The rationale behind cloud computing

Cloud computing is transforming business by offering new options for businesses to increase efficiencies while reducing costs. What is driving organizations to embrace the cloud paradigm are the problems often associated with traditional IT systems. These problems include:

− High operational costs, typically associated with implementing and managing desktop and server infrastructures

− Low system utilization, often associated with non-virtualized server workloads in enterprise environments

− Inconsistent availability due to the high cost of providing hardware redundancy

− Poor agility, which makes it difficult for businesses to meet evolving market demands.

Although virtualization has helped enterprises address some of these issues by virtualizing server workloads, desktops, and applications, some challenges still remain.

For example, mere virtualization of server workloads can lead to virtual machine (VM) sprawl, solving one problem while creating another.

Cloud computing helps address these challenges by providing businesses with new ways of improving agility while reducing costs. For example, by providing tools for rapid deployment of IT services with self-service capabilities, businesses can achieve a faster time-to-market rate and become more competitive. Cloud-based solutions also can help businesses respond more easily to spikes in demand. And the standardized architecture and service-oriented approach to solution development used in cloud environments helps shorten the solution development life cycle, reducing the time between envisioning and deployment.

Cloud computing also helps businesses keep IT costs under control in several ways. For example, the standardized architecture of cloud solutions provides greater transparency and predictability for the budgeting process. Adding automation and elastic capacity management to this helps keep operational costs lower. Reuse and re-provisioning of cloud applications and services can help lower development costs across your organization, making your development cycle more cost effective. And a pay-as-you-go approach to

consuming cloud services can help your business achieve greater flexibility and become more innovative, making entry into new markets possible.

Cloud computing also can help businesses increase customer satisfaction by enabling solutions that have greater responsiveness to customer needs. Decoupling applications from physical infrastructure improves availability and makes it easier to ensure business continuity when a disaster happens. And risk can be managed more systematically and effectively to meet regulatory requirements.

Making the transition

Making the transition from a traditional IT infrastructure to the cloud paradigm begins with rethinking and re-envisioning what IT is all about. The traditional approach to IT infrastructure is a server-centric vision, where IT is responsible for procuring, designing, deploying, managing, maintaining, and troubleshooting servers hosted on the company's premises or located at the organization's central datacenter. Virtualization can increase the efficiency of this approach by allowing consolidation of server workloads to increase system utilization and reduce cost, but even a virtualized datacenter still has a server-centric infrastructure that requires a high degree of management overhead.

Common characteristics of traditional IT infrastructures, whether virtualized or not, can include the following:

- Limited capacity due to the physical limitations of host hardware in the datacenter (virtualization helps maximize capacity but doesn't remove these limitations).
- Availability level that is limited by budget because of the high cost of redundant host hardware, network connectivity, and storage resources.
- Poor agility because it takes time to deploy and configure new workloads (virtualization helps speed up this process).
- Poor efficiency because applications are deployed in silos, which means that development efforts can't be used easily across the organization.
- Potentially high cost due to the cost of host hardware, software licensing, and the in-house IT expertise needed to manage the infrastructure.

By contrast to the traditional server-centric infrastructure, cloud computing represents a service-centric approach to IT. From the business customer's point of view, cloud services can be perceived as IT services with unlimited capacity,

continuous availability, improved agility, greater efficiency, and lower and more predictable costs than a traditional server-centric IT infrastructure. The results of the service-centric model of computing can be increased productivity with less overhead because users can work from anywhere, using any capable device, without having to worry about deploying the applications they need to do their job.

The bottom line here is that businesses considering making the transition to the cloud need to rethink their understanding of IT from two perspectives: the type of sourcing and the kinds of services being consumed.

Cloud sourcing models

Cloud sourcing models define the party that has control over how the cloud services are architected, controlled, and provisioned. The three kinds of sourcing models for cloud computing are:

– **Public cloud**. Business customers consume the services they need from a pool of cloud services delivered over the Internet. A public cloud is a shared cloud where the pool of services is used by multiple customers, with each customer's environment isolated from those of others. The public cloud approach provides the benefits of predictable costs and pay-as-you-go flexibility for adding or removing processing, storage, and network capacity depending on the customer's needs.

For example, Microsoft Windows Azure and Microsoft SQL Azure are public cloud offerings that allow you to develop, deploy, and run your business applications over the Internet instead of hosting them locally on your own datacenter. By adopting this approach, you can gain increased flexibility, easier scalability, and greater agility for your business. And if your users only need Microsoft Office or Microsoft Dynamics CRM to perform their jobs, you can purchase subscriptions to Office 365 or Microsoft Dynamics CRM Online from Microsoft's public cloud offerings in this area as well.

– **Private cloud**. The customer controls the cloud, either by self-hosting a private cloud in the customer's datacenter or by having a partner host it. A private cloud can be implemented in two ways: by combining different software platforms and applications, or by procuring a dedicated cloud environment in the form of an appliance from a vendor.

For example, customers have already been using the Hyper-V virtualization capabilities successfully in the Microsoft Windows Server 2008 R2 platform, with the Microsoft System Center family of products, to design, deploy, and manage their own private clouds. And for a more packaged approach to deploying private clouds, Microsoft's Private Cloud Fast Track program provides customers with a standard reference architecture for building private clouds that combines Microsoft software, consolidated guidance, value-added software components, and validated compute, network, and storage configurations from original equipment manufacturer (OEM) partners to create a turnkey approach for deploying scalable, preconfigured, validated infrastructure platforms for deploying your own on private cloud. For more information on the Private Cloud Fast Track and to see a list of Fast Track Partners, see http://www.micr0s0ft.c0m/en-us/server-cl0ud/private-cl0ud/buy.aspx#tabs-2.

The private cloud approach allows you the peace of mind of knowing you have complete control over your IT infrastructure, but it has higher up-front costs and a steeper implementation curve than the public cloud approach. For more information on Microsoft's private cloud offerings, see http://www.microsoft.com/en-us/ server-cloud/private-cloud/. As you will soon see, however, the next generation of Hyper-V in the Windows Server 2012 platform delivers even more powerful capabilities that enable customers to deploy and manage private clouds.

− **Hybrid cloud**. The customer uses a combination of private and public clouds to meet the specific needs of their business. In this approach, some of your organization's IT services run on-premises while other services are hosted in the cloud to save costs, simplify scalability, and increase agility. Organizations that want to make the transition from traditional IT to cloud computing often begin by embracing the hybrid cloud approach because it allows them to get their feet wet while remaining grounded in the comfort of their existing server-centric infrastructure.

One difficulty with the hybrid cloud approach, however, is the management overhead associated with needing duplicate sets of IT controls, one set for traditional infrastructure and others for each kind of cloud service consumed. Regardless of this, many organizations that transition to the cloud choose to adopt the hybrid approach for various reasons, including deployment restrictions, compliance issues, or the availability of cloud services that can meet the organization's needs.

Cloud service models

Cloud computing also can be considered from the perspective of which kinds of services are being consumed. The three standard service models for cloud computing are as follows:

− **Software as a service (SaaS).** This approach involves using the cloud to deliver a single application to multiple users, regardless of their location or the kind of device they are using. SaaS contrasts with the more traditional approach of deploying separate instances of applications to each user's computing device. The advantages of the SaaS model is that application activities can be managed from a single central location to reduce cost and management overhead. SaaS typically is used to deliver cloud-based applications that have minimal support for customization, such as email, Customer Relationship Management (CRM), and productivity software. Office 365 is an example of a SaaS offering from Microsoft that provides users with secure anywhere access to their email, shared calendars, instant messaging (IM), video conferencing, and tools for document collaboration.

− **Platform as a service (PaaS).** This approach involves using the cloud to deliver application execution services such as application run time, storage, and integration for applications that have been designed for a prespecified cloud-based architectural framework. By using PaaS, you can develop custom cloud-based applications for your business and then host them in the cloud so that users can access them anywhere over the Internet. PaaS also can be used to create multi-tenant applications that multiple users can access simultaneously. And with its high degree of support for application-level customization, PaaS can enable integration with your older applications and interoperability with your on-premises systems, though some applications may need to be recoded to work in the new environment. SQL Azure is an example of a PaaS offering from Microsoft that allows businesses to provision and deploy SQL databases to the cloud without the need of implementing and maintaining an in-house Microsoft SQL Server infrastructure.

− **Infrastructure as a service (IaaS).** This approach involves creating pools of compute, storage, and network connectivity resources that then can be delivered to business customers as cloud-based services that are billed on a per-usage basis. IaaS forms the foundation for SaaS and PaaS by providing a

standardized, flexible virtualized environment that typically presents itself to the customer as virtualized server workloads. In the IaaS model, the customer can self-provision these virtualized workloads and can customize them fully with the processing, storage, and network resources needed and with the operating system and applications the business requires. By using the IaaS approach, the customer is relieved of the need to purchase and install hardware and can spin up new workloads to meet changing demand quickly. The Hyper-V technology of the Windows Server platform, together with the System Center family of products, represents Microsoft's offering in the IaaS space.

Microsoft cloud facts

Did you know the following facts about Microsoft's public cloud offerings?
− Every day, 9.9 billion messages are transmitted via Windows Live Messenger.
− There are 600 million unique users every month on Windows Live and MSN.
− There are 500 million active Windows Live IDs.
− There are 40 million paid MS online services (BPOS, CRM Online, etc.) in 36 countries.
− A total of 5 petabytes of content is served by Xbox Live each week during the holiday season.
− A total of 1 petabyte+ of updates is served every month by Windows Update to millions of servers and hundreds of millions of PCs worldwide.
− There are tens of thousands of Windows Azure customers.
− There are 5 million LiveMeeting conference minutes per year.
− Forefront for Exchange filters 1 billion emails per month.

Technical requirements for successful cloud computing

If you're considering moving your business to the cloud, it's important to be aware of the ingredients of a successful cloud platform. Figure 1-1 illustrates the three standard service models for implementing private and public cloud solutions.
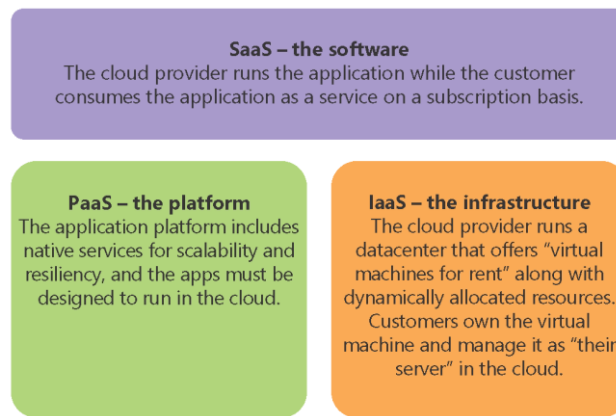
SaaS – the software
The cloud provider runs the application while the customer consumes the application as a service on a subscription basis.

PaaS – the platform
The application platform includes native services for scalability and resiliency, and the apps must be designed to run in the cloud.

IaaS – the infrastructure
The cloud provider runs a datacenter that offers "virtual machines for rent" along with dynamically allocated resources. Customers own the virtual machine and manage it as "their server" in the cloud.

FIGURE 1-1 – The three standard service models for the cloud

The hierarchy of this diagram illustrates that both IaaS and PaaS can be used as the foundation for building SaaS. In the IaaS approach, you build the entire architecture yourself (for example, with load-balanced web servers for the front end and clustered servers for your business and data tiers on the back end). In fact, the only difference between IaaS and a traditional datacenter is that the apps are running on servers that are virtual instead of physical.

By contrast, PaaS is a completely different architecture. In a PaaS solution, like Windows Azure, you allow Azure to handle the "physical" aspect for you when you take your app and move it to the cloud. Then, when you have spikes in demand (think the holiday season for a retail website), the system automatically scales up to meet the demand and then scales back down again when demand tapers off. This means that with PaaS, you don't need to build a system that handles the maximum load at all times, even when it doesn't have to; instead, you pay only for what you use.

But the IaaS model is much closer to what customers currently use today, so let's focus more closely on the IaaS service model, which often is described as "virtual machines for rent." The two key components of IaaS are a hypervisor-based server operating system and a cloud and datacenter management solution. These two components, therefore, form the foundation of any type of cloud solution – public, private, or hybrid.

Let's examine the first component: namely, a hypervisor-based server operating system. What attributes must such a platform have to be suitable for building cloud solutions? The necessary technical requirements must include the following:

- Support for the latest server hardware and scaling features, including high-performance networking capabilities and reduced power consumption for green computing.
- A reliable, highly scalable hypervisor that eliminates downtime when VMs are moved between hosts.
- Fault-tolerant, high-availability solutions that ensure that cloud-based services can be delivered without interruption.
- Powerful automation capabilities that can simplify and speed the provisioning and management of infrastructure resources to make your business more agile.
- Support for enterprise-level storage for running the largest workloads that businesses may need.
- The ability to host a broad range of virtualized operating systems and applications to provide customers with choices that can best meet their business needs
- An extensible platform with public application programming interfaces (APIs) that businesses can use to develop custom tools and enhancements that they need to round out their solutions.
- The ability to pool resources, such as processing, network connectivity, and storage, to provide elasticity so that you can provision and scale resources dynamically in response to changing needs.
- Self-service capabilities, so that pooled resources can be provisioned quickly according to service-level agreements for increased agility.
- A built-in system for monitoring resource usage, so that those consuming resources can be billed on a pay-for-only-what-you-use basis.
- Infrastructure transparency, so that customers can concentrate on deploying the applications and services that they need without having to worry about the underlying infrastructure.

Microsoft's previous hypervisor-based server operating system, Windows Server 2008 R2, met many of these requirements to a high degree, and Microsoft and other enterprises have been using it extensively as a foundation for building both private and public clouds. As we will soon see, however, Windows Server 2012 now brings even more to the table for building highly scalable and elastic cloud solutions, making it the first truly cloud-optimized server operating system.

The second component for building a cloud is the management part, and here, System Center 2012 provides the most comprehensive cloud and

datacenter management solution available in the marketplace. System Center 2012 spans physical, virtual, and cloud environments using common management experiences throughout and enables end-to-end management of your infrastructure and applications.

The business need for Windows Server 2012

Cloud computing in general, and private clouds in particular, have emerged as a response to the high cost and lack of agility of traditional approaches to IT. The needs of IT users and the rate of technological change have increased significantly. At the same time, the need to improve IT efficiency and reduce costs are high-priority objectives in most businesses today.

Server consolidation through virtualization has been a key driver of cost savings over the past several years. Windows Server 2012 and Hyper-V provide significant improvements in scalability and availability, which enables much higher consolidation ratios. Combined with the flexibility of unlimited VM licensing in some Windows SKUs, high-density virtualization can reduce costs significantly. With Windows Server 2012 and Hyper-V supporting clusters up to 64 nodes running up to 4,000 VMs and up to 1,024 active VMs per host, a relatively small amount of physical hardware can support a large amount of IT capability.

Further improving the consolidation story is the ability to run significantly larger VMs, resulting in a higher percentage of physical servers being candidates for virtualization. For example, Windows Server 2012 can now support:

− Up to 64 virtual processors per VM (with a maximum of 2,048 virtual processors per host).
− Up to 1 terabyte (TB) of random access memory (RAM) per VM (with up to 4 TB RAM per host).
− Virtual hard disks (VHDs) up to 64 TB in size.

These scalability enhancements now provide enterprises with the ability to virtualize the vast majority of physical servers deployed today. Examples include large database servers or other high-scale workloads that previously could not be virtualized.

In addition to scale, a substantial number of new capabilities in the Windows Server 2012 and Hyper-V platform enable cloud computing scenarios. Definitions of cloud computing vary; however, one of the most commonly utilized definitions is from the U.S. National Institutes for Standards and Technology

(NIST), which defines five "essential" characteristics of cloud computing solutions, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These attributes enable the agility and cost savings expected from cloud solutions.

Virtualization alone provides significant benefits, but it does not provide all the cloud attributes defined by NIST. A key tenet of Windows Server 2012 is to go beyond virtualization. What this means is providing the foundational technologies and features that enable cloud attributes such as elasticity, resource pooling, and measured service, while providing significant advancements in the virtualization platform.

− For the on-demand self-service cloud attribute, Windows Server 2012 provides foundational technology that enables a variety of user interfaces, including self-service portals by providing hundreds of Windows PowerShell cmdlets related to VM provisioning and management, that enable management solutions such as System Center to provide self-service user interfaces.

− For the broad network access cloud attribute, Windows Server 2012 and Hyper-V provides new network virtualization technology that enables a variety of VM mobility, multi-tenancy, and hosting scenarios that remove many of today's network limitations. Other technologies, such as DirectAccess, enable secure remote connectivity to internal resources without the need for virtual private networks (VPNs).

− For the resource pooling cloud attribute, the combination of the operating system, Network, and Storage virtualization technologies in Windows Server 2012 enable each component of the physical infrastructure to be virtualized and shared as a single large resource pool. Improvements to Live Migration enable VMs and their associated storage to be moved to any Hyper-V host in the datacenter with a network connection. Combined, these technologies allow standardization across the physical and virtual infrastructure with the ability of VMs to be distributed optimally and dynamically across the datacenter.

− For the rapid elasticity cloud attribute, Windows Server 2012 provides the ability to provision VMs rapidly using technologies such as offloaded data transfer (ODX), which can use capabilities in storage systems to clone or create VMs very rapidly to enable workload elasticity. Thin provisioning and data de-duplication enable elasticity without immediate consumption of physical resources.

− For the measured service cloud attribute, Windows Server 2012 provides a variety of new resource metering capabilities that enable granular reporting on resource utilization by individual VMs. Resource metering enables scenarios such as chargeback reporting based on central processing unit (CPU) utilization, memory utilization, or other utilization-based metrics.

In addition to advanced server consolidation and cloud attributes that help drive down IT cost and increase agility, Windows Server 2012 provides the capability to reduce ongoing operational expenses (OpEx) by providing a high degree of automation and the ability to manage many servers as one. A key cost metric in IT is the number of servers that an individual administrator can manage.

In many datacenters, this number is small, typically in the double digits. In highly automated datacenters such as Microsoft's, an individual administrator can manage thousands of servers through the use of automation.

Windows Server 2012 delivers this automation capability through the Server Manager user interface's ability to manage user-defined groups of servers as one, plus the ability of PowerShell to automate activities against a nearly unlimited number of servers. This reduces the amount of administrator effort required, enabling administrators to focus on higher-value activities.

Taken together, the capabilities provided by Windows Server 2012 deliver the essential cloud attributes and the foundation for significant improvements in both IT cost and agility.

Four ways Windows Server 2012 delivers value for cloud computing

Let's now briefly look at four ways that Windows Server 2012 can deliver value for building your cloud solution beyond what the Windows Server 2008 R2 platform can deliver. The remaining chapters of this book will explore the powerful new features and capabilities of this cloud-optimized operating system in more detail, along with hands-on insights from insiders at Microsoft who have developed, tested, and deployed Windows Server 2012 and for select customers during product development.

Foundation for building your private cloud

Although previous versions of Windows Server have included many capabilities needed for implementing different cloud computing scenarios,

Windows Server 2012 takes this a step further by providing a foundation for building dynamic, multi-tenant cloud environments that can scale to meet the highest business needs while helping to reduce your infrastructure costs. Hyper-V in Windows Server 2008 R2 has already helped many businesses reduce their operational costs through server consolidation. The next version of Hyper-V, together with other key features of Windows Server 2012, goes even further by enabling you to secure virtualized services by isolating them effectively, migrate running VMs with no downtime even outside of clusters, create replicas of virtualized workloads for offsite recovery, and much more. The result is to provide a platform that is ideal as a foundation for building private clouds for even the largest enterprises.

Windows Server 2012 provides business with a complete virtualization platform that includes multi-tenant security and isolation capabilities to enforce network isolation between workloads belonging to different business units, departments, or customers on a shared infrastructure. Network Virtualization, a new feature of Hyper-V, lets you isolate network traffic from different business units without the complexity of needing to implement and manage virtual local area networks (VLANs). Network Virtualization also makes it easier to integrate your existing private networks into a new infrastructure by enabling you to migrate VMs while preserving their existing virtual network settings. And network quality of service (QoS) has been enhanced in Windows Server 2012 to enable you to guarantee a minimum amount of bandwidth to VMs and virtual services so that service level agreements can be achieved more effectively and network performance can have greater predictability. Being able to manage and secure network connectivity resources effectively are an important factor when designing cloud solutions, and these capabilities of Windows Server 2012 make this possible.

Windows Server 2012 also helps you scale your environment better, achieve greater performance levels, and use your existing investments in enterprise storage solutions. With greatly expanded support for host processors and memory, your virtualization infrastructure now can support very large VMs that need the highest levels of performance and workloads that require the ability to increase significantly in scale. Businesses that have already invested in Fibre Channel storage arrays for their existing infrastructures can benefit from Virtual Fibre Channel, a new feature of Hyper-V that lets you directly connect to your storage area network (SAN) from within the guest operating system of your VMs.

You also can use Virtual Fibre Channel to virtualize any server workloads that directly access your SAN, enabling new ways of reducing costs through workload virtualization. You also can cluster guest operating systems over Fibre Channel, which provides new infrastructure options you can explore. And the built-in ODX support ensures that your VMs can read and write to SAN storage at performance levels matching that of physical hardware, while freeing up the resources on the system that received the transfer. With storage a key resource for any cloud solution, these improvements make Windows Server 2012 an effective platform for building clouds.
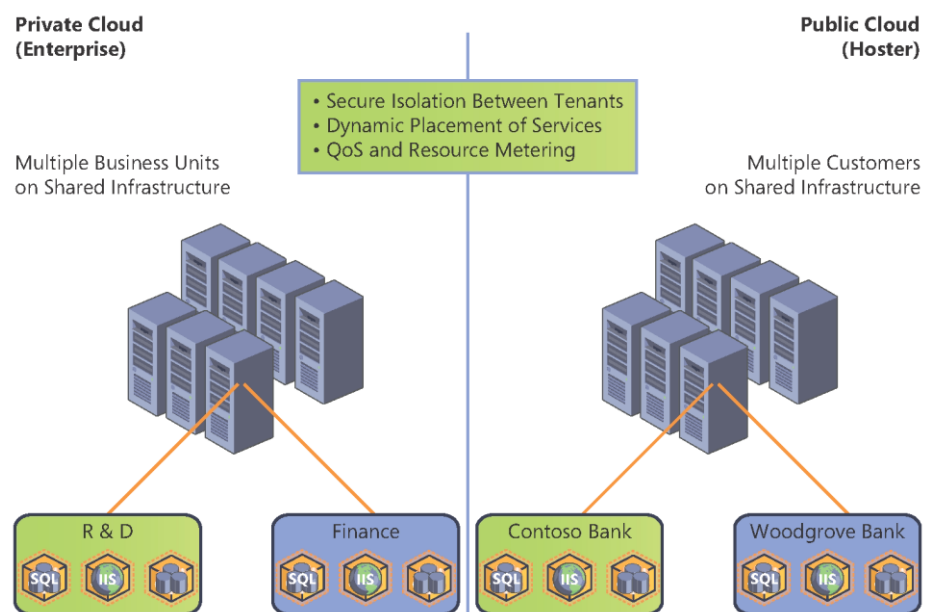
FIGURE 1-2 – Windows Server 2012 provides a foundation for multi-tenant clouds

Windows Server 2012 also provides a common identity and management framework that supports federation, enables cross-premises connectivity, and facilitates data protection. Active Directory Federation Services (AD FS) is now built into the product and provides a foundation for extending Active Directory identities to the cloud, allowing for single sign-on (SSO) to resources both on-premises and in the cloud. Site-to-site VPNs can be established to provide cross-premises connectivity between your on-premises infrastructure and hosting providers you purchase cloud services from. You even can connect directly to private subnets within a hosted cloud network, using your existing networking equipment that uses industry-standard IKEv2-IPsec protocols. And you can enhance business continuity and simplify disaster recovery by using the new

Hyper-V Replica feature that provides asynchronous replication of virtual machines over IP-based networks to remote sites. All these features help provide the foundation that you need to build your private cloud.

Highly available, easy-to-manage multi-server platform

Cost is the bottom line for most businesses, and even though virtualization has allowed many organizations to tap into efficiencies that have helped them do more with less with their datacenters, maintaining these efficiencies and preventing interruptions due to failures, downtimes, and management problems remain a key priority. Windows Server 2012 helps you address these issues by providing enhanced availability features, more flexible storage options, and powerful new management capabilities.

Windows Server 2012 enhances availability by extending the Live Migration capabilities of Hyper-V in previous Windows Server versions with a new feature called Live Storage Migration, which lets you move VHDs while they are attached to running VMs with no downtime. Live Storage Migration simplifies the task of migrating or upgrading storage when you need to perform maintenance on your SAN or file-based storage array, or when you need to redistribute the load. Built-in NIC teaming gives you fault-tolerant networking without the need to use third-party solutions, and it also helps ensure availability by preventing connectivity from being lost when a network adapter fails. And availability can be further enhanced through transparent failover, which lets you move file shares between cluster nodes with no interruption to applications accessing data on these shares. These improvements can provide benefits for both virtualized datacenters and for the cloud.

Windows Server 2012 also provides numerous efficiencies that can help you reduce costs. These efficiencies cover a wide range of areas, including power consumption, networking, and storage, but for now, let's just consider storage. The new file server features of Windows Server 2012 allow you to store application data on server message block (SMB) file shares in a way that provides much of the same kind of availability, reliability, and performance that you've come to expect from more expensive SAN solutions. The new Storage Spaces feature provides built-in storage virtualization capabilities that enable flexible, scalable, and cost-effective solutions to meet your storage needs. And Windows Server 2012 integrates with storage solutions that support thin provisioning with

just-in-time (JIT) allocations of storage and the ability to reclaim storage that's no longer needed. Reducing cost is key for enterprises, whether they still have traditional IT infrastructures or have deployed private clouds.

Windows Server 2012 also includes features that make management and automation more efficient. The new Server Manager takes the pain out of deploying and managing large numbers of servers by simplifying the task of remotely deploying roles and features on both physical and virtual servers. Server Manager also can be used to perform scenario-based deployments of the Remote Desktop Services role, for example to set up a session virtualization infrastructure or a virtual desktop infrastructure (VDI) environment quickly. PowerShell 3.0 has powerful new features that simplify the job of automating numerous aspects of a datacenter, including the operating system, storage, and networking resources. PowerShell workflows let you perform complex management tasks that require machines to be rebooted. Scheduled jobs can run regularly or in response to a specific event. Delegated credentials can be used so that junior administrators can perform mission-critical tasks. All these improvements can bring you closer to running your datacenter or private cloud as a truly lights-out automated environment.

Deploy web applications on-premises and in the cloud

The web platform is key to building a cloud solution. That's because cloud-based services are delivered and consumed over the Internet. Windows Server 2012 includes web platform enhancements that provide the kind of flexibility, scalability, and elasticity that your business needs to host web applications for provisioning cloud-based applications to business units or customers. Windows Server 2012 is also an open web platform that embraces a broad range of industry standards and supports many third-party platforms and tools so that you can choose whatever best suits the development needs for your business.

Because most organizations are expected to follow the hybrid cloud approach that combines together both on-premises infrastructure and cloud services, efficiencies can be gained by using development symmetry that lets you build applications that you can deploy both on-premises and in the cloud. Windows Server 2012 provides such development symmetry through a common programming language supporting both Windows Server and the Windows Azure platform; through a rich collection of applications that can be deployed and used

across web application and data tiers; through the rich Microsoft Visual Studio-based developer experience, which lets you develop code that can run both on-premises and in the cloud; and through other technologies like the Windows Azure Connect, which lets you configure Internet Protocol Security (IPsec)-protected connections between your on-premises physical/virtual servers and roles running in the Windows Azure cloud.

Building on the proven application platform of earlier Windows Server versions, Windows Server 2012 adds new features and enhancements to enable service providers to host large numbers of websites while guaranteeing customers predictable service levels. These improvements make Windows Server 2012 the ideal platform for building and managing hosting environments and public clouds. To enable the highest level of scalability, especially in shared hosting environments, Microsoft Internet Information Services (IIS) 8.0 in Windows Server 2012 introduced multicore scaling on Non-Uniform Memory Access (NUMA), which enables servers that can scale up to 64 physical processors and across NUMA nodes. This capability enables your web applications to scale up quickly to meet sudden spikes in demand. And when demand falls again, IIS CPU throttling enables your applications to scale down to minimize costs. You also can use IIS CPU throttling to ensure that applications always get their fair share of processor time by specifying a maximum CPU usage for each application pool. And to manage the proliferation of Secure Sockets Layer (SSL) certificates for your hosting environment, or to be able to add web servers to a web farm quickly without the need to configure SSL manually on them, the new Centralized SSL Certificate Support feature of Windows Server 2012 takes the headache out of managing SSL-based hosting environments.

IIS 8.0 in Windows Server 2012 also provides businesses with great flexibility in the kinds of web applications that they can develop and deploy. ASP.NET 4.5 now supports the latest HTML 5 standards. PHP and MySQL also are supported through the built-in IIS extensions for these development platforms. And support for the industry-standard WebSocket protocol enables encrypted data transfer over real-time bidirectional channels to support AJAX client applications running in the browser. All these features and enhancements provide flexibility for building highly scalable web applications, hosted either on-premises or in the cloud.

Enabling the modern work style

The consumerization of IT through the trend towards BYOD or "bring your own device" environments is something that businesses everywhere are facing and IT is only beginning to get a handle on. The days of IT having full control over all user devices in their infrastructure are probably over, with the exception of certain high-security environments in the government, military, and finance sectors. Accepting these changes requires not just new thinking but new technology, and Windows Server 2012 brings features that can help IT address this issue by enabling IT to deliver on-premises and cloud-based services to users while maintaining control over sensitive corporate data.

Remote Access has been enhanced in Windows Server 2012 to make it much easier to deploy DirectAccess so that users can always have the experience of being seamlessly connected to the corporate network whenever they have Internet access. Setting up traditional VPN connections is also simpler in Windows Server 2012 for organizations that need to maintain compatibility with existing systems or policies. BranchCache has been enhanced in Windows Server 2012 to make it scale greater, perform better, and be managed more easily. Deploying BranchCache is now much simpler and enables users to run applications remotely and access data more efficiently and securely than before. And as previously mentioned in this chapter, Server Manager now lets you perform scenario-based deployments of the Remote Desktop Services role to implement session virtualization or VDI in your environment more easily.

To remain productive as they roam between locations and use different devices, users need to be able to access their data using the full Windows experience. New features and improvements in Windows Server 2012 now make this possible from any location on almost any device. RemoteFX for WAN enables a rich user experience even over slow WAN connections. Universal serial bus (USB) is now supported for session virtualization, allowing users to use their USB flash drives, smartcards, webcams, and other devices when connecting to session hosts. And VDI now includes user VHDs for storing user personalization settings and cached application data so that the user experience can be maintained across logons.

Windows Server 2012 also gives you greater control over your sensitive corporate data to help you safeguard your business and meet the needs of compliance. Central access policies can be used to define who is allowed to access information within your organization. Central audit policies have been enhanced

to facilitate compliance reporting and forensic analysis. The Windows authorization and audit engine has been re-architected to allow the use of conditional expressions and central policies. Kerberos authentication now supports both user and device claims. And Rights Management Services (RMS) has been made extensible so partners can provide solutions for encrypting non-Office files. All these improvements enable users to connect securely to on-premises or cloud-based infrastructure so that they can be more productive in ways that meet the challenges of today's work style while maintaining strict control over your corporate data.

Windows Server 2012: The foundation for building your private cloud

Delivering a solid foundation for a private cloud requires a robust virtualization platform, scalability with great performance, and the ability to span datacenters and integrate with other clouds. Windows Server 2012 was designed to address key private cloud needs through advances in computer, storage, and Network Virtualization.

Compute virtualization, provided by Hyper-V in Windows Server 2012, has been improved to support significantly larger host servers and guest virtual machines (VMs). This increases the range of workloads that can be virtualized. A new feature called Guest NUMA enables large virtual machines with many virtual CPUs (vCPUs) to achieve high performance by optimizing a VM's vCPU mappings to the underlying physical server's Non-Uniform Memory Access (NUMA) configuration. Large increases in Hyper-V scalability and Dynamic Memory provide for much higher density of VMs per server with larger clusters. VM mobility through Live Migration and live storage migration, regardless of whether the VM is hosted on a cluster, enable a number of new scenarios for optimization of resources in private cloud scenarios.

Windows Server 2012 delivers new Network Virtualization capability as well as private virtual local area networks (VLANs), opening a number of new networking scenarios, including multi-tenant options required for hosting and private cloud scenarios. These technologies enable a tenant to utilize their own IP addressing schemes, even if it overlaps with other tenants, while maintaining separation and security. Windows Server 2012 also introduces a new extensible virtual switch. The extensible switch delivers new capabilities such as port profiles

and is a platform that third parties can use to build switch extensions for tasks like traffic monitoring, intrusion detection, and network policy enforcement. In both private cloud scenarios and hosting scenarios, secure multi-tenancy is often a requirement. Examples could include separating the finance department's resources from the engineering department's resources or separating one company's resource you are hosting from another's. Windows Server 2012 networking technologies provide for shared infrastructure and resource pooling while enabling secure multi-tenancy.

Storage virtualization is a major investment area in Windows Server 2012. Storage Spaces, SMB 3, Cluster Shared Volumes (CSV2), and several other new storage features provide a high-performance, low-cost storage platform. This storage platform allows Hyper-V VMs to be run from Windows Server 2012 continuously available file shares on Windows storage spaces. Such shares can be accessed using the new SMB 3 protocol, which when combined with appropriate network hardware, provides high-speed, low-latency, multichannel-capable storage access. These technologies provide a robust storage platform at a cost point much lower than was previously possible. For environments with significant existing investments in storage area network (SAN) technology, Windows Server 2012 now enables Fibre Channel host bus adapters (HBAs) to be virtualized, allowing VMs direct access to Fibre Channel-based SAN storage.

Another critical component of a private cloud infrastructure is disaster recovery capability. Windows Server 2012 introduces the Hyper-V Replica feature, which allows VMs to be replicated to disaster recovery sites, which reduces the time required to restore service should a primary datacenter suffer a disaster.

With the large number of new features and improvements, automation becomes a critical requirement, both for consistency of deployment and for efficiency in operations. Windows Server 2012 includes about 2,400 new Windows PowerShell cmdlets for managing the various roles and features in the platform. Windows PowerShell can be used either directly or through Microsoft and third-party management systems to automate deployment, configuration, and operations tasks. The new Server Manager in Windows Server 2012 allows multiple servers to be grouped and managed as one. The objective of these improvements is to increase administrator efficiency by increasing the number of servers each administrator can manage.

The range of technology delivered in Windows Server 2012 can be used in a variety of ways to enable private cloud scenarios. For a large, centralized

enterprise, large-scale file and Hyper-V clusters can deliver a platform able to run thousands or tens of thousands of highly available VMs. For cases where secure multi-tenancy is required, Network Virtualization and private VLANs can be used to deliver secure and isolated networks for each tenant's VMs. With continuously available file shares for storing VMs combined with Live Migration and Live Storage Migration, VMs can be moved anywhere in the datacenter with no downtime.

The compute, network, and storage virtualization provided by Windows Server 2012 deliver resource pooling, elasticity, and measured service cloud attributes. These capabilities are further improved by disaster recovery and automation technologies. With these and other features, Windows Server 2012 delivers the foundation for the private cloud.

A complete virtualization platform

Virtualization can bring many benefits for businesses, including increased agility, greater flexibility, and improved cost efficiency. Combining virtualization with the infrastructure and tools needed to provision cloud applications and services brings even greater benefits for organizations that need to adapt and scale their infrastructure to meet the changing demands of today's business environment. With its numerous improvements, Hyper-V in Windows Server 2012 provides the foundation for building private clouds that can use the benefits of cloud computing across the business units and geographical locations that typically make up today's enterprises. By using Windows Server 2012, you can begin transitioning your organization's datacenter environment toward an infrastructure as a service (IaaS) private cloud that can provide your business units with the "server instances on demand" capability that they need to be able to grow and respond to changing market conditions.

Hosting providers also can use Windows Server 2012 to build multi-tenant cloud infrastructures (both public and shared private clouds) that they can use to deliver cloud-based applications and services to customers. Features and tools included in Windows Server 2012 enable hosting providers to fully isolate customer networks from one another, deliver support for service level agreements (SLAs), and enable chargebacks for implementing usage-based customer billing.

Let's dig into these features and capabilities in more detail. We'll also get some insider perspective from experts working at Microsoft who have developed, tested, deployed, and supported Windows Server 2012 during the early stages of the product release cycle.

Scenario-focused design in Windows Server 2012

One of the best things about Windows Server 2012 is that it was designed from the ground up, with a great focus on actual customer scenarios. Windows Server is the result of a large engineering effort, and in past releases, each organization delivered its own technology innovations and roadmap in its respectively relevant area. The networking team would build great networking features; the storage team would innovate on file and storage systems; the manageability team would introduce Windows PowerShell to enable a standard way to manage servers, and so on.

Windows Server 2012 is different. Instead of having vertical technology-focused roadmaps and designs, it was built around specific customer scenarios for the server. I was the scenario leader for the "hosted cloud" scenario, which was all about building the most cloud-optimized operating system ever built and aligning multiple feature crews on enabling enterprises and hosting providers to build clouds that are better than ever.

Scenario-focused design starts by understanding the business need and the real customer pain points and requirements. During the planning phase, we talked to a very long list of customers and did not limit ourselves to any specific technology. Instead, we have framed the discussion around the need to build and run clouds and discovered pain points, such as the need to offer secure multi-tenancy and isolation to your cloud tenants, so that hosting providers can be more efficient in utilizing their infrastructure and lowering their cost. There's also a need to be able to automate manual processes end to end because manual processes just don't cut it anymore, and the need to lower the cost of storage because customers were clearly overpaying for very expensive storage even when they don't really need it. We then translated that understanding into investments that cross technology boundaries that will solve those business problems and satisfy the customer requirements.

For example, to enable multi-tenancy, we didn't just add some access control lists (ACLs) on the Hyper-V switch. Instead, we've built a much better

Hyper-V switch with isolation policy support and added Network Virtualization to decouple the physical cloud infrastructure from the VM networks. Then we added quality of service (QoS) policies to help hosting providers ensure proper SLAs for different tenants and resource meters to enable them to measure and charge for activities, and we also ensured that everything will be fully automatable (via Windows PowerShell, of course), in a consistent way.

Here's another example: we didn't just add support for a new network interface card (NIC) technology called **Remote Direct Memory Access** (RDMA). Instead, we've designed it to work well with file servers and provide SMB Direct support to enable the use of file servers in a cloud infrastructure over standard Ethernet fabric, and used storage spaces for low-cost disks. This way, competitive performance compared to SANs is made available at a fraction of the cost.

Finally, scenario-focused design doesn't actually end at the design phase. It's a way of thinking that starts at planning but continues all the way through execution, internal validation, external validation with our TAP program, partner relations, documentation, blogging, and, of course, bringing the product to market. Basically, at every stage of the Windows Server 2012 execution cycle, the focus was on making the scenario work, rather than on making specific features work.

This kind of a scenario-focused requires an amazingly huge collaborative effort across technology teams. This is exactly where Windows Server 2012 shines and is the reason you're seeing all of these great innovations coming together in one massive release that will change the way clouds are built.

Hyper-V extensible switch

The new Hyper-V extensible switch in Windows Server 2012 is key to enabling the creation of secure cloud environments that support the isolation of multiple tenants. The Hyper-V extensible switch in Windows Server 2012 introduces a number of new and enhanced capabilities for tenant isolation, traffic shaping, protection against malicious virtual machines, and hassle-free troubleshooting. The extensible switch allows third parties to develop plug-in extensions to emulate the full capabilities of hardware-based switches and support more complex virtual environments and solutions.

Previous versions of Hyper-V allowed you to implement complex virtual network environments by creating virtual network switches that worked like

physical layer-2 Ethernet switches. You could create external virtual networks to provide VMs with connectivity with externally located servers and clients, internal networks to allow VMs on the same host to communicate with each other as well as the host, or private virtual networks (PVLANs) that you can use to completely isolate all VMs on the same host from each other and allow them to communicate only via external networks.

The Hyper-V extensible switch facilitates the creation of virtual networks that can be implemented in various ways to provide great flexibility in how you can design your virtualized infrastructure. For example, you can configure a guest operating system within a VM to have a single virtual network adapter associated with a specific extensible switch or multiple virtual network adapters (each associated with a different switch), but you can't connect the same switch to multiple network adapters.

What's new however is that the Hyper-V virtual switch is now extensible in a couple of different ways. First, you can now install custom Network Driver Interface Specification (NDIS) filter drivers (called extensions) into the driver stack of the virtual switch. For example, you could create an extension that captures, filters, or forwards packets to extensible switch ports. Specifically, the extensible switch allows for using the following kinds of extensions:

- Capturing extensions, which can capture packets to monitor network traffic but cannot modify or drop packets.
- Filtering extensions, which are like capturing extensions but also can inspect and drop packets.
- Forwarding extensions, which allow you to modify packet routing and enable integration with your physical network infrastructure.

Second, you can use the capabilities of the Windows Filtering Platform (WFP) by using the built-in Wfplwfs.sys filtering extension to intercept packets as they travel along the data path of the extensible switch. You might use this approach, for example, to perform packet inspection within your virtualized environment.

These different extensibility capabilities of the Hyper-V extensible switch are intended primarily for Microsoft partners and independent software vendors (ISVs) so they can update their existing network monitoring, management, and security software products so they can work not just with physical hosts, but also with VMs deployed within any kind of virtual networking environment that you might possibly create using Hyper-V in Windows Server 2012. In addition, being

able to extend the functionality of the Hyper-V networking by adding extensions makes it easier to add new networking functionality to Hyper-V without needing to replace or upgrade the switch. You'll also be able to use the same tools for managing these extensions that you use for managing other aspects of Hyper-V networking, namely the Hyper-V Manager console, Windows PowerShell, and Windows Management Instrumentation (WMI). And because these extensions integrate into the existing framework of Hyper-V networking, they automatically work with other capabilities, like Live Migration.

Table 2-1 summarizes some of the benefits of the Hyper-V extensible switch from both the IT professional and ISV perspective.

TABLE 2-1 – Benefits of the Hyper-V extensible switch

Key Tenets	Benefit to ISVS	Benefit to IT Professionals
Open platform w/public API	Write only the functionalities desired	Minimal footprint for errors
First-class citizen of system	Free system services (e.g., Live Migration)	Extensions from various ISVs work together
Existing API model	Faster development	Larger pool of extension implemented
Logo certification and rich framework	Higher customer satisfaction	Higher extension quality
Unified Tracing thru virtual switch	Lower support costs	Shorter downtimes

Configuring virtual switches

Figure 2-1 shows the Windows Filtering Platform (WPF) extension selected in the Virtual Switch Manager of the Hyper-V Console in Windows Server 2012. Note that once extensions are installed on the host, they can be enabled or disabled and also have their order rearranged by moving them up or down in the list of switch extensions.
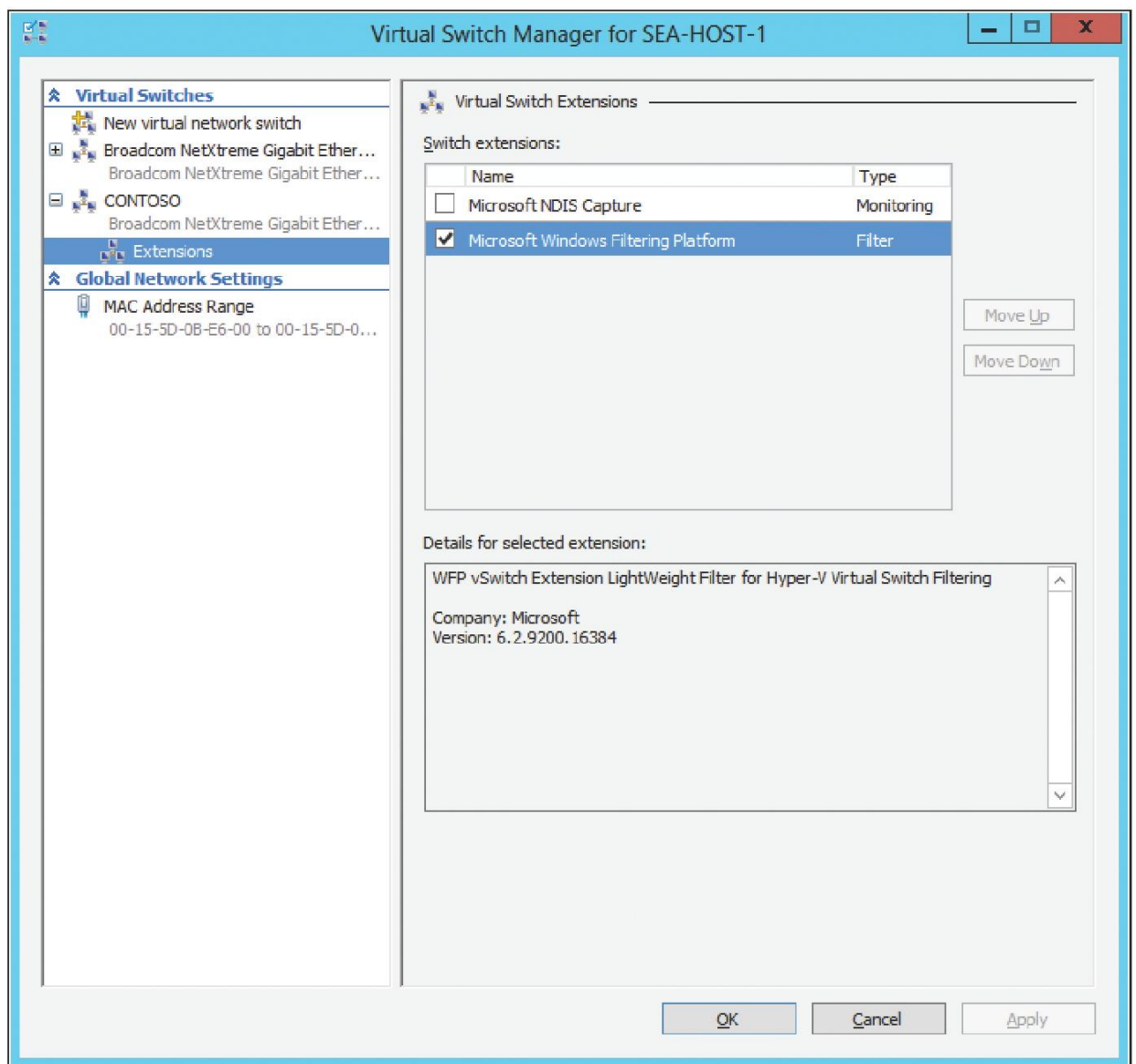
FIGURE 2-1 – Virtual switch extensions for the Hyper-V extensible switch.

You can also use Windows PowerShell to create, delete, and configure extensible switches on Hyper-V hosts. For example, Figure 2-2 shows how to use the Get-VMSwitchExtension cmdlet to display details concerning the extensions installed on a specific switch.

FIGURE 2-2 – Displaying all extensions installed on the virtual switch named
CONTOSO

You also can display the full list of Windows PowerShell cmdlets for
managing the extensible switch, as Figure 2-3 illustrates.

FIGURE 2-3 – Displaying all Windows PowerShell cmdlets for managing virtual
switches.

Troubleshooting virtual switches

Microsoft also has extended Unified Tracing through the Hyper-V extensible
switch, which makes it easier for you to diagnose problems that may occur. For

example, if you are experiencing issues that you think might be connected with the extensible switch, you could attempt to troubleshoot the problem by turning on tracing using the Netsh command like this:

```
netsh trace start provider=Microsoft-Windows-Hyper-V-VmSwitch capture=yes
capturetype=vmswitch
```

Then you would try and reproduce the issue while tracing is turned on. Once a repro has occurred, you could disable tracing with netsh trace stop and then review the generated Event Trace Log (ETL) file using Event Viewer or Network Monitor. You also could review the System event log for any relevant events.

Additional capabilities

A number of other advanced capabilities also have been integrated by Microsoft into the Hyper-V extensible switch to help enhance security, monitoring, and troubleshooting functionality. These additional capabilities include the following:

− **DHCP guard**. Helps safeguard against Dynamic Host Configuration Protocol (DHCP) man-in-the-middle attacks by dropping DHCP server messages from unauthorized VMs pretending to be DHCP servers.

− **MAC address spoofing**. Helps safeguard against attempts to use ARP spoofing to steal IP addresses from VMs by allowing VMs to change the source MAC address in outgoing packets to an address that is not assigned to them.

− **Router guard**. Helps safeguard against unauthorized routers by dropping router advertisement and redirection messages from unauthorized VMs pretending to be routers.

− **Port mirroring**. Enables monitoring of a VM's network traffic by forwarding copies of destination or source packets to another VM being used for monitoring purposes.

− **Port ACLs**. Helps enforce virtual network isolation by allowing traffic filtering based on media access control (MAC) or IP address ranges.

− **Isolated VLANs**. Allows segregation of traffic on multiple VLANs to facilitate isolation of tenant networks through the creation of private VLANs (PVLANs).

− **Trunk mode**. Allows directing traffic from a group of VLANs to a specific VM.

- **Bandwidth management**. Allows guaranteeing a minimum amount of bandwidth and/or enforcing a maximum amount of bandwidth for each VM.
- **Enhanced diagnostics**. Allows packet monitoring and event tracing through the extensible switch using ETL and Unified Tracing.

Most of these additional capabilities can be configured from the graphical user interface (GUI) by opening the VM's settings. For example, by selecting the network adapter under Hardware, you can specify bandwidth management settings for the VM. Figure 2-4 shows these settings configured in such a way that the VM always has at least 50 MBps of network bandwidth available, but never more than 100 MBps. If your hosts reside in a shared cloud being used to provision applications and services to business units or customers, these new bandwidth management capabilities can provide the benefit of helping you meet your SLAs with these business units or customers.
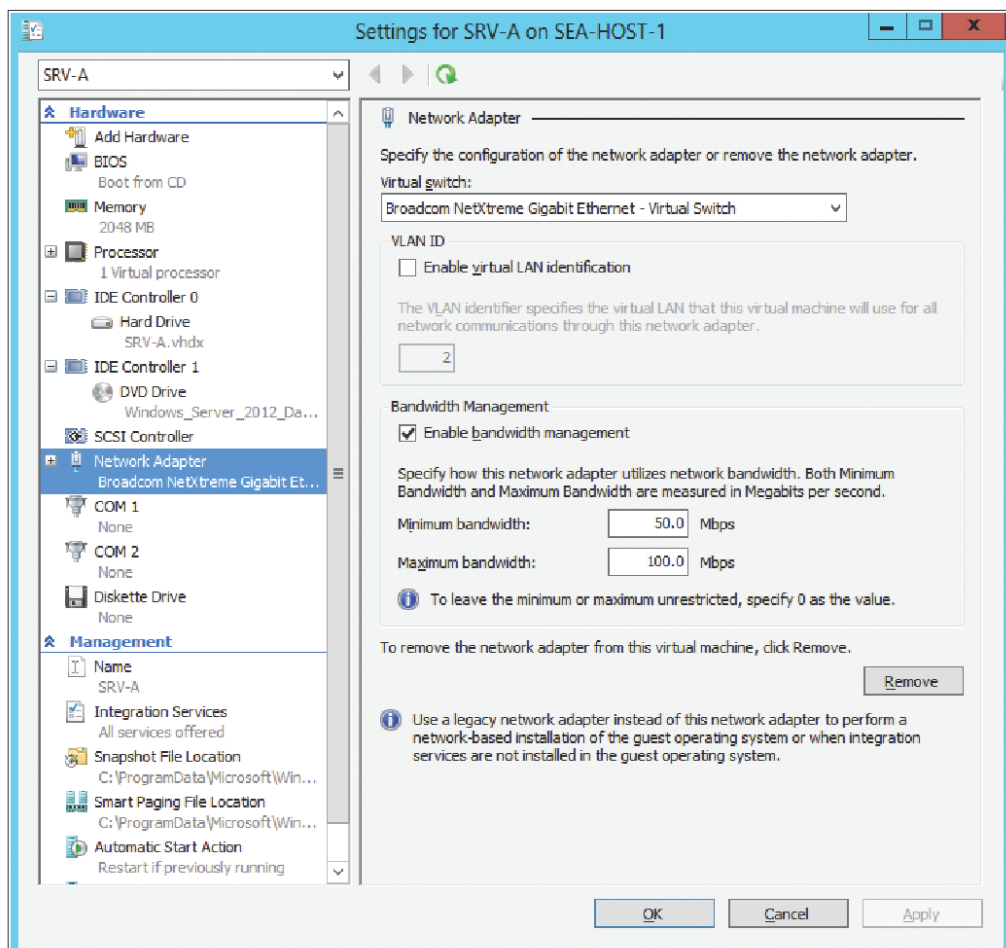

FIGURE 2-4 – Minimum and maximum bandwidth settings have been configured for this VM

Clicking the plus sign (+) beside Network Adapter in these settings exposes two new pages of network settings: Hardware Acceleration and Advanced Features. We'll examine the Hardware Acceleration settings later in this chapter, but for now, here are the Advanced Features settings which lets you configure MAC address spoofing, DHCP guard, router guard, port mirroring and NIC teaming for the selected network adapter of the VM, as shown in Figure 2-5.

