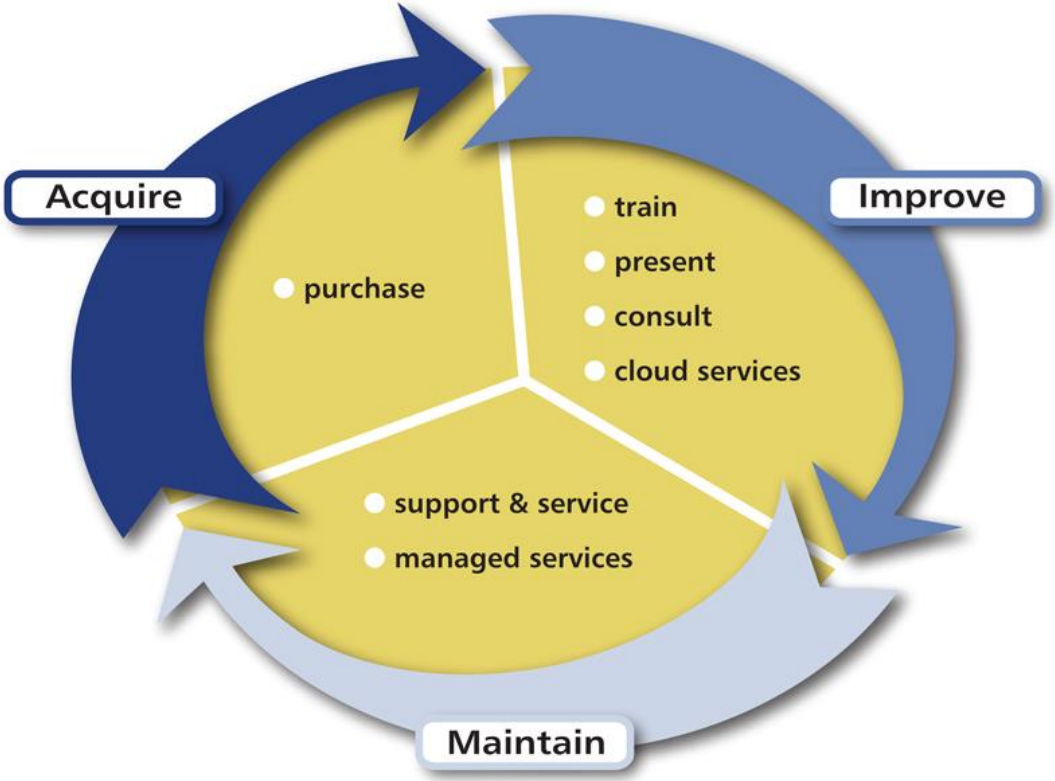
Exploring Windows Server 2016

February 16, 2017

David Piehl
Lead Technical Trainer
Senior Systems Engineer

Scott Rippey
Solutions Architect


Acquire
Improve
Maintain
purchase
train
present
consult
cloud services
support & service
managed services

System Source & Microsoft:

- **Microsoft Certified Partner…since 1980's**
  - **Silver – Learning Solutions**
    - Train 6,000 students/year
    - Our Instructors rate 20% higher than Microsoft National Average Customer Satisfaction Scores.
  - **Silver – Infrastructure**
- **1,000's of Microsoft implementations**
  - **Small Business to Enterprise**
  - **Non-profit**
  - **Education**

System Source & Microsoft:

- **Microsoft Competencies**
  - **Server Platform**
    - **Windows Server 2012 & 2016**
  - **Management and Virtualization**
    - **Microsoft Cloud Solutions, Microsoft Private Cloud, Configuration Manager, Windows Server**
  - **Messaging**
    - **Exchange Server, Exchange Online, Exchange Online Protection**
  - **Hosting**
    - **Exchange Server, SQL Server, Microsoft Server**
  - **Devices & Deployment**
    - **Windows 10, Office**
  - **Small Business**
    - **Office 365, Windows 10**
  - **Mid-Market Solutions Provider**
    - **Microsoft Cloud Solutions, Office 365, Windows Server 2012 & 2016, Windows 10**

Your presenters

Your presenters

Topic List

- **Windows Server installation options, including Nano deployments**
- **Improvements to existing features**
  - **Hyper-V**
  - **DNS and DHCP service updates**
  - **Active Directory improvements**
  - **Remote Desktop Services and VDI**
  - **Server Management Tools**
  - **Patch management of new servicing branches for Windows 10 client support**

Topic List, continued

- **New features**
  - **Containers and Docker**
  - **Powershell v5**
  - **Storage Replica**
  - **Storage Spaces Direct**
- **Windows 2016 Training and Certification**
- **Door Prizes and Lunch**

Windows Server
Editions and Installation Options

Available Editions and differences

Windows Server 2016 edition	Ideal for	Licensing model	CAL requirements*	Pricing Open NL ERP (US$)
Datacenter**	Highly virtualized and software-defined datacenter environments	Core-based	Windows Server CAL	$6,155
Standard**	Low density or non-virtualized environments	Core-based	Windows Server CAL	$882
Essentials	Small businesses with up to 25 users and 50 devices	Processor-based	No CAL required	$501

*CALs are required for every user or device accessing a server. See the Product Use Rights for details.

**Datacenter and Standard edition pricing is for 16 core licenses.

Standard and Datacenter Features Comparison

Feature	Datacenter	Standard
Core functionality of Windows Server	●	●
OSEs / Hyper-V containers	Unlimited	2
Windows Server containers	Unlimited	Unlimited
Host Guardian Service	●	●
Nano Server*	●	●
Storage features including Storage Spaces Direct and Storage Replica	●	
Shielded Virtual Machines	●	

*Software Assurance is required to deploy and operate Nano Server in production.

Major feature changes

- ***Nano server*** joins Server Core and Full Desktop Experience options
  - Absolutely no GUI. Zero. Zilch. Nada.
  - Can be installed directly on a host as a bootable .vhdx or deployed as a Hyper-V Virtual Machine
  - Roles are decided up front and cannot easily be added later
  - Very few local management options
    - Limited set of Powershell commands
    - No support for processing of Group Policy (even though it can be joined to a domain)
  - For all this pain, you get:
    - A bare bones footprint and attack surface (base installation ≈512MB drive space, ≈ 200MB RAM)
    - Up to a 90% reduction in patching
    - Very, very few reboots

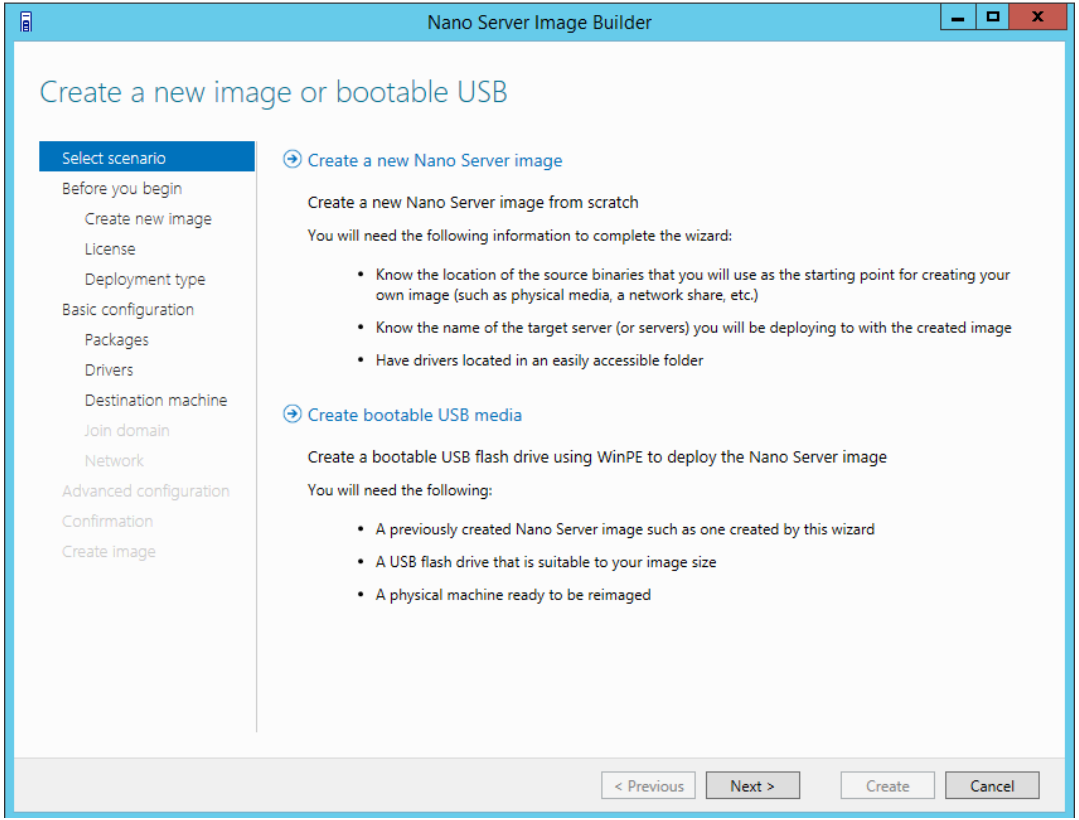
Base Memory footprint differences

Virtual Machines

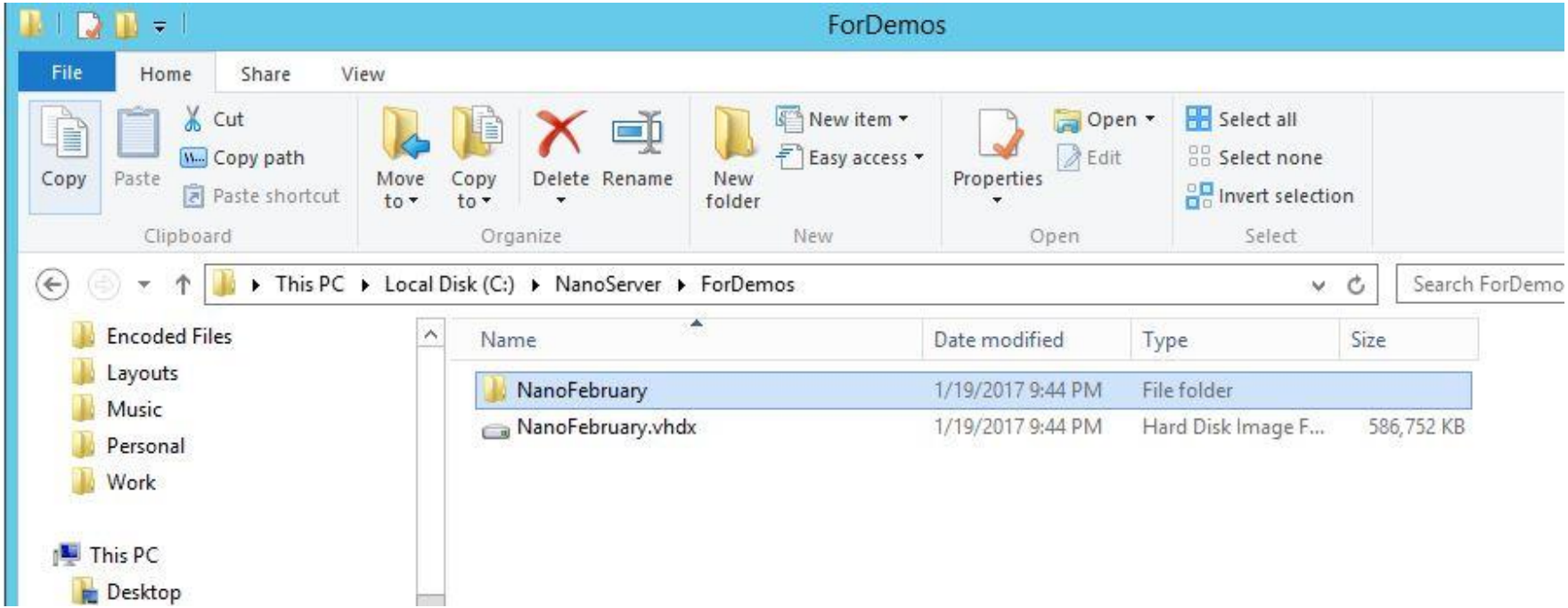
Name	State	CPU Usage	Assigned Memory
_2016-Core	Running	0 %	476 MB
_2016-Essentials-Edition	Running	0 %	2450 MB
_2016-Full-Desktop-Experience	Running	0 %	1066 MB
_2016-Nano	Running	0 %	186 MB

Nano Server Image Builder tool

- On 10/15/2016, Microsoft released a tool that makes the job of building a Nano server much easier



Nano Server Image Builder tool



Improvements to Existing Features and Technologies

Hyper-V

- Nested virtualization
  - Outer host can run any installation option: Full, Core or Nano
  - Makes Hyper-V container support possible
- Production checkpoints
  - Instead of saving the state (basically like hibernation), uses VSS inside the guest
  - Allows checkpoints to be more safely used with production workloads
- Hot-add for virtual RAM and virtual network interfaces
  - Support for hot-add of virtual SCSI devices carries over

Hyper-V (continued)

- Linux Secure Boot
  - Supports newer versions of Ubuntu, SUSE Enterprise Server, Red Hat Enterprise and CentOS
- Host resource protection
  - Prevents a VM from using more than its share of resources on a particular host
- Shielded virtual machines
  - Guards against vulnerabilities inherent in virtualization (a VM is just a set of files)
  - Uses Virtual TPM, BitLocker and the Host Guardian Service to make it harder for rogue Hyper-V admins and malware on the host to tamper with (or steal) VMs

DNS service updates

- *DNS Policies* configure how a DNS server responds to DNS queries
  - **Split-brain**: DNS records are scoped, & client responses will be different if they are internal vs. external
  - **Time of day:** redirects to different datacenters based on time of day
  - **Traffic management:** clients are directed to the closest datacenter
  - **Filtering:** queries from a list of malicious addresses or domains are blocked or sent to a sink hole
- Response Rate Limiting
  - Controls how to respond when the server receives several queries targeting the same client
  - Prevents DDoS attacks using your server as the middleman

DNS service updates

- RFC 6394 and 6698 support
  - Tells DNS clients which CA they should expect to receive SSL certs from when contacting your secure resources, such as HTTPS websites, at your organization
  - Certificates received from a different CA causes the connection to be aborted
- Addition of IPv6 root hints

DHCP service updates

- DHCP failover
  - Enables two DHCP servers to provide IP addresses and options to the same scopes
  - Supports ***Hot Standby mode*** and ***Load Sharing mode***
    - *Hot Standby Mode* provides a small percentage of a scope (5% by default) to a second server which can automatically take over during a temporary outage of the primary
    - *Load Sharing Mode* splits a scope 50-50, by default, and the servers become equal partners

Active Directory service updates

- Privileged Access Management
  - Allows you to eliminate permanent membership in highly-privileged groups by granting temporary membership only when needed
  - PAM consists of the following components and features:
    - **Parallel (Bastion) Active Directory forest:** an isolated, known clean AD forest with a PAM trust to the main AD DS environment
    - **MIM service:** provides business logic to request “just-in-time” and time-limited membership in shadow groups, created in the Bastion forest with a SID History that matches the group from the corporate forest, allowing seamless resource access without changing any ACLs
    - **KDC enhancements:** the improved KDC can grant TGTs that have different TTLs for different time-limited group memberships
    - **New monitoring capabilities:** includes auditing, alerts, and reports to see a history of privileged access requests as well as who performed specific activities

Active Directory service updates

- Azure AD Join
  - Allows certain Windows 10 settings, including personalization, accessibility settings, credentials and live tiles, to roam with the user without requiring a personal Microsoft account
  - Access organizational resources on phones and tablets that cannot be members of a Windows domain, even if they are BYOD
  - Single sign-on for Office 365
  - Add a work account from an on-premises domain or Azure AD to a personally-owned device to ensure compliance with Conditional Account Control and Device Health attestation
  - MDM integration allows auto-enrolling devices into Intune or 3rd party MDM

Active Directory service updates

- New domain and forest functional levels
  - Windows 2003 domain controllers should be removed from your domain, although this is not a technical requirement
  - Raise the domain and forest functional levels to Windows Server 2008 or higher to ensure that no 2003 DCs can be added
  - Raise the functional level to Windows Server 2008 or higher to ensure SYSVOL replication compatibility in the future
  - Migrate SYSVOL replication from FRS (which will be deprecated in future Windows versions) to DFS-R using `Dfsrmig.exe`
  - The Windows Server 2003 domain and forest functional levels and FRS replication for SYSVOL are still supported… for now

Remote Desktop Services and VDI

- Support for Gen 2 virtual machines
- Adds support for Personal Session desktops
- Connection Broker improvements:
  - Now supports a shared SQL database for high availability (instead of a dedicated one). This also means you could use Azure SQL and let Microsoft worry about the HA.
  - Database querying improvement can now handle 10,000+ concurrent connection requests to handle the “9:00 am surge problem” for larger environments

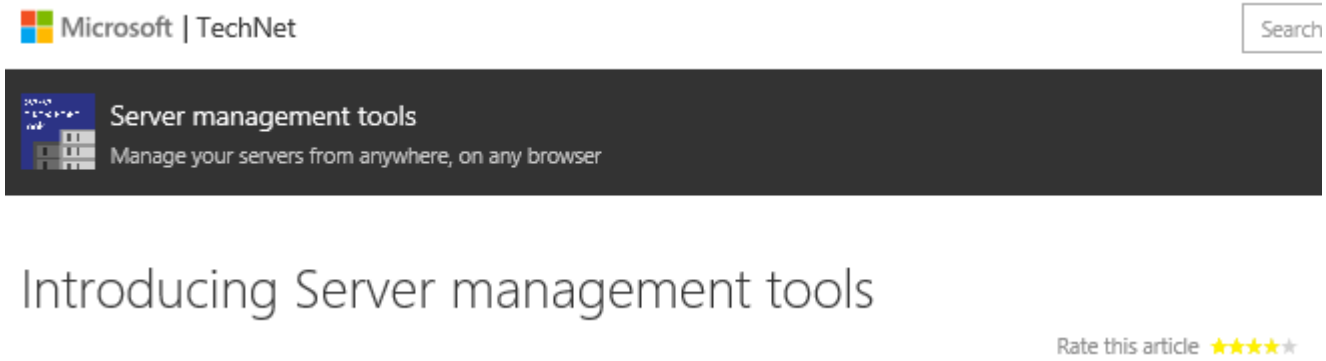
Remote Desktop Services and VDI

- VDI graphics improvements:
  - Support for OpenGL inside published desktops
  - RDP v10, which includes support for using pens inside a session
  - Direct Device Assignment for vGPUs allows VDI to be used even for very intense, graphics-heavy software packages

Server Management Tools

- As more server deployments become “headless”, cloud-based and GUI free, Microsoft is developing web-based GUI tools, tied in with the Azure portal, to manage them

- The creative name they chose to use for this?



https://portal.azure.com/#resource/subscriptions/768aa03c-7ef0-4a18-ad06-4516f40d567b/

Microsoft Intune: ... | Service Dashboard | Introducing Serve... | server2016.ada...

Microsoft Azure Piehls-Gateway > server2016.adatum.com

Search resources

DRP12017@Adatum... SELF

Piehls-Gateway

Server management tools gateway - PREVIEW

Settings | Delete | Refresh | Add computer...

Search (Ctrl+/)

- Overview
- Activity log
- Tags
- Diagnose and solve problems

SETTINGS

- Locks
- Automation script

MANAGE

- Properties
- Setup
- Gateway update

SUPPORT + TROUBLESHOOTING

- New support request

Essentials

Resource group: RG1	Gateway: Piehls-Gateway
Status: OK	Latest published MSI version: 1.0.1889.0
Location: East US	Oldest supported version: 1.0.1645.0
Subscription name: Azure Pass	Gateway update mode: Automatic
Subscription ID: 768aa03c-7ef0-4a18-ad06-4516f40d567b	Published Time: 2/1/2017 4:55:33 PM

piehls-gateway - Server management tools gateway

MACHINE NAME	VERSION	HEALTH
SERVER2016	1.0.1889.0	OK

Server management tools connections

1

NAME
server2016.adatum.com

server2016.adatum.com

Server management tools connection - PREVIEW

Settings | Restart | Shut down | Manage as | Delete | Refresh

Search (Ctrl+/)

- Overview
- Activity log
- Tags
- Diagnose and solve problems

SETTINGS

- Locks
- Automation script

SYSTEM INFO

- Properties
- Computer identification

TOOLS

- Certificate Manager
- Device Manager
- Event Viewer
- File Explorer
- Firewall rules
- Hyper-V
- Local Administrators
- Network settings

Essentials

Resource group: rg1	Connection: server2016.adatum.com
Status: OK	Gateway: piehls-gateway (OK)
Location: East US	User name: adatum\administrator
Subscription name: Azure Pass	Server: SERVER2016
Subscription ID: 768aa03c-7ef0-4a18-ad06-4516f40d567b	Operating system: Microsoft Windows Server 2016 Datacenter

Performance

Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz

Edit

100% 80% 60% 40% 20% 0%

60 s 30 s

CPU PERCENTAGE 39.67 %

Memory

100% 80% 60% 40% 20% 0%

60 s 30 s

MEMORY PERCENTAGE 71.8 %

Network adapters

1

172.16.0.100	10 Gbps

Disk 0 (C:) - Microsoft...

