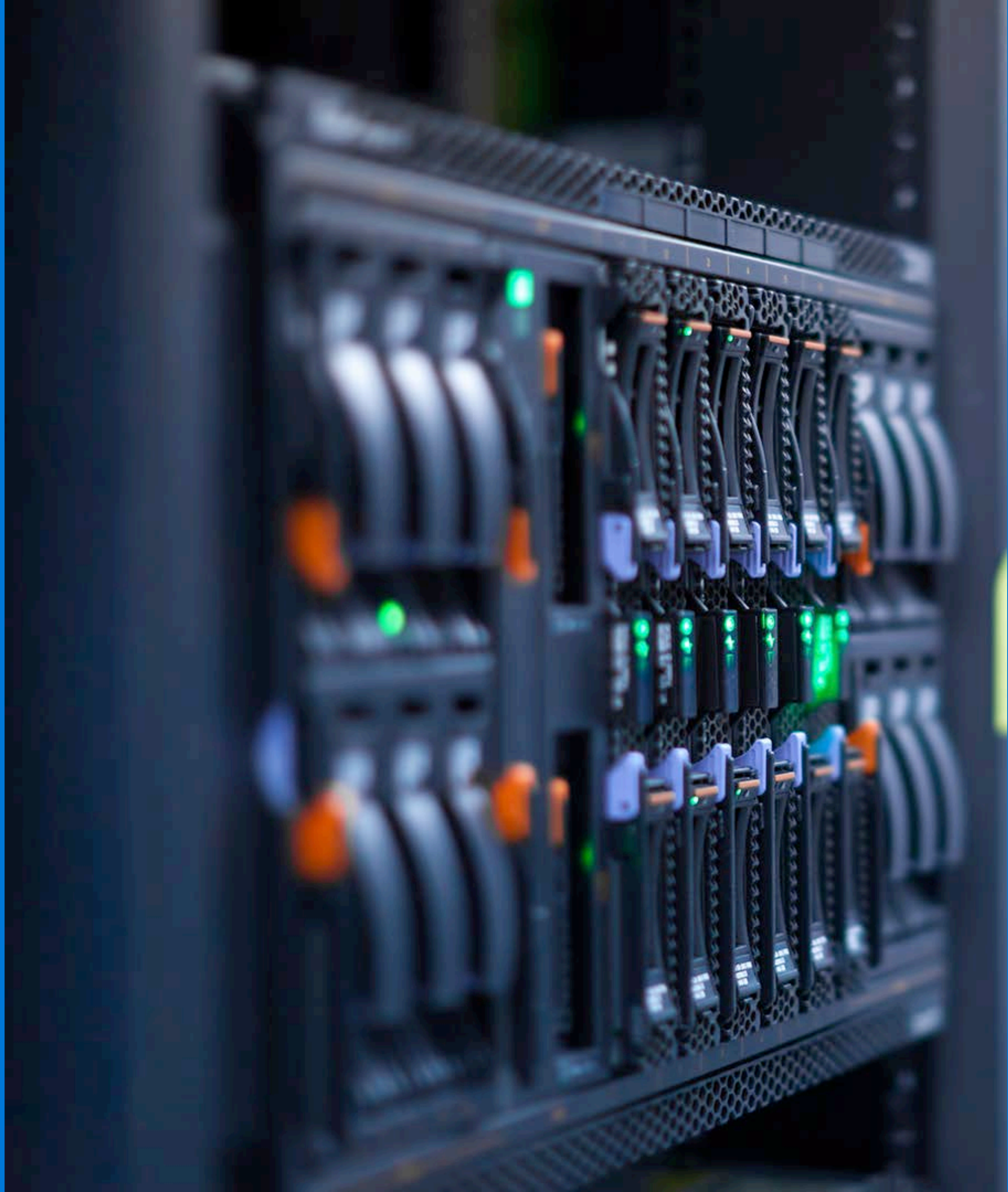
Windows Server 2016 for the hosting market - Technical preview

Herman Keijzer
hermank@microsoft.com
PTS

Microsoft



Windows Server 2016

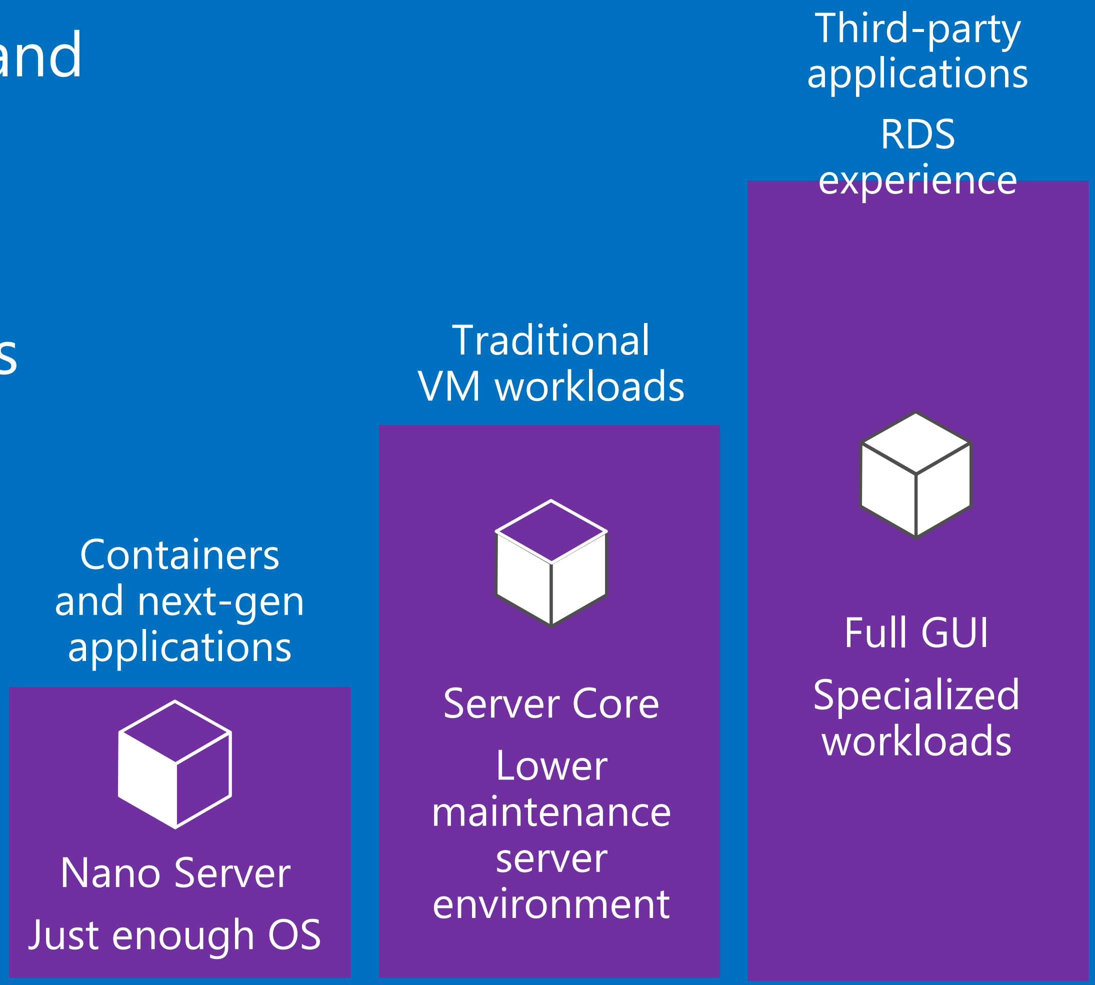
The cloud-ready server operating system that delivers new layers of security and Azure-innovation for the applications and infrastructure that power your business.

Built-in Security	Software-defined Datacenter	Cloud-ready Application Platform
Built-in layers of security Protecting Privileged Identity Secure virtualization platform	Built-in SDDC capabilities Affordable and enterprise ready Azure-inspired infrastructure	Built-in containers Lightweight Nano Server option Bring licenses to Azure

Nano Server: just enough OS

Optimized for next-gen distributed applications

- Higher density and Reduced attack surface and servicing requirements
- Next-gen distributed app frameworks
- Interoperate with existing server applications



Containers and next-gen applications

Nano Server

Just enough OS

Traditional VM workloads

Server Core

Lower maintenance server environment

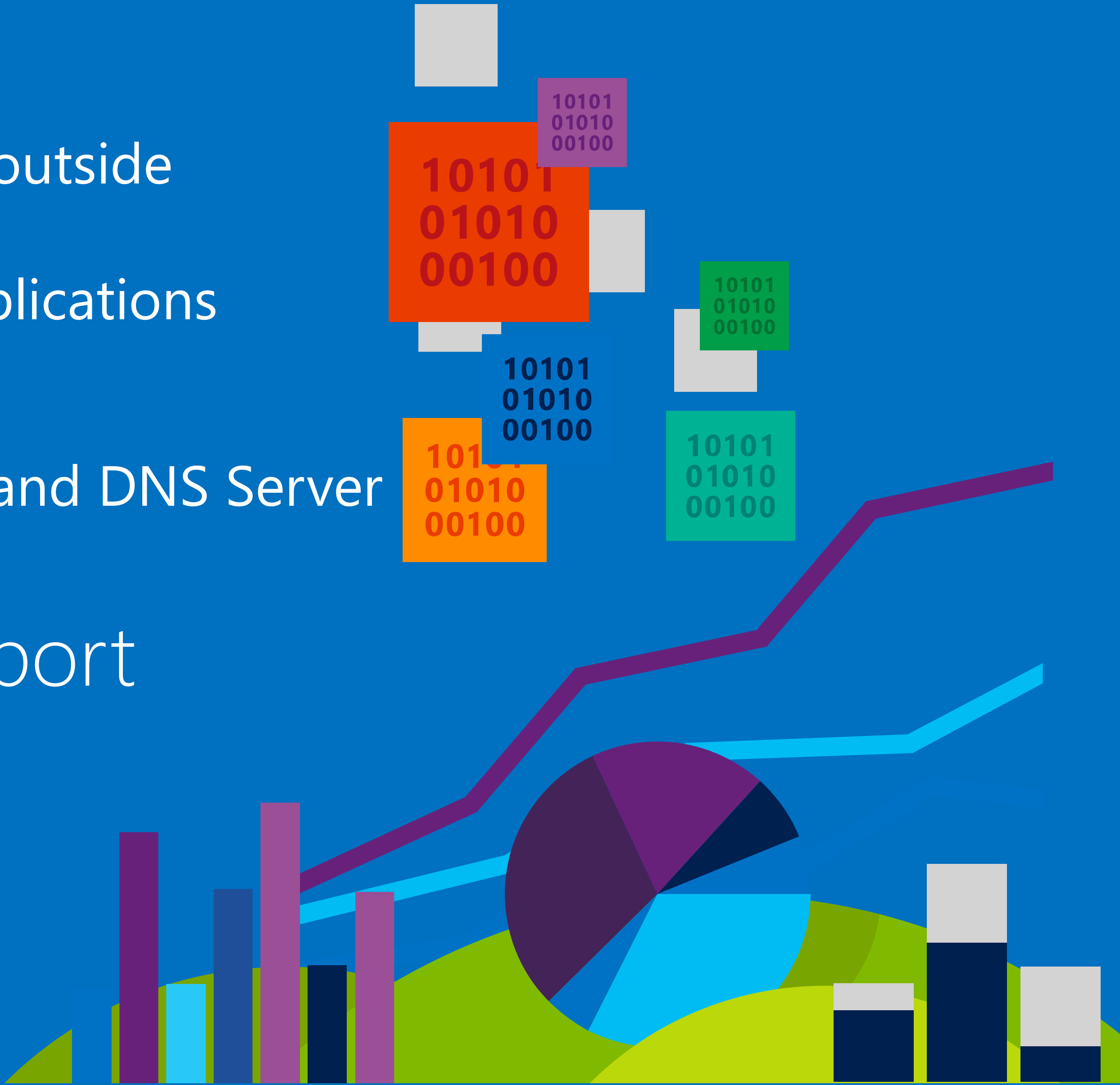
Third-party applications

RDS experience

Full GUI

Specialized workloads

Nano Server: Next step in our cloud journey



Zero-footprint model

- Server Roles and Optional Features live outside of Nano Server
- Standalone packages that install like applications

