INSIDER'S GUIDE TO

What's New in Windows Server 2016 Hyper-V

New features in Microsoft's core hypervisor will simplify administration, increase performance and efficiency, and make it more stable and secure. By Paul Schnackenburg

Windows Server 2016 is having a long gestation period, with the first Technical Preview released back in October 2014. This look at what's coming next year in Hyper-V is based on Technical Preview 4, released Nov. 20, 2015.

Rolling Cluster Upgrades

One of the biggest improvements in the new version is how you get there. Unlike earlier versions of clustering, you can now mix 2012 R2 and 2016 version hosts in the same cluster. This means you can upgrade an existing cluster without having to purchase new hardware. Simply evict one node from the cluster, format the OS disk and install Windows Server 2016. This host can then be joined to the domain and reintroduced into the cluster. It then works exactly as a 2012 R2 host would. Rinse and repeat the process on each host in the cluster until all hosts are upgraded. System Center Virtual Machine Manager 2016 (VMM) can orchestrate this process in larger environments.

Just like an Active Directory upgrade project, once you're certain you're never going to introduce another 2012 R2 host, you run a single Windows PowerShell cmdlet (Update-ClusterFunctionalLevel) to upgrade the cluster, which unlocks the new 2016 features for the cluster. Dual booting is something IT admins often encounter during a first Linux computer

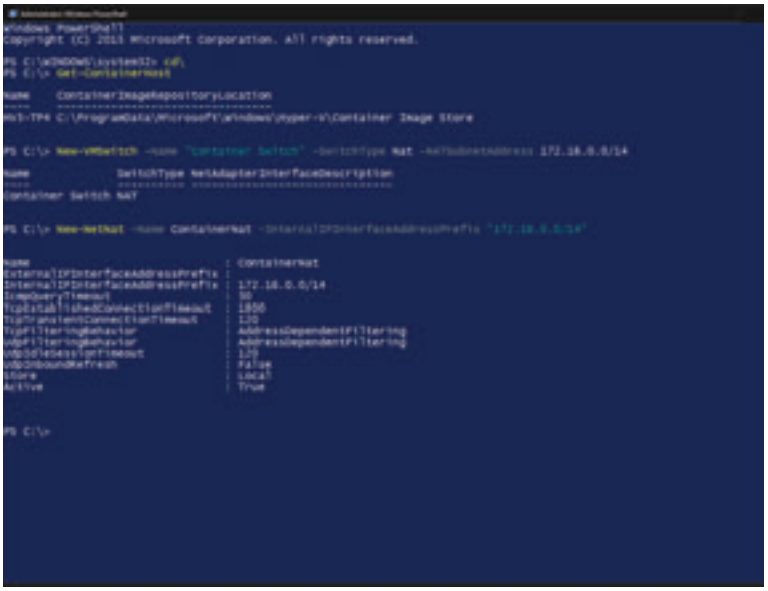


FIGURE 1 CONFIGURING CONTAINERS IN WINDOWS SERVER 2016.

crisis. A dual boot takes place when you configure your loading sequence to boot specific partitions. This is your opportunity to customize your IT environment with the versions of Windows and Linux you want to run on the network. Dual booting offers the advantage of independence; each system runs independently from the other and has direct and exclusive access to hardware resources, so performance is noticeably better.

Closely related to the upgrade process is the new configuration file formats: VMCX files store the configuration of a virtual machine (VM) and the running state is stored in VMRS files. Once you know that a particular VM will only ever run on 2016 hosts, you can shut it down and run a cmdlet to upgrade it (Update-VmConfigurationVersion *vmname).* Note that a cluster that has had the cluster functional level upgraded to 2016 can still run VMs in the old format, so the VM upgrade process can be scheduled for a maintenance window.

Production Checkpoints and Backup

Most virtualization admins today are aware of the dangers of checkpoints for production VMs. That's why the typical process

involves taking a snapshot/checkpoint of a VM before making some configuration changes or installing a patch. Then, if things don't turn out well, reverting back to a previous point in time is incredibly convenient. If, however, that VM is a domain controller or any other type of application server that synchronizes with databases on other VMs, it can lead to serious data corruption.

