure. We want any customers that are using those orchestration engines to be able to run great on Azure, and we partnered with Google to make sure Kubernetes runs on Azure. We also announced our own microservice application platform as a service (PAAS) framework called Service Fabric back in the spring and we expect over time that will incorporate container technology at well, but that's a higher level application platform -- higher than the low-level orchestration that you see with Mesos and Kubernetes.

Hykes: There are a few building blocks out there, but our approach to this at Docker is not to go out there and try and compete with that in the same way that we're not trying to go out there and re-invent how Linux does containers.

With so many other vendors jumping on container orchestration, is there a concern that Docker will be squeezed out in that space?

Hykes: Fragmentation is always a risk. There's a reason tools like Docker exist in the first place. These tools exist to try to avoid fragmentation because fragmentation is bad for developers; it makes their lives miserable, and I would say we're always out there preaching the gospel of unified interfaces with everyone. Obviously we can't tell vendors what to do. We just think we're providing a compelling story for avoiding fragmentation, and I would say Microsoft has been extremely proactive and understanding that and embracing solutions to avoid fragmentation.

There are three layers to orchestration: clustering, having lots of machines; composition, lots of containers working together; and then there's networking that interconnects it all. If you get these three building blocks you have an orchestration solution, and so the Docker stack includes a tool for each of those.

Windows Containers, Docker hit Microsoft shops

For the first time, Windows users can get their hands on Docker containers native to their preferred environment.

In this guide

Microsoft has released the third preview version of the next Windows Server, with the latest iteration allowing customers to use Docker tooling with Windows Server Containers. It's the first time Windows users can natively use Docker containers, which were previously only available with the Linux operating system.

The approach Microsoft is taking with Windows Containers essentially integrates the Docker Daemon inside Windows so Docker images -- Windows or Linux versions -- can be managed with similar or identical developer workflows, said Al Hilwa, program director for IDC, a research firm based in Framingham, Mass.

"This is an important move given the traction Docker has gotten in the market," Hilwa said.

Despite the value of the upgrades, it's important to note that Linux Docker binaries won’t run on Windows, Hilwa said.

Though this will be the first time Docker can be used natively in Windows, Microsoft previously offered Docker command line interface support on

In this guide

Windows and by deploying Linux VMs on Azure. Microsoft first announced the plans for native Docker containers on Windows earlier this year.

These containers can be deployed and managed using the Docker client or PowerShell. Microsoft is also working with Canonical on its LXD REST API, which is intended to be a cross-platform container management layer.

Opening Docker to more developers

Windows Server Containers are one of two kinds of native container initiatives, with Hyper-V Containers aimed at users who want higher isolation and an OS that separates containers from each other and from the host OS.

"Microsoft is saying, 'We're coming at it from all angles, and we want to make sure Windows developers have as much ability to start leveraging the power of containers as anyone else,'" said Dave Bartoletti, principal analyst for Forrester Research, Inc., based in Cambridge, Mass.

Hyper-V Containers will be available in the next preview, which is expected to be released in the next few months, Microsoft said. Both features are set to be fully released as part of the next Windows Server sometime in 2016.

In this guide

Docker really wants to bring containers to more than just Linux developers, and with so much attention on containers, every virtualization platform is trying to make it easier to run containers in those environments, Bartoletti said. The result will be an easier way for developers to use Docker in a way that fits the specific needs of their application and the environment they have.

"The market is evolving to the point where there's no one-size-fits-all for the best way to deploy your containers," Bartoletti said.

Microsoft's efforts with Hyper-V are similar to VMware, Inc.'s though VMware doesn't sell its own operating system, Bartoletti said. With Project Bonneville, VMware also is working on a container that runs inside a virtual machine with its own scaled-down, optimized version of Linux.

Other capabilities available in the latest preview release include improvements around networking, security and management, as well as the ability to use Nano Server on a physical host or in a VM, and the ability to manage it with PowerShell.

In this guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers—a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia