

Infrastructure Planning  
and Design

Dynamic Datacenter

Version 1.2

Published: April 2010

Updated: November 2011

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

Copyright © 2011 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility.  By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/2.5/> or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

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 Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Hyper-V, SQL Server, Windows, Windows Live, Windows PowerShell, and Windows Server 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](#_Toc299967758)

[Introduction to the Dynamic Datacenter Guide 2](#_Toc299967759)

[Step 1: Determine the Dynamic Datacenter Scope 6](#_Toc299967760)

[Step 2: Design the Virtualization Hosts 11](#_Toc299967761)

[Step 3: Design the Software Infrastructure 15](#_Toc299967762)

[Step 4: Design the Dynamic Datacenter Storage Infrastructure 25](#_Toc299967763)

[Step 5: Design the Network Infrastructure 30](#_Toc299967764)

[Conclusion 34](#_Toc299967765)

[Appendix A: Job Aids 36](#_Toc299967766)

[Appendix B: IPD in Microsoft Operations Framework 4.0 40](#_Toc299967767)

[Version History 41](#_Toc299967768)

[Acknowledgments 42](#_Toc299967769)

# 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 to the business in terms of cost, complexity, and other characteristics.
* Framing the decision in terms of additional questions to the business to ensure a comprehensive understanding of the appropriate business landscape.

The guides in this series are intended to complement and augment the product documentation. It is assumed that the reader has a basic understanding of the technologies discussed in these guides. It is the intent of these guides to define business requirements, then align those business requirements to product capabilities, and design the appropriate infrastructure.

## 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 Dynamic Datacenter.

Benefits for Business Stakeholders/Decision Makers:

* Most cost-effective design solution for an implementation. 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- 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 Dynamic Datacenter Guide

A Dynamic Datacenter is a combination of automation, control, and resource management software with a well-defined topology of virtualization, servers, storage, and networking hardware. The flexibility that this model provides is changing the business landscape by presenting new ways to develop, deliver, deploy, and manage applications and IT infrastructures. The resulting benefits are many, such as the ability to scale as needed, be more responsive to changing market conditions, and provide an opportunity for IT to align deliverables with the organization’s business requirements.

The principles guiding the development of a Dynamic Datacenter include:

* Adopt a service-centric approach. A platform exists to host services and should have service management principles applied. With this approach, business units can directly request a certain service, either new or from a catalog, without having to worry about such low-level considerations as networking, storage, and servers that are provided by the platform.
* Enable agility. A Dynamic Datacenter allows the organization to rapidly deploy new services and scale existing services up or down based on demand. Abstracting the platform from the physical infrastructure enables optimization of resources through shared use, resulting in a more efficient and effective use of the infrastructure, and ultimately driving down costs and improving agility.
* Provide utility. A Dynamic Datacenter provides dial-tone class reliability, meaning that it is expected to be as reliable as a utility service. As more services are deployed into the infrastructure, its reliability becomes critical. In a Dynamic Datacenter, business units can expect their services to be resilient, standard, and predictable, without needing to understand the underlying data center components.
* Minimize human involvement. A well-designed Dynamic Datacenter has the capability to perform operational tasks dynamically, detect and respond automatically to failures, and elastically add or reduce capacity as workloads require.
* Provide cost transparency. Each service delivered by the Dynamic Datacenter can have consumption-based pricing applied to its cost model. This enables business units to obtain a clear and predictable cost associated with the service. The business and IT are then empowered to make trade-off decisions (for example, comparing the cost and quality of internal service versus external).

Using this guide, IT professionals can plan and design an on-premises Dynamic Datacenter infrastructure that is designed for ease of manageability, being confident that critical phases are not omitted from the plan, that the components work together efficiently, and that a solid foundation is established for future expansion.

## Assumptions

To limit the scope of material in this guide, the following assumptions have been made:

* The Dynamic Datacenter will be contained within a single location for a single company. Multi-tenancy considerations are not included, but the architectural principles discussed in this guide will be generally applicable.
* The reader has familiarity with the Microsoft technologies discussed in this guide.

This guide does not attempt to educate the reader on the features and capabilities of Microsoft products. The product documentation covers that information.

The goal of this guide is to present common scenarios, decisions, and practices for implementing a Dynamic Datacenter. Using this guide will help IT professionals plan and design a successful Dynamic Datacenter infrastructure.

A Dynamic Datacenter will require:

* Hardware, in the form of servers, storage, and networking components such as switches, routers, and firewalls.
* Software infrastructure, to virtualize servers and provide the management functionality for deployment, configuration management, software and OS distribution, authentication services, and virtual machine management.

The focus of this guide will be to design a Dynamic Datacenter—including the hosts, storage, and network considerations, as well as the management software—to enable the construction of an infrastructure that is well-managed and effectively coordinated. While the virtual machine workloads provide input in to what the design should look like, the guide focuses on developing a flexible infrastructure to support heterogeneous workloads.

Note   Virtual machine guest planning is a complex topic and is considered a related but separate exercise from the Dynamic Datacenter infrastructure planning. The *Infrastructure Planning and Design Guide for Windows Server Virtualization* provides more information on virtual machine guest planning.

This guide addresses the following decisions and/or activities that need to occur in planning a Dynamic Datacenter. The five steps below represent the most critical design elements in a well-planned Dynamic Datacenter design:

* Step 1: Determine the Dynamic Datacenter Scope
* Step 2: Design the Virtualization Hosts
* Step 3: Design the Software Infrastructure
* Step 4: Design the Dynamic Datacenter Storage Infrastructure
* Step 5: Design the Network Infrastructure

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

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

Figure 1 provides a graphical overview of the steps in designing a Dynamic Datacenter infrastructure.

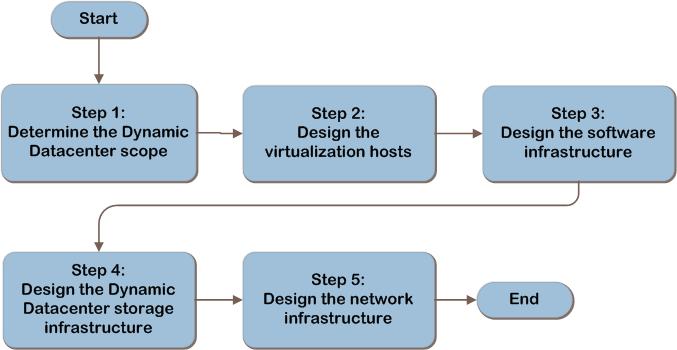


Figure 1. Dynamic Datacenter decision flow

This guide’s design process will include elements to make the data center easily managed in order to reduce the administrative burden and to make it scalable so that the designer is aware of the architectural limits of each component. A Dynamic Datacenter, by definition, should be designed to grow with the organization’s needs; however, the underlying infrastructure components will have finite scalability limits. The boundaries of Microsoft software components will be discussed in this guide, and the scaling limits of the hardware should be validated with the respective vendors to determine when additional hardware will be required.

Resiliency is a goal of the Dynamic Datacenter; however, as with traditional data centers, it is not always necessary to implement redundant components in every level of the design to achieve this goal. Instead, implementation of fault-tolerant measures should be considered at the following levels:

* Operating system and application measures. Before implementing specific component-level and system-level fault-tolerant measures, certain operating system and application-level routes, such as clustering, should be considered.
* Component-level measures. At the server level, use fault-tolerant components such as power redundant supplies, battery backup, Error Correction Code (ECC) memory, and redundant fans. At the network-level, implement fault-tolerant networking components such as redundant switches, routing, and wiring.
* System-level measures. At the system level, use fault-tolerant measures such as redundant access to Active Directory® Domain Services (AD DS) and other management software and redundant storage of data. Also, develop carefully planned backup and monitoring strategies.

In addition, consider these factors: The organization should keep in mind the trade-offs between fault tolerance and cost when designing the infrastructure. The risk mitigation steps that are being taken across the data center should also be considered. And, in some cases, be aware that the required availability levels may be reached even if there is no redundancy for some devices.

Figure 2 represents a simplified graphical overview of the major components of a Dynamic Datacenter.

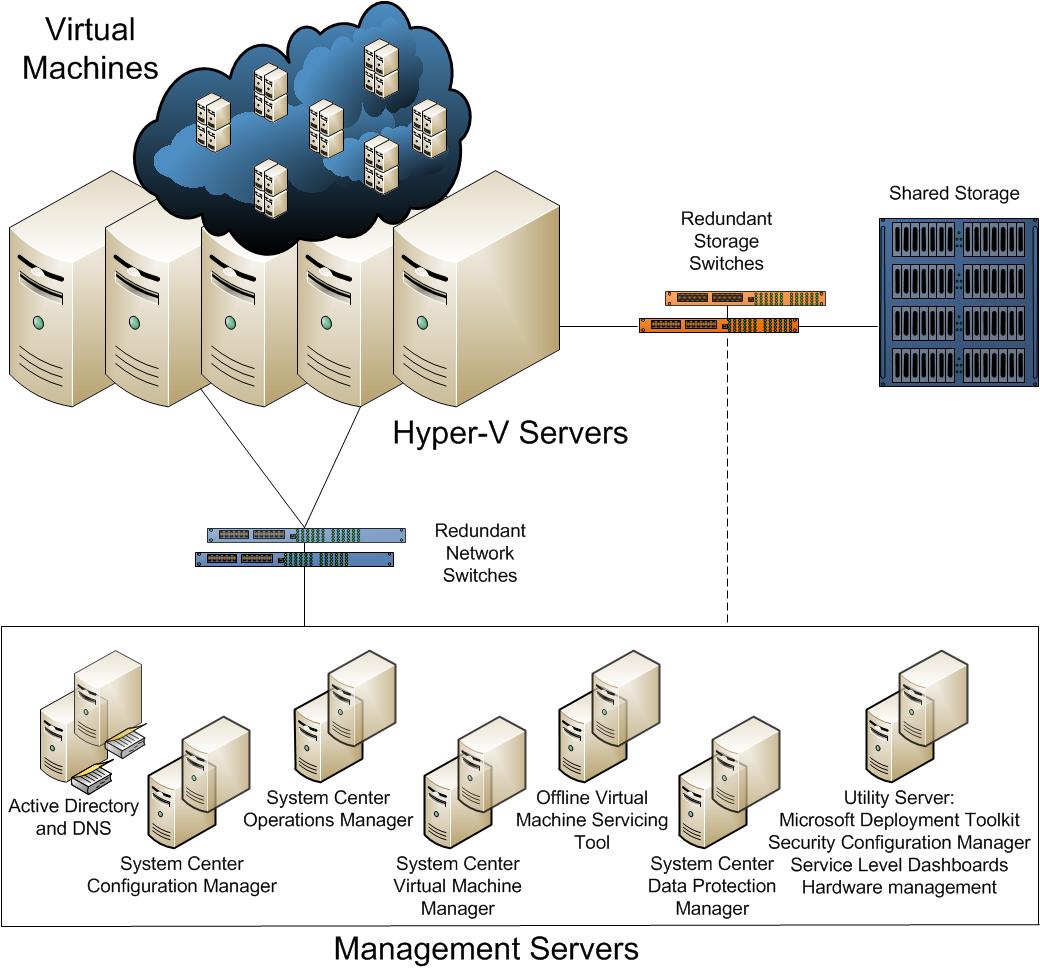


Figure 2. Example Dynamic Datacenter architecture

## Applicable Scenarios

This guide is written to address the needs of the following groups:

* Organizations that want to replace traditional IT operations and move to a flexible consumption-based model, but still require data and assets to reside on-premises.
* Organizations that are entering a new business domain and want to run the supporting IT infrastructure on a separate, scalable, flexible model.
* Organizations that want to rebuild their IT infrastructure from scratch, implementing new policies, procedures, and business processes.

## Out of Scope

This guide does not directly discuss:

* Utility service providers or hosting companies offering cloud computing, cloud computing platforms, cloud platform services, or cloud infrastructure services.
* Windows Live® network of Internet services or other consumer-oriented, cloud services.
* Microsoft Online Services or other third-party software-as-a-service organizations delivering Microsoft infrastructure technologies.
* Virtual machine guest planning. This is a complex topic, and although it informs the scoping in this guide, it is considered a related but separate exercise from planning the Dynamic Datacenter infrastructure. The *Infrastructure Planning and Design Guide for Windows Server Virtualization* (<http://go.microsoft.com/fwlink/?LinkId=160822>) provides additional guidance on this process in Step 2, Task 2, of that guide.

# Step 1: Determine the Dynamic Datacenter Scope

The goal of this step is to define the scope and determine the workloads that will be included in the Dynamic Datacenter project. The business and technical requirements will be further discussed in subsequent steps in order to make appropriate trade-offs in fault tolerance, capacity, and performance.

This document assumes that a workload represents the entire physical server or workstation that currently runs one or more applications. It further assumes that the entire physical server or workstation is to be virtualized, not just the applications that run on it. This approach maps workloads to guests on a 1:1 basis.

NoteFor server workloads, the opportunity exists to combine one or more applications from different servers into a single workload. This work may precede moving the OS to the virtualization platform, but because it can involve additional factors such as confirming application coexistence and compatibility on a shared OS, it is beyond the scope of this document.

Step 1 consists of determining the proposed initial workloads for the Dynamic Datacenter, selecting the workload fault-tolerance approach, and then determining the initial size of the Dynamic Datacenter.

Once this information has been determined, it will then be used in subsequent steps to design the virtualization hosts, management software storage system, and network infrastructure.

## Task 1: Determine the Proposed Initial Workloads for the Dynamic Datacenter

This document assumes that the organization already has existing workloads that can be used as a starting point for sizing; if it is a completely greenfield deployment, an initial starting point should be selected based on estimates of the future workloads.

Begin by analyzing the requirements of the Dynamic Datacenter project. What workloads does the organization anticipate moving to the Dynamic Datacenter? What is the largest single workload? (This will drive the minimum sizing of the virtual machine hosts that will be hosted in the Dynamic Datacenter.) Will there be virtual desktop infrastructure (VDI) workloads hosted by the Dynamic Datacenter as well as traditional server workloads?

Answers to these questions will be used to size the initial physical infrastructure. For existing workloads, in virtual or physical environments, the information can be obtained manually or through assessment tools such as the Microsoft Assessment and Planning (MAP) Toolkit, which is available at [www.microsoft.com/map](http://www.microsoft.com/map). Specific utilization may not be available or easily collectible, but the general characteristics of the workloads’ expected usage may be known—for example, high CPU utilization but low disk IOps (Input/Output per second). For each workload, record the information listed below in Table A-1 in Appendix A: “Job Aids”:

* Application. Record the name of the application used in the workload.
* Operating systems supported by the application. This will be used to determine whether the workload can be run and supported in a virtual machine and whether a Remote Desktop Session Host (RD Session Host) role service can be used to deliver the workload.
* Memory. Record the amount of memory needed by the workload. This will be used to determine the memory requirements for the physical host. Based on density requirements, the server could be scaled up to host a set number of workloads.
* CPU utilization. This information will be used to determine the amount of CPU that each workload will use during peak periods.
* Disk space. The disk space required by each workload will be used in the design of the storage system.
* Disk I/O. This information will be used to determine the maximum disk I/O (input/output) that the storage system will need to meet the workload requirements. Disk I/O is one component of the total storage throughput.
* Networking requirements. Assess the network subnets the workload needs to access and the network throughput required. This will help determine whether the physical hosts may need to have additional network adapters installed to meet network requirements.
* Isolation requirements. A need for the application to be separated from other applications due to regulatory or legal reasons will drive the design of the virtualization host servers.
* Fault-**tolerance requirements.** Determine if the workload has a requirement for fault tolerance. Workloads with similar fault-tolerance requirements may be grouped together to simplify the design.

Once the initial list is assembled, examine the compatibility of each of the candidate workloads with the Dynamic Datacenter. The *Infrastructure Planning and Design Guide for Windows Server Virtualization* (<http://go.microsoft.com/fwlink/?LinkId=160822>) provides additional guidance on this process in Step 2, Task 2, of that guide.

If the workload is not compatible with the virtualization platform for technical or business reasons, indicate that it is out of scope in Table A-1 in Appendix A. When this task is complete, a revised list of initial workloads that can be virtualized will have been defined.

## Validating with the Business

To ensure that the list of applications and their groupings for the Dynamic Datacenter is accurate, ask business stakeholders the following questions:

* Is the list of applications complete? The success of the Dynamic Datacenter design depends on determining the requirements for applications that can be supported in a virtual environment. Review the proposed workload segmentation with the business for any potential issues.
* 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, or that the terms of licensing permit its use in a virtual environment. Planners should understand the basic idea behind virtualization and verify that it is a suitable solution for each workload.

## Task 2: Select the Workload Fault-Tolerance Approach

Workload fault-tolerance requirements may 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 capabilities of the workloads that will run in the virtualized environment. Complete this task for each workload.

### Option 1: Load Balancing

Stateless applications such as website servers can have fault-tolerance support by establishing Network Load Balancing (NLB) across multiple identical instances of the application running on separate servers. 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 assume the load. This provides protection against hardware failure of the host server or failure of a specific virtual machine. Windows Server® 2008 has a software implementation of NLB built in. In addition, NLB provides scalability for stateless applications.

A hardware load balancer 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 virtual machine be added, and the virtual machines should be on different host servers. Contact the application’s manufacturer to verify that NLB is supported.

### Option 2: Virtual Machine-Level Clustering

Many enterprise applications that customers consider to be mission critical have failover capabilities built into them through cluster awareness. These applications were designed and built to run on failover clusters (formerly known as server clusters or MSCS); examples include Microsoft SQL Server® 2008 and Microsoft Exchange Server 2007.   
A cluster can be configured by using multiple virtual machines that have a common shared disk.

Virtual machine-level clustering provides protection against failure of the host server if the virtual machines are clustered across different hosts.

This option requires that at least one additional virtual machine be added on a different host for each workload that is being clustered. Contact the application’s manufacturer or developer to verify that virtual machine-level clustering is supported.

### Option 3: Host-Level Clustering

The physical virtualization hosts can be configured with Microsoft Cluster service as a failover cluster using shared storage. In this configuration, if the host server running the virtual machines fails, the virtualization host and all its virtual machines fail over to another host in the cluster. The cluster would then attempt to restart each virtual machine on the new node of the cluster, but there is no guarantee that each application will restart in the correct manner. Since this approach clusters at the host level and not the workload level, the individual workload applications are not cluster aware and will not necessarily be managed gracefully, which could result in underlying data corruption.

This option requires that at least one additional physical host be added. Contact the application’s manufacturer to verify that host-level clustering is supported.

### Option 4: Application-Level Fault Tolerance

Some applications implement their own specific fault tolerance; an example is SQL Server, which provides log shipping, database mirroring, or replication to supply multiple copies of a database for redundancy and availability. Contact the application’s manufacturer or developer to verify that application-level fault tolerance is supported.

Record the fault-tolerance approach that will be used for each workload in Table A-1 in Appendix A.

## Task 3: Determine the Initial Size of the Dynamic Datacenter

In this task, the initial size of the Dynamic Datacenter will be determined. Consult the list of selected workload candidates, and tally the overall memory, disk storage space, and disk throughput of the initial Dynamic Datacenter in Table A-1 in Appendix A.

The following items should be considered when determining the initial size of the data center:

* **Growth.** The Dynamic Datacenter will be elastic in nature and capable of growing as resources require; however, a starting point for the size of the infrastructure must be determined, plus an additional buffer, perhaps as a percentage of the initial size for expansion. This number should be based on the business’s expectations of growth.
* **Fault tolerance.** Hardware failures will occur, so the estimate should include the additional infrastructure required for fault tolerance.

Once the initial Dynamic Datacenter is in operation, the management and reporting capabilities can provide capacity reporting and metrics for accurate analysis.

## Validating with the Business

To ensure that the list of applications and their groupings for the Dynamic Datacenter is accurate, ask business stakeholders the following questions:

* What is the timeline for moving to a Dynamic Datacenter? Validate the scale and expected timeline with the business. It may be that not all workloads need to be activated from the start and that a gradual, prioritized approach to moving workloads to the Dynamic Datacenter can be taken. Such an approach allows the business to gain confidence in the Dynamic Datacenter before it moves to full production.
* What is the risk tolerance of the business for the chosen fault-**tolerance approach?** Careful consideration should be given to the fault-tolerance approach for each workload. The business should understand the risk involved of possible data loss or interruption of business, depending on the fault-tolerance approach chosen for the workloads involved.
* Are there applications on the list that are already in virtual machines? If so, confirm that they are able to be moved over to the Dynamic Datacenter.
* Are there isolation requirements for the Dynamic Datacenter? Corporate policies or government regulations may require separate servers for certain types of data or for certain parts of the organization.

Refer to the MOF Business/IT Alignment Service Management Function at <http://technet.microsoft.com/en-us/library/cc543303.aspx> to learn more about how to better align business and IT strategy to ensure that IT services provide business value.

## Step Summary

In this step, the scope of the Dynamic Datacenter project was determined, including identification of the workloads to be included in it. The proposed workloads were selected, and whether those workloads are compatible with the virtualization platform was determined. Additionally, it was confirmed whether the operating systems and applications’ suppliers will support and allow each workload to be licensed for use in a virtual machine. The fault-tolerance approach was determined for each workload and, finally, the initial size of the data center was determined. The data gathered in this step was recorded in Table A-1 in Appendix A. This data will be used in subsequent steps to design the virtualization hosts, storage system, and network infrastructure, as well the infrastructure and management software services.

## Additional Reading

* Microsoft Assessment and Planning Toolkit: [www.microsoft.com/map](http://www.microsoft.com/map)
* *Infrastructure Planning and Design Guide for Windows Server Virtualization*: <http://go.microsoft.com/fwlink/?LinkId=160822>
* Microsoft Operations Framework: [www.microsoft.com/mof](http://www.microsoft.com/mof)

# Step 2: Design the Virtualization Hosts

Now that the scope of the project has been decided and whether the workloads will be suitable for virtualizing has been determined, the next step will be to determine which workloads might be grouped together based on having similar requirements. The hardware configuration for the virtualization hosts will be selected, and the network connectivity for the virtualization hosts will be determined. The goal of this step is to design hosts that meet the capacity, performance, placement, and fault-tolerance requirements of the organization.

As discussed in the guide’s introduction regarding balancing cost with fault tolerance, some hardware options, such as redundant power supplies or fans, can be relatively inexpensive on a per unit basis; however, these options can add significant cost when purchased for an entire data center. Given that other fault-tolerance choices may mitigate the need for these options, an over-arching view of the data center’s fault-tolerance capability should be taken in order to make the most effective use of investments.

The *Infrastructure Planning and Design Guide for Windows Server Virtualization* (<http://go.microsoft.com/fwlink/?LinkID=160822>) should be used in conjunction with this guide to complete this step.

## Task 1: Group the Workloads

Refer to the information collected in Table A-1 in Appendix A, including business and technical requirements, to determine which workloads can be run together on which virtualization hosts. Group workloads based on similarities in:

* Isolation requirements. Separate workloads that must be isolated physically or administratively 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 share fault-tolerance requirements. This may enable a single fault-tolerance solution to be applied to each group, simplifying operations. For more details, refer to Step 4 in the IPD guide for Windows Server Virtualization (<http://go.microsoft.com/fwlink/?LinkId=160822>).

Use Table A-1 in Appendix A to identify and group workloads that have similar requirements; then tally the requirements of each grouping in Table A-2 in Appendix A. Examine the groupings to determine if the workloads can run concurrently on the same virtualization host servers. The organization may choose to deploy a tiered configuration for the virtualization host servers where basic, mid-range, and high-end servers are made available to host the workloads.

## Task 2: Design the Hosts’ Hardware Configurations

In this task, the hardware configuration for each virtualization host will be designed (excluding storage and network designs addressed in Step 4 and 5). An assessment of the risk factors should be completed as the design decisions are made. For example, installing fewer but more powerful servers will result in more workloads being simultaneously affected by an outage. Standardizing on a brand and model of server may allow for volume purchasing and a reduction in the variety of spare parts that need to be kept on hand.

For each workload grouping, determine:

* **Host-level clustering.** If it was determined in Step 1, Task 2, that the fault-tolerant approach used for the workloads would be host-level clustering, decide how many servers will be in each cluster.
* **Form factor.** Will blade or standard rack-mount servers be used? The options for rack-based servers versus blade servers can force customers to make significant trade-offs between density, features, memory, capacity, and in some cases, additional power and cooling. Blade and 1U servers may have less expansion space available, which may be important if additional network adapters are added to achieve the required number of network ports.
* **CPU.** A combination of processors and cores should be implemented in each server to sufficiently support the workload grouping’s requirements as defined in Step 2, Task 1.
* **Memory.** An ample amount of RAM will need to be available for the virtual machines on each host as defined in Step 1, Task 1. Redundant memory can be implemented to protect against failure of a memory bank, and cost should be balanced against other fault-tolerance measures in place.
* **Power supplies**. Determine whether redundant power supplies will be implemented in each host, or if other fault-tolerant mechanisms such as clustering are sufficient to maintain uptime requirements. If redundant power supplies are used, each power supply should be connected to separate power sources, or the source will become a single point of failure.

Using the information from Step 1, and Step 2, Task 1, and excluding network and storage requirements as these will be determined in later steps, consult the IPD guide for Windows Server Virtualization (<http://go.microsoft.com/fwlink/?LinkID=160822>) to assist in designing the virtualization hosts using this as input:

* The workload scope determined in Step 1 of this guide should be transferred to Step 5 of the Windows Server Virtualization guide.

The organization should plan to support the peak load of each workload, plus include a buffer to ensure that the host system can handle the maximum loads at all times.

Record the information from this step in Table A-3 in Appendix A. Then, record the total number of physical servers in every field of Table A-4 in Appendix A (except for virtual machines managed by Microsoft System Center Virtual Machine Manager, which should have the total number of virtual machines in the Dynamic Datacenter, not hosts). This will serve as the starting point for the management software scaling in Step 3.

## Task 3: Determine Host Network Connectivity Requirements

In this task, the network connectivity for the virtualization hosts will be determined. The following options exist for defining network access settings for virtual machines:

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

When designing network connectivity to enable the Dynamic Datacenter to be well-managed, the virtualization hosts have the following specific networking requirements:

* Support for 802.1Q virtual local area network (VLAN) tagging, to provide network segmentation for the core infrastructure and workloads.
* Optionally, remote out-of-band management capability, to monitor and manage servers by remote control over the network regardless of whether the machine is turned on.
* Optionally, support for Pre-Boot Execution Environment (PXE) version 2 or later, to facilitate automated server provisioning.

A minimum of one network adapter will be needed; however, additional network adapters may be beneficial in order to:

* Dedicate one network adapter on each host server for network I/O and management of the host itself, such as for host OS patching.
* Dedicate at least one network adapter on each host server for an isolated VLAN to manage the virtual machine update process. This will inform decisions in Step 3, Task 5, for the Offline Virtual Machine Servicing Tool.
* Provide a network adapter for backup operations. This might be shared with other functions, such as the virtual machine update process or host OS patching.
* Dedicate one network adapter on each host server to the private (heartbeat) network, and cluster shared volume communications if the host is part of a failover cluster.
* Dedicate at least one network adapter on each host server for guest virtual machine network I/O. Also refer to the network throughput requirements gathered in Step 1 to determine whether any of the workloads will need their own dedicated network adapters, rather than sharing with other guest virtual machine workloads.
* Dedicate specialized “lights out” management network adapters to allow for remote operations such as rebooting, shutdown, troubleshooting, and alarm monitoring even if the host OS is unresponsive.

Additionally, determine whether any of the network connections above will need to have teamed network connections, where two or more specialized network adapters are set up as a "team" for fault tolerance. When configured for fault tolerance, the backup network adapter takes over if there is any problem with the first one, which could also be a cable failure or port failure at the other end. For load balancing, teaming network adapters enables the workload to be distributed among all adapters. If teaming is implemented, the teamed connections should be distributed among multiple switches to eliminate single points of failure.

Determine how many network adapters will be needed in each virtualization host by analyzing the requirements listed above. Tally the number of network ports and identify on which subnets or VLANs they will be connected to, and record the answers in Table A-3 in Appendix A. This information will be used in later steps to design the network switch and the storage infrastructure for the Dynamic Datacenter.

## **Validating with the Business**

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

To validate design decisions, ask business stakeholders 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 such factors 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 in order to meet these standards. Network design should take into account methods for managing authentication, authorization, security, or data encryption requirements.

## Step Summary

In this step, it was determined which workloads can be grouped together, and the hardware configuration for the virtualization hosts was selected. Also, the network connectivity for the virtualization hosts was determined. All of the data gathered in this step was recorded in Tables A-1, A-2, A-3, and A-4 in Appendix A.

## Additional Reading

* Windows Server catalog: [www.windowsservercatalog.com](http://www.windowsservercatalog.com/)
* Windows Server 2008 Hyper-V library: <http://technet2.microsoft.com/windowsserver2008/en/library/5341cb70-0508-4201-a6da-dcac1a65fd351033.mspx>
* Microsoft Virtualization: [www.microsoft.com/virtualization/](http://www.microsoft.com/virtualization/)
* Hardware Considerations: <http://technet.microsoft.com/en-us/library/cc816844(WS.10).aspx>

# Step 3: Design the Software Infrastructure

In the previous step, the hosts were designed to meet the capacity, performance, placement, and fault-tolerance requirements of the organization. It was determined which workloads might be grouped together, and the hardware configuration for the virtualization hosts was selected. Also, the network connectivity for the virtualization hosts was determined. In this step, the Dynamic Datacenter software infrastructure will be designed.

To maintain the resiliency and availability of the Dynamic Datacenter, infrastructure and management software will be required for conducting the following activities:

* Directory and authentication services
* Virtual machine management
* Configuration management
* Software distribution, inventory, and patch management
* Operating system deployment
* Event monitoring and collection
* Remote desktop services (if needed)
* Hardware management

Unless the organization is beginning from a completely new infrastructure, it will likely already have some, if not all, of this infrastructure and management software in place. If third-party software is currently in use by the organization, this step can also be used to evaluate whether it will meet their needs in the Dynamic Datacenter.

It is important to note that the focus of this step will be to design a management infrastructure that supports the Dynamic Datacenter virtualization hosts, network, and storage infrastructure. However, the organization may elect to use the management infrastructure to also manage some of the virtual machine workloads. This decision will be made in Task 2.

The infrastructure and management servers should adhere to the same service level expectations as the workloads that are hosted in the Dynamic Datacenter; thus these servers should be monitored and managed with the same rigor used for the other components. Many of the management solutions can run in a virtual environment; but whether physical or virtual servers are used, an independent set of servers should be set up so that the management and monitoring systems are separated from the systems being monitored.

Once the organization’s software management requirements have been determined, the requirements will then be transferred from this guide to an applicable Infrastructure Planning and Design guide to design the infrastructure for each software component, ensuring that the assembled architectures will all fit together appropriately and coherently. The corresponding IPD guides that will be used are:

* *System Center Configuration Manager 2007 SP1 with R2*
* *System Center Data Protection Manager 2007 with SP1*
* *System Center Operations Manager 2007*
* *System Center Virtual Machine Manager 2008 R2*
* *Windows Server 2008 and Windows Server 2008 R2 Active Directory Domain Services*
* *Windows Server 2008 R2 Remote Desktop Services*

The guides are available at [www.microsoft.com/ipd](http://www.microsoft.com/ipd).

## Task 1: Decide Whether Existing Software Deployments Will Be Utilized

The first task will be to decide whether to utilize the existing software or to implement new software to support the Dynamic Datacenter. Particular attention should be paid to the scaling limits of each technology and any special considerations required to meet the fault-tolerance, capacity, and performance needs of a Dynamic Datacenter.

Using a Dynamic Datacenter presents the opportunity to design the infrastructure components to deploy new service management processes. It may be that the current environment is not optimized to take full advantage of today’s service management technologies, so this can present the opportunity to shed legacy systems and optimize processes.

Review the current deployments of the management software; then ask the following questions:

* Do the existing services provide all the required functionality efficiently?
* Do the existing services include the level of fault tolerance and resiliency that will be needed by the Dynamic Datacenter?
* How much external influence does the organization want on this new environment? Will the Dynamic Datacenter be managed by a separate team instead of the traditional IT organization?
* Is the organization satisfied with the current business processes and service management in place, or do they wish to restructure the IT systems?
* Is a separate environment needed for business or regulatory reasons?

The Microsoft Operations Framework (MOF) “Service Alignment Management Review” and “Business/IT Alignment Service Management Function” documents can aid the organization in conducting a deeper discussion of these questions.

Decide whether existing services may be used, or if all new core infrastructure and management components will be designed. This decision will be used in later steps as each management component is designed to determine the level of integration with existing components.

## Task 2: Decide Whether Guest Workloads Will Be Included

As a related but separate topic to Task 1, the organization must decide whether any of the guest workloads will be included in the scope of the management software. Detailed virtual machine guest planning is not included in the scope of this guide, but some organizations may decide that they want to use the same management infrastructure for the guest workloads. Not all virtual machines may need the full suite of software—for example, development virtual machines may not need operations management alerting.

Determine whether the management infrastructure will be set up to manage the Dynamic Datacenter hosts only, or if virtual machines themselves will also be included in the scope of the management infrastructure, and if so, update the counts in Table A-4 in Appendix A accordingly.

## Task 3: Design the Directory and Authentication Services

Directory and authentication services are required for both the management of the core infrastructure and operation of the virtual host servers. In addition, name resolution services will be required to locate the directory and authentication servers. These services will be designed in this task. As with all the management components, these roles should reside on servers that are not virtualized within the Dynamic Datacenter so that they will remain running even if hosts are experiencing problems.

The Microsoft offering that best meets these needs is Active Directory Domain Services (AD DS) and Domain Name System (DNS).

To provide reliable and efficient access to AD DS and DNS, the domain controllers, global catalog servers, and DNS servers will need to be well protected from possible failures. Ensure that more than one DNS server exists on the network for fault tolerance. If the primary DNS server fails, a secondary server will be able to direct users to the correct servers. Integrate Windows Server 2008 DNS zones into AD DS. In this scenario, each domain controller becomes a potential DNS server.

To initially determine the load on the domain controllers, refer to the count in Table A-4 of Appendix A. Unless the virtual machine workloads are being included, the Dynamic Datacenter itself will have a limited number of users (generally, only data center staff), with only the Hyper‑V® and other management software servers authenticating, so the utilization of these domain controllers for the Dynamic Datacenter can be expected to be very low. AD DS and DNS limitations won’t be an issue until the Dynamic Datacenter contains an extremely large number of physical computers; so in terms of scaling, two domain controllers should be able to handle the authentication needs of most initial Dynamic Datacenters.

Refer to the decision made in Task 1 about whether the organization will be integrating with existing services. The organization will need to decide whether to implement a new forest and new domain or to use an existing forest and/or domain. Implementing multiple forests and/or domains increases the complexity of managing the environment. An Active Directory environment for the Dynamic Datacenter will require fewer changes than a typical production network as it will not have as many user and computer accounts.

The Dynamic Datacenter is scoped in this document to be in a single location. Using that as a premise, consult the *Infrastructure Planning and Design Guide for Windows Server 2008 and Windows Server 2008 R2 Active Directory Domain Services* (<http://go.microsoft.com/fwlink/?LinkId=160829>) to design the Active Directory infrastructure with these inputs:

* In Step 1 of the Active Directory Domain Services IPD guide, the number of forests will be one, unless the business has requirements for more as outlined in the Active Directory Domain Services IPD guide.
* In Step 2, the number of domains will be one, unless the business has other requirements for additional domains as outlined in the Active Directory Domain Services IPD guide.
* In Step B2, the number of domain controllers can be as few as two, for fault tolerance. These may be virtualized; however, they should be in a separate virtual environment outside the Dynamic Datacenter. Note that deploying a domain controller in a virtual environment adds more requirements and considerations. See the “Additional Reading” section at the end of this step for more information.
* In Step C1, the number of sites will be one.

Domain controllers may also provide DNS.

Because the servers implemented for AD DS and DNS will need to be included in the configuration management and operations management scopes, add these to the counts in Table A-4 in Appendix A accordingly. Note that if servers are used for multiple purposes (for example, both OS deployment and hardware management), count those servers once.

## Task 4: Design the Virtual Machine Management Infrastructure

To design a Dynamic Datacenter for manageability, a virtual machine management solution with the following capabilities will be required:

* **Virtual machine library.** Contains a catalog of virtual machine hardware configurations, operating system customizations, software installation media, and individual virtual machines.
* **Provision server and desktop workloads.** The Dynamic Datacenter will need to repetitively and consistently deploy server and/or desktop virtual machines.
* **Security and access control.** Role-based permissions and rights allow fine tuning of administrative tasks, with support for delegated administration and self-service user roles.
* **Resource allocation.** The CPU, memory, network, and storage resources are presented as physical components to virtual machines. Individual templates of virtual machine hardware configurations should be centrally stored in the virtual machine library to be dynamically allocated when needed.

The Microsoft offering that best meets these requirements is System Center Virtual Machine Manager (VMM). Beginning at Step 3 in the *Infrastructure Planning and Design Guide for System Center Virtual Machine Manager 2008 R2* (<http://go.microsoft.com/fwlink/?LinkId=160869>), design the virtual machine management infrastructure with this input:

* The number of VMM clients as recorded in Table A-4 of Appendix A.

Scalability limits for a VMM deployment to support the Dynamic Datacenter are the same as for traditional deployments, that is:

* One VMM instance can support up to 400 virtual machine hosts and 8,000 virtual machines.
* A VMM instance can only connect to one Microsoft System Center Operations Manager 2007 management group. If VMM hosts are located in different Operations Manager 2007 management groups, then separate VMM instances will be required in order to provide reporting integration in the VMM console. Each VMM instance will be able to provide reports for the management group to which it is connected.
* Multiple VMM instances, however, can connect to a single Operations Manager 2007 management group, so having multiple VMM instances is not by itself a driver to implementing multiple management groups.

At the end of this task, having used the IPD guide for System Center Virtual Machine Manager, the organization will have determined the number of VMM servers required, including each server’s size, hardware configuration, placement, and connectivity.

Because the VMM servers should be included in the configuration management and operations management scope, increment the counts in Table A-4 in Appendix A to include these.

## Task 5: Design the Configuration Management and Deployment Infrastructures

The Dynamic Datacenter will require a system to provide for the initial deployment, patching, and upgrading of the hypervisor. This task is based on the Windows 2008 R2 Hyper-V edition.

The following capabilities are required and will be designed in this task:

* **Inventory and asset management.** Provides the automatic discovery of hardware added to the Dynamic Datacenter, as well as any changes to the physical components.
* **Bare metal installation.** This is required for the deployment of the hypervisor, as well as supporting core infrastructure and management services.
* **Software deployment and patch management.** Deploying current security, critical operating system, and other software updates is essential to providing stability and consistency throughout the library.
* **Configuration monitoring.** The ability to check the current configuration against the desired configuration can help ensure operational efficiency, overcome security issues, and maintain the stability of the server and network infrastructure.
* **Reporting.** Reporting on life-cycle management status and activity allows the Dynamic Datacenter to determine whether an asset should be flagged for retirement based on rules, as well as provides some of the auditing required for compliance to regulations like Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and the National Association of Securities Dealers (NASD).

The Microsoft offerings that best meet these requirements are System Center Configuration Manager, Microsoft Deployment Toolkit, and the Offline Virtual Machine Servicing Tool.

### System Center Configuration Manager 2007

Refer to the *Infrastructure Planning and Design Guide for System Center Configuration Manager 2007 SP1 with R2* (<http://go.microsoft.com/fwlink/?LinkId=160873>) to design the configuration management infrastructure using the following inputs:

* In Step 1, the projected scope for the Configuration Manager 2007 infrastructure will be the number of physical devices that will be managed in the Dynamic Datacenter, plus any virtual machine guests identified in Task 2 of this guide for inclusion.
* In Step 2, the following Configuration Manager Site System roles will be required:
* Operating System Distribution
* Software Distribution
* Software Updates
* Hardware Inventory
* Software Inventory
* Asset Intelligence
* Desired Configuration Management
* Wake On LAN
* Out of Band Management
* Remote Control
* In Step 3, the number of Configuration Manager sites that will be required will be one.

The scalability and limits for the Dynamic Datacenter solution are the same as for a traditional Configuration Manager deployment and are described in the IPD guide for Configuration Manager in Step 4, Task 1. It is unlikely that these scale limits will be an issue until the Dynamic Datacenter contains an extremely large number of physical computers. As such, the Configuration Manager infrastructure being designed in this guide will only be managing the virtualization hosts and other management software servers, and not the virtual machine guest workloads.

In addition, extend the functionality of Configuration Manager by implementing the following:

* The Microsoft System Center Configuration Manager 2007 Dashboard provides an easy-to-use, customizable website interface to track application and operating system deployments, security updates, the health status of computers, and IT compliance with key regulations. It is available at <http://technet.microsoft.com/en-us/library/ff369719.aspx>.
* The Security Compliance Management Toolkit Series helps organizations meet security and compliance requirements by providing guidance, tools, configuration packs, and additional reporting functionality. For more information, see <http://technet.microsoft.com/en-us/library/cc677002.aspx>.

### Microsoft Deployment Toolkit 2010

The Microsoft Deployment Toolkit (MDT) 2010 provides technology for performing automated deployments of Windows® operating systems and applications that run on Windows. MDT 2010 can help automate:

* Deployment of Windows Server 2008 R2 and the Hyper-V server role to physical computers that will act as hosts to the virtual machines.
* Deployment of Windows Server 2008 R2 to virtual machines, which can be used to create virtual machine templates using Virtual Machine Manager.
* Customization of existing virtual machines, such as adding applications, changing configuration settings, adding server roles, or adding role services.

MDT 2010 is installed and configured on a computer that is connected to the Dynamic Datacenter. The computer running MDT 2010 can run any current Windows client or Windows server operating system.

Determine if MDT 2010 will be used to automate deployment, and if so, which computers will be used for MDT 2010.

### Offline Virtual Machine Servicing Tool

The Offline Virtual Machine Servicing Tool helps organizations maintain virtual machines that are stored offline in a VMM library. The tool provides a way to keep offline virtual machines up-to-date so that bringing a virtual machine online does not introduce vulnerabilities into the organization’s IT infrastructure.

The Offline Virtual Machine Servicing Tool must be installed on the same server as the VMM Administrator Console. (The Administrator Console provides Windows PowerShell® support.) The VMM server and library components can reside on the same server or on one or more additional servers.

In Step 2, Task 3, for designing the network connectivity for the virtualization hosts, a decision was made whether a network adapter would be dedicated for an isolated VLAN in order to manage the virtual machine update process. The isolated VLAN approach is recommended for security reasons because stored virtual machines could be in an unhealthy state and might attack the network or be susceptible to attack themselves. Make sure that all of the servers or server roles involved in the update process can access this VLAN. The following figure is one example.

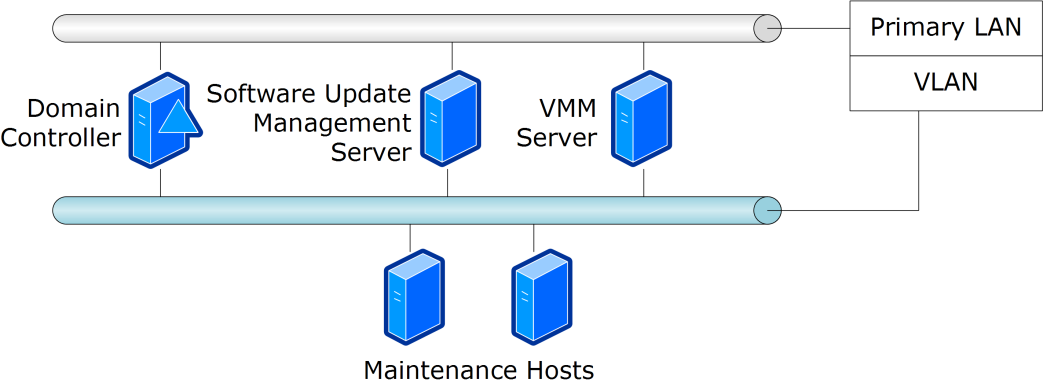


Figure 3. Example of an isolated virtual LAN used for updating virtual machines

For more information on planning the Offline Virtual Machine Servicing environment, download the Solution Accelerator at <http://technet.microsoft.com/en-us/library/cc501231.aspx>.

Determine which servers will be used to manage the Offline Virtual Machine Servicing Tool, and if separate maintenance hosts will be implemented. If needed, revisit the decision made in Step 2, Task 3, for whether a network adapter will be dedicated for updating virtual machines and the corresponding port count.

At the end of this task, the organization will have determined:

* The server roles, role placement, databases, and connectivity of the Configuration Manager infrastructure.
* The number of Configuration Manager hierarchies required, and how many sites are required within each hierarchy.
* The designated servers that will be implemented to support the Microsoft Deployment Toolkit.
* Whether an isolated VLAN will be implemented and which server will be used for the Offline Virtual Machine Servicing Tool.

Record how many servers will be used for configuration management, MDT 2010, and the Offline Virtual Machine Servicing Tool in Table A-4 in Appendix A so that they may be included in the scopes of other infrastructure components.

## Task 6: Design the Event Monitoring and Collection Infrastructures

In this task, a system to provide event monitoring and collection for the Dynamic Datacenter will be designed. A monitoring system can alert the organization when certain components are near or at capacity, or when failures occur. Continuous monitoring of the network, applications, data, and hardware is essential for high availability. Software monitoring systems enable the organization to determine the health of the system and identify potential issues before an error occurs. The monitoring system should have the following capabilities:

* **Reporting and auditing.** With resources and virtual workloads being moved and re-allocated within the Dynamic Datacenter, it is imperative to have in-depth analysis and tracking available for all events and their resulting actions.
* **Infrastructure monitoring via hardware vendor integration.** Infrastructure components, such as power, cooling, and physical rack access, can be monitored and dynamically managed.
* **Remediation.** Virtual workloads are monitored for resource usage, and then an action can be enacted based on the type of resource that is affected. For instance, when physical host CPU resources are being depleted, a remediation action is triggered to automate the seamless movement of virtual machines to other clustered hosts with available resources.
* **Dynamic resource management.** Services provided by the Dynamic Datacenter can have additional resources allocated to them dynamically, based on pre-defined thresholds and actions.
* **Chargeback (optional).** Precise monitoring of resources can allow for usage-based billing if the organization requires this capability. Some hardware vendors provide this capability as part of their management packs, allowing for any management solution to tap into the raw data to provide chargeback services.

The Microsoft offering that best meets these requirements is System Center Operations Manager 2007. Use the *Infrastructure Planning and Design Guide for System Center Operations Manager 2007* (<http://go.microsoft.com/fwlink/?LinkId=160985>) to design the event monitoring and collection infrastructure using the following inputs:

* In Step 1, the scope of the System Center Operations Manager 2007 project is the Dynamic Datacenter, plus any virtual machine guests identified in Task 2 of this guide for inclusion.
* In Step 2, Task 1, the necessary management packs include Hyper-V, Configuration Manager, Operations Manager, SQL Server, Active Directory Domain Services, Power Management, and any other packs for the core components of the Dynamic Datacenter infrastructure, as well as any products specific to the organization’s hardware and software requirements.
* In Step 4, the number of management groups will be one, unless dictated by the reason described in that step, such as more than 6,000 agents or administration or security requirements.
* In Appendix A of the Operations Manager guide, the number of workstations, member servers, and domain controllers can be transferred from Table A-4 in Appendix A of this guide.

Practical design limits, including sizing and scalability of an Operations Manager deployment for the Dynamic Datacenter, will be the same as for traditional deployments and are described in “Operations Manager 2007 R2 Supported Configurations” at <http://technet.microsoft.com/en-us/library/bb309428.aspx>. At the conclusion of this task, the organization will have determined the server roles, role placement, databases, and connectivity of the Operations Manager infrastructure. Update the counts in Table A-4 in Appendix A accordingly.

In addition, the Service Level Dashboard for System Center Operations Manager 2007 integrates with Operations Manager to monitor business-critical applications. The dashboard evaluates an application or group over a time period, determines whether it meets the defined service level commitment, and displays summary data about the service levels. It is available at <http://technet.microsoft.com/en-us/library/dd630553.aspx>.

## Task 7: Design the Hardware Management Solution

The Dynamic Datacenter will need a management system to monitor for faults in the server, storage, or network hardware components. The purpose of this task is to determine the requirements for a hardware management solution that will integrate with the management infrastructure. The hardware management solution should provide the ability to:

* Obtain hardware health and inventory details and provide automated discovery and identification of any new assets added to the Dynamic Datacenter.
* Provide out-of-band management.
* Remotely turn on or restart a device.
* Receive alerts for memory faults, temperature spikes, storage array and hard drive problems, chassis intrusions, and network device faults.
* Remotely update the BIOS or firmware, preferably with scripts that can be used with System Center Configuration Manager.
* Provide open interfaces that can natively integrate with System Center Operations Manager to provide monitoring data.
* Provide native high availability of the hardware management software or utilize technologies such as failover clusters.

Most hardware vendors offer a solution that will provide this functionality for their products. If servers are required for the hardware management solutions, design them according to the vendor’s recommendation with the Dynamic Datacenter’s fault-tolerance, capacity, and performance requirements in mind, and then increment the server count in Table A-4 in Appendix A accordingly.

## Step Summary

The focus of this step was to design a management infrastructure that supports the Dynamic Datacenter. The requirements needed by each component were listed and then the corresponding Microsoft offering was designed.

