

Managing and Operating   
a Microsoft® Private Cloud

How to Apply the Microsoft Operations Framework (MOF)

Version 1.0

Published: July 2012

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

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

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

[Overview 1](#_Toc329088738)

[Audience 1](#_Toc329088739)

[How to Use This Guide 1](#_Toc329088740)

[What Is a Private Cloud? 1](#_Toc329088741)

[Microsoft Private Cloud 2](#_Toc329088742)

[Microsoft Private Cloud Conceptual Components 3](#_Toc329088743)

[How MOF Applies to a Private Cloud 4](#_Toc329088744)

[MOF Manage Layer Overview 5](#_Toc329088745)

[MOF Operate Phase Overview 5](#_Toc329088746)

[MOF Management Reviews Overview 6](#_Toc329088747)

[MOF Manage Layer 7](#_Toc329088748)

[Managing Governance, Risk, and Compliance 7](#_Toc329088749)

[Applying GRC to the Self-Service Layer 7](#_Toc329088750)

[Applying GRC to the Orchestration Layer 7](#_Toc329088751)

[Applying GRC to the Management Layer 8](#_Toc329088752)

[Applying GRC to the Automation Layer 8](#_Toc329088753)

[Applying GRC to Virtualization 9](#_Toc329088754)

[Managing Change and Configuration 9](#_Toc329088755)

[Applying Change and Configuration to the Self-Service Layer 9](#_Toc329088756)

[Applying Change and Configuration to the Orchestration Layer 10](#_Toc329088757)

[Applying Change and Configuration to the Management Layer 10](#_Toc329088758)

[Applying Change and Configuration to the Automation Layer 11](#_Toc329088759)

[Applying Change and Configuration to Virtualization 11](#_Toc329088760)

[Managing Teams 11](#_Toc329088761)

[Applying Team Management to the Self-Service Layer 11](#_Toc329088762)

[Applying Team Management to the Orchestration Layer 12](#_Toc329088763)

[Applying Team Management to the Management Layer 12](#_Toc329088764)

[Applying Team Management to the Automation Layer 13](#_Toc329088765)

[Applying Team Management to Virtualization 13](#_Toc329088766)

[Reviewing GRC, Changes, and Teams 13](#_Toc329088767)

[Conducting Reviews of the Self-Service Layer 14](#_Toc329088768)

[Conducting Reviews of the Orchestration Layer 15](#_Toc329088769)

[Conducting Reviews of the Management Layer 16](#_Toc329088770)

[Conducting Reviews of the Automation Layer 19](#_Toc329088771)

[Conducting Reviews of Virtualization 20](#_Toc329088772)

[MOF Operate Phase 22](#_Toc329088773)

[Operating a Private Cloud 22](#_Toc329088774)

[Conducting Operations in the Self-Service Layer 22](#_Toc329088775)

[Conducting Operations in the Orchestration Layer 23](#_Toc329088776)

[Conducting Operations in the Management Layer 25](#_Toc329088777)

[Conducting Operations in the Automation Layer 26](#_Toc329088778)

[Conducting Operations for Virtualization 27](#_Toc329088779)

[Monitoring a Private Cloud 29](#_Toc329088780)

[Monitoring and Maintaining the Self-Service Layer 29](#_Toc329088781)

[Monitoring and Maintaining the Orchestration Layer 31](#_Toc329088782)

[Monitoring and Maintaining the Management Layer 33](#_Toc329088783)

[Monitoring and Maintaining the Automation Layer 35](#_Toc329088784)

[Monitoring and Maintaining Virtualization 37](#_Toc329088785)

[Servicing Private Cloud Customers 39](#_Toc329088786)

[Conducting Customer Service for the Self-Service Layer 39](#_Toc329088787)

[Conducting Customer Service for the Orchestration Layer 40](#_Toc329088788)

[Conducting Customer Service for the Management Layer 40](#_Toc329088789)

[Conducting Customer Service for the Automation Layer 41](#_Toc329088790)

[Conducting Customer Service for Virtualization 41](#_Toc329088791)

[Managing Private Cloud Problems 42](#_Toc329088792)

[Identifying Problems in the Self-Service Layer 42](#_Toc329088793)

[Identifying Problems in the Orchestration Layer 43](#_Toc329088794)

[Identifying Problems in the Management Layer 43](#_Toc329088795)

[Identifying Problems in the Automation Layer 44](#_Toc329088796)

[Identifying Problems with Virtualization 44](#_Toc329088797)

[Reviewing Operations 45](#_Toc329088798)

[Conducting an Operational Health Management Review for the Self-Service Layer 45](#_Toc329088799)

[Conducting an Operational Health Management Review for the Orchestration Layer 46](#_Toc329088800)

[Conducting an Operational Health Management Review for the Management Layer 47](#_Toc329088801)

[Conducting an Operational Health Management Review for the Automation Layer 48](#_Toc329088802)

[Conducting an Operational Health Management Review for Virtualization 48](#_Toc329088803)

[Conclusion 50](#_Toc329088804)

[Version History 51](#_Toc329088805)

[Acknowledgments 52](#_Toc329088806)

[Feedback 52](#_Toc329088807)

# Overview

This guide describes how to manage and operate a Microsoft private cloud using the service management processes of the Microsoft® Operations Framework (MOF). MOF is a framework that helps IT organizations plan, create, operate, and support IT services that deliver expected business value at an acceptable level of risk.

