

Infrastructure Planning
and Design

Windows Server® Virtualization

Version 2.2

Published: November 2007

Updated: February 2011

For the latest information, please see [www.microsoft.com/ipd](http://www.microsoft.com/ipd)

Copyright © 2011 Microsoft Corporation. This documentation is licensed to you under the Creative Commons Attribution License.  To view a copy of this license, visit <http://creativecommons.org/licenses/by/3.0/us/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.  When using this documentation, provide the following attribution: Infrastructure Planning and Design is provided with permission from Microsoft Corporation.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet website references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Excel, Hyper-V, SQL Server, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries and regions.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[The Planning and Design Series Approach 1](#_Toc283987150)

[Introduction to the Windows Server Virtualization Guide 2](#_Toc283987151)

[Step 1: Determine the Virtualization Scope 6](#_Toc283987152)

[Step 2: Create the List of Workloads 8](#_Toc283987153)

[Step 3: Select the Backup and Fault-Tolerance Approaches for Each Workload 13](#_Toc283987154)

[Step 4: Summarize and Analyze the Workload Requirements 17](#_Toc283987155)

[Step 5: Design and Place Virtualization Host Hardware 19](#_Toc283987156)

[Step 6: Map Workloads to Hosts 21](#_Toc283987157)

[Step 7: Design Backup and Fault Tolerance 23](#_Toc283987158)

[Step 8: Design the Storage Infrastructure 26](#_Toc283987159)

[Step 9: Design the Network Infrastructure 28](#_Toc283987160)

[Appendix A: Job Aids 31](#_Toc283987161)

[Appendix B: Collecting Performance Data to Determine Resource Requirements 34](#_Toc283987162)

[Appendix C: IPD in Microsoft Operations Framework 4.0 36](#_Toc283987163)

[Appendix D: Windows Server Virtualization in Microsoft Infrastructure Optimization 37](#_Toc283987164)

[Version History 38](#_Toc283987165)

[Acknowledgments 39](#_Toc283987166)

# The Planning and Design Series Approach

This guide is one in a series of planning and design guides that clarify and streamline the planning and design process for Microsoft infrastructure technologies. Each guide in the series addresses a unique infrastructure technology or scenario. These guides include the following topics:

* Defining the technical decision flow (flow chart) through the planning process.
* Describing the decisions to be made and the commonly available options to consider in making the decisions.
* Relating the decisions and options for the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions for the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment Microsoft product documentation.

## Benefits of Using This Guide

Using this guide will help an organization to plan the best architecture for the business and to deliver the most cost-effective Windows Server® virtualization technology.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. Microsoft® Infrastructure Planning and Design (IPD) eliminates over-architecting and overspending by precisely matching the technology solution to the business needs.
* Alignment between the business and IT from the beginning of the design process to the end.

Benefits for Infrastructure Stakeholders/Decision Makers:

* Authoritative guidance. Microsoft is the best source for guidance about the design of Microsoft products.
* Business validation questions to ensure the solution meets the requirements of both business and infrastructure stakeholders.
* High integrity design criteria that includes product limitations.
* Fault-tolerant infrastructure, where necessary.
* Proportionate system and network availability to meet business requirements. Infrastructure that is sized appropriately to meet business requirements.

**Benefits for** Consultants or Partners:

* Rapid readiness for consulting engagements.
* Planning and design template to standardize design and peer reviews.
* A “leave-behind” for pre-sales and post-sales visits to customer sites.
* General classroom instruction/preparation.

Benefits for the Entire Organization:

Using this guide should result in a design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements, while considering the performance, capacity, manageability, and fault tolerance of the system.

# Introduction to the Windows Server Virtualization Guide

This guide leads the reader, step by step, through the process of planning a virtualized server environment. Steps 1 through 4 focus on determining requirements for the workloads that will be virtualized; they enumerate the capacity and performance requirements that will be used in planning host systems. By addressing resource requirements, backup options, and availability expectations first, the architect can determine the size of the load that the virtualized workloads will require from the host infrastructure.

Steps 5 through 9 focus on the planning and design of the physical host infrastructure. Guest workload requirements determine the server form factor, server placement, and the storage and network architecture. Specific steps and an overview of the entire process appear later in this document.

Business objectives should be prioritized at the start of the project so that they are clearly understood and agreed on by IT and business managers.

Following this guide will result in a design that is sized, configured, and appropriately placed to deliver the stated business benefits, while considering the user experience, security, manageability, performance, capacity, and fault tolerance of the system.

The guide addresses the scenarios most likely to be encountered by someone designing a Windows Server virtualization infrastructure. Customers should consider having their architecture reviewed by Microsoft Customer Service and Support or a Microsoft Certified Partner prior to implementation as these organizations are best able to comment on the supportability of a particular design.

Figure 1 illustrates scenarios for workload consolidation onto Windows Server 2008 Hyper-V™ technology.



Figure 1. Windows Server virtualization architecture

## What’s New in Windows Server 2008 R2

This guide’s design process is valid for both Windows Server 2008 and Windows Server 2008 R2 environments. Windows Server 2008 R2 introduces new functionality and enhancements to Hyper-V virtualization technology that provide improved flexibility, increased performance, and greater scalability for users, including the following:

* Live migration
* Cluster Shared Volumes
* Dynamic virtual storage support
* Enhanced processor support
* Enhanced networking support

Note that Microsoft Virtual Server 2005 R2 with Service Pack 1 (SP1) is not supported on Windows Server 2008 R2.

For more details on the changes, see [http://technet.microsoft.com/en-us/library/dd391932(WS.10).aspx](http://technet.microsoft.com/en-us/library/dd391932%28WS.10%29.aspx).

## Virtualization Design Process

This guide addresses the most common scenarios, decisions, activities, options, tasks, and outcomes that organizations encounter when implementing a virtual server environment. It does not, however, attempt to address every possible scenario. If an environment is unique, design consultants or specialists should be employed to address specific needs.

The following steps represent the most critical design elements in a successful, well-planned implementation of Windows Server 2008 Hyper-V for server virtualization:

* Step 1: Determine the Virtualization Scope
* Step 2: Create the List of Workloads
* Step 3: Select the Backup and Fault-Tolerance Approaches for Each Workload
* Step 4: Summarize and Analyze the Workload Requirements
* Step 5: Design and Place Virtualization Host Hardware
* Step 6: Map Workloads to Hosts
* Step 7: Design Backup and Fault Tolerance
* Step 8: Design the Storage Infrastructure
* Step 9: Design the Network Infrastructure

Some of these steps include decisions that must be made. Where this is the case, a corresponding list of common response options will be presented.

Other steps in this list include tasks that must be carried out. These are addressed because their presence is significant in order to complete the infrastructure design.

Figure 2 provides a graphical overview of the steps in designing a Windows Server 2008 R2 virtualization infrastructure.



Figure 2. The Windows Server virtualization infrastructure decision flow

## Applicable Scenarios

This guide addresses considerations that are related to planning and designing the necessary components for a successful server virtualization infrastructure:

* Server consolidation.
* Using live migration to enable scheduled maintenance on server hardware.
* Using live migration to redistribute workloads between server hosts to better balance resource usage. This could be done either on a seasonal or a daily basis—for example, to enable some servers to be turned off during times of lower demand.
* Using live migration to move workloads to a different regional data center in order to align with organizational changes.
* Support for legacy operating systems and applications.
* Reducing deployment and provisioning times by delivering virtual machines instead of physical machines.
* Reducing data center power and cooling costs by dynamically consolidating onto fewer servers at times of lower demand.
* Reducing hardware costs by increasing hardware utilization.
* Desktop centralization using Virtual Desktop Infrastructure (VDI).