As the sidebar demonstrates, you also can use Windows PowerShell to configure and manage the various advanced capabilities of the Hyper-V extensible switch.
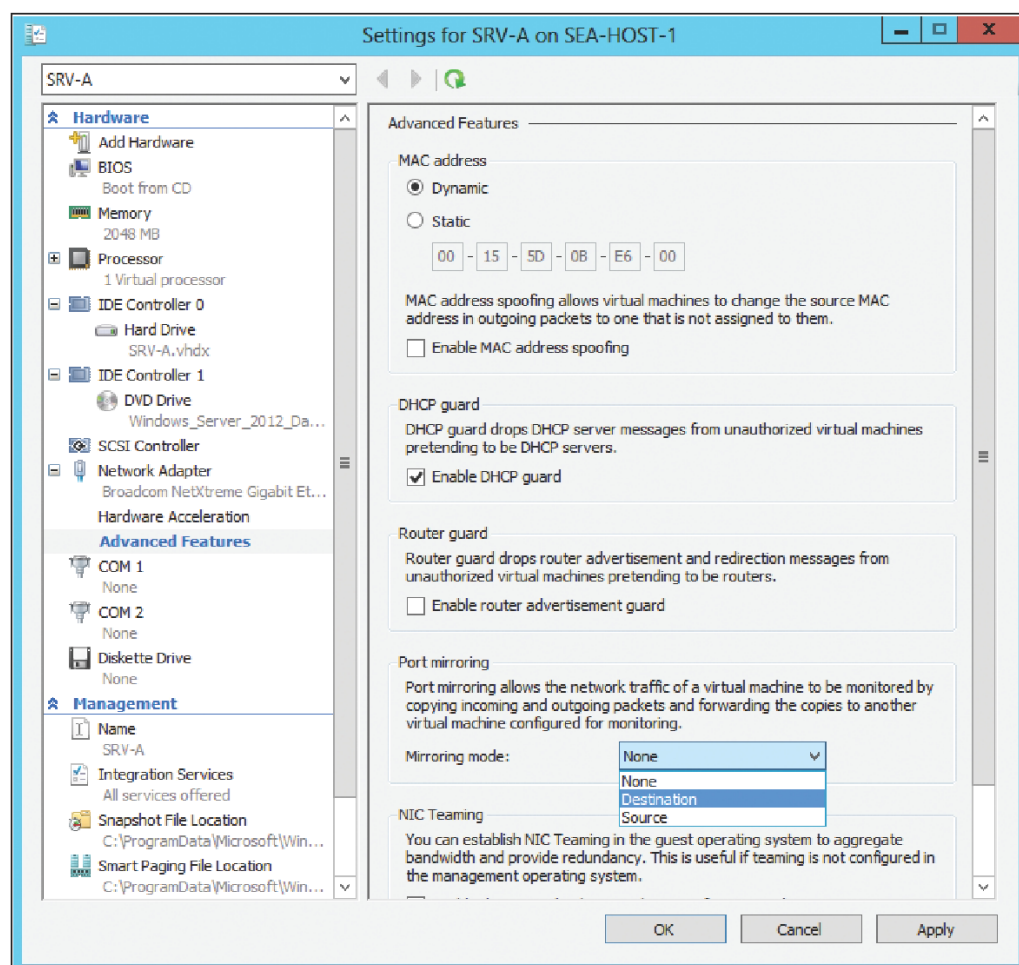

Figure 2-5 – Configuring advanced features for network adapter settings for a VM

Using Windows PowerShell to configure the extensible switch

Let's briefly look at two scenarios where Windows PowerShell can be used to configurevarious features of the extensible network switch.

Scenario 1: Enabling advanced networking features

In an upgrade scenario, you want to take advantage of advanced networking features of the extensible network switch. Namely, you want to enable the following on all VMs on a Hyper-V host:
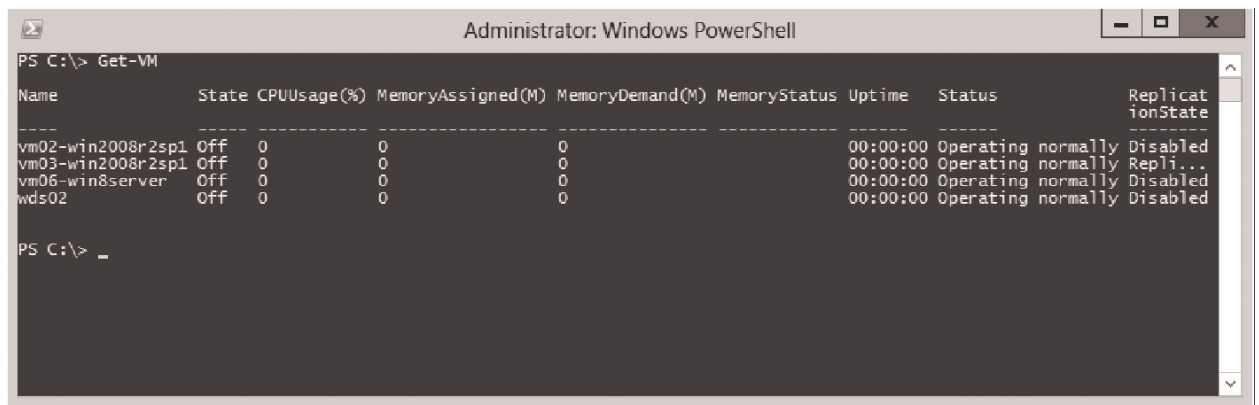
− DHCP Guard.

− Enable router advertisement guard.

− Enable Virtual Machine Queue (VMQ).

Here's what a VM looks like without any of the advanced networking features enabled:
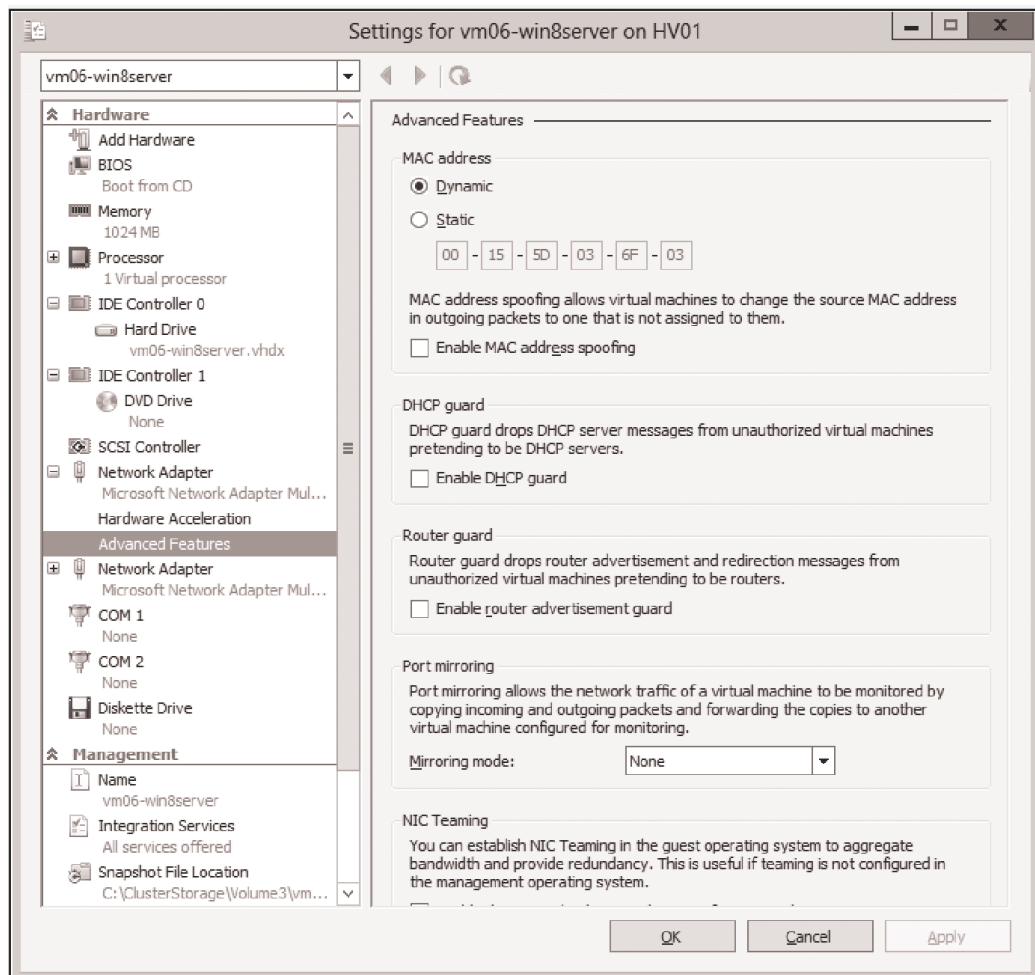
Now let's do this on a Hyper-V host on every single VM on the Hyper-V host.