The guide assumes an organization has already built an infrastructure-as-a-service private cloud environment based on one of Microsoft’s three private cloud options, using the conceptual architecture and technical components that are recommended. More information about those options can be found in the “Microsoft Private Cloud” section of this guide.

The guide applies MOF’s IT service management principles to that conceptual architecture and technology stack. However, the guide’s approach and principles can be applied to any private cloud, regardless of the technology used, with the understanding that the specific technical references will not be relevant.

## Audience

This guide is intended for the IT service management community, IT architects, IT managers, and others interested in how to effectively operate and manage a private cloud environment.

## How to Use This Guide

There are two ways you can use this guide.

One approach is to read it from start to finish. That approach will give you a fairly complete and in-context picture of how to manage and operate a private cloud. You will notice, however, that much of the material will seem similar or repetitive. That is because different sets of MOF activities are mapped against the same five conceptual architecture and technical components.

A second approach is to use the guide as a reference document. You can use the Microsoft Excel® spreadsheet that accompanies this guide for that approach. The spreadsheet maps MOF activities against private cloud conceptual layers and technical components. So, for example, if you’re interested in information about operating the Orchestration Layer of a private cloud, you would map the Operations Service Management Function (SMF) against the Orchestration Layer, and read the contents of the grid square at that intersection point. If the concise description there makes you want to know more, you could then use the table of contents of this guide to find the section that describes how to operate the Orchestration Layer.

## What Is a Private Cloud?

Cloud computing in general is delivering computing as a service rather than as a product to a homogeneous community of end-recipients. It is typically based on shared resources, software, and information that are provided to computers and other devices as a utility, over a network, typically the Internet. A private cloud is the implementation of cloud services on resources that are dedicated to an organization, whether they exist on-premises or off-premises.

### Microsoft Private Cloud

Microsoft offers private cloud options built on Windows Server® 2008 R2 Hyper-V® and Microsoft System Center. The foundation is built on the Windows Server platform with the Windows Server Active Directory® identity framework, Hyper-V virtualization, and deep application insight through System Center, which allows datacenter administrators to deploy a flexible and responsive infrastructure designed to simplify day-to-day tasks and enable management of applications at the service level, rather than the level of individual servers.

The three options for getting a Microsoft private cloud are:

* Build your own private cloud using a set of engagements to help you with assessments, proofs-of-concept, and deployments through Microsoft partners or Microsoft Services.

More information about partner options is available at [www.microsoft.com/en-us/server-cloud/private-cloud/hyperv-cloud-deployment.aspx](http://www.microsoft.com/en-us/server-cloud/private-cloud/hyperv-cloud-deployment.aspx).

More information about Microsoft Services’ Datacenter Services is available at [www.microsoft.com/microsoftservices/en/us/datacenter\_services.aspx](http://www.microsoft.com/microsoftservices/en/us/datacenter_services.aspx).

* Get a prevalidated private cloud configuration from Microsoft Private Cloud Fast Track OEM partners. Microsoft Private Cloud Fast Track partners have worked with Microsoft to combine hardware and software offerings based on a reference architecture for building private clouds.

More information is available at [www.microsoft.com/en-us/server-cloud/private-cloud/hyperv-cloud-fast-track.aspx](http://www.microsoft.com/en-us/server-cloud/private-cloud/hyperv-cloud-fast-track.aspx).

* Find a service provider in the Microsoft Private Cloud Service Provider Program who can host a dedicated private cloud for you.

More information is available at [www.microsoft.com/en-us/server-cloud/private-cloud/hyperv-cloud-service-providers.aspx](http://www.microsoft.com/en-us/server-cloud/private-cloud/hyperv-cloud-service-providers.aspx).

Microsoft private cloud architecture principles conform to the cloud attributes outlined by the National Institute of Standards and Technology (NIST) definition of cloud computing version 15. Those attributes are:

* **On-demand self-service**. Allows a consumer to automatically provision computing capabilities, such as server time and network storage, without human interaction with each service provider.
* **Broad network access**. Allows a consumer to easily access the features and services using standard devices that promote simple use. Laptops, PDAs, mobile phones, and smart phone browsers and apps are a part of this category.
* **Resource pooling**. The provider’s computing resources are pooled to serve multiple consumers using a multitenant model, with different physical and virtual resources dynamically assigned and reassigned, according to consumer demand. There is a sense of location independence because the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (for example, country/region, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.
* **Rapid elasticity**. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward depending on demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
* **Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (for example, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and the consumer of the service.

Specifically, the Microsoft private cloud architecture is based on these seven principles:

* Resource pooling
* Elasticity and the perception of infinite capacity
* Perception of continuous availability
* Predictability
* Supporting chargeback and showback capabilities
* Multitenancy
* Security and identity

### Microsoft Private Cloud Conceptual Components

Included within the reference architecture of Microsoft’s private cloud approach are five conceptual layers that address the use and maintenance of the cloud. This view is important because it provides a conceptual picture of what goes into a private cloud, and also provides attachment points for the IT service management activities used to manage and operate a private cloud.

Those conceptual layers are:

* Self-Service. The Self-Service Layer provides an interface for private cloud tenants or authorized users to request, manage, and access the services, such as virtual machines, provided by the cloud architecture. Using role-based access control and authorization, the Self-Service Layer provides the ability to delegate certain aspects of administration (such as starting/stopping virtual machines) to designated “tenant administrators.”
* Orchestration. The Orchestration Layer takes advantage of the Management and Automation layers. In much the same way that an enterprise resource planning (ERP) system manages a business process such as order fulfillment and handles exceptions such as inventory shortages, the Orchestration Layer provides an engine for IT-process automation and workflow. The Orchestration Layer is the critical interface between the IT organization and its infrastructure. It is the layer at which intent is transformed into workflow and automation.

Ideally, the Orchestration Layer provides a graphical interface in which complex workflows that consist of events and activities across multiple management-system components can be combined, so as to form an end-to-end IT business process such as automated patch management or automatic power management. The Orchestration Layer must provide the ability to design, test, implement, and monitor these IT workflows.

* Management. The Management Layer consists of the tools and systems used to deploy and operate the infrastructure. In most cases, this consists of a variety of different toolsets for managing hardware, software, and applications. Ideally, all components of the management system would take advantage of the Automation Layer and not introduce their own protocols, scripting languages, or other technologies (because it increases complexity and may require additional staff expertise).

The Management Layer is used to perform activities such as provisioning the storage area network (SAN), deploying an operating system, or monitoring an application. Key attributes are its abilities to manage and monitor every component of the infrastructure remotely and to capture the dependencies among all of the infrastructure components. This layer provides the tools and systems that deploy, operate, maintain, and monitor the infrastructure; these are the toolsets for managing hardware, software, and applications.

* Automation. The Automation Layer helps automate basic operations over the lifetime of a hardware or software component. It consists of foundational automation technologies, plus a series of single-purpose commands and scripts that perform operations such as starting or stopping a virtual machine, restarting a server, and applying a software update.
* Services Management. This layer offers a service management perspective that provides the means for automating and adapting IT service management best practices, such as those found in Microsoft Operations Framework (MOF). This guide addresses that layer by mapping MOF’s IT service management best practices against the other four layers

Those five layers are underpinned by virtualization, which provides abstraction of computer resources for storage, network, and server.

For more information about the Microsoft private cloud conceptual architecture, see <http://social.technet.microsoft.com/wiki/contents/articles/4493.private-cloud-technical-overview.aspx>.

## How MOF Applies to a Private Cloud

MOF is an IT service management framework that helps translate service management principles to everyday IT tasks and activities. Its goal is to align IT with business needs.

It defines the core processes, activities, and accountabilities required to plan, deliver, operate, and manage services throughout their lifecycles. MOF organizes those activities and processes into service management functions (SMFs). Those SMFs describe the major activities that occur within each phase of the IT lifecycle that MOF is built around.

The MOF lifecycle is divided into four segments. Three of those segments describe the typical path followed for planning, delivering, and operating a new or improved IT service. They are called *phases* in MOF. The fourth segment describes activities that occur in multiple places throughout the lifecycle. It is called a *layer* in MOF. The terms *phase* and *layer* are just words used to describe a logical grouping of activities.

The three phases and one layer are:

* Plan Phase. This phase focuses on planning and optimizing an IT service strategy that supports business goals and objectives. It addresses business/IT alignment, reliability, policy management, and financial management.
* Deliver Phase. This phase ensures that IT services are developed effectively, are deployed successfully, and are ready for operations. It addresses project level planning, building, and deploying of new services.
* Operate Phase. This phase ensures that IT services are operated, maintained, and supported in a way that meets business needs and expectations. It addresses Operations, Service Monitoring and Control, Problem Management, and Customer Service.
* Manage Layer. This layer focuses on operating principles and best practices to ensure that IT delivers expected business value at an acceptable level of risk. It addresses governance, risk, and compliance; change management; and team management. MOF treats it as a layer because its activities occur throughout the three phases of the IT service lifecycle.

Although MOF in its entirety has three phases and a layer, this guide focuses only on the SMFs in the Operate Phase and the Manage Layer, because those explain what IT pros and managers need to know about managing and operating a private cloud. Three of MOF’s management reviews—internal controls that ensure goals are met to achieve business value—are also included.

The other two MOF phases—Plan and Deliver—along with the remaining three management reviews, focus on business/IT alignment for planning new or improved services, and deploying new or improved services. Those phases and their activities have impact on and are important to managing and operating a private cloud, but are not typically part of the ongoing work for IT pros.

Although MOF is a framework designed to be used in a variety of environments and with any technology, it can be applied to managing and operating a private cloud using Microsoft technologies. There is no prescribed order in which it must be applied, but the following order should work well because it starts with management reviews, which are periodic checks on how things are going, and ends with operations-focused activities, which are the steady state of managing and operating a private cloud.

More information about MOF can be found at <http://technet.microsoft.com/en-us/solutionaccelerators/dd320379.aspx>.

The following sections of this guide show at a high level how MOF’s activities connect to the conceptual layers of the private cloud, including the technical components that support each layer. Then the remainder of the guide examines those connections in more detail.

### MOF Manage Layer Overview

Manage Layer activities are the decision making, risk management, and change management processes that occur throughout the IT service lifecycle. They help determine who does what work and who is accountable for seeing that it gets done. The Manage Layer includes:

* Governance, risk, and compliance activities. Governance, risk, and compliance helps senior executives establish IT governance; assess, monitor, and control risk; and comply with directives. IT pros and managers are responsible for complying with directives and policies and helping to manage risk.
* Change and configuration activities. The primary goal of change and configuration management is to create an environment where changes are made with the least risk and impact to the organization.
* Team activities. Team management defines who is responsible for delivering IT services and making sure they are delivered.