A running tally of the number of clients of each management infrastructure was maintained throughout the step in Table A-4 in Appendix A.

First, it was decided whether existing services will be used or if all new core infrastructure and management components will be designed; then it was decided whether guest workloads will be included in the design.

Each management software component was evaluated in turn, including any specific requirements needed to improve the manageability of the Dynamic Datacenter. Scoping from this guide was transferred to the relevant Infrastructure Planning and Design guide for a more detailed design process.

## Additional Considerations

The item described below is generally outside the scope of the primary infrastructure design; however, it is included here as an additional consideration that the architect may need to take into account.

### VDI

If it was determined in Step 1, Task 1, that virtual desktop infrastructure (VDI) workloads will be hosted in the Dynamic Datacenter, software will need to be implemented to provide the entry point for end users to the Dynamic Datacenter. Remote Desktop Services is the Microsoft offering that enables the brokering of hosted desktop connections as well as access through a website-based portal.

The *Infrastructure Planning and Design Guide for Windows Server 2008 R2 Remote Desktop Services* (<http://go.microsoft.com/fwlink/?LinkID=177881>) can be used to assist in designing the Remote Desktop Services infrastructure to support the Dynamic Datacenter. The roles that will be required to enable VDI are:

* Remote Desktop Connection Broker or third-party connection broker.
* Remote Desktop Web Access, unless clients are running Windows 7.
* Remote Desktop Virtualization Host on the machine that hosts the virtual machines.
* Virtualization Redirector.

RD Virtualization Host requires and integrates with the Hyper-V role to provide VDI virtual machines that can be used as personal virtual desktops or virtual desktop pools.

The required server roles can be either implemented as a server alongside the virtualization hosts and management servers or as a virtual workload within the Dynamic Datacenter.

## Additional Reading

* *Infrastructure Planning and Design Guide for Microsoft System Center Configuration Manager 2007 SP1 with R2*: <http://go.microsoft.com/fwlink/?LinkId=160983>
* *Infrastructure Planning and Design Guide for Microsoft System Center Data Protection Manager 2007 with Service Pack 1*: <http://go.microsoft.com/fwlink/?LinkId=160984>
* *Infrastructure Planning and Design Guide for Microsoft System Center Operations Manager 2007*: <http://go.microsoft.com/fwlink/?LinkId=160985>
* *Infrastructure Planning and Design Guide for Microsoft System Center Virtual Machine Manager 2008 R2*: <http://go.microsoft.com/fwlink/?LinkId=160986>
* *Infrastructure Planning and Design Guide for Windows Optimized Desktop Scenarios*: <http://go.microsoft.com/fwlink/?LinkId=160803>
* “Failover Clusters”: <http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx>
* Knowledge Base article 888794 “Things to consider when you host Active Directory domain controllers in virtual hosting environments”: <http://support.microsoft.com/kb/888794>
* An Overview of Windows Clustering Technologies: Server Clusters and Network Load Balancing: <http://technet.microsoft.com/en-us/library/cc739634(WS.10).aspx>
* “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>
* Understanding When to Create a Forest Trust: <http://technet.microsoft.com/en-us/library/cc771397.aspx>
* Hyper-V Security Guide: <http://www.microsoft.com/downloads/details.aspx?FamilyID=2220624b-a562-4e79-aa69-a7b3dffdd090&displaylang=en>
* Planning for Backup: <http://technet.microsoft.com/en-us/library/dd252619(WS.10).aspx>
* Microsoft Operations Framework: [www.microsoft.com/mof](http://www.microsoft.com/mof)
* MOF Business/IT Alignment Service Management Function: <http://technet.microsoft.com/en-us/library/cc543303.aspx>

# Step 4: Design the Dynamic Datacenter Storage Infrastructure

In the previous step, the management software was designed to support the Dynamic Datacenter. In this step, based on the disk storage requirements determined in Step 1, the storage infrastructure for the Hyper-V hosts in the Dynamic Datacenter will be designed. The designer might choose to include the management software’s storage needs (from Step 3 and the corresponding IPD guides for each technology) with the Hyper-V storage needs in one overall analysis and design set.

The storage infrastructure includes the storage system, host storage connections, and switches. It will need to be designed to meet the Dynamic Datacenter’s requirements in the following areas:

* Capacity, to provide the required storage space for the data and backups and forecasted growth.
* Performance delivery, to support the required number of IOps (Input/Output per second) and throughput, including forecasted growth.
* Fault tolerance, to provide the desired level of protection against hardware failures.
* Manageability, to provide a high degree of platform self-management.

These aren’t the only considerations from an operational standpoint; however, in-depth discussions of data life-cycle management, compliance, or segregation are outside the scope of this guide.

The physical storage systems that can be used with a server that runs Hyper-V to store the virtual machines are:

* Direct-attached storage, such as Serial Advanced Technology Attachment (SATA), Serial Attached SCSI (SAS), SCSI, USB, or Firewire drives.
* Storage Area Networks (SANs) using Internet SCSI (iSCSI), Fibre Channel, or SAS technologies.

Network-attached storage is not supported for Hyper-V, although the virtual machines are able to access data stored on network-attached storage as a regular file share.

The diagram below illustrates a possible storage infrastructure configuration with fault tolerance built in at multiple levels.



Figure 4. Example of a simple Dynamic Datacenter storage infrastructure

## Task 1: Design the Storage System

The maximum peak and sustained throughput at which a storage system can be accessed is determined by the type of disk, the number of physical disks in the array, the redundant array of independent disks (RAID) configuration, and the adapters that are used to connect the storage array to the system.

To determine the number of physical disks that should be included in the design of the storage system, consider the following information:

* Throughput (and often response time) improves as disks are added. The disk array must be planned so that it delivers sufficient IOps for the workload.
* Reliability, in terms of mean time to failure for the array, decreases as disks are added.
* Usable storage capacity increases as disks are added, but so does cost.

By mapping the disk capacity and throughput requirements and the RAID configuration to the size of disks in the selected subsystem, determine the number of actual drives required for performance. 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 amount of buffer to protect the system in the event of any system performance anomalies.

Additionally, the Dynamic Datacenter has these requirements to ensure that it is resilient and easy to manage:

* Multiple paths to the disk array for redundancy. Hot or warm spare disks can provide resiliency in the provisioned storage should a disk fail. Consult the storage vendor for specific recommendations.
* Automatic data recovery. A storage system with automatic data recovery allows an automatic background process to rebuild data onto a spare or replacement disk drive when another disk drive in the array fails.
* **Redundant power supplies and fans.** Implementing redundant power supplies and cooling fans can maximize the number of faults that the storage array can withstand. However, this risk can be mitigated by other fault-tolerance strategies as discussed previously.

Using the information above and the workload resource requirements from Table A-1, work with the organization’s storage vendor to design a storage system that will meet the desired redundancy and performance levels for the Dynamic Datacenter.

If the storage systems have a management port, this should be recorded in Table A-5 in Appendix A as it will affect the number of network switch ports needed.

If direct-attached storage is used, skip the remainder of this step and go to Task 4 to design the backup approach. If SANs will be used, continue to Task 2 to design the host storage connections.

## Task 2: Design the Host Storage Connections

The physical host components that are necessary for communication with the shared storage are the host itself, the connectors on the host that enable physical access to the storage, and the cables.

To provide fault tolerance, design for multipath I/O. Multipath I/O allows for more than one physical path between the computer and the storage devices through the buses, controllers, switches, and bridge devices connecting them. Should one of these components fail, the server and application will continue running.

If an external storage system is used, consider dedicating at least two host controller cards per physical server. The host controllers should be connected to separate ports on separate switches. The fault-tolerance guidelines also include:

* If the virtualization host will boot from a SAN, a minimum of two storage host bus adapters (HBAs) should be dedicated for this use. These HBAs should not be shared with virtual workloads.
* If the virtualization guest workloads will be housed on a SAN using a Fibre Channel connection, dedicate at least two HBAs per physical server.
* If an iSCSI storage architecture will be used, dedicate at least two network adapters on each host server to the iSCSI network.

Using the information above and the workload resource requirements, work with the organization’s storage vendor to design the storage connectors that will meet the desired redundancy and performance levels for the Dynamic Datacenter. Record the hosts’ storage connections in Tables A-3 and A-5 in Appendix A.

## Task 3: Design the Storage Switches

The purpose of a storage switch is to provide resilient and flexible connectivity between shared storage and physical servers. The storage switch must meet the peak storage I/O requirements for the workloads. In addition, the interconnect speeds between switches should be evaluated to determine the maximum throughput for switch-to-switch communications. This could affect the maximum number of hosts that can be placed on each switch.

While switch throughput is important, attention should also be paid to the number of available switch ports needed to support the physical virtualization hosts. Refer to the hardware vendor for each switch to ensure these requirements are met.

The protocols used for storage communications are typically either Fibre Channel or IP. General guidelines include:

* Dedicate a switch port on each switch for each host and storage processor connection. This is needed to provide redundancy and I/O optimization.
* Consider separating iSCSI traffic from all other IP traffic, preferably on its own switched infrastructure or logically through a VLAN on a shared IP switch. This segregates data access from traditional network communications for host-to-host and workload operations as well as data security.
* Redundant power supplies and cooling fans can serve to maximize the number of faults that the storage switch can withstand. However, this risk can be mitigated by other fault-tolerance strategies as discussed previously.
* If the storage switches have a management port, this should be recorded in Table   
  A-5 in Appendix A as it will increment the number of network switch ports needed.

Using the requirements above, design the storage switches and interconnects to meet the desired fault-tolerance and performance levels. Record in Tables A-3 and A-5 in Appendix A the connections for each physical host. This task may require consultation with the hardware vendor.

## Task 4: Select the Backup Approach

In this task, three approaches to backing up virtual workloads are presented. Since 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 additional 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 (RPO), 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 (RTO), 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.