Key Roles & Features

- Hyper-V, Storage (SoFS), Clustering, IIS, and DNS Server
- .NET Core and ASP.NET Core

Full Windows Server driver support

Antimalware optional package

System Center VMM and OM agents available

Nano Server - Cloud Application platform

Born-in-the-cloud application support

- CoreCLR
- PaaS & ASP.NET V.Next
- A subset of Win32

Available everywhere

- Host OS for physical hardware & Hyper-V
- Guest OS in a VM
- Container OS

Planned runtime support

- PowerShell Desired State Configuration (DSC) & OneGet
- Web Server (IIS)
- PHP
- Java
- Node.JS

Based on the current builds, compared to WS12 R 2 Server, Nano Server has:

- 93 percent lower VHD size
- 92 percent fewer critical bulletins
- 80 percent fewer reboots

Where To Run nano server

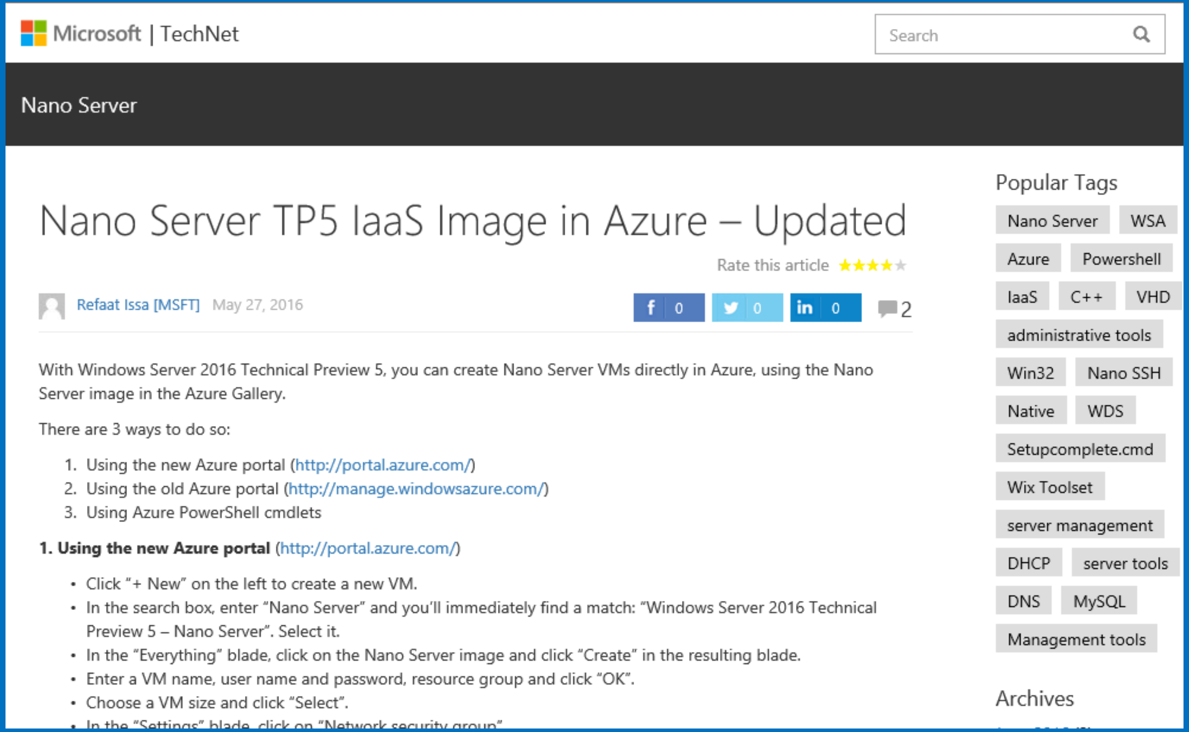
Azure

Via nano server image in VM gallery

Existing Server/Physical or VM

Install Windows Server 2016 TP5

Windows Server and/or Hyper-V Containers



Nano Server TP5 IaaS Image in Azure – Updated

Refaat Issa [MSFT] May 27, 2016

With Windows Server 2016 Technical Preview 5, you can create Nano Server VMs directly in Azure, using the Nano Server image in the Azure Gallery.

There are 3 ways to do so:

1. Using the new Azure portal (http://portal.azure.com/)
2. Using the old Azure portal (http://manage.windowsazure.com/)
3. Using Azure PowerShell cmdlets

1. Using the new Azure portal (http://portal.azure.com/)

- Click "+ New" on the left to create a new VM.
- In the search box, enter "Nano Server" and you'll immediately find a match: "Windows Server 2016 Technical Preview 5 – Nano Server". Select it.
- In the "Everything" blade, click on the Nano Server image and click "Create" in the resulting blade.
- Enter a VM name, user name and password, resource group and click "OK".
- Choose a VM size and click "Select".
- In the "Settings" blade, click on "Network security group"

Containers

A new approach to build, ship, deploy, and instantiate applications

Physical

Applications traditionally built and deployed onto physical systems with 1:1 relationship

New applications often required new physical systems for isolation of resources

Virtual

Higher consolidation ratios and better utilization

Faster app deployment than in a traditional, physical environment

Apps deployed into VMs with high compatibility success

Apps benefited from key VM features; i.e., live migration, HA

Package and run apps within **containers**

Physical/Virtual

Key Benefits

Further accelerate of app deployment

Reduce effort to deploy apps

Streamline development and testing

Lower costs associated with app deployment

Increase server consolidation

Why Containers?

Applications are fueling innovation in today's cloud-mobile world

Developers

- Containers unlock ultimate productivity and freedom
- Enable 'write-once, run-anywhere' apps
- Can be deployed as multi-tier distributed apps in IaaS/PaaS models
- Containers offers powerful abstraction for microservices

Operations

- Enhances familiar IT deployment models
- Provide standardized environments for development, QA, and production teams
- Abstract differences in OS distributions and underlying infrastructure
- Higher utilization and compute density
- Rapid scale-up and scale-down in response to changing business needs

DevOps

- Integrate people, process, and tools for an optimized app development process
- Operations focus on standardized infrastructure
- Developers focus on building, deploying, and testing apps

Windows Server Containers

Anatomy and key capabilities

Spotlight capabilities

Build: Developers will use familiar development tools, such as Visual Studio, to write apps to run within containers

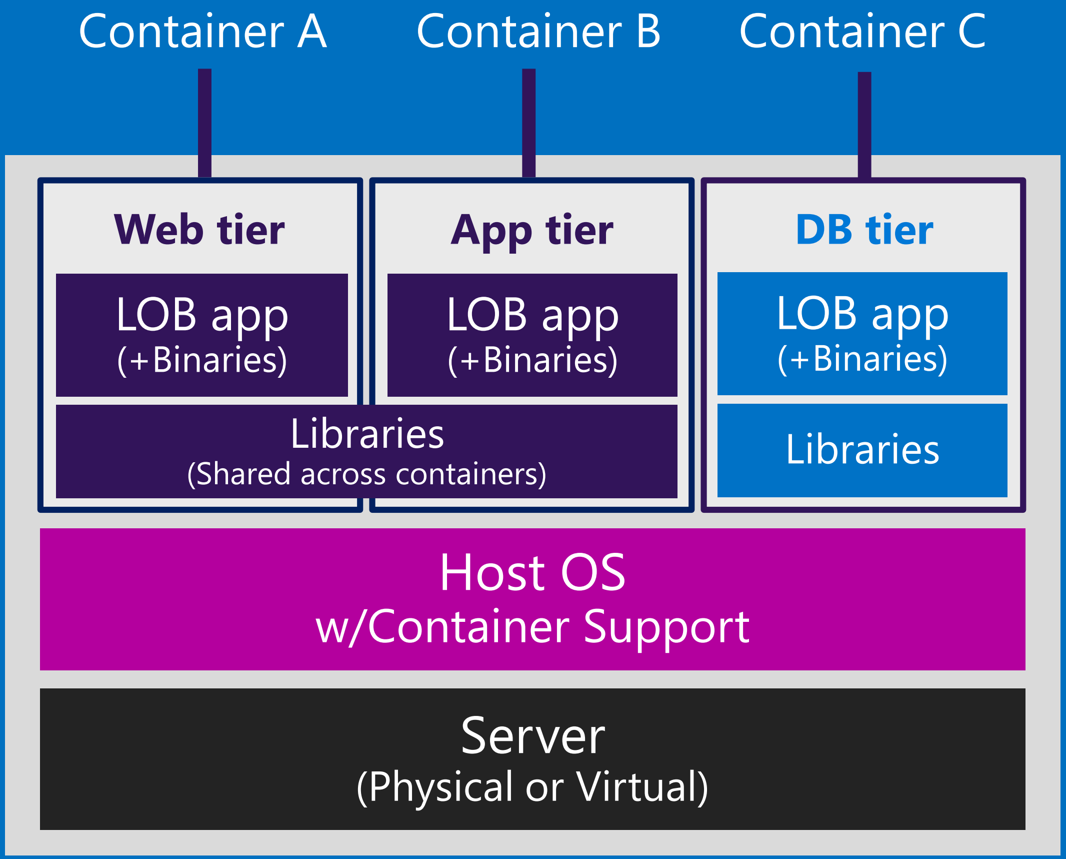
By building modular apps leveraging containers, modules can scale independently, and be updated on independent cadences

Run: Container capabilities built into Windows Server

Manage: Deploy and manage containers using PowerShell, or using Docker

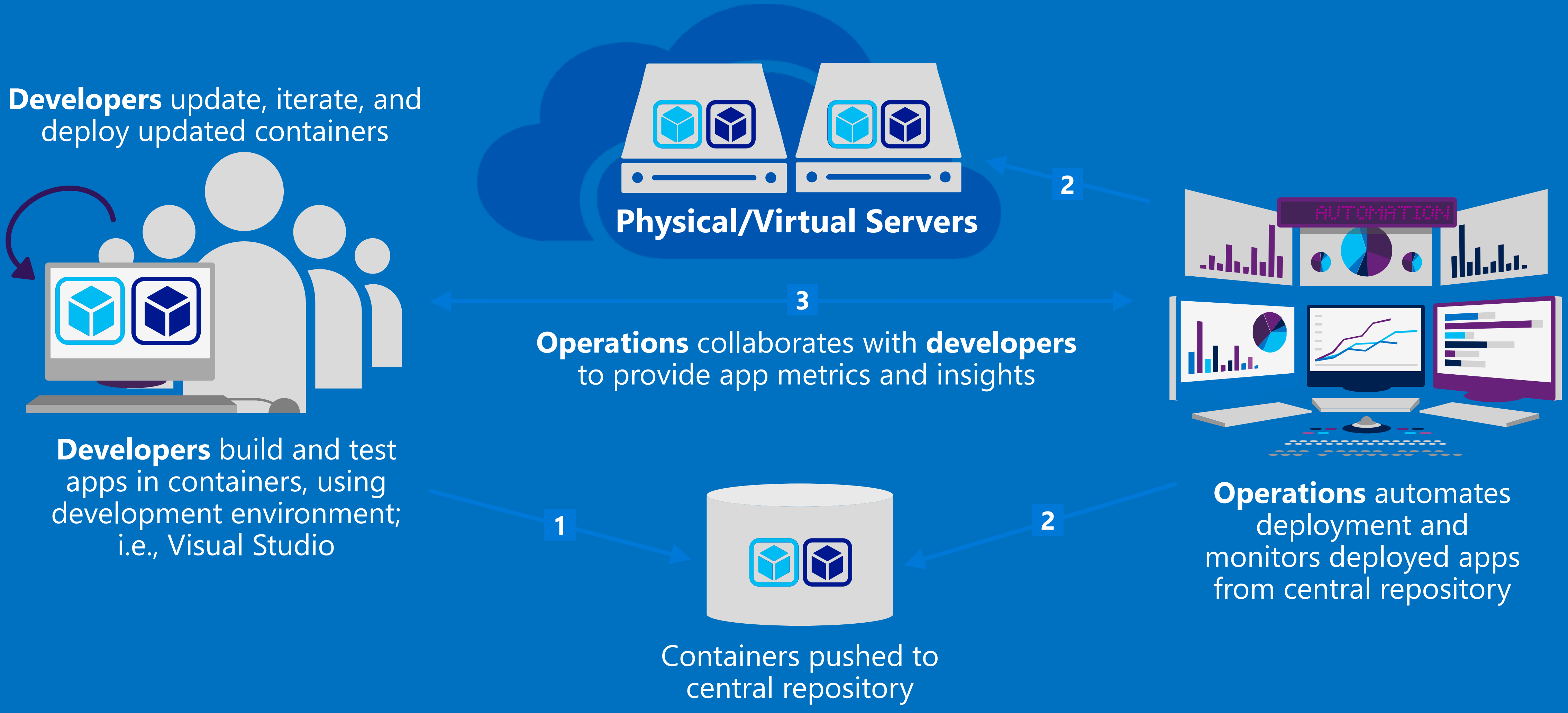
Resources: Define CPU and memory resources per container along with storage and network throughput

Network: Provide NAT or DHCP/static IP for network connectivity



Windows Server Containers

Creation, deployment, and management



Developers update, iterate, and deploy updated containers

Developers build and test apps in containers, using development environment; i.e., Visual Studio

Operations collaborates with **developers** to provide app metrics and insights

Containers pushed to central repository

Operations automates deployment and monitors deployed apps from central repository

Hyper-V Containers

Anatomy and key capabilities

Spotlight capabilities

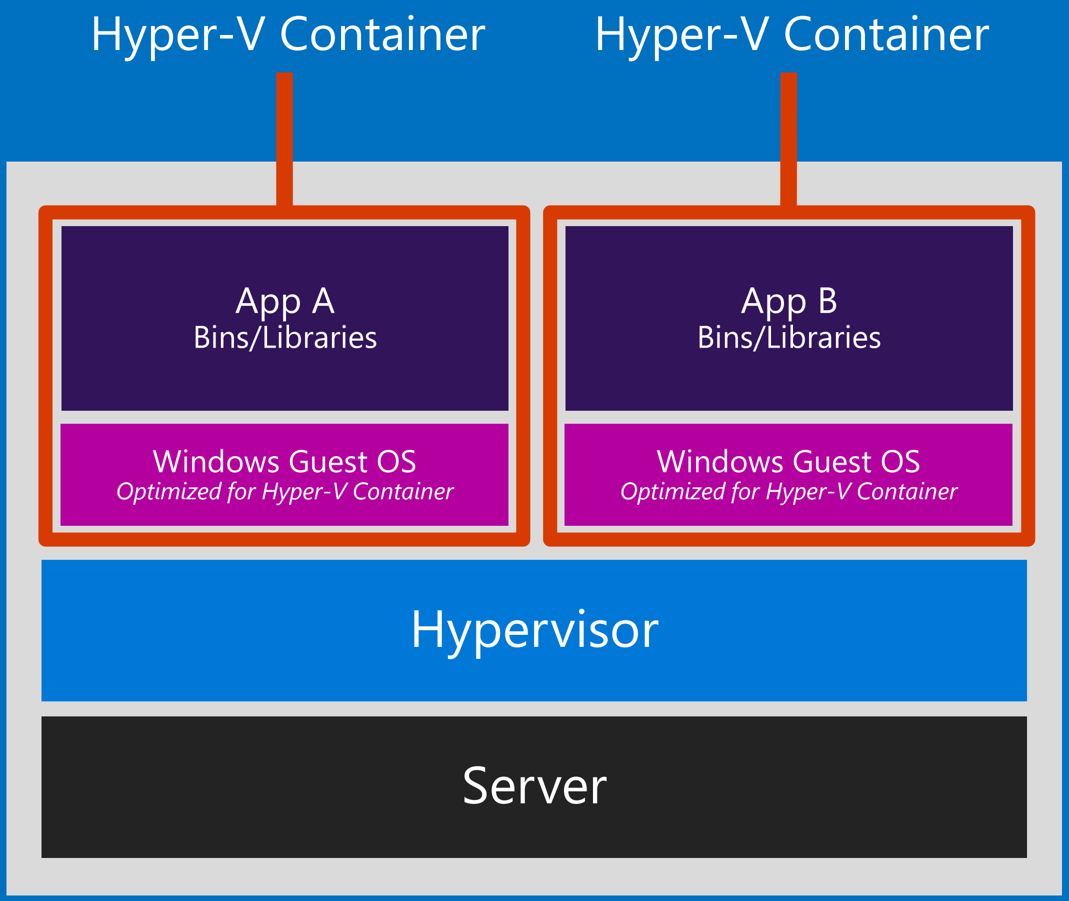
Consistency: Hyper-V containers use the same APIs as Windows Server containers ensuring consistency across management and deployment toolsets.

Compatibility: Hyper-V containers use the exact same images as Windows Server containers

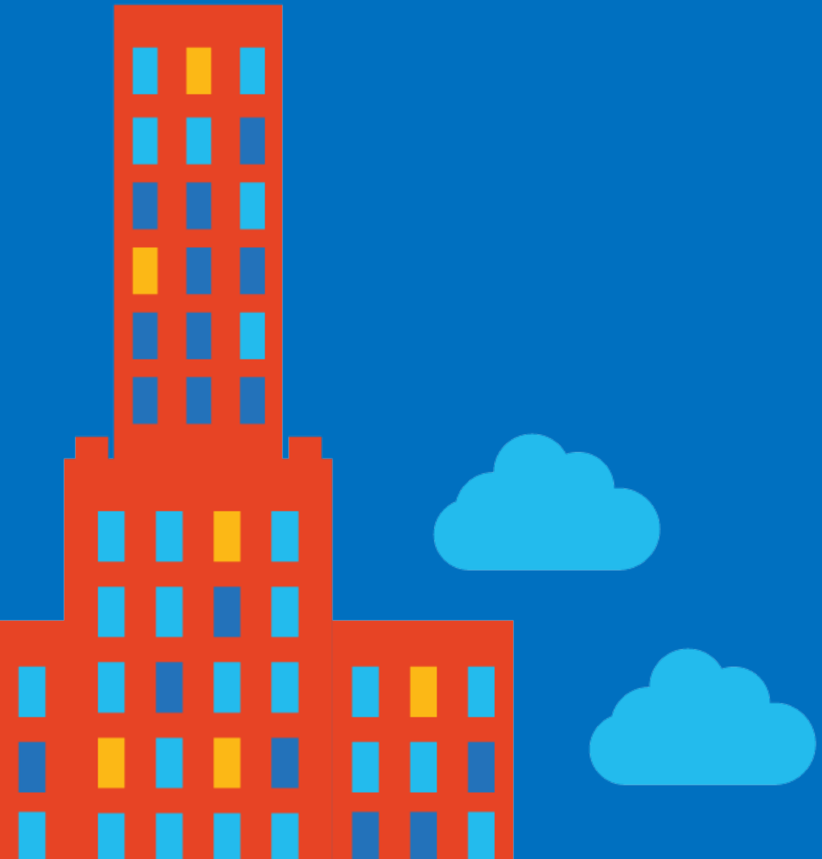
Strong isolation: Each Hyper-V container has its own dedicated copy of the kernel

Highly trusted: Built with proven Hyper-V virtualization technology

Optimized: The virtualization layer and the operating system have been specifically optimized for containers



Shielded VM’s



Central risk: Administrator privileges

Phishing attacks

Stolen admin credentials

Insider attacks

… each of these attacks seeks out & exploits privileged accounts.

1. We know that administrators have the keys to the kingdom; we gave them those keys decades ago

2. But those administrators privileges are being compromised through social engineering, bribery, coercion, private initiatives

Conclusion: *change the way we think about security*

We have to "assume breach" – not a position of pessimism, one of security rigor

Problem

A breach will (already did?) happen

Lacking the security-analysis manpower

Can't determine the impact of the breach

Unable to adequately respond to the breach

New approach (in addition to 'prevention')

Limit or block the breach from spreading

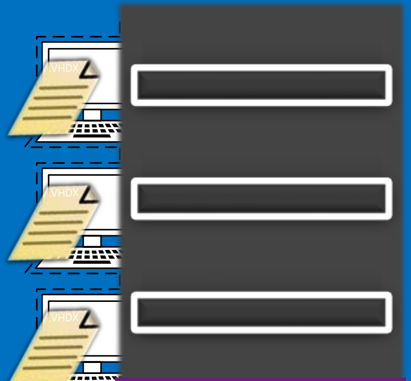
Detect the breach

Respond to the breach

Which admins have access to your machines?

Computer room

Perimeter



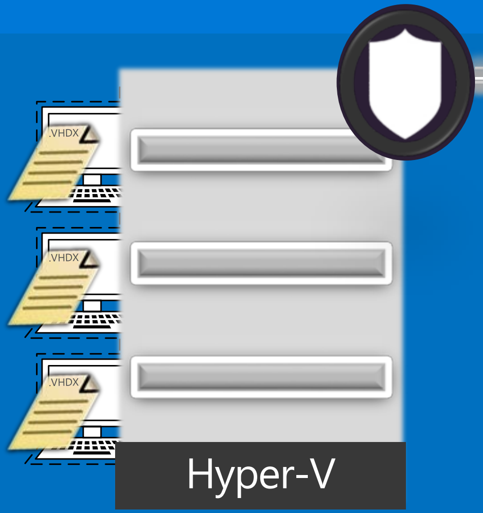
Hyper-V

	PHYSICAL MACHINES	VIRTUAL MACHINES
Server administrator	Yes	Yes
Storage administrator	No	Yes
Network administrator	No	Yes
Backup operator	No	Yes
Fabric administrator	No	Yes

Now with shielding – we encrypt VM-state and data

Computer room

Perimeter



	PHYSICAL MACHINES	VIRTUAL MACHINES
Server administrator	Yes	Configuration dependent
Storage administrator	No	No
Network administrator	No	No
Backup operator	No	No
Fabric administrator	No	No

A bit more detail…

What is it and who's it for?

As a hoster:

- “I can protect my tenants’ VMs + their data from datacenter administrators.”

As a tenant:

- “I can run my workloads in the cloud while meeting regulatory/compliance requirements.”

As an enterprise:

- “I can enforce a strong separation between Hyper-V administrators and sensitive VM-workloads.”

Implementation Spotlights

Hardware-rooted security technologies strictly isolate the VM from host administrators

A Host Guardian Service that is able to identify legitimate Hyper-V hosts and certify them to run a given shielded VM

Virtualized Trusted Platform Module (vTPM) support for Generation 2 virtual machines

Shielded VMs: Security Assurance Goals

Encryption & data at-rest/in-flight protection

Virtual TPM enables the use of disk encryption within a VM (e.g. BitLocker)

Both Live Migration and VM-state are encrypted

Admin-lockout

Host administrators cannot access guest VM secrets (e.g. can’t see disks or video)

Host administrators cannot run arbitrary kernel-mode code

Attestation of health

VM-workloads can only run on “healthy” hosts

Storage Spaces direct (Datacenter)
Hyper-converged with Windows Server 2016

Cloud design points and management

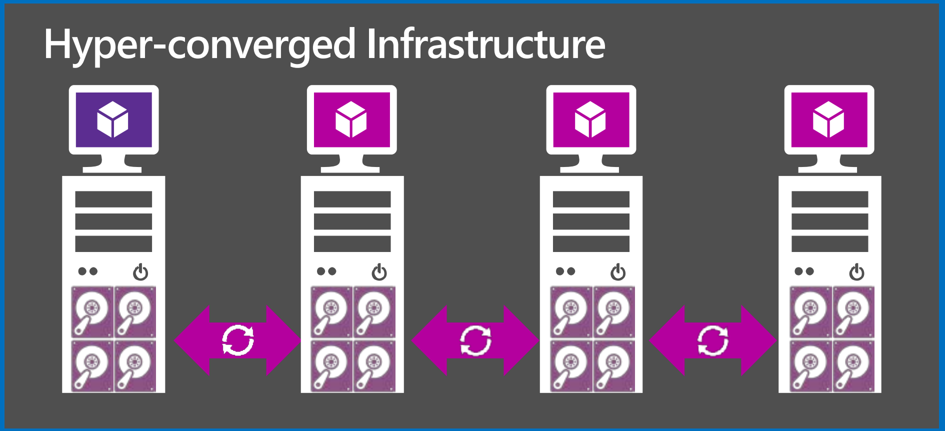
- Standard servers with local storage
- New device types such as SATA and NVMe SSD
- Prescriptive hardware configurations
- Deploy/manage/monitor with SCVMM, SCOM & PowerShell

Reliability, scalability, flexibility

- Fault tolerance to disk, enclosure, node failures
- Scale pools to large number of drives
- Simple and fine grained expansion
- Fast VM creation and efficient VM snapshots

Simplifying the datacenter

- Collapsing Storage and Compute
- Removes storage area network
- Storage controller is a software service



Hyper-converged Infrastructure

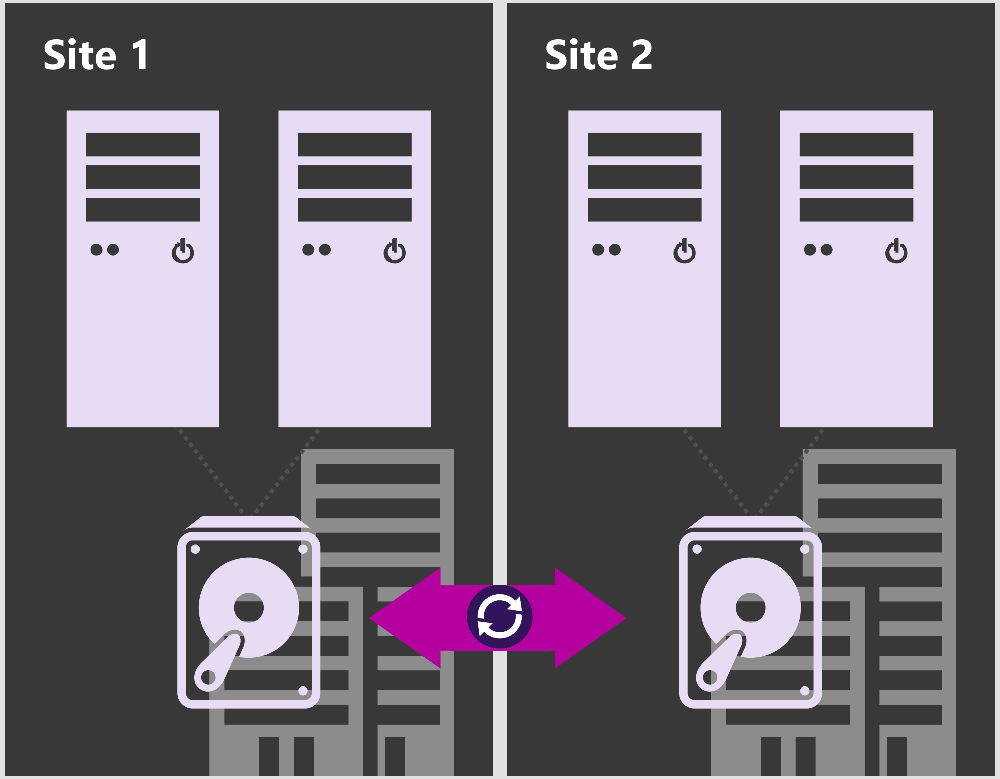
Storage Replica (Datacenter edition)

Synchronous replication: Storage agnostic mirroring of data in physical sites with crash-consistent volumes ensuring zero data loss at the volume level.

Increase resilience: Unlocks new scenarios for metro-distance cluster to cluster disaster recovery and stretch failover clusters for automated high availability.

Flexible: Server to server, cluster to cluster, and stretch cluster. Local disks, Storage Spaces Direct, clustered disks. NTFS, REFS, CSVFS. TCP, RDMA. Synchronous and asynchronous.

Streamlined management: Graphical management for individual nodes and clusters through Failover Cluster Manager and Azure Site Recovery. Full PowerShell and SMAPI support.



Software Defined Networking (Datacenter)

Network controller

Central control plane
Fault tolerant
Network monitoring

Virtual networking

BYO address space
Distributed routing
VXLAN and NVGRE

Network security

Distributed Firewall
Network Security Groups
BYO Virtual Appliances

Robust gateways

M:N availability model
Multi-tenancy for all modes of operation
BGP Transit Routing

Software load balancing

L4 load balancing (N-S and E-W) with DSR NAT
For tenants and cloud based infrastructure

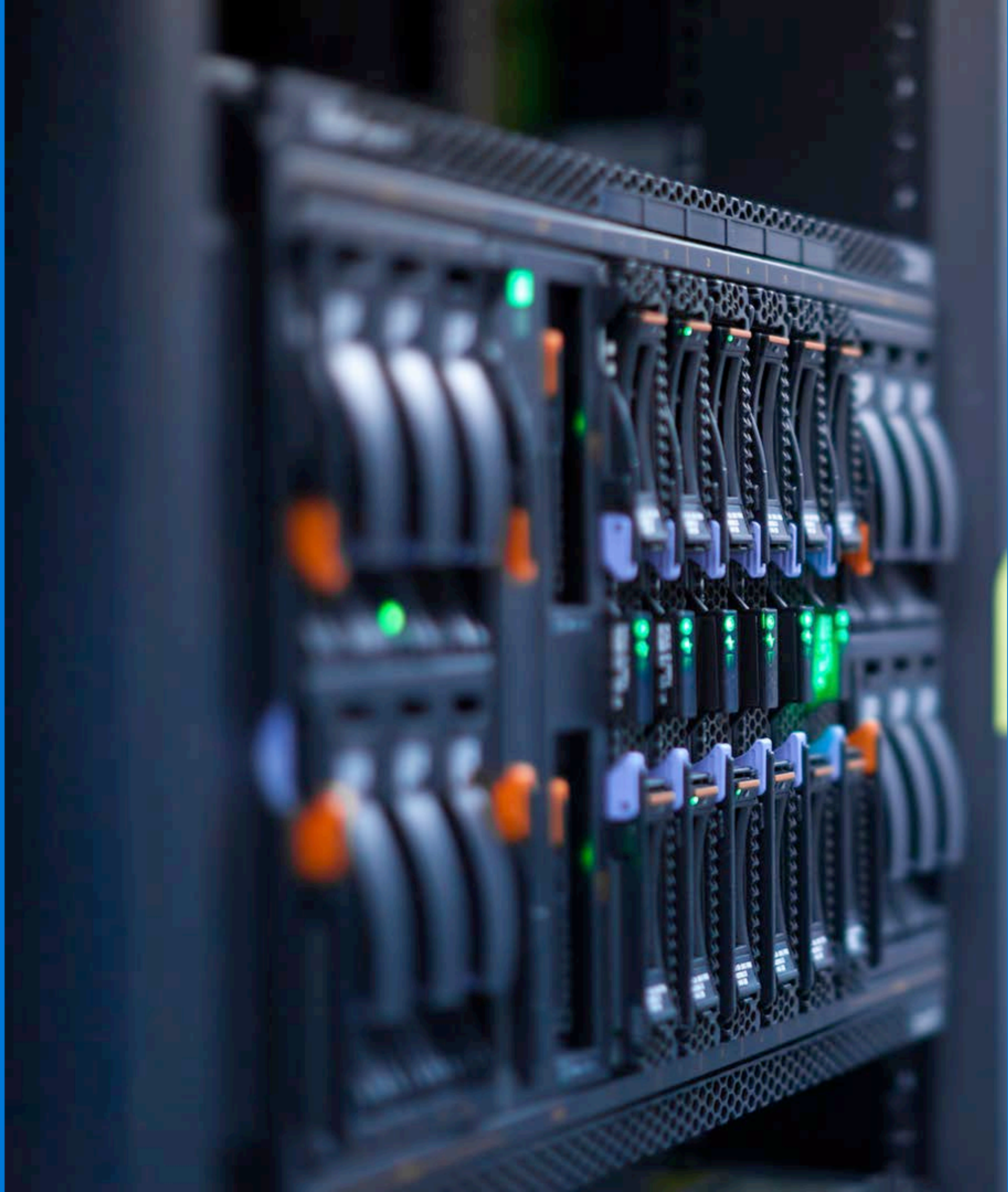
Data plane advancements

Performance: 10G, 40G, and beyond!
RDMA over Virtual Switch

Consistency with Azure in UI, API, and Services

Remote Desktop Services and Virtual Desktop Infrastructure

Microsoft

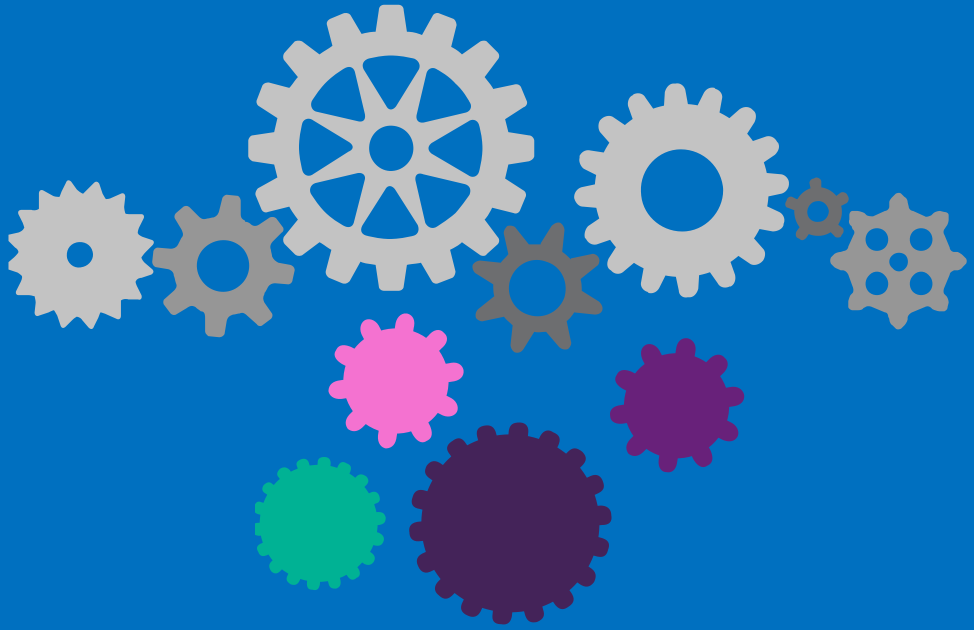


Key Windows Server 2016 RD investments

Increased performance and app compatibility – graphics improvements

Enhanced scale management – connection broker, shared SQL connections

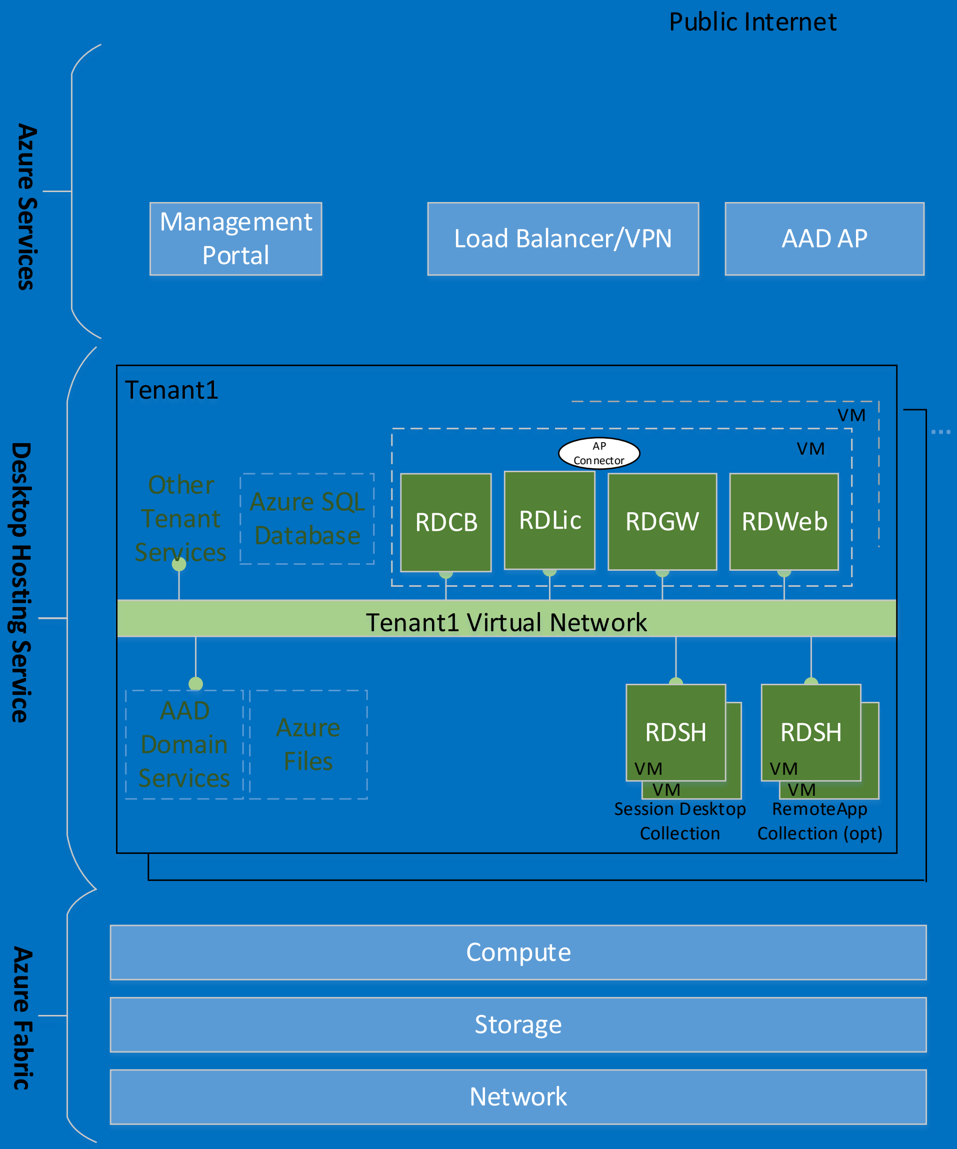
Optimized for cloud – efficient and secure architecture



Optimized server VM architecture for the cloud

RDS 2012R2 Infrastructure:

- **7 Role Services**
- **8 VMs**

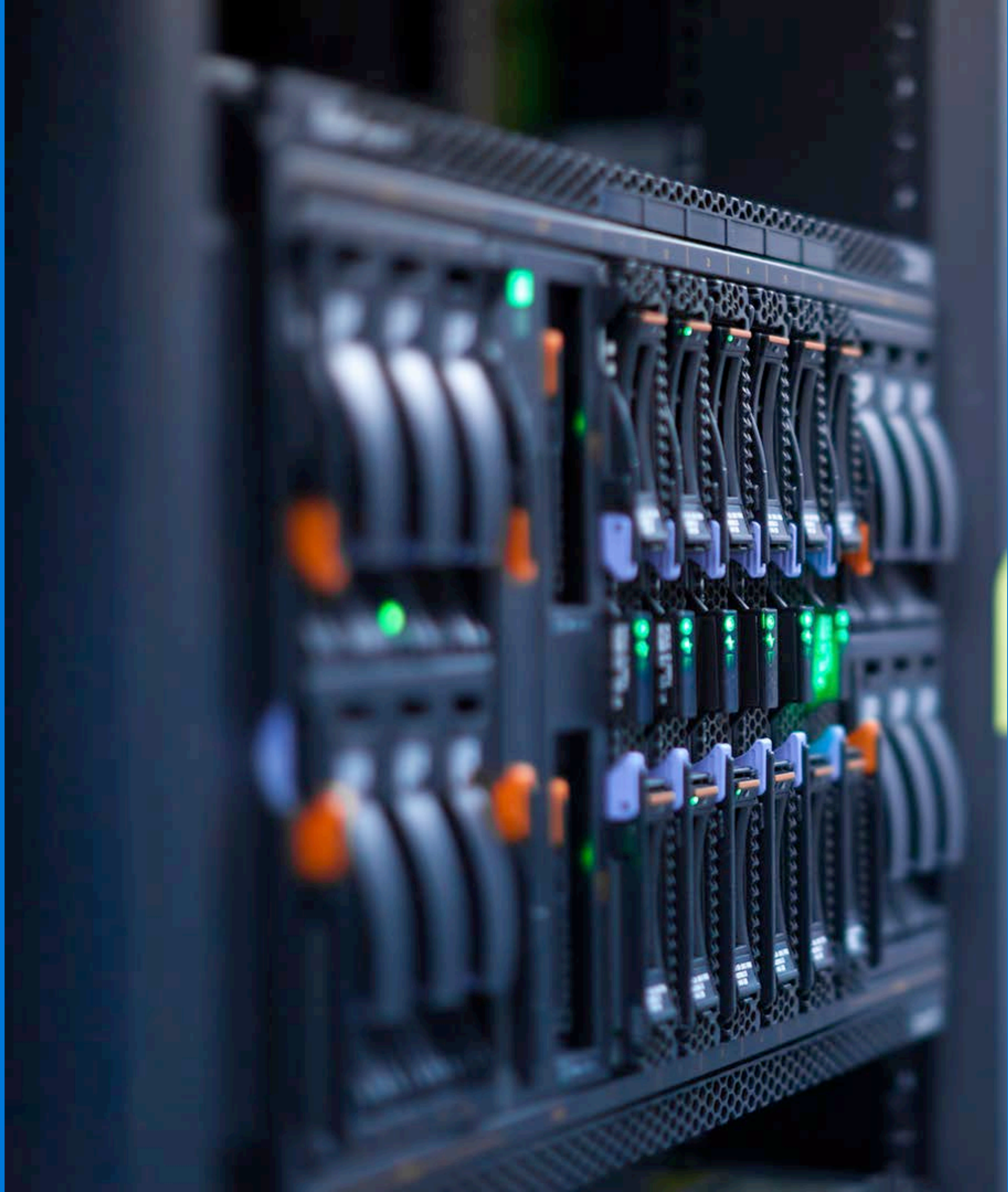


RDS 2016+:

- **4 Role Services**
- **2 VMs**

AAD App Proxy removes external endpoints on RDGW VM so RDCB, RDLic can be combined into one VM since the VM is no longer exposed to the public internet

PowerShell



Microsoft

Easier, faster automation with PowerShell

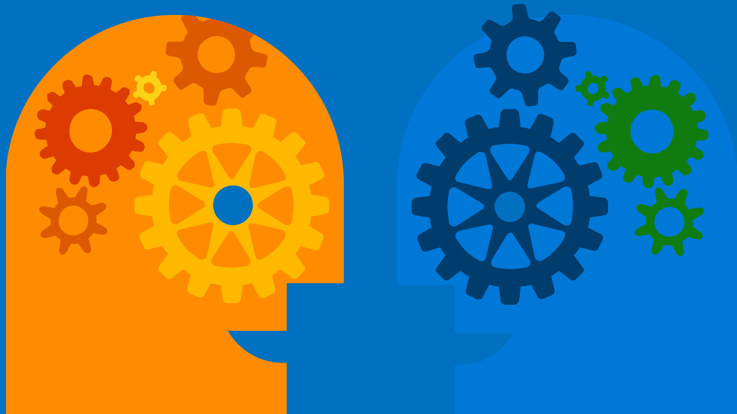
- Code Sharing: PowerShell Gallery, PowerShellGet, Github
- Editing – ISE improvements
- Debugging – Remote debugging, DSC debugging
- Security – Auditing, Just Enough Administration (JEA)
- Improving information
  - Delivering doc updates faster via Github.Com/Powershell
  - Microsoft.com/PowerShell: the hub for PowerShell information

Enabling transition to DevOps

DevOps: a set of practices emphasizing collaboration & communication between SW developers and IT pros while automating software delivery and infrastructure changes. Leverages tools to automate build, validation, & configuration.

PowerShell in Windows Server 2016 Provides

- Desired State Configuration (DSC) – defining configuration as code
- Security Improvements – Auditing, Just Enough Administration (JEA)
- Package Management
- PowerShell classes integrates dev practices configuration and automation
- PowerShell Script Analyzer – best practice analysis tool
- Pester – PowerShell validation



Same approach, everywhere

PowerShell manages your environment

- Gallery contains Dell, Citrix, VMWare, AWS, Azure, SQL cmdlets
- PowerShell DSC runs on Linux

PowerShell is a platform

- Partners include Chef, Puppet, Ansible, Octopus…

PowerShell is on Nano Server

- Nano is managed with PowerShell, configured with DSC

PowerShell 5 ships where you need it

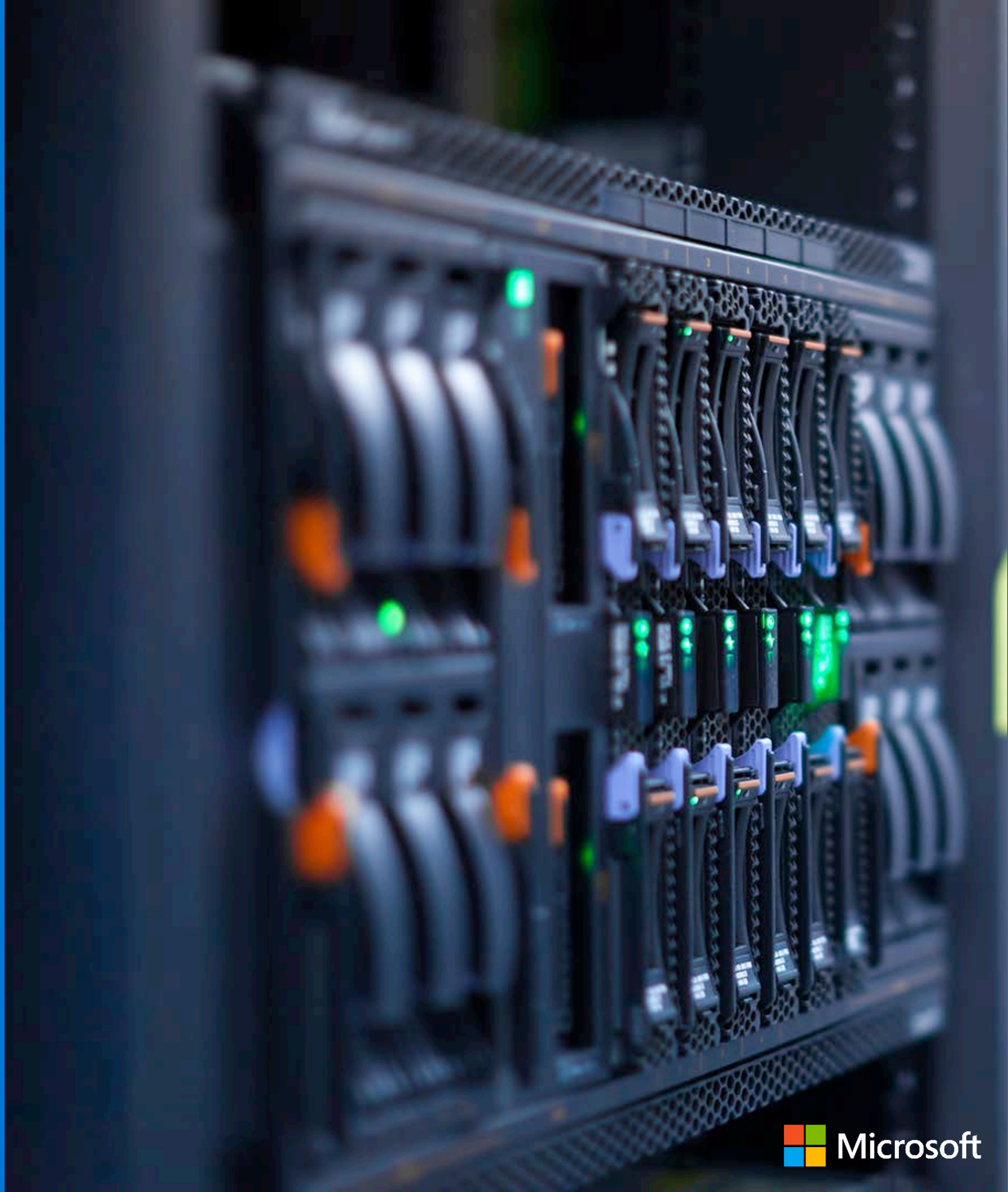
- Windows 10, Windows Server 2016
- WMF5.0 for Win7, Win8.1, Server 2008r2, 2012, 2012r2

PowerShell eases moving the cloud

- Azure PowerShell cmdlets, Azure DSC Extensions

Server Management Tools (SMT)

Microsoft



Microsoft

Overview

Nano Server provides “Just Enough” OS to reduce the security and servicing footprint of the OS, but removes the familiar local GUI that many admins use

Server management tools is a free toolset, hosted in the Azure portal, that ensures that you can manage any Windows Server 2016 instance remotely, alongside PowerShell or your other management tools

Deployment is as simple as installing a software gateway in your infrastructure, then adding machines into the Azure portal

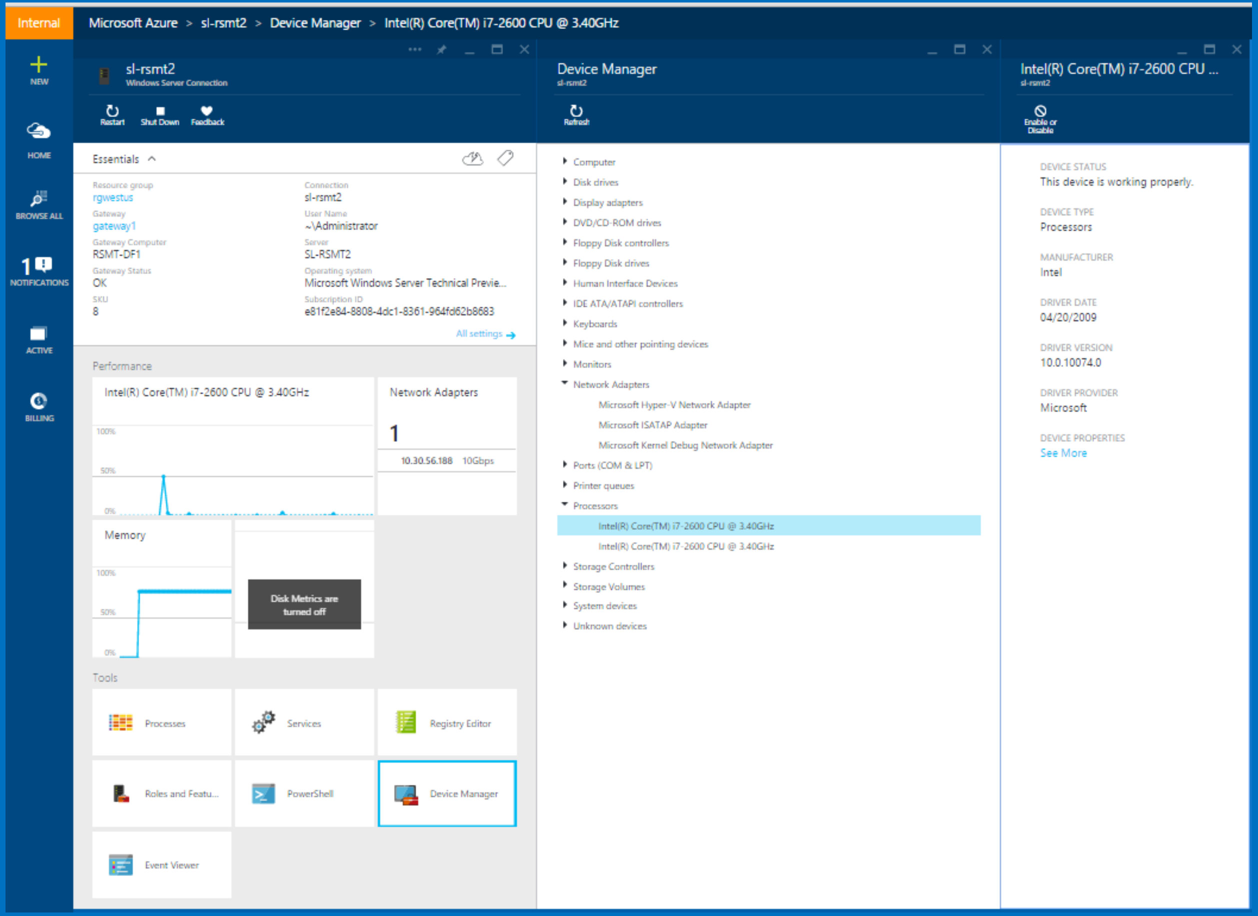
Remote Server management tools

Web-based and cross-platform

Includes replacements for local-only tools, including:

- Task Manager
- Registry Editor
- Event Viewer
- Device Manager
- Sconfig
- Control Panel
- Performance Monitor
- Disk Management
- Users/Groups Manager
- File Explorer

Also manages Server Core and Server with GUI



Microsoft Azure > sl-rsmt2 > Device Manager > Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz

sl-rsmt2
Windows Server Connection

Essentials

Resource group: rgwestus
Gateway: gateway1
Gateway Computer: RSMT-DF1
Gateway Status: OK
SKU: 8

Connection: sl-rsmt2
User Name: ~\Administrator
Server: SL-RSMT2
Operating system: Microsoft Windows Server Technical Previe...
Subscription ID: e81f2e84-8808-4dc1-8361-964fd62b8683

Performance

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

Network Adapters: 1
10.30.56.188 10Gbps

Memory

Disk Metrics are turned off

Device Manager
sl-rsmt2

- Computer
- Disk drives
- Display adapters
- DVD/CD-ROM drives
- Floppy Disk controllers
- Floppy Disk drives
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- Mice and other pointing devices
- Monitors
- Network Adapters
  - Microsoft Hyper-V Network Adapter
  - Microsoft ISATAP Adapter
  - Microsoft Kernel Debug Network Adapter
- Ports (COM & LPT)
- Printer queues
- Processors
  - Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz
  - Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz
- Storage Controllers
- Storage Volumes
- System devices
- Unknown devices

Intel(R) Core(TM) i7-2600 CPU ...
sl-rsmt2

DEVICE STATUS
This device is working properly.

DEVICE TYPE
Processors

MANUFACTURER
Intel

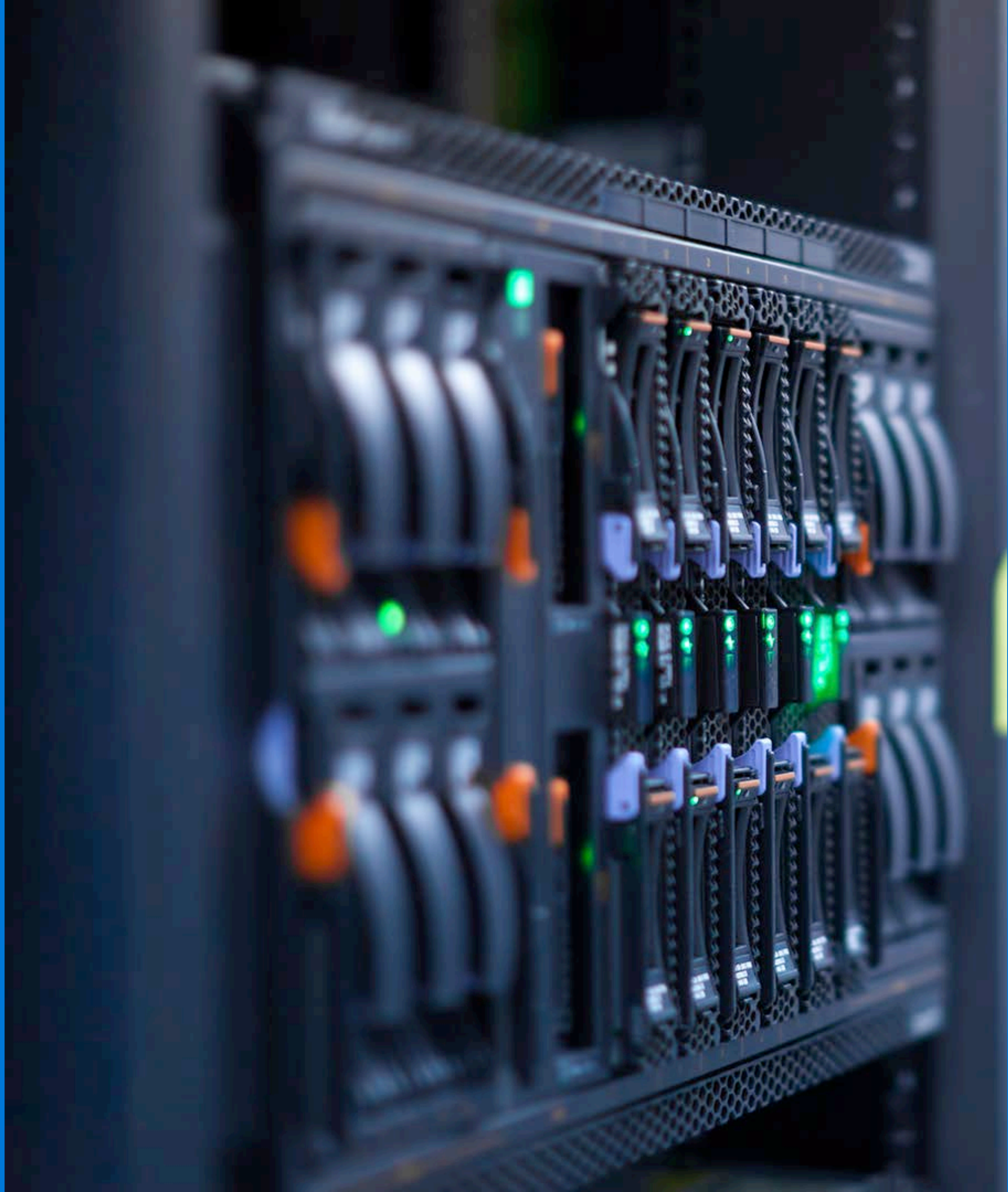
DRIVER DATE
04/20/2009

DRIVER VERSION
10.0.10074.0

DRIVER PROVIDER
Microsoft

DEVICE PROPERTIES
See More

There is more..



Microsoft

Optimize workload availability and performance

Resilience to transient storage/network failures

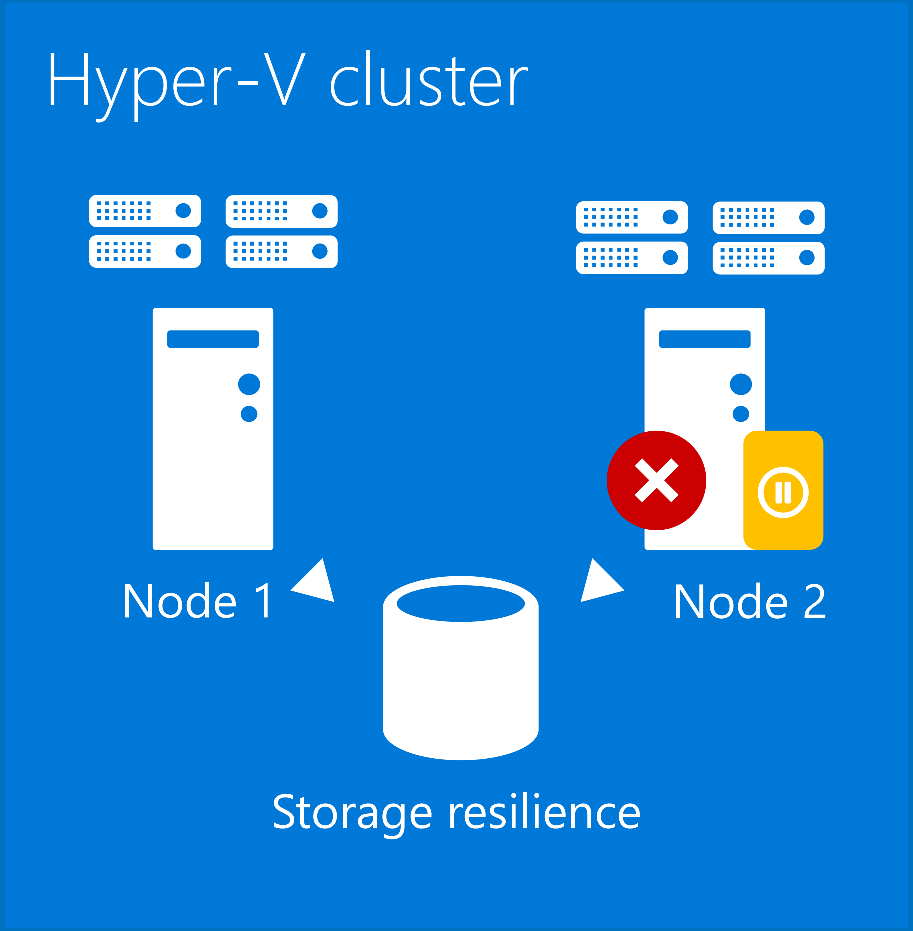
Designed for cloud-scale environments, this helps preserve VM session state in the event of transient storage or network disruptions

Guest cluster availability enhancements

Online resizing, host-level backups, and Hyper-V Replica support

Effectively control workload performance with built-in Storage QoS

Simple out-of-the-box behavior that mitigates “noisy neighbor” issues. Highly customizable via policy, deliver granular performance guarantees on a per-VM or per-tenant basis. Fully automated via System Center/PowerShell



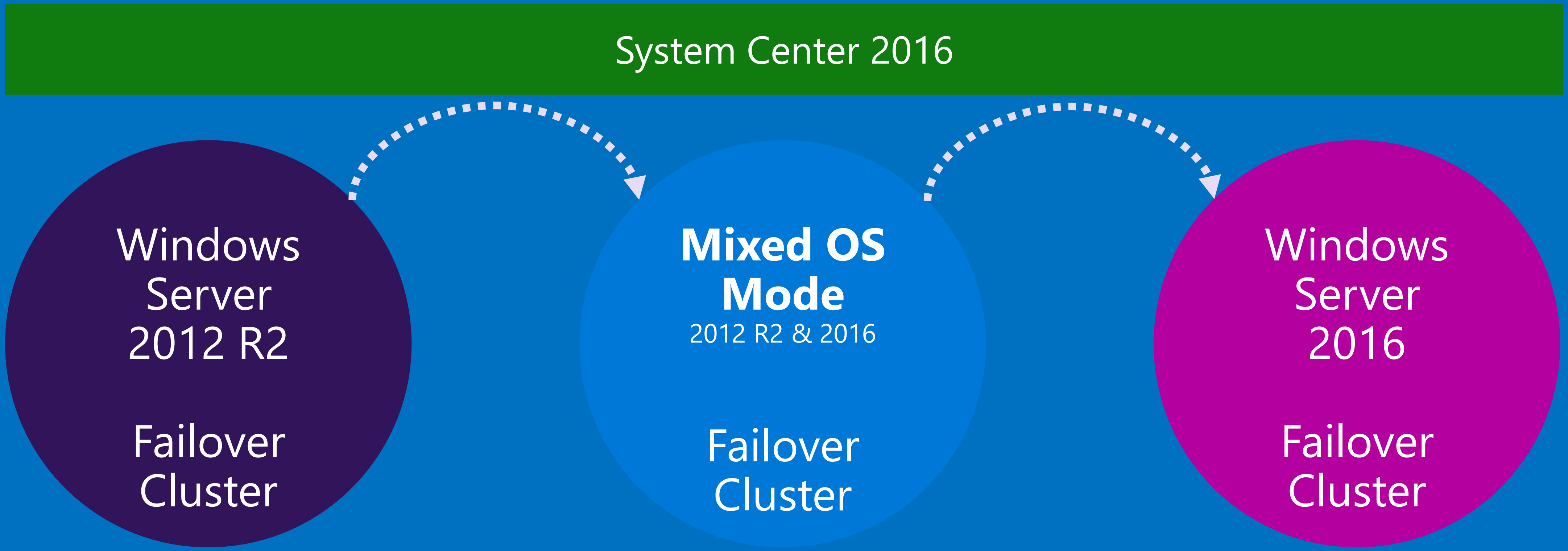
Cluster OS rolling upgrade

Mixed OS mode is a new transition state for Failover Clusters

Optimizations don’t run

New features are not available

Do not plan on running your cluster in Mixed OS Mode for longer than one month



Best-in-class Linux support on Hyper-V

Spotlight capabilities

Broad support: Run Red Hat, SUSE, OpenSUSE, CentOS, Ubuntu, Debian and Oracle Linux, with full support

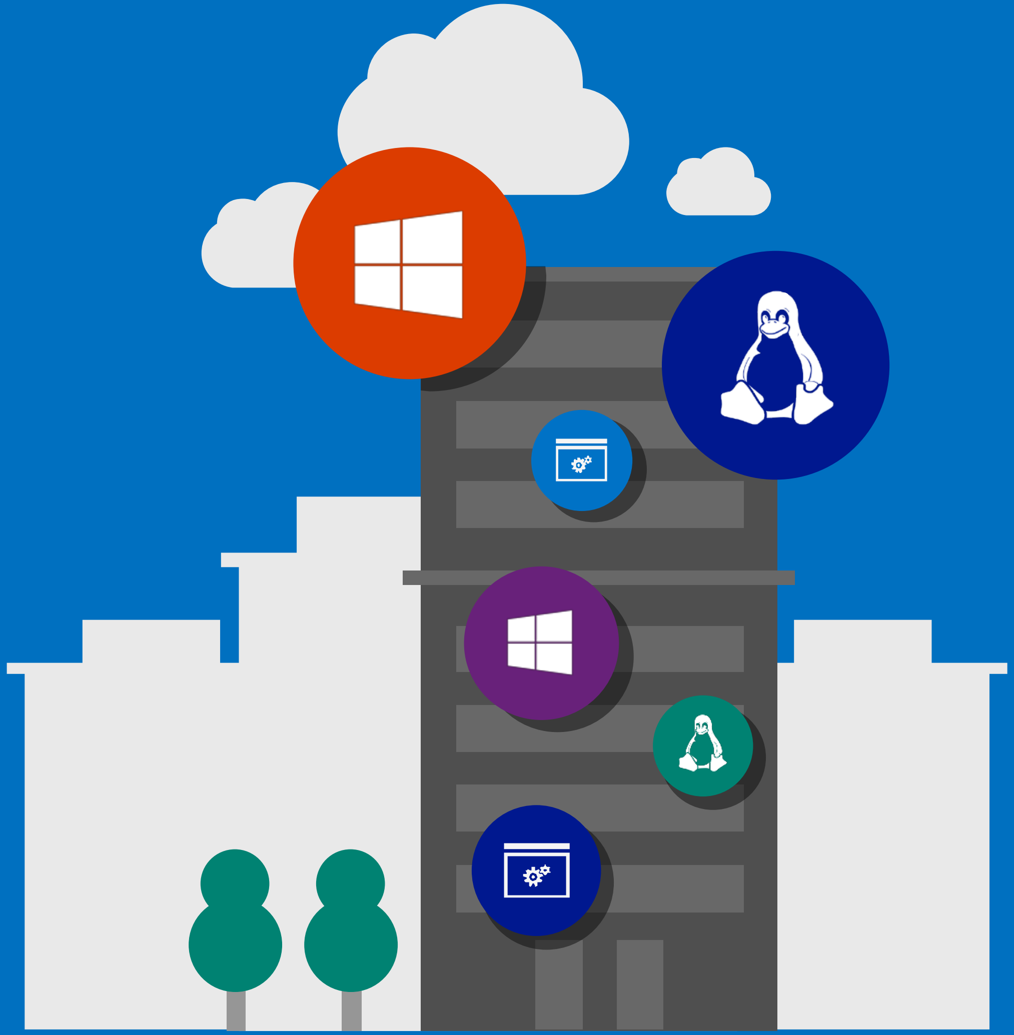
Increased utilization: Run Windows and Linux side-by-side, driving up utilization and reducing hardware costs

Enhanced networking: Highest levels of networking performance in Linux guests with virtual Receive Side Scaling (vRSS) support

Storage enhancements: Hot-add and online-resize of storage for enhanced administration flexibility

Better protection: Better-than-physical backup support for virtualized Linux guests on Hyper-V

Simplified management: Single experience for managing, monitoring, and operating the infrastructure