### MOF Operate Phase Overview

The primary goal of the Operate Phase is to ensure that deployed services are operated, maintained, and supported in line with the service level agreement (SLA) targets that have been agreed to by the business and IT. The Operate Phase includes:

* Operating activities. Operations are running, monitoring, and maintaining a service.
* Service Monitoring and Control activities. Service Monitoring and Control provides real-time monitoring of how healthy an IT system is, and real-time alerting when a system is not healthy.
* Customer Service activities. Customer Service focuses on meeting the needs of users who want a new IT service, have questions about a service, or are having trouble with a service.
* Problem Management activities. Problem Management is an effort to reduce the occurrence of failures with IT services by looking for common, underlying issues.

### MOF Management Reviews Overview

Management reviews are internal controls that ensure goals are met to achieve business value. IT pros and managers will typically participate in these reviews, and often be responsible for providing needed information. The reviews offer periodic checks on how well a private cloud is functioning. They are different from SMFs because they do not describe specific processes or activities, but the outcomes of a management review will likely initiate some of the activities described by SMFs.

Management reviews:

* Provide management oversight and guidance.
* Act as internal controls.
* Capture organizational progress—lessons learned, items to encourage or avoid.
* Measure service development and delivery so they can be improved.

Three MOF management reviews apply directly to managing and operating a private cloud. They are:

* Operational Health Management Review, which:
* Evaluates whether the cloud is operating efficiently.
* Evaluates whether the cloud is meeting expectations.
* Remediates if change is needed.
* Service Alignment Management Review, which:
* Evaluates whether the cloud is providing expected business value.
* Identifies items that can enhance business alignment and/or business innovation.
* Initiates new cloud enhancements, if they are needed.
* Policy and Control Management Review, which:
* Reviews operational experiences and determines the appropriateness and effectiveness of current policies and controls.
* Adds or modifies policies and controls as appropriate.

The other three MOF management reviews—Portfolio, Project Plan Approved, and Release Readiness—relate more to the business planning and project management activities involved in developing new services, or improving existing ones, and so are not covered in this guide.

Depending on the size of an organization, it can be useful to treat these as separate reviews done at separate times. However, they can also be done as a single, periodic review, as long as that review focuses on all three areas—operational health, service alignment, and policy and control.

More detailed information about management reviews can be found at [www.microsoft.com/download/en/details.aspx?displaylang=en&id=17647](http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17647).

The remainder of this guide addresses the details of applying Manage Layer and Operate Phase SMFs to the layers of a private cloud and the technical components that underlie those layers. The management review activities are addressed within each of those two segments.

# MOF Manage Layer

The Manage Layer of MOF represents the foundation for all phases of the lifecycle. It promotes consistency in planning and delivering IT services and provides the basis for developing and operating a resilient IT environment.

The three SMFs in the layer are:

* Governance, Risk, and Compliance (GRC)
* Change and Configuration Management
* Team Management

Two management reviews would apply as well. They are:

* Service Alignment Management Review
* Policy and Control Management Review

## Managing Governance, Risk, and Compliance

The primary tasks for GRC are:

* Identify applicable regulations and standards.
* Create the policies and map the policies to control objectives.
* Identify and prioritize risks.
* Figure out what controls can be used to mitigate said risks; create the compliance plan.
* Maintain compliance, to operate the controls, and monitor for violations.
* Audit as needed.

### Applying GRC to the Self-Service Layer

The Self-Service Layer provides an interface that allows cloud tenants or authorized users to request, manage, and access services. The GRC goal is to ensure that the Self-Service Layer is in compliance with and supports organizational goals and policies by allowing Hyper-V cloud tenants or authorized users to request, manage, and access services, such as virtual machines.

The Microsoft System Center 2012 - Service Manager Service catalog and Portal serve as the provisioning user interface that allows groups within an organization to manage their own IT needs.

### Applying GRC to the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation. The GRC goal is to ensure that the Orchestration Layer is in compliance with and supports organizational goals and policies in how it provides the IT process automation and workflow needed for the cloud, without IT staff involvement.

Microsoft System Center 2012 - Orchestrator helps manage private clouds with a workflow designer that allows users to create *runbooks* (or lists of procedures) to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operations Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager (VMM), Active Directory Domain Services (AD DS), and third-party tools.

### Applying GRC to the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the Management Layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

The GRC goal is to ensure that the Management Layer is in compliance with and supports organizational goals and policies because it provides centralized administration and management of a virtual environment without IT staff involvement.

The Management Layer is supported by:

* System Center 2012 - Virtual Machine Manager, which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the VMM Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments. Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

The Microsoft IT GRC Process Management Pack for System Center Service Manager provides end-to-end compliance management and automation that helps translate complex regulations and standards into authoritative control objectives and activities for the IT organization’s compliance program. Microsoft Security Compliance Manager provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate your organization’s ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies.

### Applying GRC to the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update without IT staff involvement.

The GRC goal is to ensure that the Automation Layer is in compliance with and supports organizational goals and policies.

The Automation Layer is made up of three components. They are:

* Windows PowerShell®, which can be used to write scripts and cmdlets that System Center 2012 - Orchestrator uses in its integration with the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on computers based on the Windows® operating system.

### Applying GRC to Virtualization

Although virtualization is not a layer of the conceptual architecture, it is key to a private cloud because it enables better management and distribution of workloads across the physical infrastructure. In addition, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

The GRC goal is to ensure that virtualization services are in compliance with and support organizational goals and policies by abstracting computer resources for storage, network, and server without IT staff involvement.

Virtualization is supported by:

* Microsoft Hyper-V Server 2008 R2. Hyper-V Server provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager. VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

## Managing Change and Configuration

The primary tasks for change and configuration management are:

* Baseline the configuration.
* Submit a change request including a proposed classification of the change type.
* Get approval or rejection of the change.
* Write a change plan for the proposed change and test it (should identify ripple effects).
* Implement the change and communicate to necessary audiences.
* Verify the change worked and update the configuration in a configuration management system.

### Applying Change and Configuration to the Self-Service Layer

The Self-Service Layer provides an interface that allows cloud tenants or authorized users to request, manage, and access services. The goal of Change and Configuration Management for the layer is to ensure that changes to the Self-Service Layer are authorized and agile so that tenants or authorized users can request, manage, and access services without IT staff involvement, with a minimum of disruptions.

Change and Configuration Management for the Self-Service Layer would apply to the System Center 2012 - Service Manager service catalog and Portal, which serve as the provisioning user interface that allows groups within an organization to manage their own IT needs.

The primary administrative issue is ensuring someone is responsible for authorizing changes. Even standard changes require preapproval, typically by a body called a change advisory board (CAB). A change manager, who oversees the process and ensures all changes are authorized, is also needed.

### Applying Change and Configuration to the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation. The goal of Change and Configuration Management is to ensure that changes to the Orchestration Layer are authorized and agile so that it can effectively provide the IT process automation and workflow needed for the cloud without IT staff involvement.

Those changes would specifically apply to System Center 2012 - Orchestrator, which helps manage private clouds with a workflow designer that allows users to create runbooks to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operation Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager, Active Directory Domain Services, and third-party tools.

### Applying Change and Configuration to the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the Management Layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

The goal of Change and Configuration Management for the layer is to ensure that changes to the Management Layer are authorized and agile so that it can effectively provide centralized administration and management of a virtual environment without IT staff involvement.

Those changes specifically apply to:

* System Center 2012 - Virtual Machine Manager (VMM), which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the VMM Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments. Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

### Applying Change and Configuration to the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update without IT staff involvement.

The goal for Change and Configuration Management in the layer is to ensure that changes to the Automation Layer are authorized and agile.

Specifically, those changes apply to three components. They are:

* Windows PowerShell, which can be used to write scripts and cmdlets that System Center 2012 - Orchestrator uses in its integration with the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

### Applying Change and Configuration to Virtualization

Virtualization is key to a private cloud because it enables better management and distribution of workloads across the physical infrastructure. In addition, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

The goal for Change and Configuration Management in the layer is to ensure that changes to the Virtualization Layer are authorized and agile so that tenants or authorized users can request, manage, and access services without IT staff involvement with a minimum of disruptions.

Specifically, those changes apply to:

* Microsoft Hyper-V Server 2008 R2. Hyper-V Server provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager.VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

## Managing Teams

The primary tasks for team management are:

* Identify the work that needs to be done.
* Identify who is responsible for that work.
* Make sure the work gets done.

### Applying Team Management to the Self-Service Layer

The Self-Service Layer provides an interface that allows cloud tenants or authorized users to request, manage, and access services.

The goal of Team Management in the layer is to ensure that someone is ultimately accountable for operating and maintaining the private cloud self-service interface so that tenants or authorized users can request, manage, and access services without IT staff involvement, with a minimum of disruptions.

Specifically, Team Management addresses who works with the VMM Self-Service Portal 2.0, which serves as the provisioning user interface that allows groups within an organization to manage their own IT needs.

Team Management, with its focus on accountability for work that needs to be done, offers an approach to resolving the people issues that can happen when moving from a data center environment to a private cloud environment that is highly automated.

### Applying Team Management to the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation.

The goal for Team Management in the layer is to ensure that someone is ultimately accountable for operating and maintaining the Orchestration Layer so it can effectively provide the IT process automation and workflow needed for the cloud without IT staff involvement.

Specifically, Team Management applies to the people who work with System Center 2012 - Orchestrator, which helps manage private clouds with a workflow designer that allows users to create runbooks to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operation Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager, Active Directory Domain Services, and third-party tools.

### Applying Team Management to the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the management layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

The goal of Team Management is to ensure that someone is ultimately accountable for operating and maintaining the private cloud Management Layer so that it can effectively provide centralized administration and management of a virtual environment without IT staff involvement.

Specifically, Team Management applies to the people who work with:

* System Center 2012 - Virtual Machine Manager, which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the Virtual Machine Manager Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments. Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

### Applying Team Management to the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update without IT staff involvement.

The goal of Team Management in the layer is to ensure that someone is ultimately accountable for operating and maintaining the private cloud Automation Layer. Specifically, Team Management applies to the people who work with:

* Windows PowerShell, which can be used to write scripts and cmdlets that System Center 2012 - Orchestrator uses in its integration of the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

### Applying Team Management to Virtualization

Virtualization is key to a private cloud because it enables better management and distribution of workloads across the physical infrastructure. In addition, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

The goal of Team Management in the Virtualization Layer is to ensure that someone is ultimately accountable for operating and maintaining the private cloud Virtualization Layer that effectively abstracts computer resources for storage, network, and server, without IT staff involvement.

Specifically, team management applies to the people who work with:

* Microsoft Hyper-V Server 2008 R2. Hyper-V Server provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager.VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

## Reviewing GRC, Changes, and Teams

Two management reviews (MR) play a role in the Manage Layer. They are:

* Service Alignment Management Review
* Policy and Control Management Review

The goal of the Service Alignment Management Review is to validate and measure the quality and effectiveness of the private cloud, specifically examining the people, process, and technology elements.

The Policy and Control Management Review determines whether policies and controls are being applied appropriately to the private cloud, both from a process point of view, as well as determining whether the technology is performing within policy boundaries.

### Conducting Reviews of the Self-Service Layer

The **Service Alignment MR** helps measure the quality and effectiveness of the Self-Service Layer interface, both from a process point of view as well as looking at the performance of the Service Manager service catalog and Portal.

Its goal is to validate and measure the quality and effectiveness of the layer, specifically examining the people, process, and technology elements. When reviewing these elements, this review:

* Evaluates whether the Self-Service Layer of the cloud is providing expected business value.
* Identifies items that can enhance business alignment and/or business innovation.
* Initiates new cloud enhancements, if they are needed.

Attendees should include:

* IT management.
* Key personnel from the Self-Service Layer.
* Service level manager.

The review should address the following:

* **Reports/inputs:**
* Does the portal provide enough control over who can ask for services and resources?
* Are sufficient controls in place to manage GRC?
* **Analysis/decisions:**
* Are service requests made available to the appropriate end users who are entitled to make requests?
* **Tools to provide data:**
* System Center 2012 - Service Manager
* **Outcomes/outputs:**
* Documentation of the Service Alignment Management Review with actions and accountabilities.
* Requests for changes to specific policies or controls.
* Requests for changes to policy management.
* Modification of access to services and service requests within the portal.
* Updates to existing service requests to apply more rigor for GRC.
* Requests for changes to control management.

The **Policy and Control MR** determines whether policies and controls are being applied appropriately to the Self-Service Layer, both from a process point of view, as well as determining whether the technology is performing within policy boundaries.

It focuses on ensuring that management properly oversees and assesses:

* The adequacy of policies to address risk, regulatory, and compliance requirements.
* The organization’s effectiveness at ensuring that internal operating processes deliver on management’s objectives through formal policies and internal controls.
* Improvements to be made to existing policies, the need for new policies, and the termination of redundant or unnecessary policies.
* The general state and performance of the internal control environment.

Attendees should include:

* IT management.
* Key personnel from the Self-Service Layer.
* A compliance and GRC representative (optional).

The review should address the following:

* **Reports/inputs:**
* Does the portal provide enough control over who can ask for services and resources?
* Are sufficient controls in place to manage GRC?
* **Analysis/decisions:**
* Are service requests made available to the appropriate end users who are entitled to make requests?
* **Tools to provide data:**
* System Center 2012 - Service Manager
* **Outcomes/outputs:**
* Documentation of the Policy and Control Management Review with actions and accountabilities.
* Requests for changes to specific policies or controls.
* Requests for changes to policy management.
* Modification of access to services and service requests within the portal.
* Updates to existing service requests to apply more rigor for GRC.
* Requests for changes to control management.

### Conducting Reviews of the Orchestration Layer

The **Service Alignment MR** helps determine whether orchestration processes are functioning well, as well as whether System Center 2012 - Orchestrator is meeting customer needs and performance goals.

Its goal is to validate and measure the quality and effectiveness of the layer, specifically examining the people, process, and technology elements.

Attendees should include:

* IT management.
* Key personnel from the Orchestration Layer.
* Service level manager.

The review should address the following:

* **Reports/inputs:**
* Number of completed workflows per period.
* Number of failed workflows per period.
* Workflows/runbooks with errors.
* Activities/procedures where runbooks are needed.
* Identified improvements or new runbooks to be created.
* **Analysis/decisions:**
* Is the number of completed workflows on the rise/decline?
* Are workflow failures on the rise/decline?
* What service requests/standard changes can be automated?
* Where can new runbooks be used to improve efficiency and cost?
* What value is orchestration and expansion of orchestration providing the business?
* What cost benefits are realized by the investment in orchestration?
* **Tools to provide data:**
* System Center 2012 - Orchestrator
* System Center 2012 - Operations Manager
* System Center 2012 - Service Manager
* **Outcomes/outputs:**
* Improvements to runbooks/workflows.
* Problem and root-cause analysis for failures.
* New runbooks/workflows to be created.
* New standard change templates and workflows to be built.

The **Policy and Control MR** determines whether policies and controls are being applied appropriately to the Orchestration Layer, both from a process point of view, as well as determining whether the technology is performing within policy boundaries.

It focuses on ensuring that management properly oversees and assesses:

* The adequacy of policies to address risk, regulatory, and compliance requirements.
* The organization’s effectiveness at ensuring that internal operating processes deliver on management’s objectives through formal policies and internal controls.
* Improvements to be made to existing policies, the need for new policies, and the termination of redundant or unnecessary policies.
* The general state and performance of the internal control environment.

Attendees should include:

* IT management.
* Key personnel from the Orchestration Layer.
* A compliance and GRC representative (optional).