## Out of Scope

Although the infrastructure planning information in this guide applies to many applications of virtualization technology, certain details are outside the scope of this document. Such details include:

* Disaster recovery and business continuity planning.
* Creating development and test environments.
* Increasing workload security through virtualization.
* Operating the virtualized environment.
* Considerations for virtualization hosting providers.
* Consolidating operating system images by running more applications together on each operating system. This work may precede moving the operating system to the virtualization platform, but because it can involve additional factors such as confirming application coexistence and compatibility on a shared operating system, it is beyond the scope of this document.

# Step 1: Determine the Virtualization Scope

The goal of this step is to define the scope of the infrastructure that will be virtualized. Once the scope of the virtualized environment has been determined, it will be used in the next step to define the list of workloads that are candidates for virtualization. Because details relating to workloads and other technical decisions vary for each option, this guide was designed as a review of each option’s required tasks, decisions, and questions. If an organization will apply this process to more than one of the options, it should complete the steps in this guide for each option.

The scope of the virtualization project drives decisions in future steps related to capacity requirements. Ensure that the entire organization is aligned with and supports the selected approach before continuing the planning process.

## Task 1: Determine the Scope of the Project

Before beginning to design a virtualization infrastructure, an organization needs to determine which parts of its environment to include in the design.

Deployment of Windows Server virtualization across the enterprise, including all corporate data centers, delivers standardization and the associated economies of scale over time. Deployment across the enterprise can maximize the return on investment (ROI), but it takes time for that return to be realized, and the risk will be increased because of the number of systems involved.

Windows Server virtualization can also be restricted to one or more hub locations, including corporate data centers where there are concentrations of users, computers, and/or network connectivity. Deploying to hub locations delivers standardization across a region and some economies of scale, but upfront costs are relatively high.

A deployment to remote or satellite locations reduces the upfront costs and risk to the project because fewer systems will be involved. However, there may be some risk of creating non-standard configurations in the remote locations that may be more challenging to support if specialized staff are not onsite.

When virtualizing workloads that run in hub and/or satellite locations, organizations may have two primary infrastructure options: They can build a virtual infrastructure within the hub or satellite office itself, or they can move server-related resources to a centralized hub or data center location.

Decide which part of the infrastructure to virtualize based on the specific needs of the organization. Record the scope of the project as enterprise, hub, or satellite in Table A-1 “Document the Requirements” in Appendix A: “Job Aids.” If it is determined that the scope should be limited to hub or satellite deployment, also record in Table A-1 which hubs or satellite locations will be included.

## Validating with the Business

When deciding which portion of the infrastructure to virtualize, business stakeholders should ask questions similar to the following to ensure that they have a complete view of how the planned infrastructure affects the business:

* What is the primary reason for implementing virtualization? Business goals should determine which portions of the infrastructure to virtualize—for example, reducing data center costs by reducing the number of physical servers as well as consolidating applications and workloads. Another business goal may be to centralize desktop workloads to reduce maintenance costs.
* What is the expected timeline for moving to virtualization? In many cases, organizations start with a limited deployment in order to gain expertise with the technology and to test various configurations.

## Step Summary

In this step the scope of the workloads that will be included in the project is determined. The scope of the project was recorded as enterprise, hub, or satellite in Table A-1 in Appendix A. If it is determined that the scope should be limited to hub or satellite deployment, which hubs or satellite locations will be included was also recorded in Table A-1.

## Additional Reading

* Windows Server 2008 Hyper-V library: <http://technet2.microsoft.com/windowsserver2008/en/library/5341cb70-0508-4201-a6da-dcac1a65fd351033.mspx>
* Windows Server 2008 Hyper-V resources: <http://www.microsoft.com/virtualization/resources.mspx#documents>
* Windows Server 2008 R2 home page: <http://www.microsoft.com/windowsserver2008/en/us/r2.aspx>
* Desktop Virtualization: <http://www.microsoft.com/virtualization/products/desktop/default.mspx>
* For information on how Microsoft IT has deployed server virtualization technology, see the Technical Solution Brief, “Server and Data Center Consolidation: Microsoft IT Enhances Cost Savings, Availability, and Performance”: <http://www.microsoft.com/technet/itshowcase/content/svrdatactrconsoltsb.mspx>

# Step 2: Create the List of Workloads

Now that the project scope has been determined, decide which workloads will be run in the virtualized environment. This document assumes that a workload represents the entire physical server or client computer that currently runs one or more applications. It is further assumed that the entire physical server or client computer is to be virtualized, not just the applications that run on it. This approach maps workloads to guests on a 1:1 basis. For server workloads, the opportunity exists to combine one or more applications from different servers into a single workload. That work may precede moving the operating system to the virtualization platform, but because it can involve additional factors such as confirming application coexistence and compatibility on a shared operating system, it is beyond the scope of this document.

Windows Server virtualization provides an environment on which a wide variety of workloads can be run—from workloads that run on their own server operating system, such as Microsoft Internet Information Services, to entire client desktops with many active client applications that run on the Windows Vista® and Windows® 7 operating systems. The list of workloads will be used in this step to determine resource requirements and then, in later steps, to design the physical host infrastructure on which the workloads will run.

## Task 1: Create the List of Candidate Workloads

Use the scope of the virtualization project as determined in Step 1 to create a table of all the candidate workloads that are in-scope for virtualization. For each workload record the following in Table A-1 in Appendix A: “Job Aids”:

* Current location. This will be used to determine the network bandwidth and connectivity requirements so that service can continue to be delivered to the same locations. It will also be used to evaluate whether there are restrictions on where the virtualized workload can be run.
* Admin contact. The person who is responsible for administration of the workload. This person will be consulted when determining the suitability of the workload for virtualization and must be advised of the change in his or her responsibilities when the workload is virtualized. The Admin contact may also be a valuable resource in understanding details of the workload.
* Operating system. This will be used to determine whether the workload can be run and supported in a virtual machine (VM).
* Applications. This will be used to determine whether the workload can be run and supported in a VM.

Once complete, this list will be used to examine the compatibility of each of the candidate workloads with the virtualization environment.

## Task 2: Determine Workload Compatibility

The goal of virtualization technology is to provide virtual environments that can support a wide variety of operating systems and applications; however, certain limitations can prevent some types of workloads from running virtualized. For each of the workloads, examine the specific technical requirements for the applications and the operating system and map those against any constraints in the virtualization technology. Factors include special hardware requirements, such as access to USB devices or host bus adapters (HBAs). HBAs are not available to VMs.

Other technical considerations related to storage and networking are covered during Steps 8 and 9 later in this guide.

In addition to verifying technical compatibility, confirm the following:

* That the operating systems and applications suppliers will support the workload when used in a VM.
* That the operating systems and applications suppliers will allow the workload to be licensed in a VM.

Finally, examine the business suitability of the workload for virtualization. Security and/or other business requirements may lead an organization to run an application on physical hardware rather than virtually.

If the workload is not compatible with the virtualization platform, remove it from the list in Table A-1 in Appendix A.

## Validating with the Business

To ensure that the list of applications for virtualization is accurate, ask business stakeholders the following questions:

* Is the list of applications complete? The success of the virtual infrastructure design depends on determining the requirements for applications that can be supported in a virtual environment.
* Are there applications on the list that should not be virtualized? It can be difficult to recognize all the potential issues with virtualization based on technical details alone. The fact that a workload can be virtualized does not necessarily mean that it should be. Business leaders should understand the basic idea behind virtualization and should verify that it appears to be a suitable solution for each workload.
* Can the business accept the risks of moving to virtualization? Making changes to any application or server involves risk. The business should ensure that the level of risk is acceptable.
* Do specific legal requirements prevent an application from running within a VM? Requirements related to physical isolation of applications or that prevent certain applications from running on the same servers can prevent the use of virtualization. Confirm also that the application can be licensed for use in a virtualized environment at a reasonable cost.
* Do support-related requirements prevent an application from being virtualized? Organizations should evaluate their support contracts before committing to run an application within a VM. If the application provider will not provide support for running it in a VM, evaluate the business risk and cost. It may be necessary to reproduce any problem in a physical server environment before requesting support.
* How should applications be prioritized? Businesses may prioritize workloads based on the expected ROI of virtualization, the availability of project funding from a particular business unit, or because of changes in the way the applications will be used by the business.
* What about applications that are used only rarely? Applications that are rarely used might translate to a lower priority or might be removed entirely from the list of applications. Alternatively, they may prove excellent candidates since virtualization may offer a way to eliminate server hardware that runs all year, but is hardly ever used.
* **Can business users assist in testing application compatibility?** IT departments are responsible for deploying and supporting applications; however, business users are often experts in application functionality. Compatibility tests should involve input from representative users who can verify that their programs are running properly in the virtual environment.

## Task 3: Determine Resource Requirements

After deciding on the list of workloads that the virtualization environment will support, the resources required to support those workloads need to be determined. In this task, the technical requirements for each workload that will be virtualized will be collected. These requirements will be used in subsequent steps to design the host infrastructure.

The organization should plan to support the peak load of each workload to ensure that the host system can handle the full load of all of the workloads. It’s also recommended that a buffer amount be added when determining specific host requirements to ensure enough resources will be provided. This can be done by adding additional capacity for each application that is appropriate for its requirements or by adding a fixed percentage that applies for all applications.

This document assumes that a workload represents the entire physical server or workstation that currently runs the workload. When collecting performance information, the counters that are being collected are for the entire machine.

For existing production workloads, there are three ways to determine the resource requirements.

### Option 1: The Microsoft Assessment and Planning Toolkit

Microsoft Assessment and Planning Toolkit (MAP) can be used to inventory a current server and workstation environment, determine which machines are underutilized, and then generate virtualization candidate assessments for implementation. It can also be used to model the environment on different hardware platforms.

The MAP toolkit is available as a free download at <http://technet.microsoft.com/en-us/solutionaccelerators/dd537566.aspx?SA_CE=NOT-MAP-EMAL-MAP4BETAANNCMTMSONLY-2009-06-15>.

### Option 2: System Center Virtual Machine Manager 2008

Microsoft System Center Virtual Machine Manager 2008 R2 can be used to manage a virtualized server environment. System Center Virtual Machine Manager can analyze performance data and resource requirements both for workloads that will be virtualized and for existing virtualized workloads. This analysis can be used to create deployment recommendations and to enable modeling workloads on existing virtualization hosts. In order to determine the resource requirements of a workload, a System Center Virtual Machine Manager agent must be installed on that workload.

For information on planning a System Center Virtual Machine Manager infrastructure, refer to the IPD guide for System Center Virtual Machine Manager at [www.microsoft.com/ipd](http://www.microsoft.com/ipd).

For additional details about System Center Virtual Machine Manager, see: <http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/default.aspx>.

### Option 3: Manually

Use one or more of the following techniques to manually determine resource requirements:

* Real-world performance data (based on monitoring existing workloads).
* Specifications and requirements from application and operating system vendors.
* Results from application benchmark testing.
* Details that application developers and systems integrators provide.
* Load-testing based on expected use patterns and metrics.

A comparison of these techniques is presented in Table 1 and Table 2.

Table 1. Technique Comparison

| Technique | Cost | Deploys agent? | Firewall friendly | Output | Data sources | Automated collection |
| --- | --- | --- | --- | --- | --- | --- |
| MAP | Free | No | Requires exception | Microsoft Office Excel® and proposal | Windows Management Instrumenta-tion calls | Yes |
| System Center Virtual Machine Manager | License | Yes | Port 80/443 | Graphical report | System Center Virtual Machine Manager agent | Yes |
| Manual | Free | No | N/A | Manual | Performance Monitor (Perfmon) | No |

Table 2. Technique Comparison (continued)

| Positioning | Discovery technique | Collection frequency | Security | Thresholds adjustable |
| --- | --- | --- | --- | --- |
| Pre-salesPre-deployment of VMs | Active Directory® Domain Services, IP address, or computer name | 5 minutes | Domain or machine account | No |
| Post-deployment | System Center Virtual Machine Manager discovery | 9 minutes | System Center Virtual Machine Manager agent | Yes |
| Manual | Manual | On demand | Machine or domain account | Yes |

When planning to virtualize a completely new workload, a more subjective approach may have to be used, such as experience with similar technologies or from published literature.

Select the technique that will be used to determine resource requirements, and record that information in Table A-2 “Record Resource Requirements” in Appendix A.

If the manual approach will be used, refer to Appendix B: “Collecting Performance Data to Determine Resource Requirements” for the details of the work that must be performed.

## Validating with the Business

This step documents the technical resource requirements for each workload. Other details will require business input. Work with business decision makers to ensure agreement on the following:

* Would any regulatory requirements or political issues prevent combining specific applications on the same servers? In addition to technical requirements for physical isolation and coexistence, business or political issues can prevent the same server hosting specific applications.
* Are there any legal concerns about the geographical location of an application? Legal requirements and international regulations can prevent certain applications from residing in specific geographic locations.
* Confirm the availability and backup requirements for each of the applications. This will be used to determine the strategy for fault tolerance and backup.
* **What are the expected growth patterns for each of the applications over the next two to three years?** This will enable sizing of the virtualization environment to accommodate that growth.

## Step Summary

The total resource requirements for all of the workloads that the organization’s virtual infrastructure will host are identified in this step. All of the data relative to the list of candidate workloads, work compatibility, and resource requirements was collected and recorded in Tables A-1 and A-2 in Appendix A.

## Additional Reading

* For information on planning a System Center Virtual Machine Manager infrastructure, refer to the IPD guide for System Center Virtual Machine Manager: Microsoft System Center Virtual Machine Manager 2008 R: [www.microsoft.com/ipd](http://www.microsoft.com/ipd)
* System Center Virtual Machine Manager home page: <http://www.microsoft.com/systemcenter/virtualmachinemanager/en/us/default.aspx>
* The MAP toolkit: <http://technet.microsoft.com/en-us/solutionaccelerators/dd537566.aspx?SA_CE=NOT-MAP-EMAL-MAP4BETAANNCMTMSONLY-2009-06-15>
* Remote Desktop Virtualization Host Capacity Planning in Windows Server 2008 R2: <http://www.microsoft.com/downloads/en/confirmation.aspx?familyId=bd24503e-b8b7-4b5b-9a86-af03ac5332c8&displayLang=en>

# Step 3: Select the Backup and Fault-Tolerance Approaches for Each Workload

In the previous step, a list of workloads was created to determine resource requirements and a decision was made about which workloads will be run in the virtualized environment. In this step, the backup approach will be selected for the virtualized workloads that will be used in the design of the host system, its storage, and network infrastructure. Backup requires that additional resources be added to the design, depending on the type of backup used. In addition, the most appropriate fault-tolerance approach for each workload being virtualized will be selected.

## Task 1: Select the Backup Approach

There are three options available to meet the workload’s backup and restore requirements. In this task, each workload is reviewed to determine which backup approach to use. The decision should be recorded in Table A-3 “Document the Backup Approach” in Appendix A: “Job Aids.”

The reason for understanding the type of backup approach for each workload is to:

* Allow for the possibility of grouping workloads with similar backup requirements onto the same hosts. For example, all workloads using the virtualization host backup approach may be placed on the same host.
* Determine the impact that backups will have on the host system from a resource perspective.

Backup can be performed in the following ways:

* While the workload is running and in use. In that case, products such as Microsoft SQL Server® and Microsoft Exchange Server have specific backup application requirements to ensure that a complete backup is obtained. For example, transactions that are in memory must be backed up, and transaction log files must be committed to the database.
* The workload can be paused while a backup is completed. This will ensure a complete backup, but the applications will be unavailable to users while the backup takes place.

### Option 1: Application Backup Approach

Performing application-level backups has the following characteristics:

* The backup and restore process may be simplified because administrators can use specific application-level capabilities to manage the backup and restore processes.
* The backup files themselves can be significantly smaller than those generated from a guest-level or host-level backup.
* Application-specific backups can have a significant impact on the host system from a CPU, disk, and network usage perspective.