In box Azure MFA

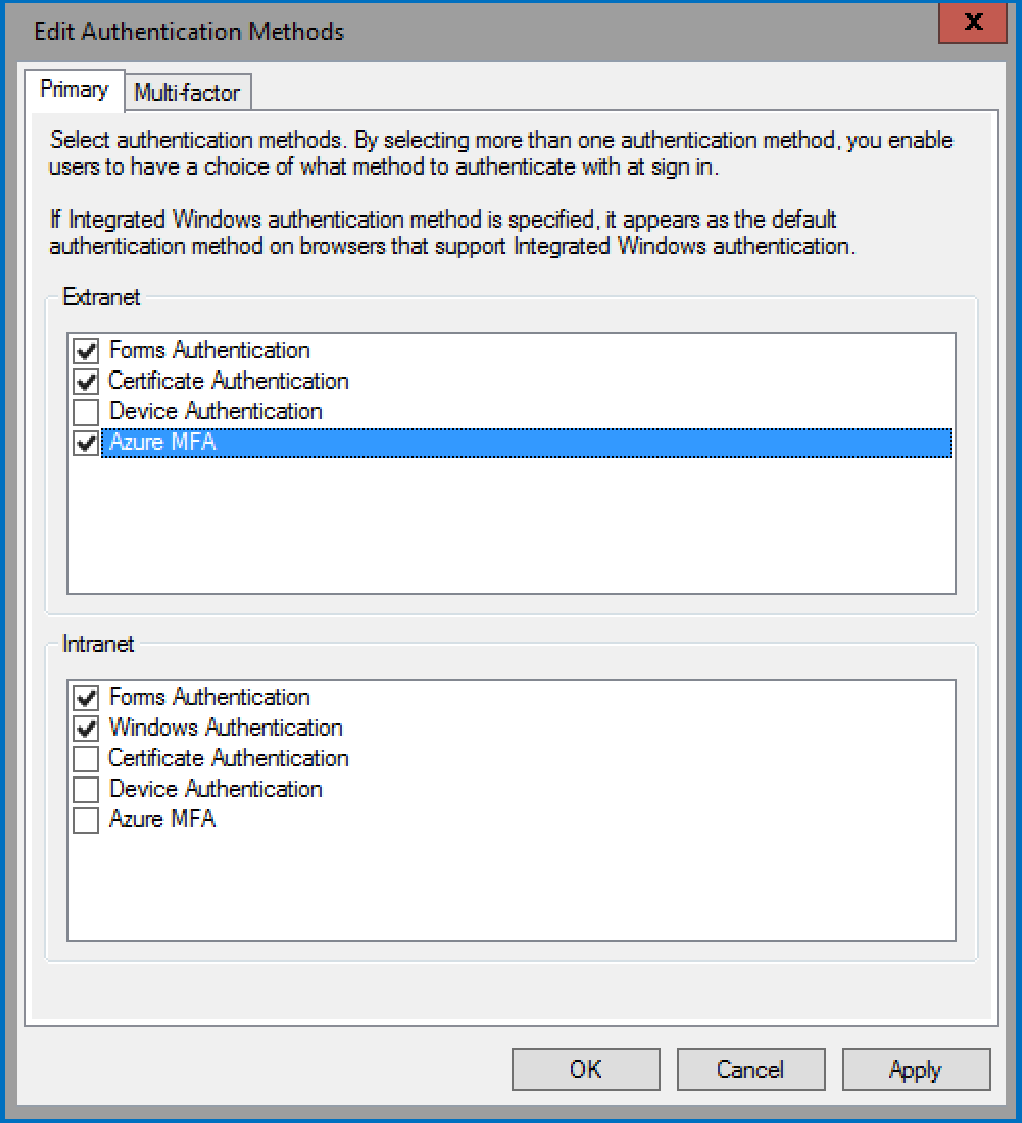
No on-premises MFA server needed

Use as primary or additional authentication method

Configure AD FS farm via PSH

- Then enable Azure MFA in AD FS policy (like you would with other providers)

Users must proof up in AAD/O365 (no inline proofing in the AD FS user experience)



Edit Authentication Methods

Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.

If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.

Extranet

- ☑ Forms Authentication
- ☑ Certificate Authentication
- □ Device Authentication
- ☑ Azure MFA

Intranet

- ☑ Forms Authentication
- ☑ Windows Authentication
- □ Certificate Authentication
- □ Device Authentication
- □ Azure MFA

New in Windows Server 2016

Compute

Industry-standard servers

- Nested virtualization
- PowerShell support for VM upgrade / versioning
- Node fairness for better resource utilization
- Shared VHDX integration

Networking

Physical network

- Network controller, including a high availability mode
- East-West load balancing
- Virtual Machine Multi-Queue to enable 10G+ performance
- Containter specific networking

Storage

Industry-standard disks

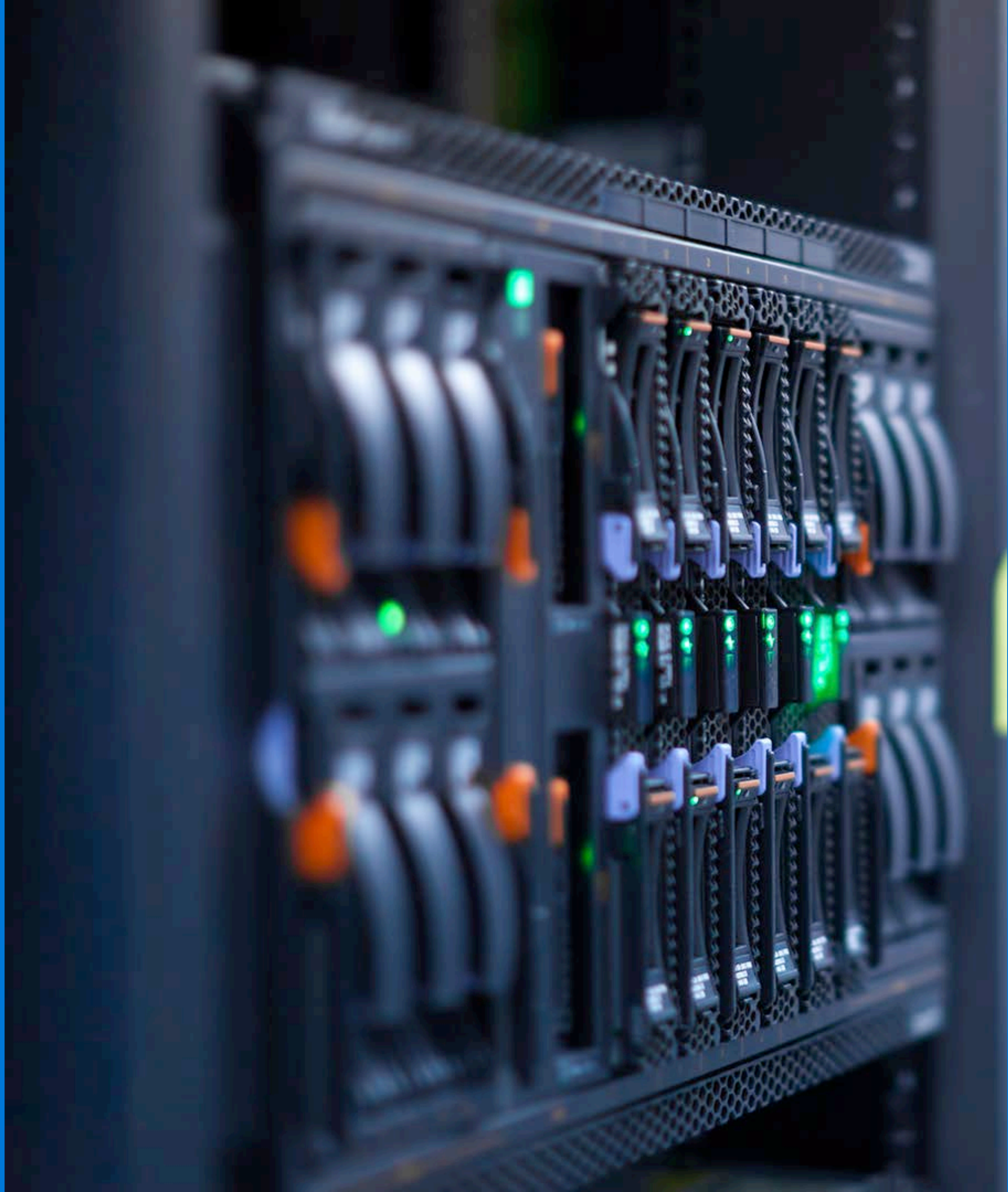
- Hyper-converged option using Storage Spaces Direct for increasing efficiency
- Storage Health Service with a single monitoring point per cluster
- Increased flexibility with maximum bandwidth settings for a VHD/X using storage QoS

Security

TPM-enabled hardware

- Shielded VMs
- Just Enough Administration and Just In Time administration for separation of roles on all systems

System center 2016



Microsoft

Managing mobile devices and PCs

Configuration Manager with Intune

- ✓ Inventory and asset management
- ✓ Compliance and settings management
- ✓ Patch management
- ✓ Flexible OS deployment
- ✓ Client health and monitoring
- ✓ Device management
- ✓ Datacenter management improvements

WHAT'S NEXT

Windows 10 support

- OS deployment support
- ConfigMgr 2012/R2 compatibility
- App policy management
- MDM enrollment with Azure AD
- Access restriction based on device enrollment and policy

Update/upgrade improvements

- In-place upgrade - 2012 SP1 and 2012 R2
- New "add-on" capabilities

Infrastructure

- Increased scale per primary site
- Extend peer caching for WinPE
- Content distribution improvements
- Client deployment update status monitoring

Manage Windows 10 devices via MDM with on-premises infrastructure

- Updates via Intune
- Customer data not stored in cloud

Enable employees to work anywhere on the devices that they choose

Multiple Devices

Protect Information

Integrated Identity

Simplified Administration

Provisioning: Private cloud & virtual datacenters

Virtual Machine Manager

- ✓ Template driven infrastructure
- ✓ Simplified provisioning & migration
- ✓ Multi-cloud management of Azure and AWS VMs
- ✓ Hyper-V and VMware management
- ✓ Virtual storage and network management
- ✓ Partner extensible solution for capacity optimization and billing

WHAT'S NEXT

Ease of Use

- Simplified Networking
- Unified experience for cluster creation
- Easier cluster upgrades with rolling upgrade
- Improved Failover Cluster consistency
- Improved diff disk features

Security and Infrastructure

- Shielded VM management
- Guarded host management
- Improved resiliency during intermittent faults for cluster availability

Expanded Fabric Management

- Enhanced SOFS management
- Azure Site Recovery integration with Storage Replica and SAN replication
- Storage QoS policy management
- Manage Port ACLs
- CDN support for guests
- Deploy and manage SDN at scale
- Nano Server management

Enables enterprise operations teams to virtualize applications simplifying datacenter and cloud management

Improved Efficiency | High Availability | Tenant Security | Cloud API Integration

Monitor and troubleshoot across environments

Operations Manager

- ✓ Infrastructure and application
- ✓ Custom log correlation & analytics
- ✓ Heterogeneous operating systems
- ✓ Flexible management packs
- ✓ Alerting and notifications
- ✓ Cloud monitoring including Azure, O365 and AWS
- ✓ Ecosystem of Partners

WHAT'S NEXT

Workload Monitoring

- Azure MP
- 0365 MP, SQL MP, Exchange MP
- VMM

Windows Server vNext

- Nano Server, Windows storage, SMI-S support

Infrastructure

- Feature updates on UR Cadence
- In-place upgrade from 2012R2
- LAMP Stack monitoring
- Networking performance (L2-L3)
- Discoverability : MP Catalog
- Scheduled Maintenance Mode
- Performance Updates
- Enhanced Data Visualization

Log Analytics

- Custom log correlation
- Search and reporting
- Security & audit collection
- Mobile Access

OM Partner Program

- Install Trial Software via OM Console

Powerful monitoring solution for the worlds most complex environments

IT Service Reliability

Speeds Troubleshooting

Enterprise Scale

Extensible Platform

Automate deployments and orchestrate any cloud

Orchestrator
Service
Management
Automation

- ✓ Automate On-Premises & Cloud
- ✓ Workflow & DSC
- ✓ Graphical & PowerShell authoring
- ✓ Integrate across systems
- ✓ Windows & Linux

WHAT'S NEXT

Hybrid Runbook Worker
- Install on-premises or any cloud
- No inbound open ports required
- Highly available architecture

PowerShell DSC
- Pull service to support large scale
- Supports on-premises or any cloud
- Management / Reporting

Linux Support
- Native SSH module
- Linux support for DSC

Gallery
- Native automation assets (Runbooks, PS Scripts, Assets, Modules, DSC)
- Automation Packs (Grouping of Assets)

Graphical Authoring
- Author processes visually that span systems
- Forms based authoring using databus

Migration to cloud
- SCO Integration Packs
- Runbooks

Role Based Access Control

Speed IT by automating the repetitive tasks and business processes across your environments

Increase productivity

Programmatic Workflow

Enable DevOps

Scalable Engine

Protection with backup

Data Protection Manager

- ✓ Physical, Virtual, Hybrid, Cloud
- ✓ Workload aware backup
- ✓ Deduplication support
- ✓ SCOM Centralized Reporting
- ✓ Long term retention of data in Azure
- ✓ Backup and Recovery for Azure
- ✓ Backup Windows and Linux VMs

WHAT'S NEXT

Azure IaaS, PaaS and workload backup

Centralized management from Azure

Recover data anywhere

Azure Express Route support

Shielded VM

Storage spaces direct

Nano Server

Mixed mode cluster upgrade

Workload aware backup for hybrid clouds

Secure

Reliable

Efficient

Simple