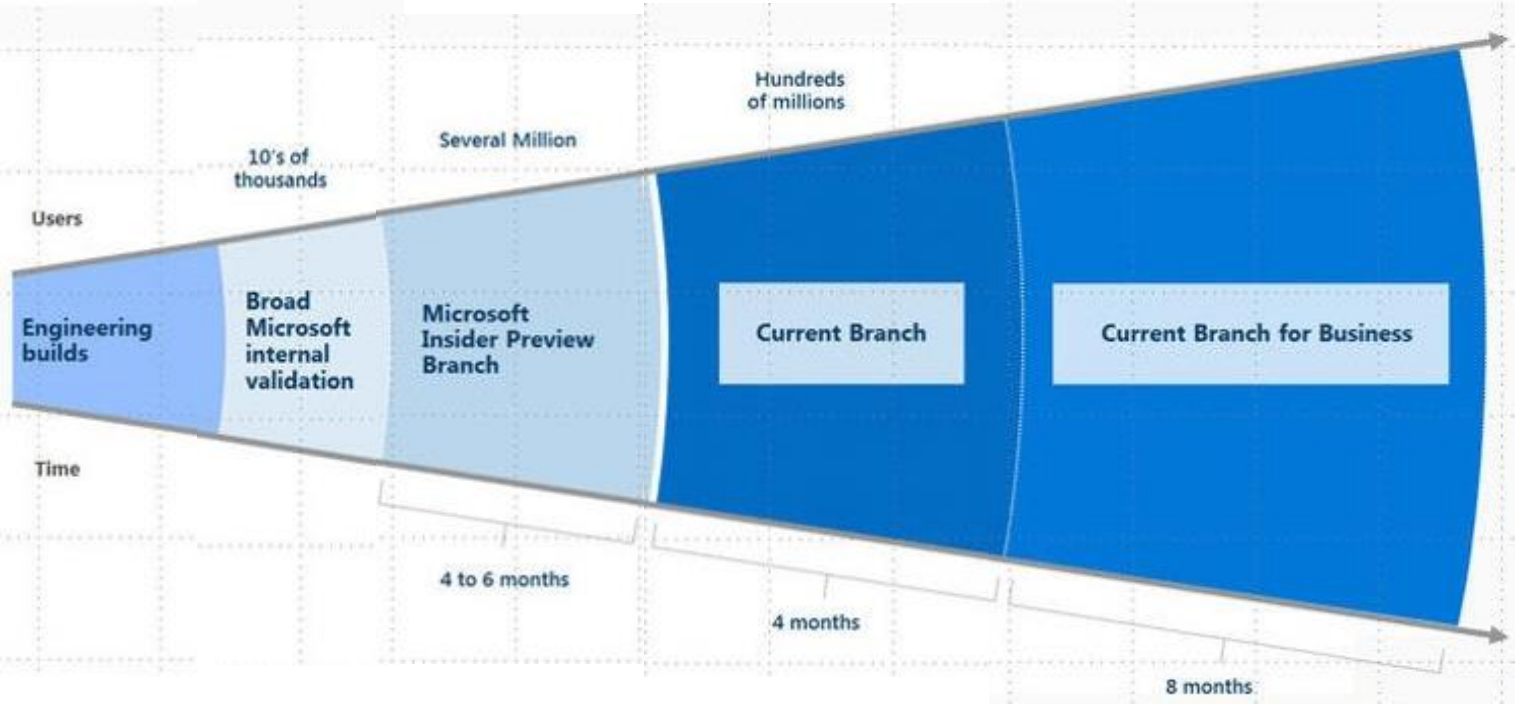
100% 50% 0%

60 s 30 s

Update Management of New Branches

- Microsoft introduced the concept of ***Windows as a Service*** when Windows 10 was released in 2015
  - Both ***"quality updates" (patches)*** and ***"feature updates"*** are now pushed down through the Windows Update pipeline
  - To accommodate different update cadences, there are now distinct ***branches*** that customers can use to deploy updates
  - Here is how those branches fit together:

How the Windows Update Branches Fit Together



Update Management of New Branches

- With the exception of Nano server (which only supports Current Branch), both major versions of Windows Server 2016 use the Long Term Servicing Branch approach (also known as “5+5”):
  - 5 years of standard support
  - 5 years of extended support
- If you use Windows Server 2016 as a WSUS server, new group policy settings allow you to select the branch you want to use for Windows 10 clients:

Update Management of New Branches

- Default Domain Policy [LON-DC1.ADATUM.CO
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy def
        - Windows Components
          - Windows Update
            - Defer Windows Updates
        - All Settings
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Setting	State	Comment
Select when Feature Updates are received	Not configured	No
Select when Quality Updates are received	Not configured	No

Select when Feature Updates are received

Select when Feature Updates are received

Previous Setting | Next Setting

- ○ Not Configured
- ◉ Enabled
- ○ Disabled

Comment:

Supported on: At least Windows Server 2016 or Windows 10

Options:

Select the branch readiness level for the feature updates you want to receive:

Current Branch
- Current Branch
- Current Branch for Business

r receiving it
for this many days:

180

☑ Pause feature updates

Help:

Enable this policy to specify what type of feature updates to receive, and when.

The branch readiness level for each new Windows 10 feature update is initially considered a "Current Branch" (CB) release, to be used by organizations for initial deployments. Once Microsoft has verified the feature update should be considered for enterprise deployment, it will be declared a branch readiness level of "Current Branch for Business" (CBB).

You can defer receiving feature updates for up to 180 days.

To prevent feature updates from being received on their scheduled time, you can temporarily pause feature updates. The pause will remain in effect for 60 days or until you clear the check box.

New Features

Containers and Docker

- ***Containers*** provide isolated environments – process isolation and namespace isolation – in which to run applications
- Native to all versions of Windows Server 2016 – Desktop Experience, Core and Nano – as well as certain Windows 10 anniversary edition computers
- Two subtypes available depending on the level of isolation needed:
  - Windows Server containers
  - Hyper-V containers
- ***Docker,*** an open-source project, originally developed for Linux, further enhances Windows containers by providing a way to automate the deployment of applications inside them

Benefits of and uses for Containers

- Containers provide a terrific development platform:
  - Using Containers ensures that when an app is ready to be deployed, all dependencies are included (middleware, runtimes, required libraries, etc.)
- Containers are secure:
  - Apps within a container have their own view of the file system and registry and are unaware of other containers on a host
- Containers provide compatibility:
  - Because multiple containerized apps on a host are unaware of each other, you can avoiding problems with applications not being compatible with each other
- Containers are portable:
  - Containers can easily be floated to a different host without reconfiguration

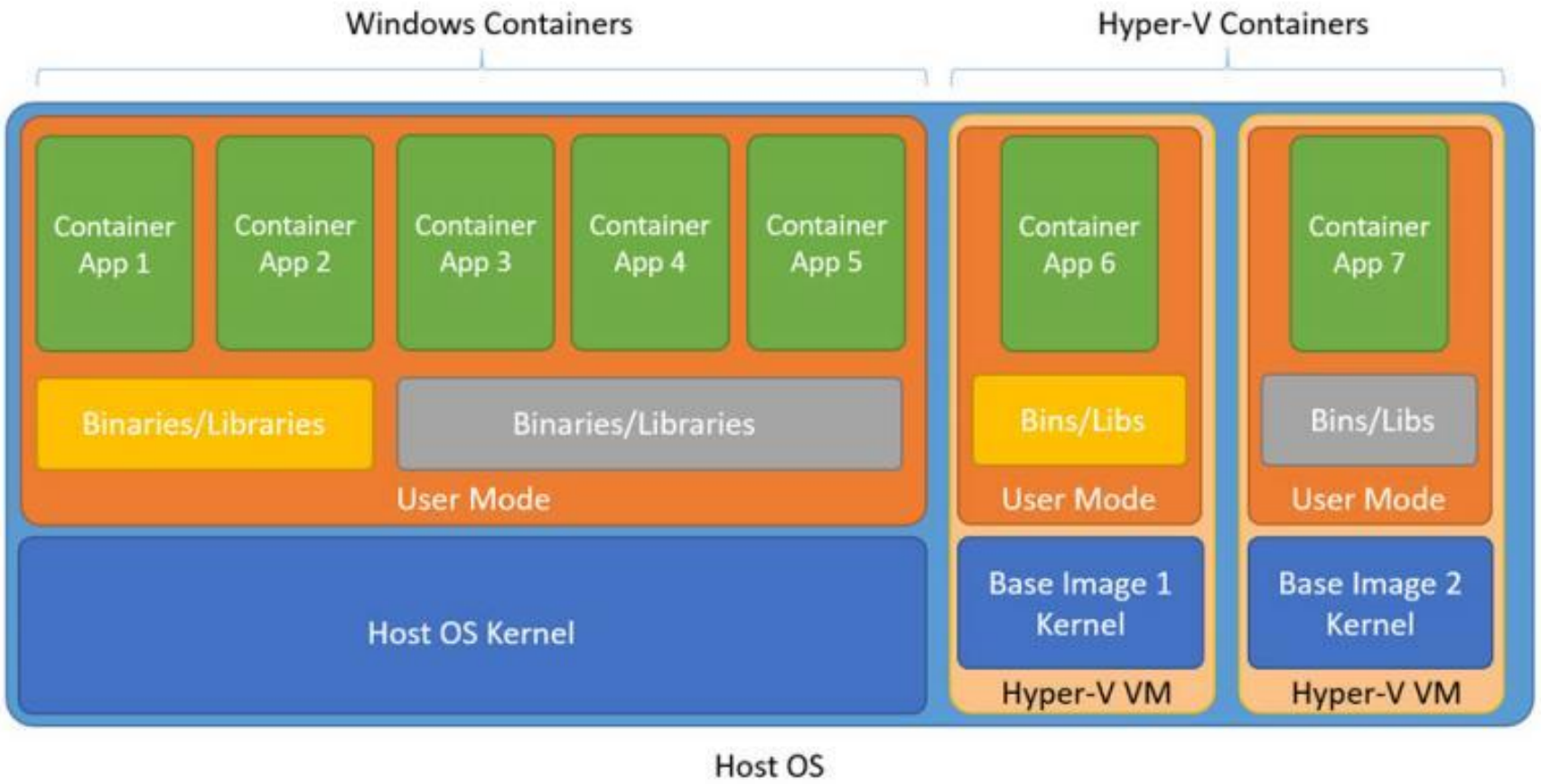
Windows Server Containers vs. Hyper-V Containers