### Option 2: Workload Backup Approach

In workload-level backups, the virtualized workload may include a backup agent such as Microsoft System Center Data Protection Manager 2007 that is responsible for transferring backups to a designated storage location, or the native Windows backup application can be used. Workload-level backups can have a significant performance impact on the host system from a CPU, disk, and network usage perspective.

### Option 3: Virtualization Host Backup Approach

When performing backups at the virtualization host level, two options are available:

* Offline backups. This approach requires turning off the VM or placing it in a saved state before copying files. After the copy process is complete, the VM can be started again. This approach involves downtime for each VM, but it provides a simple method for implementing complete backups.
* Online backups. This approach uses System Center Data Protection Manager, which takes a snapshot using Volume Shadow Copy Service (VSS) while the VM is running. Using this method avoids downtime but may affect performance momentarily.

## Evaluating the Characteristics

Additional characteristics are evaluated in Table 3.

Table 3. Characteristics Comparison

| Complexity | Justification | Rating |
| --- | --- | --- |
| Application backup approach | Different backup methods may have to be used for different applications. | High |
| Workload backup approach | Backups can be centrally managed using enterprise backup software. | Medium |
| Host backup approach | Requires no knowledge of the workload’s contents; therefore, backups can be performed in a consistent method across the entire environment. | Medium |
| Performance | Justification | Rating |
| Application backup approach | Backups include only application data. | ↓ |
| Workload backup approach | Backups are treated the same as they would be for physical machines and can include the operating system, program files, and user data. | ↓ |
| Host backup approach | Backups include the entire contents of a VM, usually requiring more time and storage space; however, backups can be performed while the VM is active. | → |

Record the backup approach that will be used for each workload in Table A-3 in Appendix A.

## Validating with the Business

Technical requirements often drive decisions about specific backup approaches. Ask the following questions to ensure that business needs are met:

* Is it necessary to back up all the content for a specific workload or application? In some cases, application experts might determine that it is necessary to store only certain information in backup files because users can easily re-create other data in the event of a failure.
* Will the recommended approach meet data loss requirements? Perform backups frequently enough to ensure that data loss is minimized for critical workloads.
* Does the recommended approach meet recovery requirements? Business users will likely have expectations related to the amount of time required to recover from a failure.

Based on answers to these questions, backup-related decisions for specific applications may need to be reviewed and revised.

## Task 2: Select the Fault-Tolerance Approach

Workload fault-tolerance requirements place specific technical requirements on the virtualization host server, storage, and network infrastructure.

Select the most appropriate fault-tolerance approach for each workload that will be virtualized. The technical approach can vary based on the details of the underlying operating system and applications that will run in the virtualized environment. Complete this task for each workload and record the option selected in Table A-4 “Document the Fault-Tolerance Approach” in Appendix A.

### Option 1: Network Load Balancing

Stateless applications such as web servers can have fault-tolerance support by establishing Network Load Balancing (NLB) across multiple identical instances of the application. NLB technology distributes the inbound traffic headed for the application across multiple machines running the same application, which allows for one server to fail and the remaining servers to pick up the load. Windows Server has a software implementation of NLB built in.

A hardware NLB solution can distribute requests based on a variety of load-distribution algorithms. It can also monitor various nodes in the server farm and ensure that they are operating properly before sending requests to them. This option requires that at least one additional VM be added for each application using NLB.

### Option 2: Application-Specific Clustering

Many enterprise applications that customers consider mission critical have failover capabilities built into them through cluster awareness. These applications were designed and built to run on a Microsoft Failover Cluster service. Examples include SQL Server and Exchange Server. A cluster can be configured by using multiple VMs that have a common shared disk. This option requires that at least one additional VM be added for each workload that is being clustered.

### Option 3: Host Clustering

The physical virtualization hosts can be configured with Microsoft Failover Cluster service as a failover cluster using shared storage. In this configuration, if the host server running the VMs fails, the virtualization host and all its VMs fail over to another host in the cluster. The cluster would then attempt to restart each VM on the new node of the cluster.

**Note**   The applications inside each VM are not cluster aware, so there is no guarantee that the application will restart in the correct manner.

Record the fault-tolerance approach that will be used for each workload in Table A-4 in Appendix A.

## Validating with the Business

Ensure that technical decisions meet business requirements. Specific questions to ask include:

* Are all critical areas of the application infrastructure protected? It is easy to focus on protecting applications by themselves. However, fault tolerance requires a focus on areas such as the power infrastructure, the network, and storage devices. Applications might have dependencies on a wide array of services, all of which must remain available to support mission-critical activities.

## Step Summary

In this step, the backup approach was selected for the virtualized workloads that will be used in the design of the host system, its storage, and network infrastructure. In addition, the most appropriate fault-tolerance approach was selected for each workload that will be virtualized. The data collected in this step was recorded in Tables A-3 and A-4 in Appendix A.

## Additional Reading

* “An Overview of Windows Clustering Technologies: Server Clusters and Network Load Balancing”: <http://technet2.microsoft.com/windowsserver/en/library/c35dd48b-4fbc-4eee-8e5c-2a9a35cf63b21033.mspx?mfr=true>
* “Windows Server 2008 Hyper-V Failover Clustering Options”: <http://blogs.technet.com/josebda/archive/2008/06/17/windows-server-2008-hyper-v-failover-clustering-options.aspx>
* “Server Clusters: Cluster Configuration Best Practices for Windows Server 2003”: <http://technet2.microsoft.com/windowsserver/en/library/5172c43a-2e6d-4d94-bd44-163a8735ef921033.mspx?mfr=true>
* “Clustering virtual machines”: <http://technet2.microsoft.com/windowsserver/en/library/73b03235-bad1-4ca8-939f-c507d00e273f1033.mspx?mfr=true>
* The Microsoft TechNet article, “NLB Design Process”: <http://technet2.microsoft.com/windowsserver/en/library/251c6d81-b2c7-43eb-892c-2488a57ec9a81033.mspx?mfr=true> provides information about implementing Network Load Balancing Service (NLBS) on Windows Server 2003.
* Infrastructure Planning and Design Guide for System Center Data Protection Manager 2007 SP1: [www.microsoft.com/ipd](http://www.microsoft.com/ipd)
* System Center Data Protection Manager home page: <http://www.microsoft.com/systemcenter/dataprotectionmanager/en/us/default.aspx>

# Step 4: Summarize and Analyze the Workload Requirements

In the preceding steps, information about specific technical and business requirements for the workloads that will move to a virtualized environment was collected. In this step, that information will be combined in order to summarize the overall requirements for the solution. By the end of the step, the information will be available to start designing the virtualization host infrastructure.

From a technical standpoint, it is possible to support a wide variety of different workloads on the same physical computer. However, business or technical characteristics may prevent more than one system from running on the same server. One example is the need for workloads to exist in different physical locations. When supporting hubs and satellite offices, specific sites may require that certain workloads be instantiated locally.

Security and regulatory compliance requirements can also drive the need to keep certain workloads separate. If specific applications, databases, and services must remain segregated, note them (along with the reasons, such as security, regulatory compliance, or business policies) in Table A-1 in Appendix A: “Job Aids.” This data will be used in Step 6 to determine the acceptable placement of guest VMs in the infrastructure.

## Task 1: Group Workloads

Refer to the information collected in Tables A-3 and A-4 in Appendix A: “Job Aids,” including business and technical requirements, to determine which workloads could be run together on which virtualization hosts. Group workloads based on similarities in:

* Physical isolation requirements. Separate workloads that must be isolated from each other into different groups.
* Coexistence and compatibility of workloads. Add workloads to groups with which they share attributes—for example where the workloads service users in the same geography.
* Backup requirements and approach. Group together workloads that are backed up in the same way to simplify backup procedures.
* Fault-tolerance requirements. Add workloads to groups with which they share fault-tolerance requirements. This may enable a single fault-tolerance solution to be applied to each group, simplifying operations.

Use Table A-1 to group workloads that have similar requirements. Then examine the groupings to determine if the workloads might be able to run concurrently on the same virtualization host servers.

## Task 2: Summarize Workload Hardware Resource Requirements

For each group of workloads, use the output of Step 2 to determine the total resource requirements of the virtualization host hardware by summing the requirements of each workload that will run in the virtual infrastructure:

* CPU. Total the CPU requirements. The final number represents the total CPU capacity requirements for the host hardware pool. There is no method for converting the CPU utilization measurement made on one processor type to another newer type, so some assumptions may be required.
* Memory. Total the physical RAM requirements that were obtained by using application estimates or production performance data. The result will be a value for the total amount of memory in gigabytes that the VM require.
* Disk (storage capacity). The specific storage requirements should include the required amount of disk space for all the virtual hard disks created for VMs.
* Disk (performance). Total the input/outputs per second (IOps) requirements to obtain a view of the total disk performance requirements.
* Network. To determine host network requirements, total the peak values of network bandwidth use. Express the result in megabits per second (Mbps) and the number of network adapters.

Record the sum of the gathered statistics in Table A-2 in Appendix A.

To provide a safeguard against underestimating resource requirements, add buffer amounts when determining specific virtualization host requirements. Obtain this by adding additional capacity for each workload or by using a percentage or constant adjustment for all workloads.

## Step Summary

Tables A-1, A-2, A-3, and A-4 in Appendix A were used to collect data in this step. This data was then combined with the data from previous steps to summarize all the requirements for the workloads that will move to the virtual infrastructure.

# Step 5: Design and Place Virtualization Host Hardware

In the last step, data was collected and combined with the data from previous steps to summarize all the requirements for the applications and operating systems that will move to the virtual infrastructure. In this step, begin to design the host infrastructure based on workload requirements collected in the preceding steps. The goal of this step is to determine the most appropriate type of virtualization host hardware on which to deploy the VMs. A design will be created for where to place the servers that will host the virtualized workloads. The current location of the workloads may have some influence on where the virtualization hosts will be placed. However, workload virtualization presents an opportunity to move workloads to their optimum locations.

Determining the optimal hardware configuration for the virtual infrastructure should involve an inventory of existing host hardware systems. Compare resource specifications to the requirements summarized in Step 4 to determine whether new purchases will be required.

It may be necessary to review this step and the defined strategy when workloads are actually allocated to each system. It may be necessary to review form factor decisions several times to find the optimal configuration.

*Task 1: Determine the Scale Strategy*

Review whether the organization has a policy for server scaling and, if so, whether that policy is to scale up or to scale out. Fewer servers with large memory and CPU support can be easier to manage and can be more cost-efficient for some infrastructures. Using smaller commodity servers with lower capacity can involve a smaller capital investment but often requires additional management effort.

Record the organization’s server scaling policy in Table A-5 “Document the Form Factor for the Hosts” in Appendix A: “Job Aids.” This will be used to guide the hardware platform selection in the next task.

*Task 2: Select the Server Hardware*

Select server hardware that supports the prerequisites for the Windows Server 2008 R2 Hyper-V platform. Then refer to the fault-tolerance approach for the workloads that was determined in Step 3. If Microsoft Failover Cluster services will be used, refer to the Microsoft Support article “The Microsoft Support Policy for Windows Server 2008 or Windows Server 2008 R2 Failover Clusters” at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;943984>, and select a hardware platform that has passed the failover cluster validation test.

If Hyper-V live migration will be used to migrate workloads within a failover cluster, both hosts in a live migration pair must use processors from the same manufacturer.

Record the hardware platform selection in Table A-5 in Appendix A.

*Task 3: Place the Virtualization Servers*

Review the organization’s overall goals relative to centralization, regionalization, and decentralization of workloads. Then, for each workload that will be virtualized, use the output of Step 4, Task 1, and the following to determine the ideal location for each server that would host that workload:

* User location, if users are concentrated in a few locations.
* Regulatory or business requirements.
* Availability of skills and resources to operate the servers.
* Maintenance strategy. If Hyper-V live migration will be used to move workloads between hosts (for example, to enable planned downtime on one of those hosts), then the hosts must be connected in a failover cluster on the same local area network (LAN) segment, with access to a shared logical unit number (LUN).

After completing this task, the location of the servers will have been determined. Record the locations in Table A-5 in Appendix A. The number of host servers that will be required in each location will be determined in Step 6.

*Task 4: Apply Fault-Tolerance Requirements*

Review the requirements for fault tolerance that were determined in Step 3. If Microsoft Failover Clustering Services will be used, refer to the Microsoft Support article “The Microsoft Support Policy for Windows Server 2008 or Windows Server 2008 R2 Failover Clusters” at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;943984>. The hosts in the failover cluster may require access to shared storage, in which case both hosts in a failover pair may need to be sited local to each other.

Record the failover partner for each host in Table A-5 in Appendix A.

## Validating with the Business

Ask the following questions to verify that the host hardware approach meets the organization’s business requirements and directions:

* Are the hardware estimates aligned with purchasing goals? Factoring in current and future purchasing decisions is a necessary step in designing the virtual infrastructure.
* Will the business realize the cost reductions and savings it anticipates? Often, total cost of ownership and ROI numbers must be calculated to ensure that the organization will achieve the expected benefits.

Server placement decisions affect all areas of the organization and can significantly affect costs and the overall user experience.

Questions to ask the business include:

* Does the location plan support future business expansion? Organizations that are planning additional sites and locations should take into account future plans when considering server placement.
* Are the server placement decisions in accordance with regulatory and security compliance requirements? Organizations might have a business need to store certain types of data and applications within the corporate data center.
* Does the organization have the expertise to support servers in the defined locations? Larger branch offices tend to have dedicated IT staff, whereas smaller environments do not.
* Are there any geopolitical considerations? There may be regulations in force that affect where workloads may be run. For example, workloads that process sensitive data may be required to run within the borders of the country or region they serve.

## Step Summary

In this step, a design was created to determine where to place the servers that will host the virtualized workloads and the server hardware was chosen. In addition, fault tolerance requirements were applied, if necessary. Data collected in this step was recorded in Table A-5 in Appendix A.

# Step 6: Map Workloads to Hosts

The purpose of this step is to determine which workloads will be placed on which physical hosts and how many of those hosts will be required. For each group of workloads that were defined in Step 4, map that group and its total resource requirements to the hardware design that was decided on in Step 5. This will be used to determine how many hosts will be required to run the workloads that contain the group.

This step is completed using data from a point in time. Workload characteristics can change over time, so be prepared to re-evaluate and adjust the mapping periodically.

## Task 1: Determine Host Resource Threshold/Buffer Limits

Decide on the optimum host resource use levels for CPU and memory since that will determine how many workloads can fit on any given host. One approach is to maximize resource use on each host while leaving sufficient buffer to handle unexpected peaks in load. For example, it might be determined that the optimum CPU utilization for virtualization host servers is 80 percent. Record these thresholds in Table A-5 in Appendix A. They will be applied in the next task.

## Task 2: Map Workloads to the Form Factor

Map all of the workloads onto as few physical servers as possible in each geography, while respecting the needs for server buffer, isolation, availability, backup type, and geographic location. To do this, refer to Step 2 and the method that was used to collect the workload requirements. If System Center Virtual Machine Manager or MAP were used, they can be used here to model and recommend workload placement. If these tools are not available or not appropriate, then this task must be performed manually. Start by categorizing the workloads based on their CPU and memory requirements.

Next combine or separate workloads based on their backup, availability, and isolation requirements. For example, if an entire VM backup is required, deploy the workload onto virtualization host servers designated for that task. System Center Data Protection Manager 2007 with SP1 provides this capability to back up an entire VM.