The review should address the following:

* **Reports/inputs:**
* Do runbooks ensure that GRC and policy is followed? For example, does approval happen prior to execution of tasks?
* **Analysis/decisions:**
* Are runbooks and workflows well enough designed and with enough rigor to ensure that GRC requirements are met?
* Are policies and procedures clear within the IT organization and the business?
* **Tools to provide data:**
* System Center 2012 - Service Manager
* System Center 2012 - Orchestrator
* **Outcomes/outputs:**
* Updates to existing service requests to apply more rigor for GRC.
* Requests for changes to existing processes and procedures to ensure that compliance to GRC is maintained.

### Conducting Reviews of the Management Layer

The goal of the **Service Alignment MR** is to validate and measure the quality and effectiveness of the Management Layer, specifically examining the people, process, and technology elements. When reviewing these elements, this review:

* Evaluates whether the cloud is providing expected business value.
* Identifies items that can enhance business alignment and/or business innovation.
* Initiates new cloud enhancements, if they are needed.

Attendees should include:

* IT management.
* Key personnel representing all layers of the private cloud.
* Service level manager.

The review should address the following:

* **Reports/inputs:**
* Actions/outcomes from any previous Service Alignment Management Review meetings and their updated status.
* Proactive monitoring and remediation with System Center 2012 - Operations Manager.
* Guest virtual machine resource utilization, to determine whether it is within suitable limits.
* Service requests that were not logged through the Service Manager Portal.
* Alert-to-incident ratio.
* Service request summary:
* Number of virtual machines provisioned this period.
* Number of virtual machines decommissioned this period.
* Maintenance activity summary:
* Number of maintenance tasks performed this period.
* Number of backups performed this period.
* Number of restores performed this period.
* Number of automated scripts run this period.
* Number of automated scripts created this period.
* **Analysis/decisions:**
* Are workflow completions on the rise/decline?
* Are workflow failures on the rise/decline?
* What service requests/standard changes can be automated?
* Where can new runbooks be used to improve efficiency and cost?
* What value is the Orchestration Layer and expansion of the Orchestration Layer providing the business?
* What cost-benefits are realized by the investment in orchestration?
* What service requests need to be added to the portal, based on a review of how many requests were logged outside the portal?
* Is demand being met or is the private cloud underutilized?
* **Tools to provide data:**
* System Center 2012 - Operations Manager
* System Center 2012 - Service Manager
* System Center 2012 - Data Protection Manager
* System Center 2012 - Virtual Machine Manager.
* **Outcomes/outputs:**
* Improvements to runbooks/workflows.
* Problem and root-cause analysis for failures.
* New runbooks/workflows to be created.
* New standard change templates and workflows to be built.
* Expansion of service request offerings to be added to the portal.
* Updates to capacity plans with private cloud growth/decline observed and incorporated.

The **Policy and Control MR** determines whether policies and controls are being applied appropriately to the Management Layer, both from a process point of view, as well as determining whether the technology is performing within policy boundaries.

It focuses on ensuring that management properly oversees and assesses:

* The adequacy of policies to address risk, regulatory, and compliance requirements.
* The organization’s effectiveness at ensuring that internal operating processes deliver on management’s objectives through formal policies and internal controls.
* Improvements to be made to existing policies, the need for new policies, and the termination of redundant or unnecessary policies.
* The general state and performance of the internal control environment.

Attendees should include:

* IT management.
* Key personnel from the Orchestration Layer.
* A compliance and GRC representative (optional), and Self-Service Layer representation.

The review should address the following:

* **Reports/inputs:**
* Do runbooks ensure that GRC and policy are followed? For example, does approval happen prior to execution of tasks?
* Does the portal provide enough control over who can ask for services and resources?
* Are Hyper-V hosts and guests patched to ensure compliance?
* Are private cloud resources provisioned/decommissioned according to GRC policies?
* Do VMM management server and service templates adhere to GRC requirements?
* **Analysis/decisions:**
* Are runbooks and workflows well enough designed and do they have enough rigor to ensure that GRC requirements are met?
* Are policies for updates/patches being met?
* Are breaches in compliance monitored sufficiently?
* Are there areas where GRC needs to be addressed?
* Do server and service templates adhere to corporate GRC standards and are server and service templates being actively managed for compliance?
* Are policies and procedures clear within the IT organization and the business?
* **Tools to provide data:**
* System Center 2012 - Service Manager
* System Center 2012 - Orchestrator
* System Center 2012 - Virtual Machine Manager
* **Outcomes/outputs:**
* Updates to existing service requests to apply more rigor for GRC.
* Requests for changes to existing processes and procedures to ensure that compliance to GRC is maintained.
* RFCs for changes to be applied to private cloud policies.
* Modifications to role-based access to the portal to ensure adherence to GRC.
* Updates to existing server and service templates to ensure adherence to GRC.
* Retirement of server/service templates that don’t comply.
* Modification to Guest and Host patching cycles to apply more rigor around GRC.
* The Microsoft IT GRC Process Management Pack for System Center Service Manager provides end-to-end compliance management and automation that helps translate complex regulations and standards into authoritative control objectives and activities for the IT organization’s compliance program. Microsoft Security Compliance Manager provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate your organization’s ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies.

### Conducting Reviews of the Automation Layer

The goal of the **Service Alignment MR** is to validate and measure the quality and effectiveness of the Automation Layer, specifically examining the people, process, and technology elements. When reviewing these elements, this review:

* Evaluates whether the layer is providing expected business value.
* Identifies items that can enhance business alignment and/or business innovation.
* Initiates new cloud enhancements, if they are needed.

Attendees should include:

* IT management.
* Key personnel from the Automation Layer.
* Service level manager.