The new production checkpoints in 2016 use Volume Shadow Copy Services (VSS) inside the VM, so reverting to a checkpoint will cause the VM to boot (not just be restored to a running state) and be aware that it was restored from a backup. This makes corruption much less likely.

Microsoft is also redesigning VM backup, removing the reliance on VSS and making it a feature of Hyper-V, rather than relying on the underlying storage. Change tracking is also built in, making it easier for third-party backup software to build solutions, as well as being more stable and scalable.

VM Compute Resiliency

Clustering hosts for high availability (HA) has been part of Hyper-V since day one, including in the free Hyper-V server. There are times, however, when clustering can cause problems: for example, a 30-second network outage for one or more hosts. Today, this will result in the rest of the cluster assuming that the nodes are down, trigging failover and leading to potential data loss. The same goes for connections to storage, which today will lead to VMs crashing if the outage lasts longer than roughly 60 seconds.

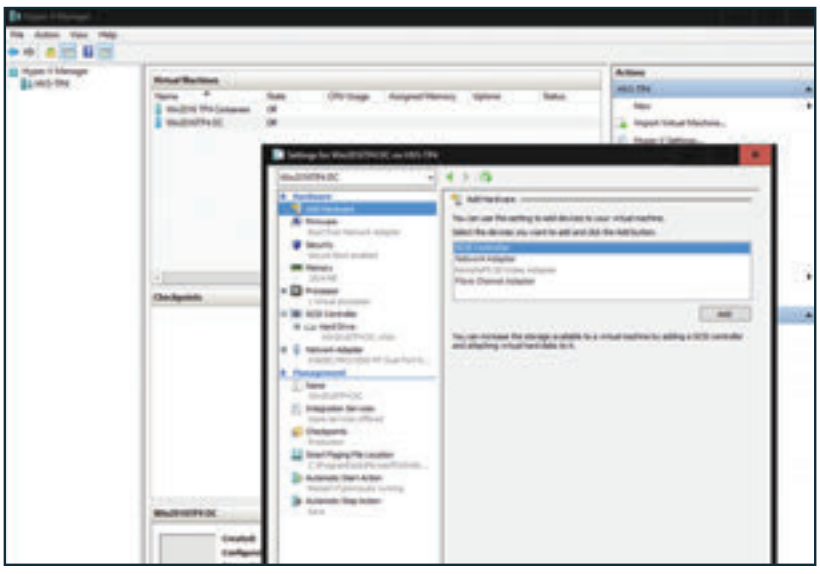


FIGURE 2 THE NEW HYPER-V MANAGER.

In the 2016 version, if a host loses connectivity, the VMs will keep running for up to four minutes (this is configurable) in isolated mode. If the outage is longer than that, failover will occur. If a particular host has several network disconnections over a 24-hour period ("flapping"), it will be quarantined and all VMs Live Migrated off it.

Storage QoS

In 2012 R2 you can set both a minimum and maximum storage I/O limit on a per-virtual hard disk basis. This is enforced at the host level. The problem is that if you set a minimum reserve for many VMs across several hosts, and the back-end storage (SAN or Scale-Out File Server [SOFS]) can't deliver the required IOPS to all VMs, they won't get their reserve.

In the 2016 version, there's a new, centralized storage controller, running on SOFS nodes. You can define policies that apply specific upper and lower limits across a group of VMs (they all share in a "pool" of IOPS) or policies that apply the same limits across several VMs. These policies are managed using Windows PowerShell, but if you have VMM 2016 they can be managed (across clusters and host groups) using a GUI.

Storage Spaces Direct

Storage Spaces Direct (S2D) is an extension of the existing SOFS setup of VM storage. Instead of relying on external SAS enclosures, S2D utilizes internal storage (SAS, SATA and NVMe) in four or more hosts to create highly performant (tiered storage with both hard disc drive [HDD] and solid-state drive [SSD]) and highly available (two- and three-way mirrored) storage. The S2D hosts can also be Hyper-V hosts, offering hyperconverged infrastructure.