Ideally, this process would be likened to an automatic coin counter where all of the coins are put in a funnel in the top of the machine and the coins are automatically separated into their respective denominations and stacked in sizes that fit the coin wrappers. When a stack is full, the machine stops until the full wrapper is removed and a new one is positioned.

At the end of this exercise, all workloads and requirements should be accounted for, and the number of physical servers should be identified. Additional servers may be required to meet fault-tolerance requirements. These are addressed later in this guide. It may be appropriate to iterate through this process using different form factor designs to find the optimal configuration. Record the workloads assigned to each host server in Table A-5 in Appendix A.

## Validating with the Business

IT can complete resource-related requirements for mapping guests to the host infrastructure. However, other details, such as fault tolerance and backup requirements, should be verified with the business.

Questions to ask the business should include:

* Are these decisions consistent with the organization’s goals for virtualization? Determine the method of workload allocation based on the expected business benefits of adding a virtual infrastructure.
* Does the current design meet the organization’s availability and backup requirements? Details such as host server placement, facility limitations, and systems administrator expertise can affect overall operations.
* Which requirements and constraints can be considered flexible? In some cases, businesses might find that relatively small investments in additional hardware can lead to better overall workload distribution decisions. The organization should reconsider details such as budgets and employee resources based on results from this step.

## Step Summary

In this step, which workloads that will be placed on which physical hosts were determined, as well as how many of those hosts will be required. The data collected in this step was recorded in Table A-5 in Appendix A.

# Step 7: Design Backup and Fault Tolerance

In the previous step, it was determined which workloads will be placed on which physical hosts, and how many of those hosts will be required. The purpose of this step is to determine the backup and fault-tolerance approaches that virtualization host servers will use to meet the workload requirements that were defined in Step 3. This information will be used to design the storage and network in Steps 8 and 9.

## Task 1: Select the Backup Approach

In this task, two approaches to backing up virtual workloads are presented. Because backup requirements are based primarily on recovery requirements, familiarity with the downtime and data-loss limitations for each workload is important. The business should consider how much data it can afford to lose as well as how quickly it needs to recover after an event occurs. The following two items provide more information to consider relative to designing the backup approach:

* **Data loss tolerance**. How much data can the business afford to lose (measured in minutes, hours, or days)? This is equivalent to the recovery point objective, which is the acceptable amount of data loss that can be tolerated, measured in time. More frequent backups will increase the cost and complexity of the implementation.
* **Speed of data recovery**. How quickly must the organization’s data be recovered after a problem occurs? This is one of the components of the recovery time objective, which is the time within which a business process must be restored to a serviceable state after a problem occurs. Restoring a business process to a serviceable state has many other dependencies in addition to the recovery of the application’s data. Indeed, the business service may be restored and made available to users prior to the recovery of protected data, which may occur over time as a background operation.

### Virtual Hard Disk Copy

Because the entire contents of a VM are encapsulated in virtual hard disk (VHD) and configuration files, a simple method of performing backups is to copy these files from the host computer’s file system. One of the advantages of this approach is that administrators can create the backups for any guest operating system. The restore process is simplified, because administrators can restore the VM using a simple file copy process. The primary challenge is that VHD files are locked as “in use” while VMs are running, and so cannot be backed up. One solution involves temporarily pausing or shutting down a VM before starting backups. However, doing so requires downtime and an interruption to application availability.

### Volume Shadow Copy Service Snapshot

System Center Data Protection Manager uses the VSS writer in Windows Server 2008 R2 Hyper-V to make consistent backups of VMs while they are in use.

Host-level backups will have an impact on the performance of the server. They can also affect the capacity and performance of the disk and network subsystems. It is necessary to account for these impacts in the server selection buffer as well as the network and disk capacity and performance planning considerations.

Record the backup design choice in Table A-5 in Appendix A: “Job Aids.”

## Validating with the Business

The specified backup approach can have a significant effect on the business. To validate its decisions, ask the following questions:

* **Are there special disaster recovery requirements for the backup solution?** In some cases, it might be much easier to maintain a disaster recovery site using full VM backups. In other cases, file system replication or other technologies might be more appropriate.
* **How are data-protection requirements expected to change in the future?** Although this question can be difficult to answer, factoring in anticipated enterprise application deployments can help the organization decide how best to invest in storage capacity to support the selected backup approach.

Update Table A-3 in Appendix A, if appropriate, to record the selection.

## Task 2: Design Fault Tolerance

In Step 3, information was collected on the fault-tolerance requirements for all the workloads that IT will support in the virtual infrastructure. Use that information to increment and adjust the virtualization server design, if necessary, and then record the fault tolerance for each host server in Table A-5 in Appendix A.

### Plan for Load Balancing

For each workload identified in Step 3 that required NLB, determine how many additional instances of the workload are needed, and then map them onto physical host systems using the same techniques as in Step 6. Ideally, load-balanced VMs should be distributed across multiple hosts to protect against the failure of a single host taking down all instances of the load-balanced application. Each load-balanced VM adds at least one more VM and often several to the list of VMs that need to be placed in the infrastructure.

### Plan for Application-specific Clustering

For each application that was identified in Step 3 as requiring fault tolerance through clustering, determine how many additional instances of the application are needed, and then map them onto physical host systems using the same techniques as in Step 6. Ideally, these VMs should be distributed across multiple hosts to protect against the failure of a single host taking down all members of the cluster. Each clustered VM adds at least one more VM and often several to the list of VMs that need to be placed in the infrastructure.

### Plan for Host Clustering

If Microsoft Failover Clustering Services will be used, count the number of servers that have workloads that require host clustering. This number represents the number of active cluster nodes required. Then, create a cluster plan that supports this defined number of active nodes. Each cluster will require at least one additional physical host server to act as the passive node in the cluster.

Host clustering can provide a simple method of ensuring that many types of VMs remain available even after the failure of a host system. The costs of implementing host clustering, however, can be significant because of hardware and storage requirements. In addition, unused capacity on standby nodes and servers lowers overall hardware resource use.

## Step Summary

In this step the design was adjusted, if necessary, to include resources required for the organization’s backup needs. The fault-tolerance requirements were also used to plan for additional resources in the virtualized server environment, if appropriate. The data collected in this step was recorded in Tables A-3 and A-5 in Appendix A.

## Additional Reading

“What's New in Failover Clusters”: [http://technet.microsoft.com/en-us/library/dd443539(WS.10).aspx](http://technet.microsoft.com/en-us/library/dd443539%28WS.10%29.aspx)

# Step 8: Design the Storage Infrastructure

In the previous step, the design was adjusted, if necessary, to include resources required for the organization’s backup needs. In addition, the fault-tolerance requirements were used to plan for additional resources in the virtualized server environment, if appropriate.

Planning a storage infrastructure for a virtualized environment requires that the performance and capacity needs of the VMs be mapped to an input/output (I/O) subsystem. In this step, the I/O performance and capacity requirements of the VMs that will run on each virtualization server will be used to design the I/O subsystem for the servers.

## Task 1: Plan for Performance

The goal of designing storage to meet disk performance requirements is to support the required number of IOps. This information was collected for each workload in Step 2 and was recorded in Table A-2 in Appendix A: “Job Aids.”

In this task, calculate the total IOps requirement for each virtualization server by totaling the IOps requirements for each VM that will run on that server. The choice of disk redundancy levels such as redundant array of independent disks (RAID) 1 or RAID 0+1 affects the IOps calculation. By mapping this IOps requirement to the selected type of disk subsystem and the drive characteristics of that subsystem, it is possible to determine the number of actual drives required to achieve the performance objectives. During the planning process, remember to account for such host-based activities as the impact of backup operations on disk performance, as well as adding an appropriate buffer to protect the system in the event of any system performance anomalies.