The Dynamic Datacenter has the following requirements to ensure that it is designed with operations in mind:

* **Integration with enterprise reporting.** The solution should provide the ability to monitor the status of backup and restore operations and to publish alerts when incidents occur.
* **Scalability.** The solution should provide the ability to scale out horizontally based on the amount of data that will be backed up. This should include the ability to utilize multiple tape libraries.
* **Backup and restore of the virtual workloads.** This does not imply protection of the applications residing in the virtual workloads, but merely the ability to back up and restore the entire virtual workload from a point in time.
* **Backup and restore of the data in the workloads.** In this scenario, the guest virtual machine would be recreated and the data restored from a point in time.

The three approaches that can be taken to backing up virtual workloads are virtual hard disk copy, volume shadow copy service snapshots, and installing backup agents in every virtual machine.

### Virtual Hard Disk Copy

Because the entire contents of a virtual machine are encapsulated in virtual hard disk (VHD) and configuration files, a simple method for 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 virtual machine using a simple file copy process. The primary challenge is that VHD files are locked as “in use” while virtual machines are running, and so cannot be backed up. One solution involves temporarily pausing or shutting down a virtual machine before starting backups. However, doing so requires downtime and an interruption to application availability.

### Volume Shadow Copy Service Snapshot

Backup software can use the VSS writer in Windows Server 2008 Hyper-V or Virtual Server 2005 R2 with Service Pack 1 to make consistent backups of virtual machines 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 host hardware design as well as when planning network and disk capacity and performance.

The Microsoft offering that best provides this functionality is System Center Data Protection Manager. Using the *Infrastructure Planning and Design Guide for Data Protection Manager 2007 with Service Pack 1* (<http://go.microsoft.com/fwlink/?LinkId=160984>), designthe backup and data restore solution to back up the workload, core infrastructure, and management data within the RTO timeframe.

### Install Backup Agent in Every Virtual Machine

In this option, backup agents are installed in each virtual machine, and a system state or bare metal backup is performed, similar to backing up a physical server. This may require more administrative overhead as the backup strategy for each virtual machine will need to be considered, instead of consolidating at the host level.

## Validating with the Business

Base the specific backup design on application and business requirements. To validate design decisions, ask business stakeholders the following question:

**Has the chosen backup design been validated by the business?** A good resource with details about backup design is the IPD guide for System Center Data Protection Manager 2007(<http://go.microsoft.com/fwlink/?LinkId=160984>).

## Step Summary

In this step, the storage infrastructure for the Hyper-V hosts in the Dynamic Datacenter was designed, including the storage system, host storage connections, storage switches, and the data backup and restore approach. The data gathered in this step was recorded in Tables A-3 and A-5 in Appendix A.

## Additional Reading

* Planning for Disks and Storage: <http://technet.microsoft.com/en-us/library/dd183729(WS.10).aspx>
* Infrastructure Planning and Design Guide for System Center Data Protection Manager 2007 with Service Pack 1: <http://go.microsoft.com/fwlink/?LinkId=160984>

# Step 5: Design the Network Infrastructure

In the previous step, the storage infrastructure for the Hyper-V hosts in the Dynamic Datacenter was designed. In this step, based on the network requirements accumulated throughout this guide and recorded in the job aids in Appendix A, the network infrastructure will be designed.

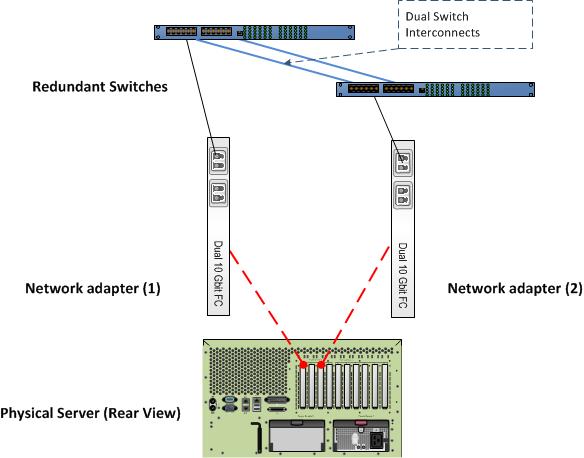
The physical network infrastructure needs to be designed to meet the Dynamic Datacenter’s requirements in these areas:

* Capacity, to provide the required number of network ports.
* Performance delivery, to support the required throughput.
* Fault tolerance, to provide the desired level of protection against hardware failures.
* Manageability, to provide a high degree of platform self-management.

## Task 1: Design Network Switches

In this task, the physical network switches will be designed. Because this guide focuses on building the infrastructure to support the overall Dynamic Datacenter, virtual network switches within the virtualization hosts will not be discussed since that functionality is more appropriately covered when planning and designing a specific workload.

The network infrastructure components that must be considered include the physical network adapters in the virtualization hosts, the network switches, and the cables connecting them. Also, take the iSCSI network design in to consideration as it has already been designed and may use the same infrastructure. The diagram below illustrates a possible network switching infrastructure configuration with fault tolerance built in at multiple levels.



**Figure 5. Example of redundancy in network switching infrastructure**

Subnets can be separated by using physical cabling or VLANs. Physical separation has the drawback of requiring the cabling to be manually reconfigured if a device needs to be moved from one subnet to another. Separation via VLANs, on the other hand, allows for more dynamic reconfiguration in that changes can be implemented via software commands. The IEEE 802.1Q standard for VLAN tagging allows for a physical network connection to transmit multiple streams of network traffic. Each stream is virtually isolated from each other so that a machine on VLAN1 and a machine on VLAN2 cannot see the other’s packets unless there is a router connected to both VLANs that performs routing between them.

The network infrastructure used in the Dynamic Datacenter should have the following characteristics:

* **Managed switches.** The switches must support programming instructions remotely in order to enable configuration automation.
* **Port mirroring.** (Also known as port monitoring, spanning port, SPAN port, roving analysis port, or link mode port.) This is needed in order to provide diagnostics on the primary port’s network packets as well as debugging when fending off network attacks.
* **SNMP monitoring.** Allows for monitoring alerts and events for the switches or network-attached devices for conditions that warrant administrative attention.
* **IEEE 802.1Q VLANs.** VLANs address issues such as scalability, security, and network management.
* **802.1X port authentication.** This standard specifies a way to achieve port-based network access control on an Ethernet LAN. IEEE 802.1x is used within the Dynamic Datacenter to prevent unauthorized computers from gaining access to the network.
* **Source port filtering.** This filtering isolates DHCP and PXE traffic so that a booting computer receives traffic only from a designated port. This mitigates rogue PXE servers.
* **Link aggregation.** (Also known as bonding, trunking, or teaming.) This is needed on the switches to provide both network scalability and connection redundancy to support scaling of the data center.

In addition, the interconnect speeds between switches and routers should be evaluated to determine the maximum bandwidth for communications. This could affect the maximum number of hosts that can be placed on each switch.

Throughout this guide, the network requirements have been gathered and recorded in Table A-1 in Appendix A. Tally these requirements to determine the number of connections required on each subnet, and record this in Table A-5 in Appendix A. Then design the network switches to support the capacity, performance, and fault-tolerance requirements*.*

Any devices that are capable of having redundant network connections should not have both connections going to the same switch as that would make the switch a single point of failure. Each switch added thereafter will also require a failover partner. Set up separate pathways for redundant sets of cables. If multiple sources of power or network communication are used, try to route the cables to the cabinets from different sources. This way, if one cable is severed, the other can continue to function.

Record the names of the switches that will serve each subnet and the port capacity in Table A-5. Alternatively, the organization’s network diagramming software may be used to represent this information.

## Task 2: Design the Hardware Load Balancers (Optional)

The Dynamic Datacenter can use a hardware load balancer to distribute network requests evenly across two or more workloads. Because not all applications are capable of relying on a load balancer to distribute network requests, this task is optional.

Hardware load balancers deployed in the Dynamic Datacenter should include the following capabilities:

* **SNMP monitoring.** This is required for providing both monitoring and event-based information to management systems.
* **Remote configuration.** Remote configuration allows for the creation/deletion of load balancing policies for both infrastructure components and workloads.
* **Health monitoring.** This is required to poll servers for application-layer health and to remove failed servers from the pool.
* **Traffic shaping.** Traffic shapingallows for prioritization of traffic in order to optimize or guarantee performance based on the workload.

To determine the size of the hardware load balancer, the following impacts should be considered:

* Number of workloads that will utilize the load balancer.
* Aggregate network bandwidth inbound/outbound per workload.
* The type of load-balancing scheduling algorithm that will be used.

Care should be taken to avoid creating a single point of failure. Hardware load balancers may need to be deployed in a fault-tolerant configuration. Record in Table A-6 in Appendix A the load balancer type as well as the quantity needed to meet required redundancy and the workloads that will be served by the load balancer. Refer to the hardware vendor for more information on configuration and scalability limitations.

Review whether the implementation of load balancers will affect the network adapters needed in each virtualization host, and thus the number of network ports required in the switches, update the switch design accordingly, and update Table A-5.

## Task 3: Design the Firewalls (Optional)

A firewall provides security filtering between two networks; so depending on the sensitivity of the data residing in the Dynamic Datacenter, one or more firewalls may be required to provide separation between the Dynamic Datacenter and the outside environment, the organization’s traditional data center, or even within the Dynamic Datacenter itself. Firewalls included in the Dynamic Datacenter should include these functionalities:

* **SNMP monitoring.** Required in order to provide both monitoring and event-based information.
* **Remote configuration.** To allow administrators to remotely edit firewall rules.
* **Intrusion detection capability.** Provides protection from network attacks against vulnerable services, data-driven attacks on applications, and host-based attacks such as privilege escalation, unauthorized logons, and access to sensitive files.
* **Interface usage (optional).** Provides the ability to monitor bandwidth usage for both incoming and outgoing communications. This allows for usage-based billing and monitoring interface usage to meet service level agreements as well as capacity thresholds.

As with all components that represent potential single points of failure, firewalls should be fault tolerant, with multiple I/O paths established for each connection to the redundant firewalls.

A firewall will require at least two network connections since it separates two networks, but possibly more depending on the resources it is protecting. Refer to the network requirements in Table A-1 in Appendix A to determine subnet assignments and firewall port needs. Switches may be used to provide additional ports for a given firewall interface’s subnet, and if so, these requirements should be transferred to the switch design so that it can be modified accordingly.