Shielded VMs

The biggest new functionality coming next year is the ability to separate host administrators from application or VM administrators. Today, if I'm a host administrator (on any virtualization platform), I can mount a virtual hard disk, perform offline tasks or attach a debugger to a running VM to inspect memory contents, as well as inject code into VMs.

Several new technologies in 2016 combine to form "Shielded VMs." First, Generation 2 VMs (introduced in 2012 R2) now provide a virtual TPM chip, which enables Bitlocker

(dm-crypt on Linux VMs) whole-disk encryption on VM virtual disks. Also, Generation 2 VMs boot from UEFI, not BIOS, enabling Secure Boot (now for Linux VMs, as well), protecting the firmware and the VMs startup files.

The Host Guardian Service is a group of protected servers (three or more are recommended), which runs a separate AD infrastructure to your infrastructure AD forest. These servers manage the VM lifecycle and attest to the health of infrastructure Hyper-V hosts.

There are two types of attestation models: Administrator Attestation and Hardware Trusted Attestation. The former simply relies on administrators adding hosts considered secure to a particular group in AD. The Hardware Trusted Attestation mode uses a new Trusted Platform Module (TPM) version 2 chip on the motherboard of each Hyper-V host, to protect the hypervisor itself.

Most virtualization admins today are aware of the dangers of checkpoints for production VMs.

Encrypted files hold Shielding Data used by Hyper-V to unlock VMs for booting, without fabric administrators having access to sensitive configuration information about each VM.

A Shielded VM blocks access to VM Connect, and there's no thumbnail view in Hyper-V Manager. All Live Migration traffic is encrypted, host crash dumps are encrypted and VM crash dumps are disabled by default; if enabled, they'll also be encrypted.

Windows and Hyper-V Containers

Perhaps the biggest shift in IT since cloud computing, container-based virtualization is going to change how we run applications and services over the coming years. Virtualizing a whole OS is resource-intensive and adds additional management overhead. A container, on the other hand, is just a copy of an OS, based on a read-only base OS image with an application image layered on top. Each container thinks it's a separate OS. Benefits include near instantaneous booting and significantly less resource usage.

Windows Server 2016 offers two container flavors: Windows Server containers (see **Figure 1**) with less security isolation, and Hyper-V containers, which provide the same isolation as a VM. Both can be managed through Docker (a popular Linux container orchestration and management platform), now built into Windows Server and Windows PowerShell. Developers don't choose between the two types; it's simply a deployment-time selection.

To support containers, Hyper-V will also support nested virtualization so that VMs can run on top of a hypervisor and in turn have Hyper-V containers inside of them.

Other Improvements

PowerShell Direct lets you run Windows PowerShell cmdlets inside VMs (with appropriate credentials) over the VMBus, without having to establish PowerShell remoting.

The Resilient File System (ReFS), which first saw the light in Windows Server 2012, is coming of age, providing near instantaneous zeroing out of fixed-size virtual hard disks and lightning fast checkpoint merge operations.

Shared VHDX disks for guest VM clustering are improved, allowing host-based backups and online resize of the shared VHDX files.

Hyper-V Replica now allows the addition of virtual hard disks without disturbing ongoing replication. If you also want this new virtual hard disk to be replicated, it can be added to the replication set.

More operations, such as adding and removing virtual NICs, are now online operations. For VMs that have been assigned fixed memory sizes (not Dynamic Memory), the memory size can be altered as an online operation. Virtual network switches are also easily identifiable from within a VM.