Windows Server containers

- Isolate apps using ***namespace and process isolation***, but share the kernel with the container host and all containers running on the host
- Not as isolated as Hyper-V containers

Hyper-V containers

- Isolate apps using encapsulation in a lightweight and highly-optimized virtual machine without sharing the host kernel with other Hyper-V Containers
- The host operating system cannot be affected in any way by any running container


Windows Containers
Hyper-V Containers
Container App 1
Container App 2
Container App 3
Container App 4
Container App 5
Container App 6
Container App 7
Binaries/Libraries
Binaries/Libraries
Bins/Libs
Bins/Libs
User Mode
User Mode
User Mode
Host OS Kernel
Base Image 1 Kernel
Base Image 2 Kernel
Hyper-V VM
Hyper-V VM
Host OS

Difference between Hyper-V Containers and Hyper-V VMs

So, how are Hyper-V containers any different from Hyper-V Virtual machines?

- With Hyper-V virtual machines:
  - Each VM is created and managed manually
  - Boot times are roughly the same as booting a physical host with similar configuration
- With Hyper-V Containers
  - VMs are created automatically from the same base image as the container is provisioned
  - Container VMs are optimized and boot faster than a regular VM (although not as quickly as a Windows Server container)

Powershell v5

- First off, Powershell guidance is now being consolidated and curated from one central hub at Microsoft: **`www.microsoft.com/powershell`**

- Server 2016 includes Powershell v5 which adds:

  - New features for developers, such as being able to define formal classes for scripts

  - New features for administrators, including:
  - Dozens of new cmdlets
  - A new ***Network Switch*** module enables you to apply switch, virtual LAN (VLAN), and basic Layer 2 network switch port configuration to supported network switches from Arista, Cisco, Huawei and others

Powershell v5

- Enhancements for admins (cont):
  - Addition of ***Just Enough Administration*** whereby a “runspace” is defined and assigned to users that limits, right down to the cmdlet, what they’re able to do on a certain machine. More information and demonstrations:

    `https://blogs.technet.microsoft.com/privatecloud/2014/05/14/just-enough-administration-step-by-step/`

  - New capabilities for ***Desired State Configuration*** including an integrated way to acquire them resource using `Find-DSCResource` and NuGet

Powershell v5 – DSC

- ***Desired State Configuration*** ensures that server configuration is consistent and can reduce configuration drift using the following methods:

  1. Installing and removing roles and features
  2. Installing and managing packages
  3. Managing user and group accounts
  4. Managing registry settings, file and directories
  5. Running Powershell scripts

- DSC's main advantage is its ability to configure machines identically and ensure at all times that the configurations remain as intended

Powershell v5 – DSC

- DSC supports two modes: ***push mode*** and ***pull mode***
  - **<u>Push mode</u>**: configuration is created and pushed to servers manually
  - **<u>Pull mode</u>**: a separate server stores the configuration files, is periodically polled for changes, and then delivers configuration changes using https: or SMB
- A ***DSC Resource*** is a managed element of DSC. Examples include: *file, registry, group, package, script, Windows Feature*, etc.
- The ***Local Configuration Manager*** is the client-side component of DSC that carries out the directives

Storage Replica overview

Storage Replica establishes storage agnostic, block-level, and synchronous replication between clusters or servers for disaster recovery

- **Replicates blocks, not files,** using **SMB 3.0**
- **Does not replace DFSR** – DFSR is better for branch office scenarios which often have relatively high latency & utilization, and low bandwidth, making synchronous replication impractical
- **Does not care if files are in use**, but the destination volume is not accessible while replicating (it is dismounted and not visible in File Explorer)
- **Is not a replacement for backups:** Storage Replica replicates all changes to all blocks of data on the volume, regardless of the change type
  - For example, if a user deletes all data from a volume, Storage Replica will replicate the deletion instantly to the other volume

Storage Replica use cases

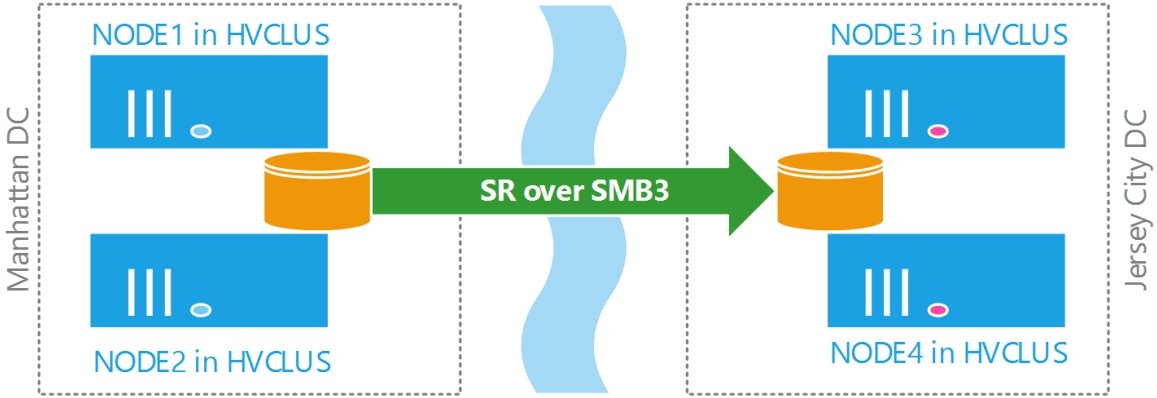
So what are some good uses for Storage Replica?