Using the requirements above, and the workload resource requirements, record in Table A-7 in Appendix A the firewall used, as well as its quantity to meet required redundancy, and the workloads that will be connected. This may require consultation with the hardware vendor.

## **Validating with the Business**

Ensure that technical decisions meet business requirements. A specific question to ask:

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 network infrastructure was designed. The physical network switches were designed to provide redundancy and fault tolerance. The load balancer types and quantities were designed, as well as the firewalls, if required by the business. The data gathered in this step was recorded in Tables A-5, A-6, and A-7 in Appendix A.

## Additional Reading

“Virtual LAN (VLAN) support in Hyper-V”: [www.virtualizationadmin.com/articles-tutorials/microsoft-hyper-v-articles/networking/introduction-vlan.html](http://www.virtualizationadmin.com/articles-tutorials/microsoft-hyper-v-articles/networking/introduction-vlan.html)

# Conclusion

This guide has outlined the step-by-step process for planning a Dynamic Datacenter infrastructure. Delivering dynamically scalable IT resources can provide dramatic benefits to nearly all aspects of an organization’s IT environment. Analyzing business and technical requirements for the applications and services in scope will assist the designer in planning a successful Dynamic Datacenter implementation. The infrastructure will be designed to meet the usual requirements for capacity, performance, and fault tolerance. Incorporating the automation and configuration management structure required will reduce the need for manual administration of the computing infrastructure.

Microsoft and its partners lower the cost of delivering data center services through integrated, end-to-end management of physical and virtual environments and support the optimization of the data center in three primary ways:

* Reduction of data center costs through server and resource management automation.
* Optimization of the data center infrastructure through integrated physical and virtual management.
* Increased simplicity through integrated management capabilities.

These benefits are delivered through integrated tools that take advantage of a deep understanding of both the Microsoft and third-party data center environments, along with specialist partner knowledge relative to hardware, applications, virtualization, compliance, and security.

For validation of the Dynamic Datacenter, consider conferring with Microsoft Consulting Services or a qualified Microsoft Partner.

Prior to deploying a Dynamic Datacenter, it is important to ensure that the organization’s infrastructure—the hardware, operating systems, and management applications that comprise the data center—is deployed, operated, and secured in accordance with best practices. These Microsoft Solution Accelerators provide this guidance:

* Microsoft Operations Framework 4.0, which provides best practices for service management from planning through operations.
* Reliability workbooks, which provide best practices for operations management guidance for Microsoft products.
* Security guides, which provide best practices for securing Microsoft products.

Prior to deploying the Cloud Infrastructure Solution Accelerator, it is important to ensure that the organization’s infrastructure—the hardware, operating systems, and management applications that comprise the data center—is deployed, operated, and secured in accordance with best practices. These Microsoft Solution Accelerators provide this guidance:

* Microsoft Operations Framework 4.0, which provides best practices for service management from planning through operations.
* Reliability workbooks, which provide best practices for operations management guidance for Microsoft products.
* Security guides, which provide best practices for securing Microsoft products.

## Additional Reading

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

* Microsoft Operations Framework: [www.microsoft.com/mof](http://www.microsoft.com/mof)
* Security Solution Accelerators tools and guidance: <http://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx>
* Windows Server 2008 Hyper-V library: <http://technet2.microsoft.com/windowsserver2008/en/library/5341cb70-0508-4201-a6da-dcac1a65fd351033.mspx>
* Microsoft Virtualization Resources page: [www.microsoft.com/virtualization/resources.mspx#documents](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>
* Microsoft Virtual Server 2005 R2 home page: [www.microsoft.com/windowsserversystem/virtualserver/default.aspx](http://www.microsoft.com/windowsserversystem/virtualserver/default.aspx)
* Improving IT Efficiency at Microsoft Using Virtual Server 2005: [www.microsoft.com/technet/itshowcase/content/virtualserver2005twp.mspx](http://www.microsoft.com/technet/itshowcase/content/virtualserver2005twp.mspx). This white paper provides details on how Microsoft has implemented a Virtual Server 2005 infrastructure.
* Microsoft TechNet Radio, “How Microsoft Does IT: The Future of Server Virtualization”: [www.microsoft.com/technet/community/tnradio/archive/june262007.mspx](http://www.microsoft.com/technet/community/tnradio/archive/june262007.mspx)

# Appendix A: Job Aids

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

**Step 1.** The table below is used to record the resource requirements for the workloads.

Table A-1. Resource Requirements

| Resource | Workload 1 | Workload 2 | Workload N | Total |
| --- | --- | --- | --- | --- |
| **Application name** | App-1 | App-2 |  |  |
| **Operating systems supported** | Windows Server 2008 R2 | Windows 7 |  |  |
| **Memory** | 2 GB | 1 GB |  |  |
| **CPU utilization** | 8% | 2% |  |  |
| **Disk space required** | 150 GB | 2 GB |  |  |
| **Disk IOps** | 750 | 20 |  |  |
| **Network subnets** | 192.168.4.x | 192.168.22.x |  |  |
| **Network throughput** | 800 mbps | 10 mbps |  |  |
| **Isolation requirements** | Yes | No |  |  |
| **Virtualization supported** | Yes | Yes |  |  |
| **Requirement for fault tolerance** | Yes | No |  |  |
| **Fault-tolerance approach** | Cluster | Not applicable |  |  |
| **In scope** | Yes | Yes |  |  |
| **Workload grouping** | A | B |  |  |

**Step 2.** The table below is used to tally the resource requirements for each grouping.

Table A-2. Workload Groupings Requirements

| Workload grouping name | Grouping A | Grouping B | Grouping C |
| --- | --- | --- | --- |
| **Total memory** | 24 GB | 8 GB |  |
| **Total CPU utilization** | 75% | 50% |  |
| **Total disk space required** | 1.2 terabytes | 250 GB |  |
| **Total disk IOps** | 20000 | 3000 |  |
| **Network subnets** | 192.168.4.x | 192.168.22.x |  |
| **Total network throughput** | 4 Gbps | 1 Gbps |  |

**Steps 2, 3, and 4.** The table below is used to record the configuration of the physical hosts.

Table A-3. Physical Hosts Design

|  | Host #1 | Host #2 | Host #3 |
| --- | --- | --- | --- |
| **Quantity, if clustered at host level** | 2 | Not applicable |  |
| **Form factor** | Rack | Blade |  |
| **CPU** | 12x3.0 GHz | 4x3.0 GHz |  |
| **Memory** | 24 GB | 8 GB |  |
| **Power supplies** | Redundant | Not redundant |  |
| **Network adapters** | 2x 4 ports | 2 |  |
| **Network access available** | Cluster Heartbeat, Patching, 2 ports on Subnet 192.168.4.x | 2 on Subnet 192.168.22.x |  |
| **Network teaming** | 2 ports for Subnet 192.168.4.x | None |  |
| **Storage systems** | SAN-DDC-STOR1 | SAN-DDC-STOR2 |  |
| **Storage connections** | 4 HBAs connected to SAN-DDC-SW1 | 2 HBAs connected to SAN-DDC-SW2 |  |

**Step 3.** The table below is used to record the number of servers that will be managed by each software service.

Table A-4. Number of computers being served by each service

| Type of service | Quantity included |
| --- | --- |
| Authenticating to the domain controllers |  |
| Querying DNS |  |
| Hosts managed by VMM |  |
| Virtual machines managed by VMM |  |
| Managed by ConfigMgr |  |
| Managed by MDT |  |
| Serviced by OVMST |  |
| Monitored by OpsMgr |  |
| Monitored by hardware management |  |

**Steps 4 and 5.** The table below is used to record network switch connection data and is optional.

Table A-5. Network Switch Connections

|  | Subnet X | Subnet Y | Subnet Z |
| --- | --- | --- | --- |
| **Purpose** | Cluster Heartbeat | Patching |  |
| **IP range** | 10.140.1.1/24 | 10.141.1.1/24 |  |
| **Number of ports required** | 64 | 32 |  |
| **Assigned to switch** | SW-DDC-14 | SW-DDC-18 |  |

**Step 5.** The table below is used to record load balancer data and is optional.

Table A-6. Load Balancers

|  | Load balancer #1 | Load balancer #2 | Load balancer #3 |
| --- | --- | --- | --- |
| **Load balancer type** |  |  |  |
| **Number needed for redundancy** |  |  |  |
| **Workloads served** |  |  |  |

**Step 5.** The table below is used to record firewall data and is optional.

Table A-7. Firewalls

|  | Firewall #1 | Firewall #2 | Firewall #3 |
| --- | --- | --- | --- |
| **Firewall type** |  |  |  |
| **Number needed for redundancy** |  |  |  |
| **Workloads served** |  |  |  |

# Appendix B: IPD in Microsoft Operations Framework 4.0

Microsoft Operations Framework (MOF) 4.0 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 B-1. The architecture of MOF 4.0

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.2 | Minor updates to template/formatting. | November 2011 |
| 1.1 | Terminology update. | July 2010 |
| 1.0 | First release. | April 2010 |

# Acknowledgments

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

**Contributors:**

* Jude Chosnyk – *GrandMasters*
* Joe Coulombe – Microsoft
* Fred Harmon – Microsoft
* Michael Kaczmarek – Microsoft
* Anthony Marusic – Microsoft
* Fergus Stewart – Microsoft
* Melissa Stowe – Microsoft

**Reviewers:**

* Luis Camara Manoel – *Microsoft*
* Jurjen de Vries – *Capgemini*
* Edo Jorritsma – *Capgemini*
* Udo Karten – *Capgemini*
* Bert Kruizenga – *Capgemini*
* Don Lemmex – *Microsoft*
* Ron Mandjes – *Capgemini*
* Martin Ruiter – *Capgemini*
* Kevin Sangwell – *Microsoft*
* Rene Scholten – *Capgemini*

**Editor:**

* Laurie Dunham – *Xtreme Consulting Group*
* Pat Rytkonen – *Volt Technical Services*

## Feedback

Please direct questions and comments about this guide to [ipdfdbk@microsoft.com](mailto:ipdfdbk@microsoft.com?subject=IPD%20-%20Dynamic%20Datacenter).