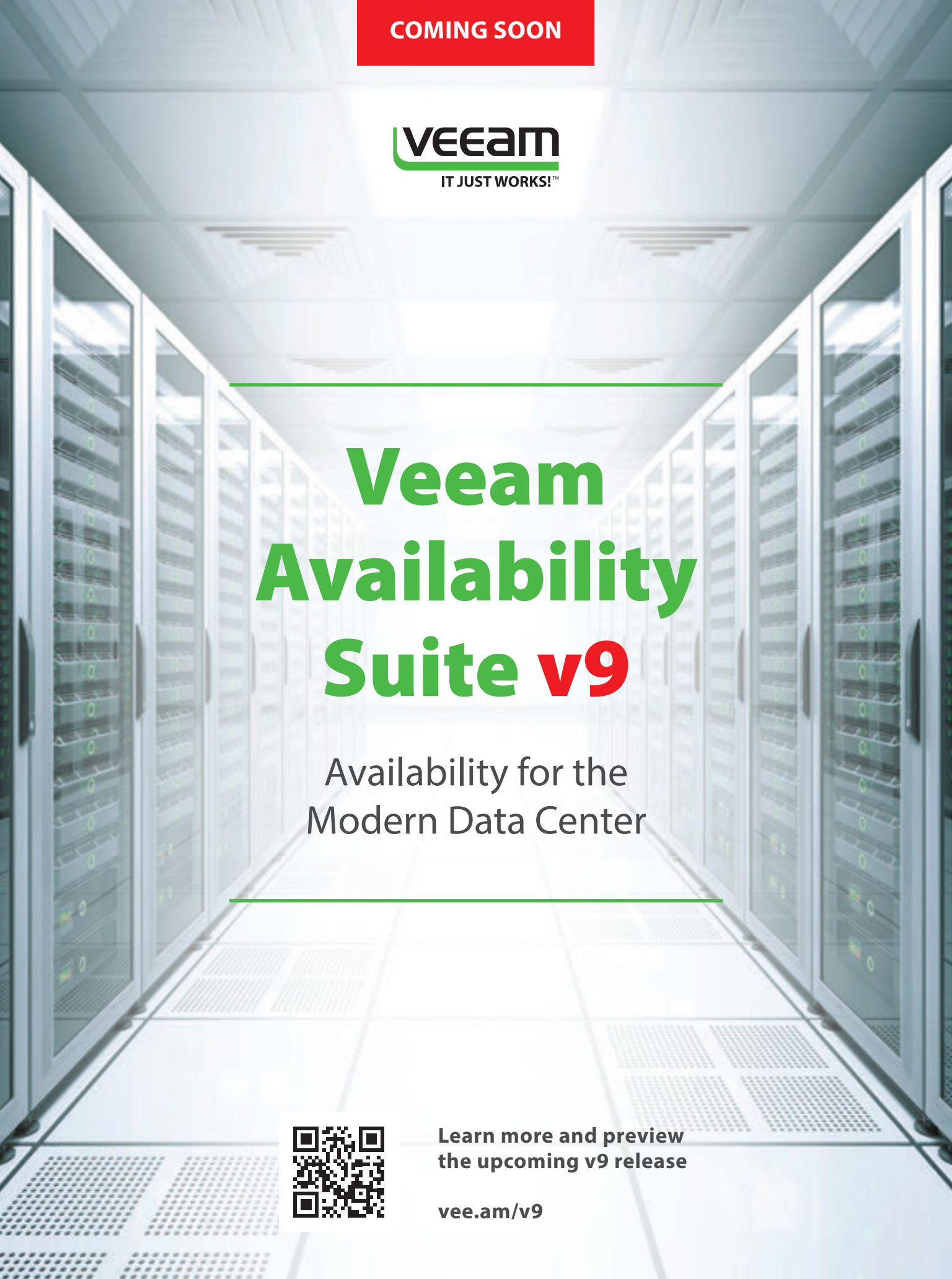
Hyper-V Manager (see **Figure 2**) can now manage 2012/2012 R2 hosts, as well as 2016 hosts, and lets you connect with alternate credentials.

Integration Components are going to be distributed through Windows Server Update Services instead of being updated as a host operation.

You've Got Options

There are many smaller, incremental improvements coming in Hyper-V, as well as some game-changing advances such as Nano Server and Shielded VMs. If you're looking for the best virtualization platform for private cloud, as well as the best stepping stone to the public cloud, the coming version of Hyper-V is a compelling choice. VR

Paul Schnackenburg, MCSE, MCT, MCTS and MCITP, started in IT in the days of DOS and 286 computers. He runs IT consultancy Expert IT Solutions, which is focused on Windows, Hyper-V and Exchange Server solutions.


COMING SOON
VEEAM
IT JUST WORKS!™
Veeam Availability Suite v9
Availability for the Modern Data Center
Learn more and preview the upcoming v9 release
vee.am/v9