- The three replication possible uses for Storage Replica are:
  - Hyper-V stretch cluster
  - Server-to-server
  - Cluster-to-cluster

Storage Replica for a Hyper-V stretch cluster

Hyper-V Stretch cluster

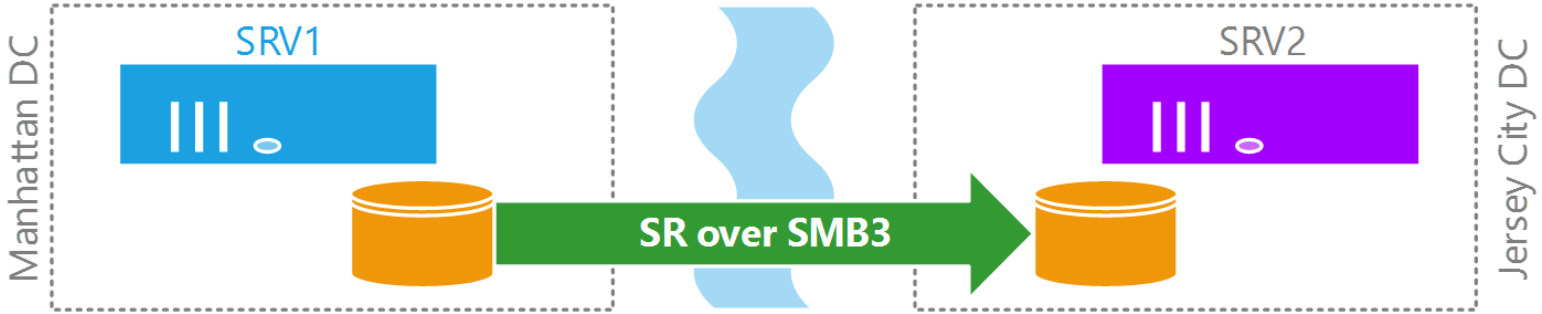
- Requires a Hyper-V cluster with domain-joined physical hosts and SCSI JBODs, Fibre Channel SAN, or iSCSI storage in two locations
- Storage Replica handles synchronous replication of all needed files
- Failover clustering handles automatic failover to the other location



Storage Replica for Server-to-server replication

Server-to-Server replication

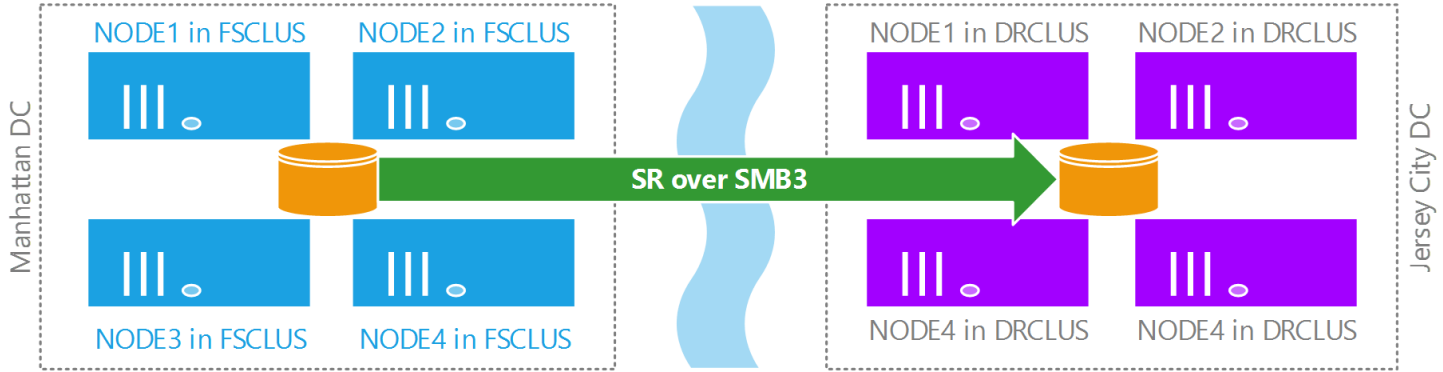
- Two separate servers (physical or virtual) with two sets of storage that use DAS, serial-attached SCSI JBODs, Fibre Channel SAN, or iSCSI Targets
- Manual failover using Failover Cluster Manager or Powershell
- Synchronous or asynchronous replication of data



Storage Replica for Cluster-to-cluster replication

Cluster-to-Cluster replication

- Two separate clusters of domain-joined servers and Storage Spaces Direct, serial attached SCSI JBODs, Fibre Channel SAN, or iSCSI Targets for storage
- Manual failover using Failover Cluster Manager or Powershell
- Can choose synchronous or asynchronous replication of data



