Sweet Sixteen, or Just Server 2012R3? A Glance at the Awesome, the Irritating, the Improved and the Expensive in Server 2016

Presented by Mark Minasi
mark@minasi.com
Twitter @mminasi

Not long from now, in a datacenter very, very near by...

(cue the trumpet fanfare...)

Topics

- Two big pictures
- Pricing & Licensing
- The UI Gauntlet
- Smaller VMs: Nano Server
- Hyper-V: The basis of it all
- Tenancy: Hyper-V security
- "Switch" hitter: Network Controller
- Cheap SANs, cooler file server
- Easier reliability / clusters
- Active Directory upgrades
- Containers
- DNS takes on The Dark Side

Why, When, Where, How Much?

Big Picture #1: Azure To Server

- Azure is huge, millions of boxes and they all run Server
- They do a new build every couple of weeks
- They learn stuff
- So every couple of years, they stuff the "learning" into Server
- This mainly applies in Hyper-V, software networking, storage and PowerShell, Desired State mostly

Big Picture #2: Crush VMWare

- I think it's fair to guess that almost all of you have "gone virtual" and you're using the VMWare suite
- Well, Microsoft wants them *dead*
- Comparable to the Novell competition back in 1993
- Hyper-V: an excellent hypervisor
- Storage spaces: 85% of what a SAN can do for 35% of the cost
- Commodity hardware leads to cheap, good clusters

Pricing

- Server 2012: all features, no matter the SKU
- Server 2016: Most of the new good stuff is only in DataCenter
- And the pricing… well
  - Before, prices were per-physical socket – Standard Server was $882 for up to two sockets
  - Now, it's per-*core*, in 16-core chunks. $882 for Standard, $6155 for Datacenter

Pricing, Continued

- The big price jump comes from the fact that Standard is essentially useless VM-wise and new-feature-wise, so $6155 is the entry cost for just about everyone
- Branching is LTSB thankfully, except…
- Nano uses the Common Branch for Business, making it like Windows 10, *and* it requires you to buy Software Assurance
- But the Nano stuff kind of makes sense as we'll see

The New UI: PowerShell

- Look closely, and you'll see that well over 50 percent of the all-new stuff in 2016 has no GUI, even new features in old subsystems
- Go ahead, read that again. Yup, you read it right.
- Being a 2016 admin means being a PowerShell user. Really.
- And while you're at it, learn Desired State Configuration
- So…
- PLEASE. Learn PowerShell if you want to keep running servers. It's just inevitable.

Speaking of UIs… Choose Your Install Carefully!

- As with 2012 or 2012, at Setup you choose… Full GUI or Server Core?
- Unlike 2012 & R2, you cannot switch between Full GUI and Server Core once the system's installed
- Nano Server is a completely different install so there's no way to switch between Nano and, say, Full Server… it'd require a fresh rebuild from scratch
- So choose your GUIs carefully when you install Server!

Say Hi to the New Guy: Nano Server

- Neat innovation
- Sort of the uber-Server-Core / MinWin, very very shrunken
- Very limited in what roles it can serve, but Microsoft continues and will continue to change it, so anything I say "can't" might change
- It is a bit of a pain to configure and there almost nothing runs locally – it's headless – so Setup can be a bit cumbersome
- Can execute only a limited version of PowerShell
- Runs on physical systems or as a virtual machine

In Nano, Little is Good

- Offers very small disk / RAM / CPU footprints, so a *lot* less patching in theory, and far less attack surface
- Only a trimmed-down .NET ("CoreCLR")
- Disk footprint ½ gig
- Runs in about 2 GB in my experience, smaller may be possible
- Boots insanely fast

Setup and Deploy Nano Server

- There is a base VHD in the install media
- You use that and a PowerShell script to get it as you want it
- With that VHD, you can
- Deploy to a physical machine (boot from VHD), or
- Just roll out the VHD as a virtual machine
- Nano supports a reduced version of Desired State Configuration so some configuration that way works also
- If the Nano is a Hyper-V VM, you can run cmdlets on the Hyper-V host that control the Nano VM even without networking, a tool called "PowerShell Direct" that can even bypass firewalls

Once You Have a Nano Server...

- Nano can
  - Run 64 bit code
  - DNS
  - IIS
  - Hyper-V
  - Containers
  - File Server
  - Scale-Out File Server
  - Run Windows Defender
- Nano can't
  - Run 32-bit code
  - Be a DHCP server
  - Act as an Active Directory domain controller
  - Host Exchange
  - Host SQL Server

Another interesting "can" for Nano: you can use an Azure service to reach into your network and control that Nano server. No, Nano's not running on Azure, it's just an Azure thing that connects on-premise.

Hyper-V: The Core Competency

- Plurality of new 2016 features live here
- Way too much, so just a few highlights:
- Migrating clusters 2012/R2 -> 2016 easier & flexible
- You can restore VM snapshots in production
- VMs can now be Hyper-V hosts, "nested" virtualization
- Hyper-V now uses the Reliable File System (ReFS)
- VMs can have virtual TPMs, Secure Boot, Bitlocker
- You can create "dependencies" among VMs, so VM2 shouldn't start until VM1's up and running
- Even better ability to let special VMs to connect directly to PCIe hardware (for speed)

Tenancy: Are Our VMs Secure from Admins?

- Recent concern: do you trust your Hyper-V/ESX folks? Do you trust your cloud vendors?
- What keeps them from copying the virtual drives from your VMs, taking them home and learning your secrets?
- Well, right now, nothing

Answer: Bitlockered VHDs

- Answer: after building your VMs, just BitLocker your virtual drives
- Problem: VMs don't have virtual TPMs
- Solution:
  - Don’t put a "virtual TPM" on the VMs
  - Instead have some servers act as "host guardian servers," acting as "TPMs for the cluster"
  - Result: admins can turn on BitLocker for their virtual servers' C: drives

Container Intro: Containerize-able Services

- We run things on our servers, pieces of software called "services," right?
- They tend to have two limitations:
  - They tend to take a lot of fussing to get installed – such-and-such verson of IIS, another bit of .NET, some third party thing we're not excited about sticking on our servers
  - Sometimes we want to run more than one instance of them on the same host (for security, separate billing, troubleshooting etc) but many services don't like being installed multiple times
  - Answer: Containers

Containers in Two Minutes

- We can make services easier to install *and* perfectly happy to coexist with other copies of themselves by, well, lying to them
  - Give them a "virtual Registry," some "virtual RAM," and virtual disk space.
  - Kind of like "VMs Lite"
  - Ever used App-V to wrangle troublesome apps into working? Containers is "App-V for Server Applications."
- So when developers create their server apps in a standard packaged container format, admins can just drop them on the "container server" and it all runs without a hitch
- The popular format of containers is from a company named "Docker," and 2016 includes Docker support

In the Real World

- A company named Docker has been doing this with specialized Linux apps
- Hyper-V supports those now
- Standard Docker-ish apps can have as many instances in a single virtual machine as you like, as I said
- Or you can use "Hyper-V containers," which is just containers built in separate Linux/Server 2016 virtual machines… "thicker walls" between the instances
- And you can now build *Windows* services in Docker containers
- Thus, containers offer both "virtualization lite" and now support building them with Windows rather than Linux tools

Switch Hitter: Network Controller

- Virtual servers/services live on real servers on real networks
- Thus, if "VM1" needs the physical port 3488 to be open on its Hyper-V server's firewall AND if there are a million servers that
- VM1 might be shuffled around to…
- …And if it's all kinds of commodity equipment, so that physical firewall might be a Cisco, Juniper, or you name it…
- … it'd be nice to be able to guarantee that the system knew how t open 3488 on any kind of firewall
- Network Controller is a chunk of 2016 that enables that, as it in theory can talk to most switches, firewalls and the like
- Oh, and most of how you control it involves…

Security Improvements

- Windows Defender on every copy of Server
- Anti malware and anti spyware *and* of course Early Launch Anti-Malware (ELAM)
- Plus, of course, Secure Boot's still around
- Hyper-V Gen 2 VMs can support both Windows and Linux instances running Secure boot
- Logs can be encrypted
- Rougher times ahead for malware writers

Storage Spaces

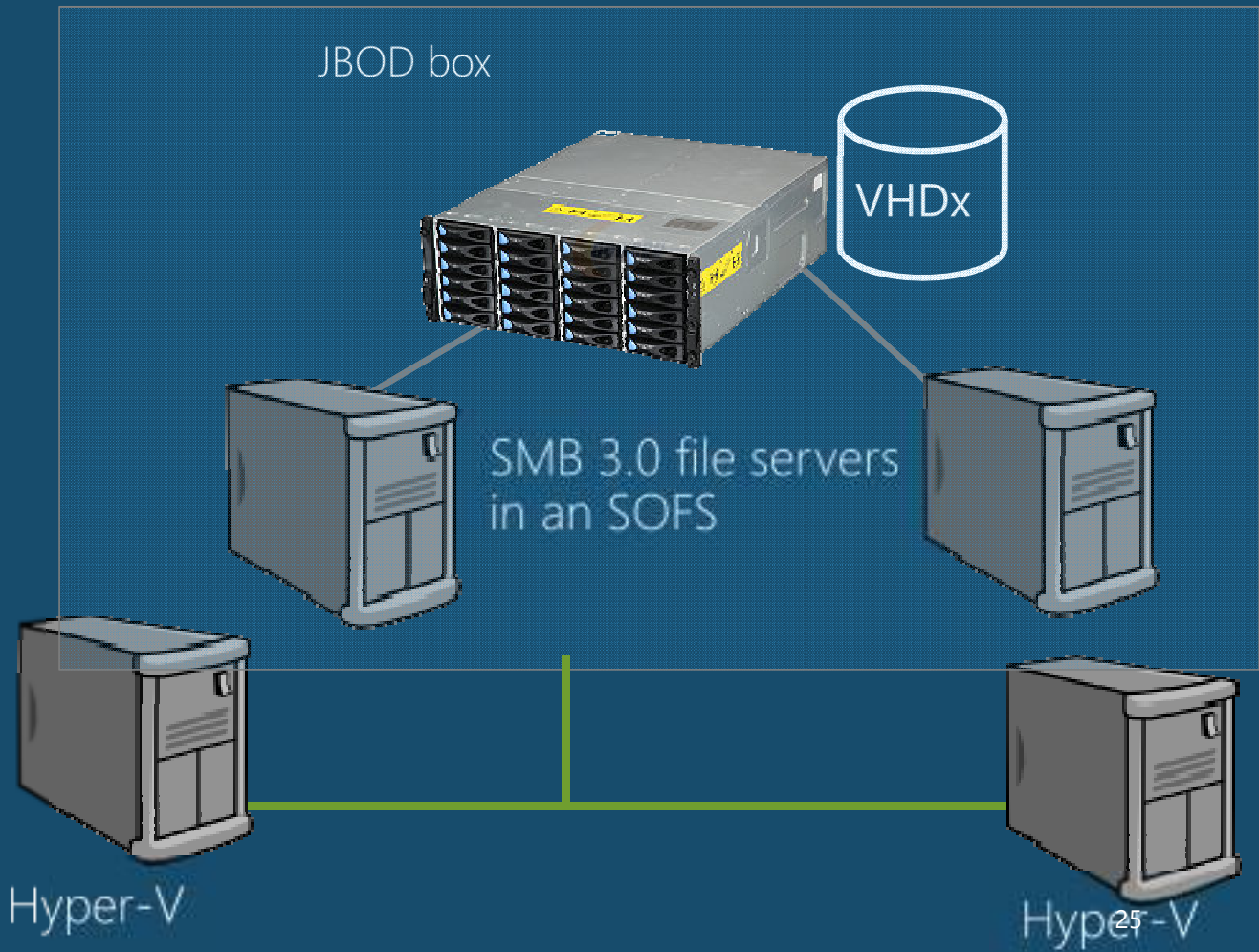
- In case you haven't been following, Windows has a SAN-like tech proving storage for Windows clusters
- They're cheap compared to SANs
- Big driver was SMB 3.0/3.1, which does way more than sharing files
- Result in 2012 and 2012 R2: much cheaper clusters
- But they *could* get cheaper…
- … which is where 2016 steps in
- First, a quick review of 2012/2012 R2 clusters:

Cheaper, Easier Clusters: SOFS / Hyper-V Now

This is a super-basic version of how Microsoft wants you to build a Hyper-V cluster

It's driven by a file server cluster

Which needs expensive SAS drives and hardware to enable the cluster

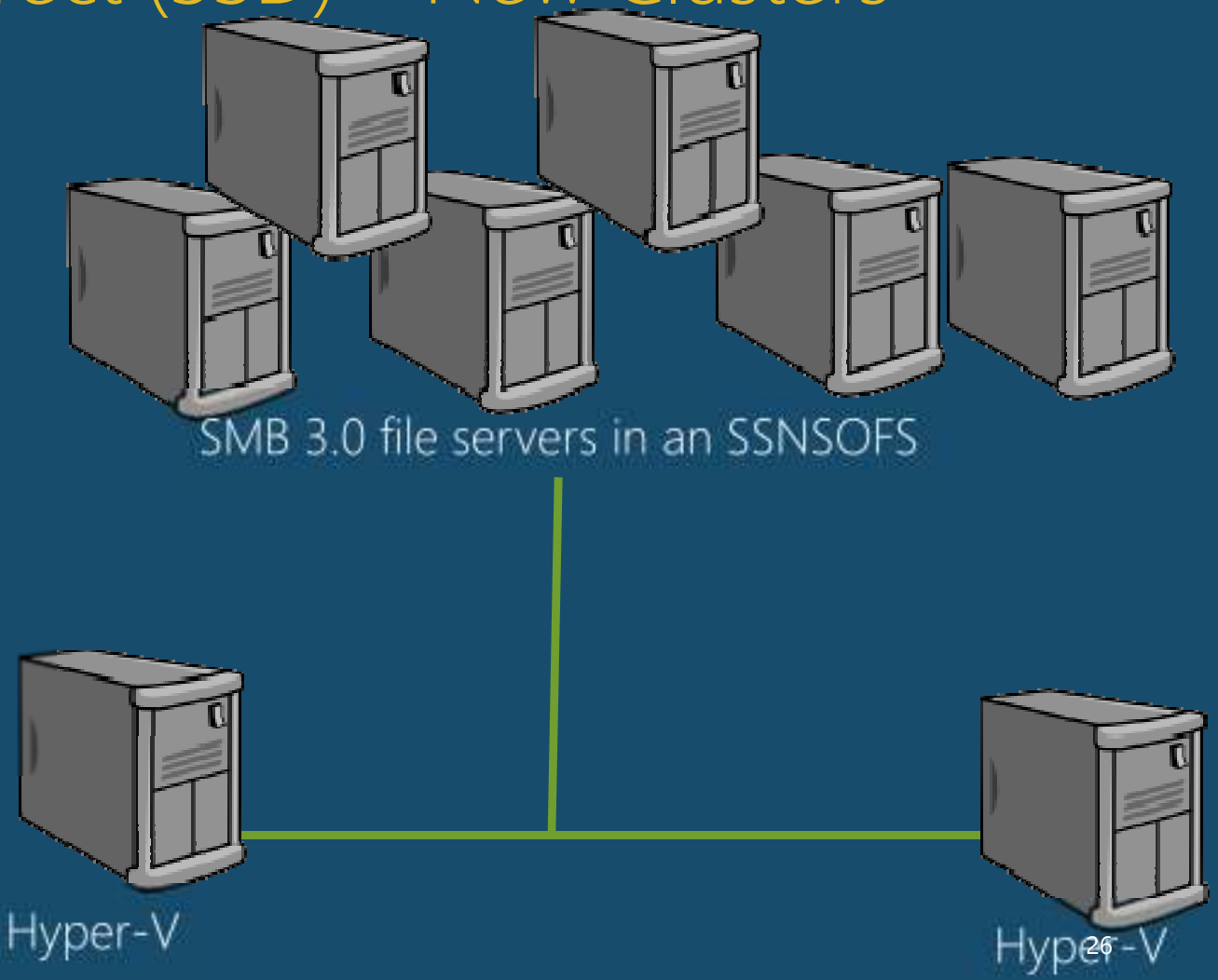


Storage Spaces Direct (SSD) – New Clusters

Here, there's no shared box.

Data is stored on the DASD on the servers.

The drives could be SATA drives.

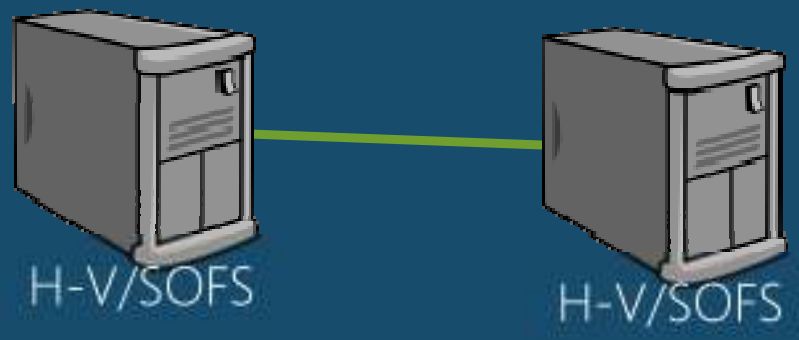


S2D Concepts

- No JBOD, no SAS fabric needed… SMB is doing SAS's job
- Basically SMB 3.0 is the shared data bus, not Serial Attached SCSI (SAS) cabling
- Any internal drives can contribute to the cluster
- Enlarges Storage Spaces pool sizes above 80 disks
- Built for Hyper-V, VHDs, ReFS
- Add a Hyper-V server, the loads rebalance automatically
- You can lose up to two disks on a volume
- You can lose up to one entire PC (node on the FS cluster)
- Inexpensive, needs only three servers to try it out, four to try out all resiliency levels

Which All Ultimately Leads Us to…

- Take two systems, add cheap drives and install 2016
- Make them Hyper-V hosts and Scale-Out File Server nodes
- Result: "Hyper-converged Hyper-V"
- Yes, just two systems become a fault tolerant H-V cluster



Storage Replication

- Sort of the Storage Spaces version of SAN LUN replication
- Lets you replicate volumes between machines
- Doesn't care about underlying hardware… you could replicate between an EMC system and a Left Hand
- Transport is SMB3, only ports 445 or 5445
- Doesn't care about distance, can go cluster to cluster
- Synchronous (multiple nodes update immediately, good for short distances) or asynchronous (faster as it needn't wait for acknowledgement from other nodes, so a little riskier)
- Block level, so file system agnostic

Active Directory Changes in 2016

- Um. None.
- Really, kinda.
- What's up with *that*? I guess on-premises AD just isn't interesting any more. Oh well.

DNS Takes on The Dark Side

- There is a class of attacks called a "DNS-based distributed denial of service" attack
- Most DNS servers are vulnerable to it
- 2016 offers some smart, common-sense tools to combat it
- The attacks ask the same dumb, bandwidth-killing question over and over
- 2016's DNS server just ignores repetitive behavior under your control
- Very elegant and useful answer

Thank You For Attending!

- In 45 minutes we couldn't do everything, so no JIT/JEA, some of the security and other things, but I tried to get the biggest stuff
- Please do an evaluation
- Contact me: @mminasi, mark@minasi.com
- Thanks again, enjoy the rest of the show