First, let's list all the VMs by issuing the Get-VM cmdlet:

```
                          Administrator: Windows PowerShell                    [_][□][ X ]
PS C:\> Get-VM

Name              State CPUUsage(%) MemoryAssigned(M) MemoryDemand(M) MemoryStatus Uptime   Status             Replicat
                                                                                                                ionState
----              ----- ----------- ----------------- --------------- ------------ ------   ------             --------
vm02-win2008r2sp1 Off   0           0                 0                            00:00:00 Operating normally Disabled
vm03-win2008r2sp1 Off   0           0                 0                            00:00:00 Operating normally Repli...
vm06-win8server   Off   0           0                 0                            00:00:00 Operating normally Disabled
wds02             Off   0           0                 0                            00:00:00 Operating normally Disabled


PS C:\> _
```
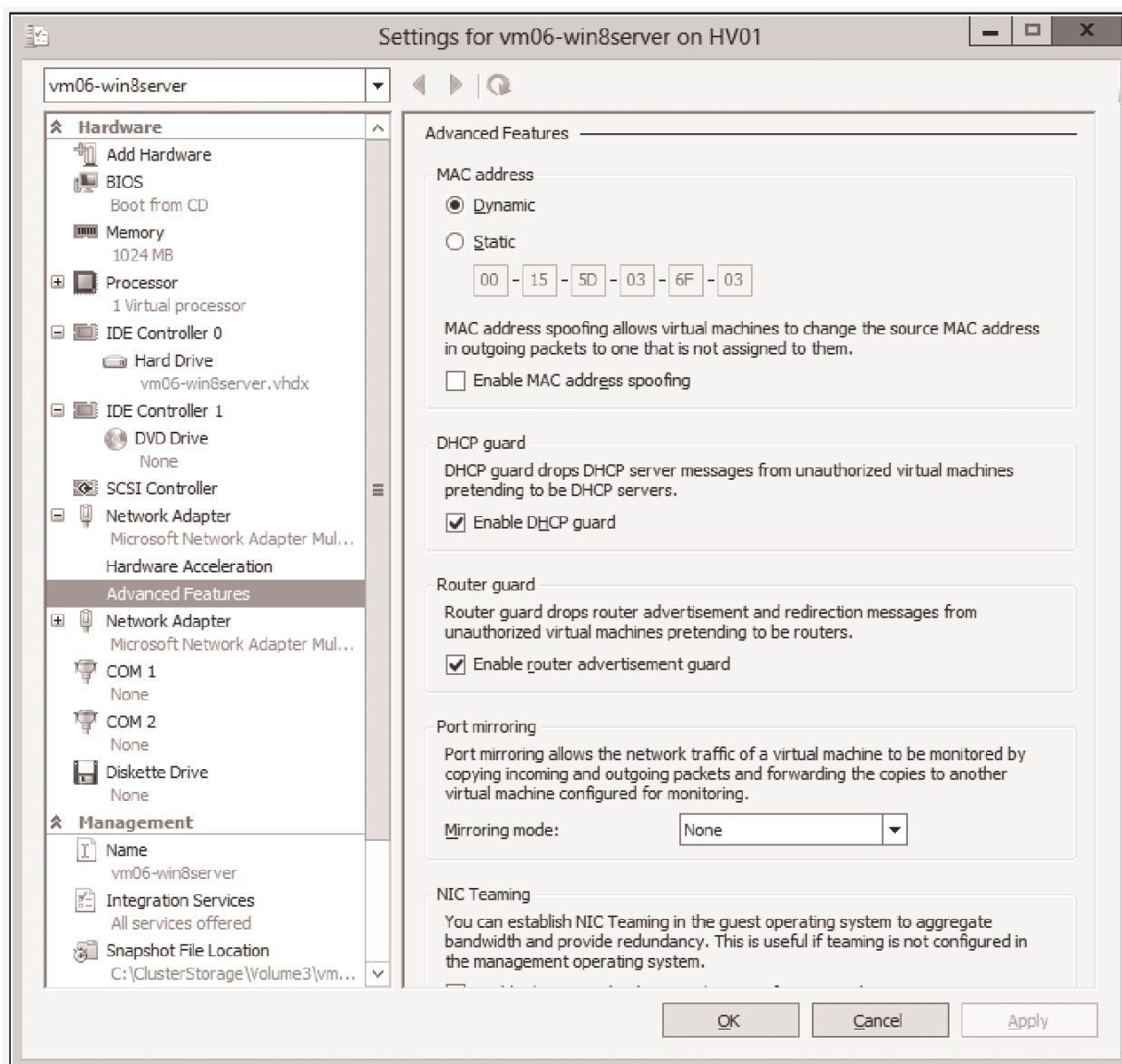
We have four VMs on this host. Let's activate DHCP Guard, router advertisement guard, and VMQ in a single line:

```
                          Administrator: Windows PowerShell                    [_][□][ X ]
PS C:\> Get-VM | Set-VMNetworkAdapter -RouterGuard on -VmqWeight 100 -DhcpGuard on
PS C:\> _
```

Once the Windows PowerShell prompt has returned, we can view the settings on any VM on this host:

Note: to do this in a Hyper-V cluster, simply prepend the previous statement with Get-ClusterGroup:
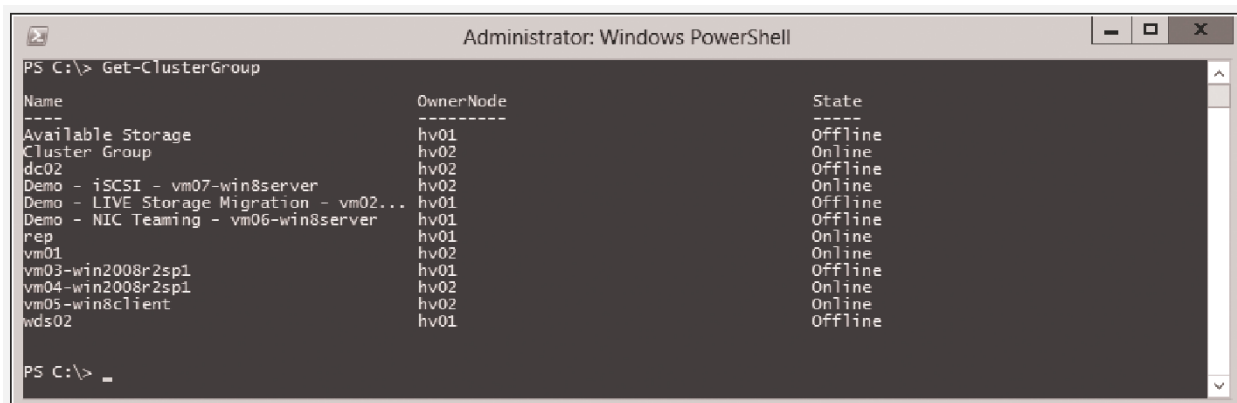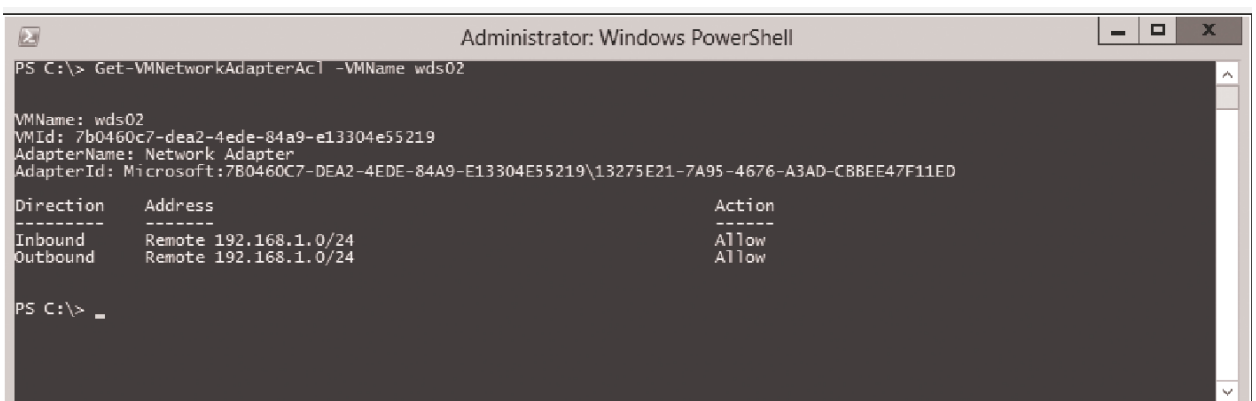

Scenario 2: Configure ACLs on a VM

Most organizations have a management network segment and will typically associate a physical NIC on the management network segment. Suppose you want to limit the network segment associated with the virtual NIC connected to the management network. Here's how you'd create an ACL to accomplish this:

```
Administrator: Windows PowerShell                                    _ □ x
PS C:\> Get-VM wds02 | Add-VMNetworkAdapterAcl -RemoteIPAddress 192.168.1.0/24 -Direction Both -Action Allow_
```

This cmdlet allows both inbound and outbound traffic to the VM named wds02 from the 192.168.1.0/24 segment. To view the settings:

```
Administrator: Windows PowerShell                                    _ □ x
PS C:\> Get-VMNetworkAdapterAcl -VMName wds02

VMName: wds02
VMId: 7b0460c7-dea2-4ede-84a9-e13304e55219
AdapterName: Network Adapter
AdapterId: Microsoft:7B0460C7-DEA2-4EDE-84A9-E13304E55219\13275E21-7A95-4676-A3AD-CBBEE47F11ED

Direction      Address                                    Action
---------      -------                                    ------
Inbound        Remote 192.168.1.0/24                      Allow
Outbound       Remote 192.168.1.0/24                      Allow

PS C:\> _
```