## Task 2: Plan for Capacity

In this task, calculate the disk capacity requirements for each virtualization server by totaling the capacity requirements for each workload that will run on the server plus the space that backups need (if any). The capacity requirement for each workload was collected in Step 2 and was recorded in Table A-2 in Appendix A.

By mapping this disk capacity requirement and the RAID configuration to the size of disks in the selected subsystem, it is possible to determine the number of actual drives required for performance.

Note   The actual number of disks required is the greater of the number determined in Task 1 (performance) and the number determined in this task. Usually that will be the number determined by performance.

## Task 3: Select an I/O Subsystem

The choice of the form factor for the storage system should reflect the ability to provide the performance and capacity requirements as well as clustering support, if applicable, and VSS snapshot backup capabilities, if required. Record the selection for each host server in Table A-5 in Appendix A: “Job Aids.”

Record the I/O subsystem design in Table A-5 in Appendix A: “Job Aids.”

## Step Summary

In this step the I/O performance and capacity requirements of the VMs that will run on each virtualization server were used to design the I/O subsystem for the servers.

## Additional Reading

“Storage options for Windows Server 2008 Hyper-V”: <http://blogs.technet.com/b/josebda/archive/2008/02/14/storage-options-for-windows-server-2008-s-hyper-v.aspx>

# Step 9: Design the Network Infrastructure

In the previous step, the storage infrastructure was designed. Most production applications require access to one or more networks to communicate with users and other applications. In addition, the virtualization hosts may require network connections for management, backup, and storage purposes. In this step, the network infrastructure will be designed.

## Task 1: Determine Host Connectivity Requirements

Refer to Step 2 where the requirements for network connectivity were determined for each workload. Windows Server 2008 Hyper-V provides the ability to configure network settings based on workload requirements. The following options exist for defining network access settings for VMs:

* No network connectivity. In this configuration, the VM does not have network access to other VMs or physical servers.
* VM-only (logical) networks. For security purposes, VMs can be configured to communicate only with other VMs that are on the same virtualization host computer.
* Physical network access. This method allows VMs to access one or more physical networks to which the virtualization host is connected.

Design the number and types of network connections that will be required for each virtualization host based on the needs of the VMs that will run on it. The general rule should be to provide each VM with minimal network access based on specific application requirements. Doing so helps ensure security and reduces network traffic.

If Hyper-V live migration will be used to move workloads between hosts (for example, to enable planned downtime on one of those hosts), then the hosts must be connected in a failover cluster on the same LAN segment, with access to a shared LUN.

Record the connections for each host server in Table A-5 in Appendix A: “Job Aids.”

## Task 2: Determine Host Network Throughput Requirements

In Step 2, the network bandwidth required for each workload was established. Translate this information into specific host network requirements based on which VMs will reside on which servers. In the simplest configuration, a single physical host server network interface might be sufficient to handle the needs of all the VMs on a server.

Sum the bandwidth requirement for each host server and record that in Table A-5 in Appendix A: “Job Aids.”

## Task 3: Plan for Network Reliability and Availability

In addition to providing multiple network connections based on functional needs, ensure that physical host network connections meet reliability and availability needs. Many network vendors offer network adapter “port teaming” functionality to provide fault tolerance. This approach works by allowing multiple physical network adapter ports to act as a single port, ensuring reliability and availability. Features like automatic failover and bandwidth aggregation require switch and network-layer support, and specific configurations depend on the standards in use.

For each virtualization host, calculate the number of physical network adapters required. The determinations made for this step may inform changes in the host server design if the selected host chassis cannot support the number of physical network adapters required. Record the number of network adapters for each host server in Table A-5 in Appendix A.

## Validating with the Business

Base the specific design of network connections on application and business requirements.

To validate design decisions, ask the business the following questions:

* Does the design accommodate all the supported user access scenarios? When designing virtual network access, it is often easy to overlook some segments of the user population. Consider factors such as remote access, access from the Internet, and support for branch offices.
* Does the network infrastructure meet security and regulatory compliance requirements? Organizations must ensure that communications and data remain secure to meet these standards. Network design should take into account methods for managing authentication, authorization, and security.

## Step Summary

The network infrastructure was designed in this step. Data was collected and recorded in Table A-5 in Appendix A.

## Conclusion

Virtualization technology can provide dramatic benefits to nearly all aspects of an organization’s IT environment. A successful implementation depends on determining the business and technical requirements for the applications to be deployed to the virtual infrastructure. The process begins by collecting detailed information about the applications to be deployed. Details include specific hardware resource requirements in addition to availability, security, backup, and other considerations.

After all of this information is collected and analyzed, it can be used to design the virtualization host infrastructure. Specific decision points include determining server placement, selecting a server form factor, mapping guests to hosts, and choosing backup and availability approaches. The storage and network infrastructure is designed to support the virtualized host environment.

By following an organized process for designing a virtualization infrastructure, organizations can help ensure that they meet business and technical requirements.

## Additional Reading

In addition to product documentation, the following sites offer supplemental information on the product concepts, features, and capabilities addressed in this guide:

* Windows Server 2008 Hyper-V library: <http://technet2.microsoft.com/windowsserver2008/en/library/5341cb70-0508-4201-a6da-dcac1a65fd351033.mspx>
* Microsoft Virtualization Resources page: <http://www.microsoft.com/virtualization/resources.mspx#documents>
* “What’s New in Hyper-V in Windows Server 2008 R2”: [http://technet.microsoft.com/en-us/library/dd446676(WS.10).aspx](http://technet.microsoft.com/en-us/library/dd446676%28WS.10%29.aspx)
* Microsoft TechNet Server Virtualization forum: <http://forums.microsoft.com/TechNet/ShowForum.aspx?ForumID=583&SiteID=17>. This forum provides a location in which architects, implementers, and users can discuss issues related to designing and deploying Virtual Server.

# Appendix A: Job Aids

Use the job aids in this appendix to enhance the success of planning and designing the Windows Server virtualization process. The grey text represents sample language that illustrates how each task might be completed.

Steps 1 and 2. Table A-1 is used to determine and total the requirements for the virtualization infrastructure.

**Table A-1. Document the Requirements**

| Type of location (enterprise, hub, or satellite) Step 1 | Current locationStep 2, Task 1 | Admin contact Step 2, Task 1 | Operating system Step 2, Task 1 | Application name and version Step 2, Task 1 |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Table A-1. Document the Requirements (continued)**

| Description/purpose (optional) | Application owner (optional) | Is the application supported as virtual? Step 2, Task 2 | Approved by business? Step 2, Task 2 | Segregation required? (If yes, list reason: security, regulatory compliance, or business policy) |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Steps 2 and 4**

**Table A-2. Record Resource Requirements**

| Resource | Workload 1 | Workload 2 | Workload N | Total |
| --- | --- | --- | --- | --- |
| Technique | VMM | Manual |  |  |
| CPU % | 60 | 30 |  |  |
| Memory | 2048 | 1024 |  |  |
| Disk storage capacity | 500 GB | 20 GB |  |  |
| Disk IOps | 750 | 100 |  |  |
| Network bandwidth | 800 mbps | 100 mbps |  |  |
| Number of network adapters | 1 | 1 |  |  |
| Backup | Guest Level | None |  |  |
| Network access required | Private network | Subnet xx.xx.xx |  |  |
| Fault tolerance? | Yes | Yes |  |  |
| Fault tolerance approach | Cluster | Load Balance |  |  |
| Physical isolation requirement | Yes | No |  |  |

**Steps 3 and 7**

**Table A-3. Document the Backup Approach**

| Workload name | Backup approach |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Step 3**

**Table A-4. Document the Fault Tolerance Approach**

| Workload name | Fault-tolerance approach |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Steps 5–9**

**Table A-5. Document the Form Factor for the Hosts**

| Resource | Host 1 | Host 2 | Host N | Total |
| --- | --- | --- | --- | --- |
| Server scaling policy (scale up or scale out) |  |  |  |  |
| Hardware platform |  |  |  |  |
| Server location |  |  |  |  |
| Fault tolerance |  |  |  |  |
| Threshold/buffer |  |  |  |  |
| Workloads assigned |  |  |  |  |
| Backup design |  |  |  |  |
| I/O subsystem |  |  |  |  |
| Network connectivity  |  |  |  |  |
| Host network throughput |  |  |  |  |
| Number of network adapters |  |  |  |  |

# Appendix B: Collecting Performance Data to Determine Resource Requirements

This appendix presents the manual approach for collecting resource requirements for a running workload. An understanding of the process may also be helpful when using MAP or System Center Virtual Machine Manager to collect the resource information.

