Microsoft | Solution Accelerators

Infrastructure Planning and Design

Microsoft® System Center 2012 - Virtual Machine Manager

Version 1.0

Published: July 2012

For the latest information, please see www.microsoft.com/ipd

Copyright © 2012 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 Azure, 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**
Introduction to the Microsoft System Center 2012 - Virtual Machine Manager Guide **2**
Step 1: Define the Project Scope and Requirements **7**
Step 2: Design the Operations Manager Integration **11**
Step 3: Determine the VMM Instances **14**
Step 4: Design the VMM Management Server Infrastructure **16**
Step 5: Design the VMM Library Server **21**
Step 6: Design the Update Services Infrastructure **24**
Step 7: Design the App Controller Infrastructure **26**
Conclusion **29**
Appendix A: Job Aids **30**
Appendix B: The Self-Service Portal **33**
Appendix C: IPD in Microsoft Operations Framework 4.0 ..... **34**
Appendix D: VMM in Microsoft Infrastructure Optimization **35**
Version History **36**
Acknowledgments **37**

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.

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 virtual machine management technology.

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 Microsoft System Center 2012 - Virtual Machine Manager Guide

Microsoft System Center 2012 - Virtual Machine Manager (VMM) is a management solution for the virtualized data center, enabling organizations to configure and manage virtualization host, networking, and storage resources to create and deploy virtual machines and services to private clouds.

This guide leads the reader through the process of planning a VMM infrastructure up to the point of designing and scaling the VMM management servers, databases, and portals.

In VMM, a *service* is a set of virtual machines that are configured and deployed together and are managed as a single entity to collectively deliver a business function (for example, a deployment of a multitier line-of-business application).

A *private cloud* is a grouping of virtual machine hosts and networking, storage, and library resources that is assigned to users to deploy services.

System Center 2012 - Virtual Machine Manager has the ability to carry out virtual machine-centric and service-based deployments. The former is virtualization-focused and operated at a virtual machine level, while the latter is a service-centric approach and intended for private cloud deployment.

Figure 1. System Center 2012 capabilities and components

Customers should consider having their architecture reviewed by Microsoft Customer Service and Support prior to implementation because that organization is best able to comment on the supportability of a particular design.

This guide has been adapted from the *Infrastructure Planning and Design Guide for Microsoft System Center Virtual Machine Manager 2008 R2*. For a listing of what is new in this version of VMM, see http://technet.microsoft.com/en-us/library/gg671825.aspx.

Virtual Machine Manager Design Process

This guide addresses the decisions and activities that must occur in planning the design for a functional infrastructure. The seven steps that follow represent the most critical design elements in a well-planned VMM design:

- Step 1: Define the Project Scope and Requirements
- Step 2: Design the Operations Manager Integration
- Step 3: Determine the VMM Instances
- Step 4: Design the VMM Management Server Infrastructure
- Step 5: Design the VMM Library Server
- Step 6: Design the Update Services Infrastructure
- Step 7: Design the App Controller Infrastructure

Figure 2 provides a graphical overview of the steps involved in designing a VMM infrastructure.

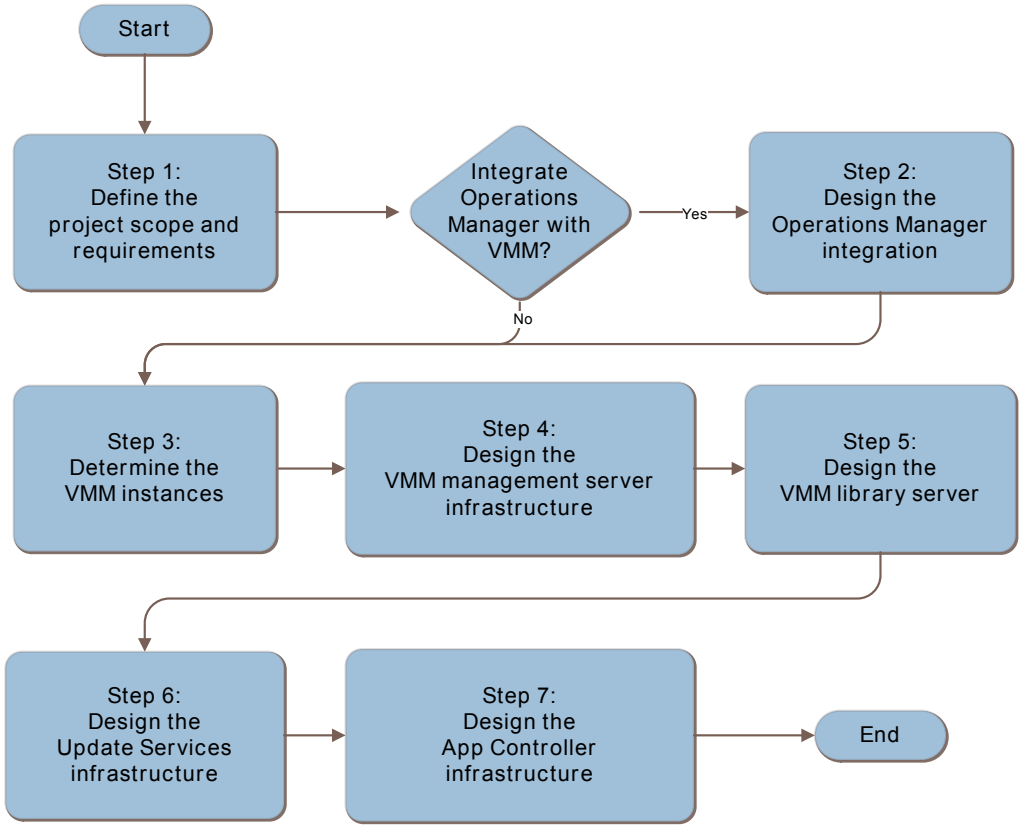

Figure 2. The Virtual Machine Manager infrastructure decision flow

The components of a typical VMM infrastructure are shown in Figure 3.

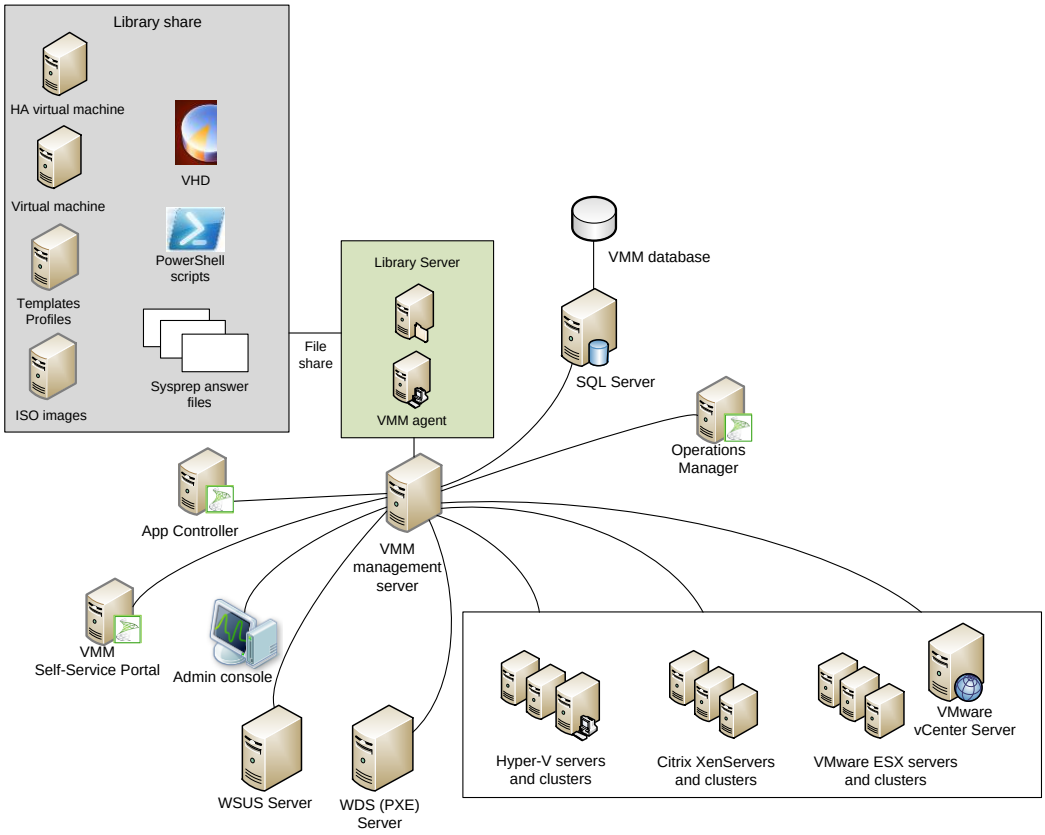

Figure 3. Example Virtual Machine Manager architecture

The mandatory roles for a VMM implementation are:

- VMM management server
- VMM database
- VMM console
- VMM library

The optional components of a VMM implementation are:

- System Center 2012 - App Controller
- VMM Self-Service Portal

Note The VMM Self-Service Portal is deprecated, meaning that it will not be included in future releases of VMM. In System Center 2012, it is recommended to use System Center 2012 - App Controller as the self-service portal solution. For more information about App Controller, see App Controller in the TechNet Library at http://technet.microsoft.com/en-us/library/hh546834.aspx.

Table 1 provides descriptions of these VMM roles.

Table 1. Virtual Machine Manager Roles

Role	Description
VMM management server	The computer on which the Virtual Machine Manager service runs and which processes commands and controls communications with the VMM database, the library server, and virtual machine hosts.
VMM database	A Microsoft SQL Server® database that stores VMM configuration information.
VMM console	The console that provides access for a connection to a VMM management server to centrally view and manage physical and virtual resources, such as virtual machine hosts, virtual machines, services, and library resources.
VMM library	The catalog of resources (for example, virtual hard disks, templates, and profiles) used to deploy virtual machines and services. A library server hosts shared folders used to store file-based resources in the VMM library.
System Center 2012 - App Controller	Another component of System Center 2012 that allows users to perform self-service virtual machine tasks, including the configuration, deployment, and management of virtual machines in private and public clouds. App Controller is the recommended self-service portal solution.
VMM Self-Service Portal	A website that users assigned to a self-service user role can use to deploy and manage their own virtual machines to private clouds. **Note** The VMM Self-Service Portal will not be included in future releases of VMM. For information about App Controller, the recommended self-service portal solution, see App Controller in the TechNet Library at http://technet.microsoft.com/en-us/library/hh546834.aspx.

Applicable Scenarios

This guide is intended for the design of the actual VMM infrastructure to be created and used by the organization (not the infrastructure that VMM in turn manages). It addresses these considerations when planning and designing the components for a successful VMM infrastructure:

- Managing virtual machine hosts that use:
  - Hyper-V® in Enterprise or Datacenter editions of Windows Server® 2008 with Service Pack 2. See “System Requirements: Hyper-V Hosts” at http://technet.microsoft.com/en-us/library/gg610649.aspx for more information.
  - VMware vCenter 4.1, VMware ESXi 4.1, VMware ESX 4.1, VMware ESXi 3.5, and VMware ESX 3.5. See “System Requirements: VMware ESX Hosts” at http://technet.microsoft.com/en-us/library/gg697603.aspx for more information.
  - Citrix XenServer 6.0 with the Citrix XenServer — Microsoft System Center Integration Pack. See System Requirements: Citrix XenServer Hosts at http://technet.microsoft.com/en-us/library/gg610587.aspx for more information.
- Designing VMM infrastructures that organizations can use for server consolidation and self-service provisioning.

- Designing topologies that best fit the organization's requirements, such as:
  - VMM in a data center to manage a private cloud within a data center.
  - VMM in a central location to manage multiple private clouds in multiple data centers.
  - Multiple instances of VMM to enable each location to manage its own private cloud.

Assumptions

This guide assumes that the reader is familiar with VMM and virtualization technology. It also assumes that the organization is planning a VMM implementation and, if the decision is made to integrate VMM with System Center 2012 - Operations Manager, that the organization has already planned the respective infrastructure.

The design is for use in a production environment. This guide assumes that a test environment will be created to mirror the production environment in configuration.

Out of Scope

The following topics are out of scope for this guide:

- **Planning virtualization infrastructures.** This guide does not address the planning or design of server virtualization infrastructure. Rather, it addresses planning and design of the VMM infrastructure that is used to *manage* a server virtualization environment. For guidance about planning and designing virtualization infrastructure, see the *Infrastructure Planning and Design Guide for Windows Server Virtualization* at http://go.microsoft.com/fwlink/?LinkID=147617.
- **Administration and use of VMM.** The next steps for deployment, administration, and operations of VMM, such as configuring the fabric to provide the resources for hosts, virtual machines, and services, are beyond the scope of this guide and are provided by other guidance. For additional information regarding VMM administration, refer to Administering Virtual Machine Manager at http://technet.microsoft.com/en-us/library/gg610615.aspx.
- **Planning Operations Manager infrastructures.** Although this guide discusses integrating Virtual Machine Manager and Operations Manager, it does not discuss planning or designing an Operations Manager infrastructure. For more information, see the *Infrastructure Planning and Design Guide for Microsoft System Center Operations Manager 2007* at http://go.microsoft.com/fwlink/?LinkId=160985.
- **Planning Configuration Manager infrastructures.** Although this guide discusses integrating Virtual Machine Manager and Windows Server Update Services (WSUS) servers that are a part of System Center 2012 Configuration Manager, it does not discuss planning or designing a Configuration Manager infrastructure. For more information, see the *Infrastructure Planning and Design Guide for Microsoft System Center Configuration Manager 2007 R3 and Forefront Endpoint Protection* at http://go.microsoft.com/fwlink/?LinkId=160983.
- **Planning VMware ESXi or ESX virtualization hosts.** This guide does not address the planning or design of VMware ESXi or ESX virtual machine hosts.
- **Planning Citrix XenServer virtualization hosts.** This guide does not address the planning or design of Citrix XenServer virtual machine hosts.

Step 1: Define the Project Scope and Requirements

Before designing a VMM infrastructure, an organization needs to determine the objectives for the project and which parts of its environment to include in the design.

The tasks to be performed in this step are:

1. Determine the business requirements.
2. Determine the technical requirements.

In this step, the systems and/or applications that will be integrated with the VMM infrastructure project will be identified.

In addition, questions will be asked (for example, availability requirements) of the business decision makers in the organization to determine the scope and requirements of the VMM implementation. Information will then be gathered (for example, information relative to capacity and management packs) from the technical decision makers.

The outputs of this step are a detailed list of locations in scope for VMM, self-servicing requirements and management requirements, as well as determining whether to integrate with Operations Manager reporting.

The information collected in this step will drive decisions relative to designing the VMM instances, sizing and placement of the VMM management servers, databases, and library servers, and determining network connectivity requirements.

Task 1: Determine the Business Requirements

Ask the business the following questions to determine the scope and the features that will be implemented:

- **Which parts of the organization will participate?** Before the architecture can be designed, the scope of the project must be determined so that the planners know the boundaries for which they are building a solution. The scope of the project could be enterprise-wide, one or many locations, or just a single department.
- **Would a business or governance policy affect the design of the system?** Organizations may have administrative boundaries that will affect the VMM infrastructure. For instance, separate systems may currently be used for management for each IT department or region. The management tasks may be performed by the IT organizations, and are separate from managing the services or applications in which they are contained. Determine whether a centralized management approach will be used or management responsibilities will be distributed or delegated across the organization.
- **Does the business want users to be able to perform self-service provisioning?** Examine the organization's current and planned practices to provide self-service management tasks. Even if local IT pros are not available at a location, users at that location may desire to perform self-service management tasks.

  If so, determine which locations and users will require self-service provisioning.
- **Will additional locations be used for geographic failover or disaster recovery?** Examine the organization's fault-tolerance and disaster recovery plans to identify whether additional locations will be used for geographic failover (for improved fault-tolerance) or disaster recovery (in the event of an outage for an entire location). These locations may require their own separate VMM instance.
- **Will the organization require virtual desktop infrastructure (VDI)?** VDI is an alternative delivery model that allows users to access secure and centrally managed desktops running in the data center. This will determine the need for additional instances.

- **Will VMM integrate with Operations Manager to monitor the health and availability of the virtual machines and virtual machine hosts that VMM manages?** The health and availability of the VMM management server, the VMM database server, library servers, and VMM Self-Service Portal web servers can also be monitored, and the viewing of virtualization environment diagrams through the Operations console in Operations Manager enabled. Operations Manager integration will be required to use the following features:
  - Performance and Resource Optimization (PRO).
  - Maintenance mode integration.
  - Reporting in VMM. Create and view reports relating to VMM-managed components, including virtual machine hosts, virtual machines, and VMM-related servers (for example, library servers).
  - Support for SQL Server Analysis Services (SSAS). Provides forecasting reports.

  This will affect the number of VMM instances that will be required.
- **What are the availability requirements for VMM?** Give careful consideration to the availability requirements for each functional area. The business should understand and rate the significance of the risk of possible data loss or interruption of business, and then the architect will use this information to select an appropriate fault-tolerance approach for the systems involved.

  For each of the areas listed below, IT should assess the importance of the functionality as High or Low impact relative to interruption of service:
  - Administrators' and users' access to the console to perform management functions.
  - Administrators' ability to provision virtual machines, create services, or access the baseline configuration.
  - Self-service capabilities for private clouds (if applicable).

  Note that each High impact answer increases the cost and complexity of the design.

Record this information in Table A-1 in Appendix A: "Job Aids." This information will determine the number of VMM instances in Step 3 and, for each instance, the number and locations of library servers in Step 5, as well as the fault-tolerance requirements in Steps 4, 5, and 7 (if applicable).

Task 2: Determine the Technical Requirements

In this task, information is gathered from the technical decision makers in the organization to determine the scope and requirements of the VMM implementation.

More details will be collected about each location that has virtual machine hosts that will be included in the private clouds managed by VMM.

Record the following information in Table A-2 in Appendix A:

- **What virtualization technology will each location use?** VMM can manage virtual machine hosts running Hyper-V on Windows Server 2008 or Windows Server 2008 R2, Citrix XenServer, and VMware ESXi and ESX. Servers running Citrix XenServer will require the Citrix XenServer — Microsoft System Center Integration Pack be installed. VMware ESX hosts and host clusters must be managed by a vCenter Server that will be managed by VMM.
- **What virtual machine management technology will each location use?** The most common pre-existing virtual machine management technologies include Virtual Machine Manager and VMware vCenter. Identify the virtual machine management technologies and record the version number, if any, that each location uses to manage hosts and virtual machines.

- **How many virtual machine hosts will be implemented at each location?** Record the number of existing and planned virtual machine hosts for each location, as this will impact the sizing and placement of VMM instances in Step 3.
- **How many virtual machines will be implemented at each location, and what type will they be?** When sizing and placing VMM instances in Step 3, it will also be necessary to know how many virtual machines are at each location, and whether they will be server or desktop virtualization. Record the number of existing and planned virtual machines and the type for each location.
- **If the business decision makers decided in Task 1 to implement self-service provisioning, what is the approximate number of users and where are they located?** Record the approximate number of users expected to access the provisioning interface concurrently. This information will assist in determining self-service provisioning server sizing and placement.
- **Does the organization plan to implement a new update server or integrate with an existing software updates infrastructure, and if so which one?** Integrating VMM and WSUS enables users to reduce the effort required to help ensure the fabric resources are in compliance with established configuration baselines. When using a new WSUS server, VMM administrators can manage configuration compliance using the VMM console. Alternatively, if the WSUS server that is part of a Configuration Manager infrastructure is used, VMM administrators can use the existing configuration baselines and existing infrastructure in Configuration Manager.

Step Summary

After completing this step, the following business and technical requirements were collected and recorded in Tables A-1 and A-2 in Appendix A:

- Organization locations participating in scope.
- Business or governance policy influence on design.
- Requirements for supporting self-service provisioning of services and virtual machines, plus location and number of users.
- Geographic failover/disaster recovery inclusion in design.
- Use of virtual desktop infrastructure.
- Whether to integrate with Operations Manager for reporting.
- Availability requirements.
- Virtualization technology to be utilized.
- Virtual machine management technology to be used.
- Number and location of virtual machine hosts and virtual machines.
- Implementation of a new update server or integration with existing software updates infrastructure, and which one.

This information will determine the number of VMM instances in Step 3, size and place VMM and web servers in Step 4, and size and place library servers in Step 5.

If the decision was made to integrate both System Center products, continue with Step 2 to design the integration. If the decision is not to integrate the products or if Operations Manager is not used in the organization, continue to Step 3.

Additional Reading

- Planning your VMM Deployment: http://technet.microsoft.com/en-us/library/gg610669.aspx
- *Infrastructure Planning and Design Guide for Windows Server Virtualization:* http://go.microsoft.com/fwlink/?LinkID=147617

- Microsoft Server and Cloud Platform: www.microsoft.com/en-us/server-cloud/system-center/datacenter-management.aspx
- *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 System Center 2012 - Service Manager*: http://go.microsoft.com/fwlink/?LinkId=245470
- System Center 2012 - App Controller home page: http://technet.microsoft.com/en-us/library/hh546834.aspx
- System Requirements: Monitoring and Reporting: http://technet.microsoft.com/en-us/library/hh427297.aspx
- Configuring Security in Virtual Machine Manager: http://technet.microsoft.com/en-us/library/gg675078.aspx
- *Virtual Machine Manager 2008 R2 Security Guide*: http://go.microsoft.com/fwlink/?LinkId=161997

Step 2: Design the Operations Manager Integration

This step assumes the organization is planning to deploy or has already deployed Operations Manager. If it was decided to integrate with Operations Manager, continue with this step for each location. The decision in this step will affect the number of VMM instances that will be defined in Step 3 and can also affect the number of Operations Manager management groups defined in the Operations Manager infrastructure.

To deliver integrated reporting, VMM uses the Operations Manager Connector Framework to connect to a management group. The scope of the reporting data available from that connection is limited to virtual machine hosts within that management group. If more than one management group contains a virtual machine host, there are two options to deliver integrated reporting on those virtual machine hosts:

1. Design at least one VMM instance for each Operations Manager management group that contains virtual machine hosts. In this scenario, the organization will maintain multiple VMM instances. The section, “Option 1: Multiple VMM Instances,” describes this option.
2. Dedicate an Operations Manager management group to VMM and multihome the Operations Manager agents on virtual machine hosts. In this scenario, the organization will maintain the additional management group with its associated reporting database. The section, “Option 2: Dedicated Management Group for VMM,” describes this option.

A VMM instance must be monitored by a single management group in Operations Manager. However, an Operations Manager management group can monitor multiple VMM instances.

Record the design decision in Table A-3 in Appendix A.

Option 1: Multiple VMM Instances

The first option is to design a separate VMM instance for each Operations Manager management group that contains virtual machine hosts. The VMM management server in each VMM instance will be connected to an Operations Manager management server.

If this option is chosen, determine which management groups will contain virtual machine hosts. Record the decision and list the management groups in Table A-3 in Appendix A. This information will be used to design the number of VMM instances in Step 3 and to design and place VMM management servers in Step 4.

Benefits

This option works within the organization of the existing management groups.

Challenges

- Must deploy additional VMM instances, each with a VMM management server, database, and fabric resources.
- Makes placing and sizing VMM management servers more complex.
- Prevents the organization from consolidating management of virtual machines.

Option 2: Dedicated Management Group for VMM

The Operations Manager agent can be configured to multihome so that it simultaneously sends event, alert, and performance data to more than one management group. The VMM design group must work with the Operations Manager group to define a new management group that will be dedicated to integration with VMM. The Operations Manager agents running on virtual machine hosts are then configured to multihome so that they provide performance data to both their regular management group and to the management group that is connected to VMM.

If this option is chosen, for each new Operations Manager management group that will be designed, record the following in Table A-3 in Appendix A:

- The management group name.
- The names of the Operations Manager agents that will be multihomed to the management group.

The number of VMM instances will be designed in Step 3 and the VMM management servers will be placed in Step 4 based on this decision.

Benefits

- Simplifies deployment by using fewer VMM management servers.
- Simplifies placing and sizing of VMM management servers.
- Enables the organization to consolidate virtual machine management.

Challenges

Requires the addition of a new Operations Manager management group and its associated infrastructure.

Evaluating the Characteristics

Technical criteria are not the only factors that should be considered when making infrastructure decisions. Mapping decisions to the appropriate operational criteria or characteristics should be done as well. Tables 2 and 3 compare each option for characteristics that are applicable to this decision-making topic.

Table 2. Complexity Options

Complexity	Justification	Rating
Multiple instances	The organization must manage multiple VMM management servers.	High
Dedicated management group	The organization can manage as few as one VMM management server and centralize management.	Low

Table 3. Cost Options

Cost	Justification	Rating
Multiple instances	The organization must deploy and manage multiple VMM management servers.	High
Dedicated management group	The organization can deploy and manage as few as one VMM management server.	High

Step Summary

After completing this step, the design decision for Virtual Machine Manager and Operations Manager integration was recorded in Table A-3 in Appendix A.

This decision will be used to:

- Determine the number of VMM instances in Step 3.
- Determine VMM management server placement in Step 4.
- Communicate requirements to the people responsible for the Operations Manager infrastructure.

Additional Reading

- System Requirements: Monitoring and Reporting: http://technet.microsoft.com/en-us/library/hh427297.aspx
- *Infrastructure Planning and Design Guide for System Center Operations Manager 2007*: http://go.microsoft.com/fwlink/?LinkId=160985

Step 3: Determine the VMM Instances

In this step, the business requirements and the Operations Manager design requirements recorded from Step 1 will determine the number of VMM instances required.

This guide defines a *VMM instance* as a VMM management server or cluster connected to a unique VMM database instance. Each VMM management server must be installed on a separate computer (physical or virtual), and each must have a separate database instance, although these instances can be on the same database server as long as the instances are unique. Note the following:

- Each virtual machine host can be managed by using only one VMM instance. In other words, virtual machine hosts cannot connect to multiple VMM instances.
- VMM instances do not integrate and do not share data. There is no relationship between separate instances.

Task 1: Determine the Number of Instances

In Table A-4 in Appendix A, begin with recording one VMM instance to manage all the virtual machine hosts, and add others only if needed for:

- **Isolated networks or test environments.** Each location containing virtual machine hosts was recorded in Step 1. Determine whether any of these networks are isolated and will require a separate VMM instance. For example, organizations often isolate lab networks from production networks and require a separate instance of VMM for each.
- **Scaling limits exceeded.** Each VMM instance supports up to 400 virtual machine hosts and 8,000 virtual machines for all private clouds managed by VMM. Refer to the information gathered in Step 1, where the number of in-scope virtual machine hosts was identified and documented in Table A-2 in Appendix A.
- **Self-service provisioning only applying to parts of the scope.** In Step 1, the locations requiring self-service provisioning were determined and recorded in Table A-2 in Appendix A. If the decision was made to separate private clouds with self-service provisioning from secure private clouds, the decision might be to define a new instance for self-service provisioning.
- **Self-service provisioning scaling limits exceeded.** In addition, if there will be a population of more than 1,000 virtual machines within a private cloud that is dedicated for use by self-service users, the VMM engineering team suggests deploying a separate VMM instance for them. Before doing this, examine the workflow of the self-service users to understand whether they normally place a different load on the VMM management server infrastructure than non-self-service users. If the workflow and behaviors of the users are the same, a separate instance might not be needed.
- **Supporting VDI desktops.** Virtual desktop infrastructures (VDIs) can be co-located in the same instance as server loads; however, if the organization is deploying a non-trivial VDI, the VMM engineering team recommends that the organization dedicate a VMM instance for VDI management. There are no formal guidelines on how many VDI desktops can be included in a VMM instance before requiring migration into a separate instance.
- **The number of Operations Manager management groups required.** In Step 2, the design decisions for VMM and Operations Manager integration were documented in Table A-3 in Appendix A. Each of the Operations Manager management groups that will be integrated with VMM requires a separate VMM instance.

- **Matching the desired management model.** In Step 1, the organization's management model and each location containing services to be placed within a new cloud or existing virtualized environments to be placed within a new cloud were recorded in Table A-1 in Appendix A. The management model determines the need for additional instances:
  - **Local management model.** Define a new VMM instance for each location that has existing services or virtualized environments to be included in a private cloud, which enables each location to manage its own private cloud.
  - **Centralized management model.** Choose the locations where the centralized VMM instances will be located, which will in turn be used to manage the private clouds for all locations, such as specifying a new VMM instance for multiple global data centers.
  - **Hybrid model.** Identify locations that required local management and a new VMM instance for these locations and a new VMM instance for centralized data centers.
- **Organizational or political considerations.** Determine if organizational or political considerations require new VMM instances. For example, if two business units have their own IT departments, define a VMM instance for each business unit.
- **Disaster recovery functionality.** Examine the organization's disaster recovery strategy and its relationship to the private clouds and services within the clouds. If the private cloud-based services and private clouds are part of a disaster recovery strategy, additional VMM instances will be needed for each disaster recovery location.

There is no limit to the number of VMM instances that could exist in an organization, but additional instances add complexity and cost, because each requires a separate management server, database, and library server. VMM instances exist as separate entities that cannot connect directly to each other.

Refer to the scope defined in Step 1 and the Operations Manager integration impacts, if any, to determine whether multiple VMM instances will be required.

Step Summary

After completing this step, the number of required VMM instances was determined and recorded in Table A-4 in Appendix A.

This information will be used in Step 4 to size and place VMM management servers, database servers, databases, and Self-Service Portals for each VMM instance.

Additional Reading

- System Center Virtual Machine Manager home page: www.microsoft.com/en-us/server-cloud/system-center/virtual-machine-manager.aspx
- Supported Configurations for VMM: http://technet.microsoft.com/en-us/library/cc764231.aspx

Step 4: Design the VMM Management Server Infrastructure

In the previous step, the number of VMM instances was determined, and the information collected in the step was recorded in Table A-4 in Appendix A. This step focuses on the design of the VMM management servers and databases within the VMM instance.

The tasks to be performed in this step are:

1. Determine the placement of each component for the VMM management server infrastructure.
2. Apply the fault-tolerance requirements for the VMM management server infrastructure.
3. Determine the hardware configuration for the VMM management server infrastructure.

Only one VMM management server can connect to a VMM database. The VMM management server performs the following functions:

- Reads the configuration of the instance from the VMM database at startup and writes configuration changes to that database.
- Communicates with VMM agents running on the VMM database server and the servers hosting the private cloud fabric resources, such as the VMM library servers and virtual machine hosts.
- Manages physical-to-virtual (P2V) conversions that run on connected servers.
- Manages provisioning of services and virtual machines onto connected virtual machine hosts within the private cloud. Virtual machine images do not pass through the VMM management server, but rather are transferred directly from the VMM library servers to the virtual machine hosts.
- Receives performance data from each of the virtual machines and virtual machine hosts in the private clouds and writes that data to the VMM database. This data is transferred once every 9 minutes.
- Performs intelligent virtual machine performance optimization calculations upon demand to move virtual machines to the virtual machine host within the same private cloud that has lower utilization than the original virtual machine host.
- Performs intelligent power optimization by automatically turning off virtual machine hosts not currently in use. These computers can be automatically turned on if user demand increases.
- Sends configuration and performance data to the VMM console for display.
- Optionally, requests and receives performance data from Operations Manager, which it then sends to the VMM console for display. Operations Manager data is not written to the VMM database.

The VMM database and VMM database server perform the following functions:

- Stores the configuration of the instance.
- Receives performance data from the VMM management server for each of the virtual machine hosts and writes that data to the VMM database once every 9 minutes. This data is recorded as a set of rolling averages; each average is updated every 9 minutes. So after the first record has been written it is only updated; it does not grow any larger.
- Delivers virtual machine host performance data to the VMM management server so that it can perform intelligent placement calculations, on user demand, to recommend on which host a virtual machine should run.

If it was decided in Step 3 that multiple instances of VMM will be required, then this step must be repeated for each instance. Once complete, proceed to the next step to design the VMM library server.

Task 1: Determine the Placement of Each Component

In this task, the placement of the VMM management servers and VMM database will be decided.

- The VMM management server and VMM database can be co-located on a single server, or they can be run on separate servers. For better performance, when a VMM instance is managing more than 150 hosts, the VMM engineering team recommends using a dedicated computer for the VMM management server. The database server should be placed in a location that has high-speed connectivity with the VMM management servers.
- Each role can be run in a virtual machine.
- The VMM management server must be a member of an Active Directory® domain; therefore, place it on the network where that requirement can be met. If the VMM management server and the computer on which SQL Server is running are not both members of the same Active Directory Domain Services (AD DS) domain, there must be a two-way trust between the two domains.
- If VMM will process a very large volume of updates, consider installing the WSUS server on a separate computer from the VMM management server. (WSUS integration will be described further in Step 6.)

Record the placement of the VMM management servers and VMM database in Table A-5 in Appendix A.

Task 2: Apply the Fault-Tolerance Requirements

To have a fully fault-tolerant VMM infrastructure, the fault tolerance of the VMM management server, VMM database, and VMM library servers each needs to be addressed. Fault-tolerance options for the VMM management server and the VMM database will be evaluated in this step. The VMM library server will be described in the next step.

The VMM management server is stateless; the state of the VMM instance is held in the VMM database.

Table 4 describes the impact of a service failure for each component.

Table 4. Impact of Service Failures

Service failure	Description of interruption
VMM management server	Administrators and users unable to access the console to perform management functions. Virtual machine hosts and virtual machines remain running.
VMM database	Administrators and users unable to access the console to perform management functions. Virtual machine hosts and virtual machines remain running.
VMM library server	Administrators will be unable to provision virtual machines, create services, or access the WSUS baseline configuration.

VMM Management Server

The VMM management server is cluster aware and supports fault tolerance by either using failover clustering at the host level, or running it in a clustered virtual machine. If a VMM management server in the cluster fails, the cluster automatically fails over to another VMM management server in the cluster without any data loss. This helps guard against hardware and operating system failures.

Important facts to consider regarding a clustered VMM management server include:

- There can be only one active management server at a time, so it does not add scale-out capacity or increase performance.
- There can be as many as 16 nodes in a clustered VMM installation, but there can be only one active node at any time.
- VMM consoles will connect to the VMM service cluster name so that consoles can reconnect during migrations or failures.

For more information about installing a VMM management server in a failover cluster, see Installing a Highly Available VMM Management Server at http://technet.microsoft.com/en-us/library/gg610675.aspx.

Determine whether the VMM management server will be clustered for fault tolerance, and record the answer in Table A-5 in Appendix A.

VMM Database

The VMM database can be made fault tolerant by using a clustered SQL Server.

If the VMM instance requires fault tolerance, the VMM engineering team recommends that an installation of SQL Server that meets fault-tolerance standards be used for the database, and that it be installed on a separate failover cluster from the failover cluster used for the VMM management server.

Refer to the *Infrastructure Planning and Design Guide for Microsoft SQL Server 2008 and SQL Server 2008 R2* at http://go.microsoft.com/fwlink/?LinkId=163302 for more information on SQL Server design.

Determine whether one of the SQL Server fault-tolerance options will be implemented, and record the answer in Table A-5 in Appendix A.

Task 3: Determine the Hardware Configuration

In this task, the hardware configuration will be determined. This includes designing the VMM management server, the database server, and the database. These designs will be affected by decisions regarding server performance and availability.

VMM Management Server

Tables 5 and 6 list the minimum and recommended hardware requirements for the VMM management server based on the number of hosts managed. For more information, see System Requirements: VMM Management Server at http://technet.microsoft.com/en-us/library/gg610562.aspx.

Table 5. VMM Management Server Minimum and Recommended Hardware Requirements for Managing Less than 150 Hosts

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2 gigahertz (GHz) (x64)	Dual-processor, dual-core, 2.8 GHz or greater (x64)
RAM	2 gigabytes (GB)	4 GB
Hard disk space (without a local VMM database)	2 GB	40 GB
Hard disk space (with a local, full version of Microsoft SQL Server)	80 GB	150 GB

Table 6. VMM Management Server Minimum and Recommended Hardware Requirements for Managing More than 150 Hosts

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz (x64)	Dual-processor, dual-core, 3.6 GHz or greater (x64)
RAM	4 GB	8 GB
Hard disk space	10 GB	50 GB

Decide what the VMM management server hardware configuration will be, and then document the applicable information in Table A-5 in Appendix A. This information will be used in the tasks to size and place the database and web servers.

VMM Database

The VMM database stores the configuration and performance for the instance. Unlike the VMM management server, it is stateful.

Tables 7 and 8 list the minimum and recommended hardware requirements for the VMM database based on the number of hosts managed. For more information, see System Requirements: VMM Database at http://technet.microsoft.com/en-us/library/gg610574.aspx.

Table 7. VMM Database Minimum and Recommended Hardware Requirements for Managing Less than 150 Hosts

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Dual-core, 2 GHz (x64)
RAM	2 GB	4 GB
Hard disk space	80 GB	150 GB

Table 8. VMM Database Minimum and Recommended Hardware Requirements for Managing More than 150 Hosts

Hardware component	Minimum	Recommended
Processor	Dual-core, 2 GHz (x64)	Dual-core, 2.8 GHz (x64)
RAM	4 GB	8 GB
Hard disk space	150 GB	200 GB

Decide what the VMM database server hardware configuration will be, and then document the applicable information in Table A-5 in Appendix A.

Step Summary

After completing this step, the VMM server infrastructure has been designed, including the VMM management server and the VMM database server, and recorded in Table A-5 in Appendix A:

- The VMM management server for each VMM instance, including the size, placement, performance, and fault tolerance.
- The VMM database server for each VMM instance, including the size, placement, performance, and fault tolerance. Multiple VMM instances can share a single database server using separate SQL Server instances.
- The hardware configuration for the VMM management server and database server.

Proceed to Step 5 to design the VMM library server.

Additional Reading

- Cloud and Datacenter Management: www.microsoft.com/en-us/server-cloud/system-center/datacenter-management.aspx
- System Requirements for System Center 2012 - Virtual Machine Manager: http://technet.microsoft.com/en-us/library/gg610592.aspx
- Deploying Virtual Machine Manager: http://technet.microsoft.com/en-us/library/gg610669.aspx
- Installing a Highly Available VMM Management Server: http://technet.microsoft.com/en-us/library/gg610675.aspx
- Configuring Distributed Key Management in VMM: http://technet.microsoft.com/en-us/library/gg697604.aspx
- SCVMM 2012 - Creating a Highly Available VMM Server: http://blogs.technet.com/b/scvmm/archive/2011/03/28/scvmm-2012-creating-a-highly-available-vmm-server.aspx

Step 5: Design the VMM Library Server

In the previous step, the VMM management server infrastructure was designed and recorded in Table A-5 in Appendix A. This step's goal is to design the library servers for each instance that was identified in Step 3. The step should be repeated for each library server.

The *VMM library* is a catalog of resources that provides access to file-based resources such as virtual hard disks, virtual floppy disks, ISO images, scripts, driver files and application packages stored on library servers, and to non-file-based resources such as virtual machine and service templates and profiles that reside in the VMM database.

The *VMM library server* is a file server with one or more shares. A VMM agent runs on the file server, which defines it as a VMM library server and provides communication with the VMM management server. Only one VMM agent can be run on each library server, so the library server can connect to only one VMM management server. However, a VMM management server can be connected to more than one VMM library server.

The VMM library server performs the following functions:

- Stores the file-based resources listed above.
- Sends the files to the virtual machine hosts where they will be implemented as running virtual machines.

The tasks to be performed in this step are:

1. Determine the placement of the VMM library server.
2. Determine the number of servers required for scaling.
3. Apply the fault-tolerance requirements for the VMM library server.
4. Determine the hardware configuration for the VMM library server.

After completing this step, there will be a list of library servers, their scaling and fault-tolerance requirements, and their placement.

Task 1: Determine the Placement of the VMM Library Server

Each VMM instance must have at least one VMM library server, and VMM instances cannot share library servers because each library server runs a VMM agent.

The images stored in the VMM library can be very large, and when they are transferred to a virtual machine host during virtual machine creation, a significant traffic load is created on the network. For this reason, the VMM engineering team recommends that VMM library servers be placed in the same location as the virtual machine hosts that they will service. The library server must be in the same domain as the VMM management server, or in a domain that has a two-way trust with the domain of the VMM management server (including domains with disjointed namespaces).

Note Do not create clustered file shares for the VMM library on the same cluster as a clustered VMM management server installation. VMM does not support this configuration.

Determine where to place the VMM library server and record the answer in Table A-6 in Appendix A.

Task 2: Determine the Number of Servers Required for Scaling

In this task, the constraints of the software are applied to determine the number of VMM library servers required for scaling.

A VMM management server can be connected to more than one VMM library server. The number of VMM library servers required may vary depending on a number of factors, including but not limited to, the quantity and size of the files that will be stored in the library.

Use Table A-6 in Appendix A to estimate the expected size. Determine whether one server is sufficient, and if not, add additional library servers as needed. If a VMM instance requires more than one library server, Tasks 3 and 4 should be completed for each server.

Task 3: Apply the Fault-Tolerance Requirements

If the VMM library were to fail, administrators will be unable to provision virtual machines or create services.

To provide fault tolerance for file-based resources on a VMM library server, cluster the file server containing the shared folder. For more information, see Create a Shared Folder in a Clustered File Server at http://technet.microsoft.com/library/dd197480(WS.10).aspx.

If there is a requirement for fault tolerance of the VMM library, do not create clustered file shares for the VMM library on the same cluster as a clustered VMM management server installation. VMM does not support this configuration.

Another way to provide functionality similar to fault tolerance without clustering is through the use of equivalent objects. For more information on equivalent objects, refer to How to Create or Modify Equivalent Objects in the Library at http://technet.microsoft.com/en-us/library/gg610650.aspx.

Equivalent objects allow the use of any instance of certain file-based resources (specifically .vhd files, .iso images, and custom resources) instead of the site-specific one. This allows VMM to perform virtual machine and service deployment in the event of a VMM library server failure. For example, a Windows Server 2008 R2-based VHD file that is located on a library share in Seattle and a Windows Server 2008 R2-based VHD file that is located on a library share in New York may be marked as equivalent.

Note VMM does not provide a method for replicating physical files in the VMM library or metadata for objects stored in the VMM database. Physical files must be replicated outside of VMM and metadata must be transferred by using scripts or other means. VMM does not support DFS Namespaces (DFSN), formerly known as Distributed File System (DFS), or DFS Replication.

For each set of resources in a given VMM library, decide the fault-tolerance methods to be used and record the decision in Table A-6 in Appendix A.

Task 4: Determine the Hardware Configuration

In this task, the hardware configuration for the VMM library server will be determined. Table 9 lists the minimum and recommended hardware requirements for the VMM library server.

For more information, such as the software requirements and the operating systems supported, see System Requirements: VMM Library Server at http://technet.microsoft.com/en-us/library/gg610631.aspx.

Table 9. VMM Library Server Minimum and Recommended Hardware Requirements

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Dual-core, 3.2 GHz or greater (x64)
RAM	2 GB	2 GB
Hard disk space	Varies based on the number and size of files stored in the library.	Varies based on the number and size of files stored in the library.

For more information about the storage supported by VMM, see Configuring Storage Overview at http://technet.microsoft.com/en-us/library/gg610600.aspx. After deciding what the VMM library server's hardware configuration will be, the applicable information should be documented in Table A-6 in Appendix A. If a VMM instance requires more than one library server, each server must be recorded separately.

Step Summary

After completing this step, the following information was recorded in Table A-6 in Appendix A for each VMM instance to determine each library server's requirements:

- The placement of the VMM library servers in relation to the virtual machine hosts.
- The number of VMM library servers required for scaling.
- The fault-tolerance methods to be used for VMM library resources.
- The hardware configuration for the VMM library server.

Proceed to Step 6 to design the Update Services infrastructure.

Additional Reading

- Managing the VMM Library: http://technet.microsoft.com/en-us/library/cc764248.aspx
- Configuring the Library Overview: http://technet.microsoft.com/en-us/library/gg610598.aspx
- System Requirements: VMM Library Server: http://technet.microsoft.com/en-us/library/gg610631.aspx
- Overview of Failover Clusters: http://technet.microsoft.com/library/cc730692.aspx
- Installing a SQL Server 2008 R2 Failover Cluster: http://msdn.microsoft.com/en-us/library/ms179410(v=sql.105).aspx
- Installing a SQL Server 2008 Failover Cluster: http://msdn.microsoft.com/en-us/library/ms179410(v=sql.100).aspx

Step 6: Design the Update Services Infrastructure

In the previous step, the library servers and libraries were designed. The goal of this step is to determine if integration with Windows Server Update Services (WSUS) is required and the placement of the WSUS server, which is used to perform updates.

VMM provides the capability to use a WSUS server to manage updates for the following computers in the VMM environment:

- Virtual machine hosts
- Library servers
- VMM management server
- PXE servers
- WSUS server

In addition to utilizing the WSUS infrastructure, VMM provides additional capabilities such as the ability to create and configure update baselines, on-demand scanning of computers for compliance, on-demand performance of update remediation, and orchestrated Hyper-V cluster remediation.

VMM supports using a WSUS server that is part of a Configuration Manager 2007 R2 or System Center 2012 Configuration Manager environment, but additional configuration steps are required. This will also enable the use of the reporting capabilities of Configuration Manager to provide compliance information. For more information, see How to Integrate Fabric Updates with Configuration Manager at http://go.microsoft.com/fwlink/p/?LinkID=226439.

Note If an existing WSUS server from a Configuration Manager environment is used, changes to configuration settings for the WSUS server (for example, update classifications, languages, and proxy settings) should only be made from Configuration Manager. The VMM administrator can view the configuration settings from the VMM console, but cannot make changes. For details on setting VMM as the non-authoritative source, see the previous article.

Integrating VMM and WSUS enables users to reduce the effort required to help ensure the fabric resources are in compliance with established configuration baselines. When using a new WSUS server, VMM administrators can manage configuration compliance using the VMM console.

The relationship between VMM instance and WSUS is one-to-one. A WSUS instance cannot be shared by more than one VMM instance. However, a WSUS instance used by Configuration Manager can also be used by a VMM instance.

VMM can use either a WSUS root server or a downstream WSUS server. VMM does not support using a WSUS replica server.

If VMM will process a very large volume of updates, consider installing the WSUS server on a separate computer from the VMM management server.

Record the decision made in this step in Table A-7 in Appendix A. If the plan is to integrate VMM and WSUS, continue with this step. If the decision is not to integrate, or if the organization does not use WSUS, skip this step.

Option 1: Yes

Businesses that use WSUS can take advantage of the ability to perform configuration baseline compliance scanning and remediation using automated or on-demand methods. If the plan is to integrate VMM with WSUS, determine whether to:

- Deploy a new WSUS server that is dedicated to VMM.
- Use an existing WSUS server that is part of a Configuration Manager environment.

Benefits

New WSUS server:

- Ability to manage configuration baselines within the VMM console.
- Does not require existing Configuration Manager environment.

Existing WSUS server:

- Reduced deployment cost by using existing WSUS server.
- Centralized reporting via Configuration Manager reporting.

Challenges

New WSUS server:

- The cost of deploying a dedicated WSUS server.
- Potential duplication of administrative effort if WSUS server exists as a part of a Configuration Manager environment.

Option 2: No

If the decision is made not to integrate VMM with WSUS, users can still take advantage of the configuration baselines and remediation that Configuration Manager provides. They will not be able to manage the fabric compliance within the VMM console. The result of no integration is that users must rely on two consoles instead of one.

If the organization does not use WSUS, or if the decision is made not to integrate VMM with WSUS, the design is complete.

Validating with the Business

If VMM is not integrated with WSUS, then fabric configuration compliance with established baselines must be performed using another method. This will require VMM administrators to use multiple consoles and potentially multiple products from multiple vendors to manage configuration compliance.

An evaluation of the cost and complexity of integrating VMM with WSUS should be reviewed with the business stakeholders and the people responsible for configuration compliance updates and/or Configuration Manager to see if the integration is warranted.

Step Summary

After completing this step, the decision of whether to integrate VMM with WSUS was made and recorded in Table A-7 in Appendix A.

Proceed to Step 7 to design self-service capabilities using App Controller.

Additional Reading

- Windows Server Update Services home page: http://technet.microsoft.com/en-us/windowsserver/bb332157
- *Infrastructure Planning and Design Guide for System Center Configuration Manager 2007*: http://go.microsoft.com/fwlink/?LinkId=160983

Step 7: Design the App Controller Infrastructure

In the previous step, the update services infrastructure was designed. In this step, the infrastructure for App Controller will be determined. (If it was decided in Step 1 that self-service capabilities will be required, then complete this step to design that functionality.)

System Center 2012 - App Controller provides self-service capabilities for private clouds managed by VMM and Windows Azure™ public clouds. This guide focuses only on using App Controller with VMM to provide self-service capabilities for private clouds.

App Controller consists of:

- The App Controller server. Multiple servers may be added for fault tolerance but do not increase the scaling limits of App Controller.
- The App Controller database server.

The App Controller server performs the following functions:

- Provides a web-based interface for self-service users.
- Reads and writes the App Controller configuration from the App Controller database.
- Manages services and virtual machines for connected private clouds managed by VMM.
- Reads and writes private cloud content stored in the VMM library, network file shares, or Windows Azure storage accounts.
- Runs Windows PowerShell® cmdlets and scripts to manage App Controller.
- Runs App Controller jobs.

The App Controller database server performs the following functions:

- Contains the App Controller configuration.
- Communicates with the App Controller server.

The tasks to be performed in this step are:

1. Determine the number of App Controller instances required.
2. Determine the placement of the App Controller server and App Controller database server.
3. Apply the fault-tolerance requirements for the server and database.
4. Determine the hardware configuration for the server and database.

Record the information gathered in this step in Table A-8 in Appendix A. Repeat this step for each VMM instance identified in Step 3.

Note The VMM Self-Service Portal is deprecated, meaning that it will not be included in future releases of VMM. In System Center 2012, it is recommended to use System Center 2012 - App Controller as the self-service portal solution. For more information about App Controller, see App Controller in the TechNet Library at http://technet.microsoft.com/en-us/library/hh546834.aspx. If the organization needs the VMM Self-Service Portal for temporary backward compatibility, then see Appendix B: "The Self-Service Portal" in this guide for more information on the design process for that product.

Task 1: Determine the Number of App Controller Instances Required

In this task, the number of App Controller instances required for the VMM infrastructure will be determined. An App Controller instance is composed of a server and database. Instances are separate and do not communicate with each other.

Start with a single instance of App Controller, and add additional instances only if the following scale limits are exceeded:

- Up to 5 VMM management servers.
- Up to 75 concurrent users.
- Up to 10,000 jobs run in a 24-hour interval.

Record this information in Table A-8 in Appendix A. The remaining tasks in this step should be repeated for each App Controller instance identified.

Task 2: Determine the Placement

In this task, the placement of the App Controller server or servers will be decided.

The App Controller server interacts with these components:

- App Controller database server
- VMM management servers
- AD DS
- Other file shares as specified by the App Controller administrator

Note The App Controller server can also interact with Windows Azure, but this guide focuses on VMM.

Place the App Controller servers with a persistent, high-speed connection to all of these components.

All roles can be run in a virtual machine. They can be co-located on the same computer or they can be run on separate computers. For better performance, separate the roles onto different servers, including being separated from the VMM management server.

Ensure that all roles are in the same AD DS forest or are in a domain that has a two-way trust with the domains where these components are located.

Record the placement of the App Controller server and database server in Table A-8 in Appendix A.

Task 3: Apply the Fault-Tolerance Requirements

In this task, if the self-service provisioning must be made fault tolerant, then the methods for achieving it and the impacts to the design will be decided.

App Controller Server

The App Controller server is stateless and can be made fault tolerant by installing multiple App Controller servers behind a load balancer using a hardware load balancer or Network Load Balancing (NLB).

App Controller Database Server

The App Controller database server is stateful and can be made fault tolerant by installing the database on a clustered SQL Server.

Additional resiliency to failure can be achieved by implementing App Controller and its dependencies on clustered Hyper-V hosts.

Record the method for achieving fault tolerance and the number of App Controller servers added as a result of this design decision in Table A-8 in Appendix A.

Task 4: Determine the Hardware Configuration

In this task, the hardware configuration for the App Controller servers and App Controller database servers will be determined.

App Controller Server

Table 10 lists the minimum and recommended hardware requirements for the App Controller server. For more information, see System Requirements—Server: Hardware Requirements at http://technet.microsoft.com/en-us/library/gg696060.aspx.

Table 10. App Controller Server Minimum and Recommended Hardware Requirements

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2 GHz (x64)	Dual-processor, dual-core, 2.8 GHz or greater (x64)
RAM	2 GB	4 GB
Hard disk space (without a local VMM database)	512 megabytes (MB)	1 GB
Hard disk space (with a local, full version of Microsoft SQL Server)	80 GB	150 GB

App Controller Database Server

Standard SQL Server requirements are sufficient for the App Controller database server. For more information on SQL Server requirements, refer to System Requirements: VMM Database at http://technet.microsoft.com/library/gg610574.aspx.

Record the hardware configurations of the server and database server in Table A-8 in Appendix A.

Step Summary

After completing this step, the following App Controller infrastructure has been designed and recorded in Table A-8 in Appendix A:

- The number of App Controller instances required.
- The App Controller server for each VMM instance, including the number, placement, fault tolerance, and hardware configuration.
- The App Controller database server for each App Controller instance, including the number, placement, fault tolerance, and hardware configuration.

Additional Reading

- Setting up App Controller: http://technet.microsoft.com/en-us/library/gg696035.aspx
- About the App Controller Library: http://technet.microsoft.com/en-us/library/hh221363.aspx
- System Requirements: http://technet.microsoft.com/en-us/library/gg696060.aspx

Conclusion

This guide summarized the critical design decisions, activities, and tasks required to successfully design a VMM infrastructure. This guide addressed the fundamental decisions and tasks involved in:

- Identifying the business and technical requirements for managing virtualization.
- Determining whether to integrate VMM with Operations Manager and how to design that integration.
- Determining the number of VMM management servers the organization requires, including each server's size, hardware configuration, and placement.
- Determining whether to integrate VMM with WSUS and how to design that integration.
- Determining whether to integrate VMM with App Controller and how to design that integration.

This guide described steps for creating a design based on the organization's business and technical requirements. This guide illustrated typical usage scenarios in the decisions and tasks. It discussed the technical aspects, characteristics, and business requirements needed to complete a comprehensive review of the decision-making process.

After planning and designing the architecture, limited pilot tests should be conducted before beginning a major rollout. Incorporate lessons learned from the pilot tests back into the design.

When used in conjunction with the VMM product documentation, this guide allows organizations to confidently plan the implementation of VMM.

Appendix A: Job Aids

Use the following job aids to record the decisions made in each step. The grey text represents sample language that illustrates how each task might be completed.

Step 1. Use Table A-1 to record the answers asked of the business to determine the features and scope of the project.

Table A-1. Business Requirements

Question	Answer
Which parts of the organization will participate?	
Would a business or governance policy affect the design of the system?	
Does the business want users to be able to perform self-service provisioning?	
Will additional locations be used for geographic failover or disaster recovery?	
Will the organization require virtual desktop infrastructure (VDI)?	
Will VMM integrate with Operations Manager to monitor the health and availability of the virtual machines and virtual machine hosts that VMM manages?	
What are the availability requirements for VMM?	

Step 1. Use Table A-2 to record the answers asked of the technical decision makers to determine the scope and requirements of the project.

Table A-2. Technical Requirements

Question	Answer
What virtualization technology, if any, will each location use?	
What virtual machine management technology, if any, will each location use?	
How many virtual machine hosts, if any, will be implemented at each location?	
How many virtual machines, if any, will be implemented at each location, and what type will they be?	
If the business decision makers decided in Task 1 to implement self-service provisioning, what is the approximate number of users and where are they located?	
Does the organization plan to implement a new update server or integrate with an existing software updates infrastructure, and if so which one?	

Step 2. Use Table A-3 to record the decision made by the business regarding Operations Manager integration.

Table A-3. Operations Manager Integration

Type of integration	Selection
Option 1: Multiple VMM instances or Option 2: Dedicated management group for VMM?	
If Option 1: Which management groups will contain virtual machine hosts?	
If Option 2: Specify the management group name.	
If Option 2: Specify the names of the Operations Manager agents that will be multihomed to the management group.	

Step 3. Use Table A-4 to record criteria for the need for additional VMM instances.

Table A-4. VMM Instances

Instance	Yes/No	Number
Isolated networks or test environments		
Scaling limits exceeded		
Self-service provisioning only applying to parts of the scope		
Self-service provisioning scaling limits exceeded		
Supporting VDI desktops		
The number of Operations Manager management groups required		
Matching the desired management model (local/centralized/hybrid)		
Organizational or political considerations		
Disaster recovery functionality		

Step 4. Use Table A-5 to record the placement, fault tolerance, and hardware configuration of the VMM management servers and VMM database.

Table A-5. VMM Server Instance Configuration and Placement

	Management servers	Database servers
Placement		
Fault tolerance		
Hardware configuration		

Step 5. Use Table A-6 to record the placement, scaling, fault tolerance, and hardware configuration of the VMM library server.

Table A-6. VMM Library Server Configuration and Placement

	Library servers
Placement	
Number required for scaling	
Fault tolerance	
Hardware configuration	

Step 6. Use Table A-7 to record whether the organization will integrate VMM and WSUS.

Table A-7. VMM and WSUS Integration

Question	Answer
Will the organization integrate VMM and WSUS?	
If yes, will new or existing deployments of WSUS be used?	

Step 7. Use Table A-8 to record the number, placement, fault tolerance, and hardware configuration of the App Controller server and App Controller database server.

Table A-8. App Controller Configuration and Placement

	App Controller server	App Controller database server
Number		
Placement		
Fault tolerance		
Hardware configuration		

Appendix B: The Self-Service Portal

VMM provides a Self-Service Portal that allows users to provision virtual machines to virtual machine hosts without administrator intervention. Alternatively, users can use the VMM console to provision virtual machines.

Note The VMM Self-Service Portal is deprecated, meaning that it will not be included in future releases of VMM. In System Center 2012, it is recommended to use System Center 2012 - App Controller as the self-service portal solution. For more information about App Controller, see App Controller in the TechNet Library at http://technet.microsoft.com/en-us/library/hh546834.aspx.

The VMM Self-Service Portal server is used to communicate between the VMM management server and Self-Service Portal users. It performs the following functions:

- Receives display requests from the web consoles.
- Sends configuration and performance data to the web consoles for display.

The Self-Service Portal requires a Microsoft Internet Information Services (IIS) server. For more information about planning and designing an IIS infrastructure, see the *Infrastructure Planning and Design Guide for Internet Information Services 7.0 and Internet Information Services 7.5* at http://go.microsoft.com/fwlink/?LinkId=157703.

Note Installing the VMM Self-Service Portal on a domain controller is not supported.

The Self-Service Portal is based on IIS; the fault-tolerance options available are hardware or software load balancing. This is incompatible with clustering, so the Self-Service Portal should not be co-located with the VMM management server or VMM database if fault tolerance is required.

Note For improved performance, deploy the Self-Service Portal on a dedicated server.

Tables B-1 and B-2 list the minimum and recommended hardware requirements for the VMM Self-Service Portal based on the number of concurrent connections to the web server. For more information, see System Requirements: VMM Self-Service Portal at http://technet.microsoft.com/en-us/library/gg697607.aspx.

Table B-1. VMM Self-Service Portal Minimum and Recommended Hardware Requirements for Maintaining Less than 10 Concurrent Connections

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2.8 GHz	Dual-core, 2 GHz (x64)
RAM	2 GB	4 GB
Hard disk space	80 GB	150 GB

Table B-2. VMM Self-Service Portal Minimum and Recommended Hardware Requirements for Maintaining More than 10 Concurrent Connections

Hardware component	Minimum	Recommended
Processor	Dual-core, 2 GHz (x64)	Dual-core, 2.8 GHz (x64)
RAM	4 GB	8 GB
Hard disk space	150 GB	200 GB

Appendix C: 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 C-1. The architecture of Microsoft Operations Framework (MOF) 4.0

Appendix D: VMM in Microsoft Infrastructure Optimization

The Infrastructure Optimization (IO) Model at Microsoft groups IT processes and technologies across a continuum of organizational maturity. (For more information, see http://go.microsoft.com/fwlink/?LinkId=229236.) The model was developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR), and Microsoft's own experiences with its enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can easily be applied as the benchmark for technical capability and business value.

IO is structured around three information technology models: Core Infrastructure Optimization, Application Platform Optimization, and Business Productivity Infrastructure Optimization. According to the Core Infrastructure Optimization Model, automated, centralized management of virtual machine hosts can move an organization to the Rationalized level. On the path to the Dynamic level, organizations can use self-service provisioning to enable users to automatically provision virtual machines to the most suitable hosts.

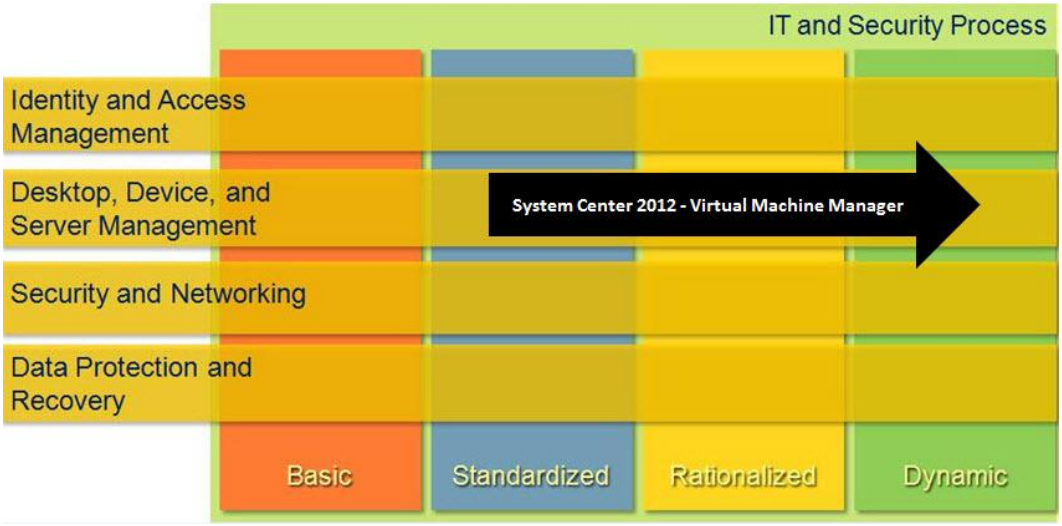

Figure D-1. Mapping of Virtual Machine Manager technology into the Core Infrastructure Optimization Model

Version History

Version	Description	Date
1.0	First release.	July 2012

Acknowledgments

The Solution Accelerators–Management and Infrastructure (SA-MI) team acknowledges and thanks the people who produced the *Infrastructure Planning and Design Guide for System Center 2012 - Virtual Machine Manager*. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this guide or its predecessor, the *Infrastructure Planning and Design Guide for System Center Virtual Machine Manager 2008*.

Contributors:

- Jude Chosnyk – *GrandMasters*
- Joe Coulombe – *Microsoft*
- Jerry Honeycutt – *Studio B Productions*
- Michael Kaczmarek – *Microsoft*
- Robin Maher – *Microsoft*
- Doug Steen – *Xtreme Consulting Group*
- Fergus Stewart – *Microsoft*
- Melissa Stowe – *Microsoft*
- Michelle Travis – *GrandMasters*

Reviewers:

- Virginia Benedict
- Tabrez Mohammed – *Microsoft*
- Richard Rundle – *Microsoft*
- Carmen Summers – *Microsoft*

Editor:

- Laurie Dunham – *Xtreme Consulting Group*

Feedback

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