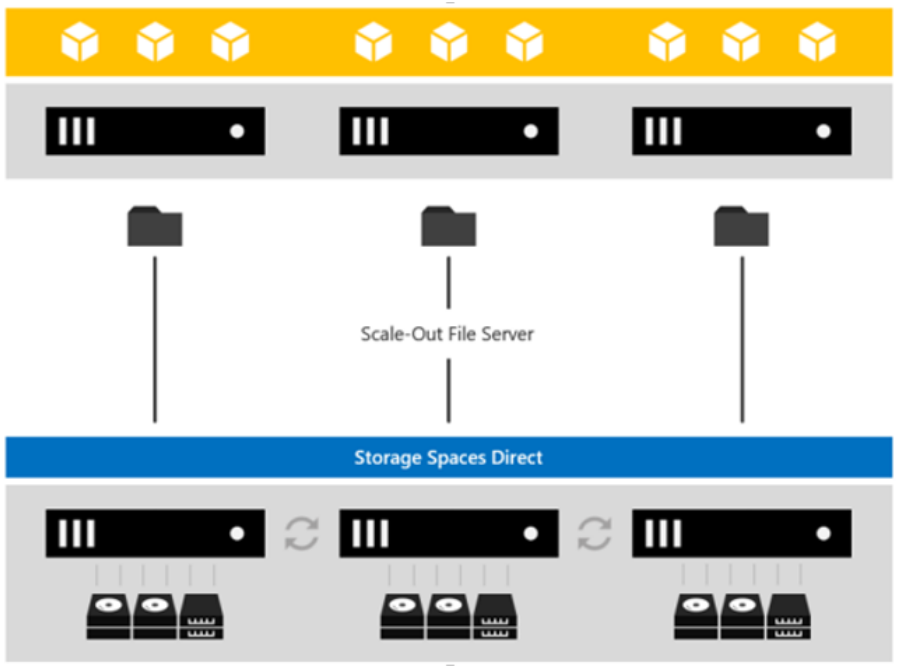
Storage Spaces Direct

Storage Spaces Direct is software-defined, “shared-nothing” storage

- Enables building highly available storage systems with features expected from a high-end storage solution, including cache, resiliency and tiers, using only:
  - Local disks, and
  - Ethernet
- Works with SAS, SATA (HDD/SSD) and Non-Volatile Memory Express (NVMe) disks
- Integrates with existing Windows features, including ***Scale-Out File Server***, ***Clustered Shared Volume File System (CVS-FS)***, ***Storage Spaces***, ***failover clustering*** and ***ReFS***

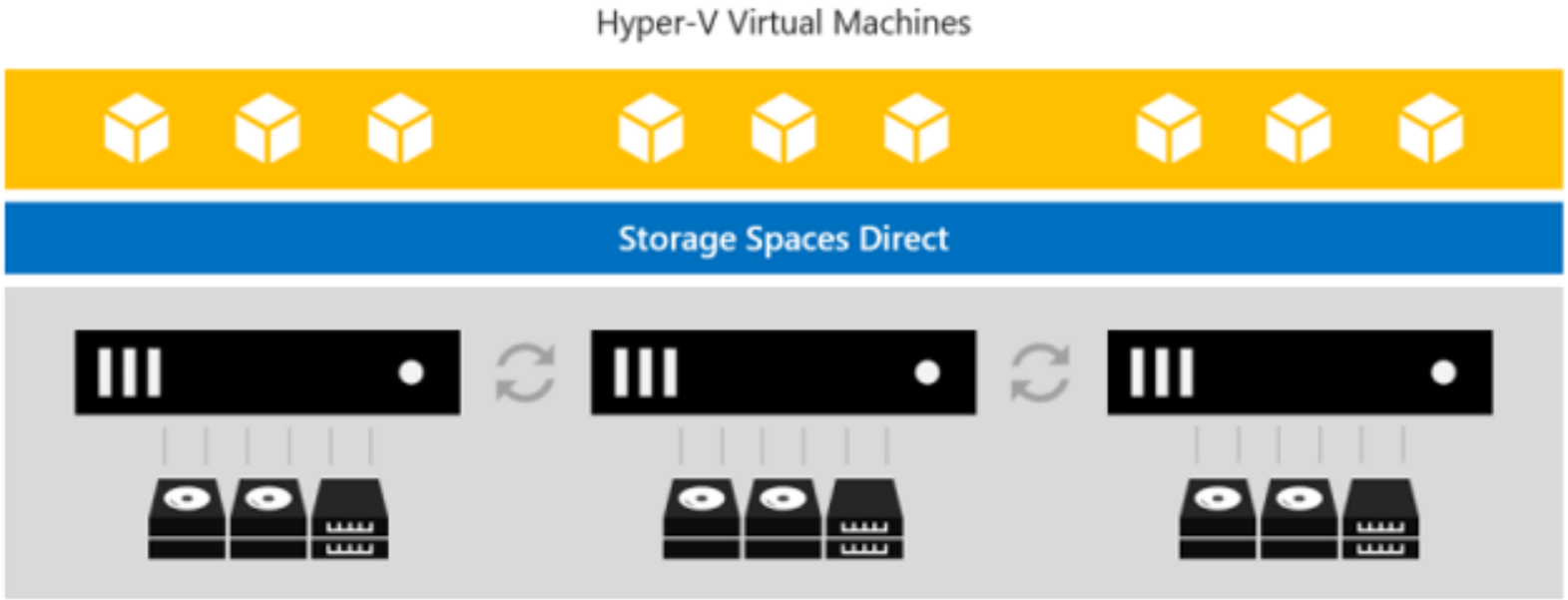
Storage Spaces Direct

In a ***converged*** or ***disaggregated*** deployment, a Scale-out File Server sits atop Storage Spaces Direct to provide network-attached storage using SMB3 file shares, providing the ability to scale the storage and computer tiers separately



Storage Spaces Direct

In a ***Hyper-Converged*** deployment, both tiers (compute and storage) reside on the same cluster



Windows 2016 Training at System Source

- Course 20740: Installation, Storage and Compute with Windows Server 2016
  - March 13-17 (Hunt Valley)
  - May 22-26 (Columbia)
- Course 20741 Networking with Windows Server 2016
  - April 10-14 (Hunt Valley)
  - June 19-23 (Columbia)
- Course 20742 Identity with Windows Server 2016
  - April 3-7 (Columbia)
  - June 12-16 (Hunt Valley)
- Any of the above – group of 10
  - Your site or ours

To register:

Online: www.syssrc.com/html/training/index.shtml

Email: training@syssrc.com

Phone: 410-771-5544 x5

Windows 2016 Training at System Source

- Course 20743 Upgrading Your Skills to MCSA: Windows Server 2016
  - June 6-9 (Hunt Valley)
  - August 14-18 (Hunt Valley)
- PowerShell Quickstart for Administrators (3 days)
  - March 27-29 (Hunt Valley)
  - July 19-21 (Columbia)

Any of the above – group of 10

Your site or ours

To register:

Online: www.syssrc.com/html/training/index.shtml

Email: training@syssrc.com

Phone: 410-771-5544 x5

Learning Center Offer
Evaluations
Door Prizes

THANK YOU!