## CPU

Overcommitting CPU resources can adversely affect all the workloads on the same host server, causing significant performance issues for a larger number of users. Because CPU resource use patterns can vary significantly, measure the CPU demand for each workload over a period when usage will be high. Table B-1 illustrates the Perfmon statistic to collect CPU usage over time.

Table B-1. Performance Monitor Statistics

| Object | Counter | Instance |
| --- | --- | --- |
| Processor | % Processor time | \_Total |

## Memory

Workloads that do not have sufficient memory will experience frequent disk page faults, resulting in decreased performance and additional disk resource use. In contrast, allocating too much physical memory leaves physical hardware resources unused, leading to lower overall host server utilization.

Collect memory use information when the system is running at peak load to ensure that the appropriate amount of memory is allotted. Table B-2 shows the Perfmon statistics that should be collected. For each machine being virtualized, add approximately 24 megabytes of memory to provide enough memory needed by the virtualization host.

Table B-2. Performance Monitor Statistics for Required Memory

| Object | Counter |
| --- | --- |
| Memory | Committed bytes |

## Disk Capacity

Every workload requires disk space to store files such as:

* Operating system storage, including binaries and the paging file.
* Application-related storage space.
* User data storage.
* Databases and other required files.

Planning disk space use is similar for physical and virtual workloads. For existing systems, record the total disk space in use and add a factor for future growth. Record the total amount of disk storage capacity required for each workload.

## Disk Performance

To determine the actual disk performance, measure the IOps over a period of time—that is, the total number of I/O operations that occur per second, and plot this over the time period to determine requirements at peak usage.

By using Perfmon, what the current system is actually using in terms of IOps can be measured. However, that number does not indicate whether the system has a bottleneck in the disk subsystem. To see whether the system is disk-bound, look at the queue length of the physical disk. The queue length should be zero on a well-performing system.

## Disk Performance Counters

Table B-1 provided the Windows Performance Monitor statistics that should be collected. Total the Physical Disk counters from Table B-3 to calculate the I/O usage for each system.

Table B-3. Performance Monitor Statistics for Disk Performance

| Object | Counter | Instance |
| --- | --- | --- |
| Physical disk | Disk Reads/sec | \_Total |
| Physical disk | Disk Writes /sec | \_Total |

## Network

Most workloads require access to one or more networks to ensure communication with other applications and services and to communicate with users. The workload may also require more than one network adapter for any of the following:

* Public network access
* Networks for performing backups and other maintenance tasks
* Dedicated remote-management connections
* Network adapter teaming for performance and failover
* Connections to the physical host server
* Connections to network-based storage arrays

The network connections must provide the required throughput for the traffic that the workload will generate.

However, that number does not indicate whether the system has a bottleneck in the network interface. To check that, look at the queue length of the network adapter. The queue length should be zero on a well-performing system.

## Network Performance Counters

Table B-4 provides the Perfmon statistics that should be collected over time and graphed to record peak usage.

Table B-4. Perfmon Statistics for Network Performance

| Object | Counter | Instance |
| --- | --- | --- |
| Network interface | Bytes Total/sec | (Specific network adapters) |

# Appendix C: IPD in Microsoft Operations Framework 4.0

Microsoft Operations Framework (MOF) offers integrated best practices, principles, and activities to assist an organization in achieving reliable solutions and services. MOF provides guidance to help individuals and organizations create, operate, and support technology services, while helping to ensure the investment in technology delivers expected business value at an acceptable level of risk. MOF’s question-based guidance helps to determine what is needed for an organization now, as well as providing activities that will keep the organization running efficiently and effectively in the future.

Use MOF with IPD guides to ensure that people and process considerations are addressed when changes to an organization’s technology services are being planned:

* Use the Plan Phase to maintain focus on meeting business needs, consider business requirements and constraints, and align business strategy with the technology strategy. IPD helps to define an architecture that delivers the right solution as determined in the Plan Phase.
* Use the Deliver Phase to build solutions and deploy updated technology. In this phase, IPD helps IT pros design their technology infrastructures.
* Use the Operate Phase to plan for operations, service monitoring and control, as well as troubleshooting. The appropriate infrastructure, built with the help of IPD guides, can increase the efficiency and effectiveness of operating activities.
* Use the Manage Layer to work effectively and efficiently to make decisions that are in compliance with management objectives. The full value of sound architectural practices embodied in IPD will help deliver value to the top levels of a business.



Figure 3. The architecture of MOF 4.0

# Appendix D: Windows Server Virtualization in Microsoft Infrastructure Optimization

The Microsoft Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see <http://www.microsoft.com/infrastructure>.) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the IO Model was to develop a simple way to use a maturity framework that is flexible and can easily be used as the benchmark for technical capability and business value.

IO is structured around three information technology models: Core IO, Application Platform Optimization, and Business Productivity IO (see Figure 4). According to the Core IO Model, organizations that are actively pursuing server consolidation for production workloads with virtualization are meeting one of the requirements necessary to move to the Rationalized level. This guide will assist in planning and designing the infrastructure for virtualizing server workloads using Windows Server 2008 Hyper-V.



Figure 4. Mapping of Windows Server virtualization technology into Core IO

# Version History

| Revision | Description | Date |
| --- | --- | --- |
| 2.2 | Minor updates to the architecture diagram and minor format changes. | February 2011 |
| 2.1 | Removed references to Virtual Server 2005, where appropriate, since Windows Server 2008 R2 doesn’t support this.Minor updates to this guide to reflect current IPD template. | July 2010 |
| 2.0 | The number of steps was reduced from 14 to 9.Scope expanded to include virtualization of client OS workloads, including VDI.References provided to tools that collect resource requirements for virtualization and model Hyper-V environments (MAP and VMM).Joe Coulombe added as a contributor. | September 2009 |
| 1.0 | Updated. | February 2008 |
| 1.0 | First release. | November 2007 |

# Acknowledgments

The Solution Accelerators - Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the *Infrastructure Planning and Design Guide for Windows Server Virtualization*. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide.

**Contributors:**

* Jeremy Chapman – *Microsoft*
* Jude Chosnyk – *GrandMasters*
* Joe Coulombe – *Microsoft*
* Charles Denny – *Microsoft*
* Anil Desai – *Studio B*
* Dave Field – *Studio B*
* Michael Kaczmarek – *Microsoft*
* Lex Liao – *Microsoft*
* Robin Maher – *Microsoft*
* Lisa Pere *– Studio B*
* Fergus Stewart – *Microsoft*
* Melissa Stowe – *Microsoft*

**Reviewers:**

* Ben Armstrong – *Microsoft*
* René Scholten – *Capgemini*
* Allen Stewart – *Microsoft*

**Editors:**

* Michelle Anderson – *Extreme Consulting Group, Inc.*
* Vernon Barr *– Volt Technical Services*
* Laurie Dunham – *Extreme Consulting Group, Inc.*
* Kris Maxwell – *Extreme Consulting Group, Inc.*
* Pat Rytkonen – *Volt Technical Services*

## Feedback

Please direct questions and comments about this guide to ipdfdbk@microsoft.com.

We value your feedback on the usefulness of this guide. Please complete the following **Solution Accelerators Satisfaction Survey**, available at: <http://go.microsoft.com/fwlink/?LinkID=132579>, and help us build better guidance and tools.