The review should address the following:

* **Reports/inputs:**
* Number of automated scripts run this period.
* Number of automated scripts created this period.
* **Analysis/decisions:**
* Where has automation reduced manual tasks?
* Time and efficiency gained through automation activities.
* **Tools to provide data:**
* Windows PowerShell
* Windows Management Instrumentation (WMI)
* Web Services for Management (WS-Management)
* **Outcomes/outputs:**
* Maintenance activities where automation needs to be implemented.
* New automation activities to be defined.

The **Policy and Control MR** determines whether policies and controls are being applied appropriately to the Automation Layer, both from a process point of view, as well as determining whether the technology is performing within policy boundaries.

It focuses on ensuring that management properly oversees and assesses:

* The adequacy of policies to address risk, regulatory, and compliance requirements.
* The organization’s effectiveness at ensuring that internal operating processes deliver on management’s objectives through formal policies and internal controls.
* Improvements to be made to existing policies, the need for new policies, and the termination of redundant or unnecessary policies.
* The general state and performance of the internal control environment.

Attendees should include:

* IT management.
* Key personnel from the Orchestration Layer.
* A compliance and GRC representative (optional).

The review should address the following:

* **Reports/inputs:**
* Automation in place to ensure adherence, what compliance activities are automated and reported on.
* Number of automated compliance activities run this period versus the number of manual compliance activities run this period.
* Whether resources are provisioned according to policies.
* Number of resources provisioned against policy.
* Breaches in policy.
* **Analysis/decisions:**
* Do automation efforts support GRC initiatives?
* Areas where compliance needs to be addressed.
* Are policies and automation sufficient to address risk, regulatory, and compliance requirements?
* **Tools to provide data:**
* System Center 2012 - Operations Manager
* System Center 2012 - Orchestrator
* System Center 2012 - Virtual Machine Manager
* Scripts from Windows PowerShell.
* **Outcomes/outputs:**
* Updates to policies and automation to address gaps in risk, regulatory, and compliance policies.
* Updates to formal policies and internal controls.
* Improvements to existing policies.
* New policies to be created and the termination of redundant or unnecessary policies.

### Conducting Reviews of Virtualization

The goal of the **Service Alignment MR** is to validate and measure the quality and effectiveness of the Virtualization Layer, specifically examining the people, process, and technology elements. When reviewing these elements, this review:

* Evaluates whether the layer is providing expected business value.
* Identifies items that can enhance business alignment and/or business innovation.
* Initiates new cloud enhancements, if they are needed.

Attendees should include:

* IT management.
* Key personnel from Virtualization.
* Service level manager.

The review should address the following:

* **Reports/inputs:**
* Number of VMM migrations this period and this year to date (YTD).
* Power optimization statistics this period and YTD.
* Host optimization activities this period.
* Physical to virtual conversions this period and YTD.
* Fabric management capabilities.
* SAN storage available per period and YTD.
* Host density reporting.
* Network capacity reports.
* VMM backlog.
* **Analysis/decisions:**
* How well is the business adopting the private cloud?
* How is capacity being managed? Under/over?
* **Tools to provide data:**
* System Center 2012 - Virtual Machine Manager
* **Outcomes/outputs:**
* Capacity planning and capacity plans.
* Growth/decline patterns for the private cloud.

The **Policy and Control MR** determines whether policies and controls are being applied appropriately to Virtualization, both from a process point of view, as well as determining whether the technology is performing within policy boundaries.

It focuses on ensuring that management properly oversees and assesses:

* The adequacy of policies to address risk, regulatory, and compliance requirements.
* The organization’s effectiveness at ensuring that internal operating processes deliver on management’s objectives through formal policies and internal controls.
* Improvements to be made to existing policies, the need for new policies, and the termination of redundant or unnecessary policies.
* The general state and performance of the internal control environment.

Attendees should include:

* IT management.
* Key personnel from Virtualization.
* A compliance and GRC representative (optional).

The review should address the following:

* **Reports/inputs:**
* Number of server and service templates that adhere to policy.
* Number of server and service templates that do not adhere to policy.
* **Analysis/decisions:**
* Do server and service templates adhere to corporate GRC standards?
* Are server and service templates being actively managed for compliance?
* **Tools to provide data:**
* System Center 2012 - Virtual Machine Manager
* System Center 2012 - App Controller
* **Outcomes/outputs:**
* Updates to existing server and service templates to ensure compliance.
* Retirement of server and service templates that do not adhere to compliance standards.

# MOF Operate Phase

The MOF Operate Phase focuses on what to do after services are in place. It is, in effect, the steady state for the environment in which IT services exist. There are four SMFs that address that steady state. They are:

* Operations
* Service Monitoring and Control
* Customer Service
* Problem Management

Two management reviews apply as well. They are:

* Service Alignment Management Review
* Policy and Control Management Review

## Operating a Private Cloud

Operating a private cloud involves defining, documenting, and maintaining daily, weekly, monthly, and ad-hoc tasks for running the private cloud service. These operations tasks are driven by what the technical components of the service can do, and what the service itself is designed and intended to do.

Operating also includes execution on maintenance and monitoring tasks. The details of how those tasks are created are in the “Monitoring a Private Cloud” section of this guide.

### Conducting Operations in the Self-Service Layer

The Self-Service Layer uses the System Center 2012 - Service Manager service catalog and Portal to allow groups within an organization, such as cloud tenants or authorized users, to request, manage, and access services.

A key issue is determining which operating tasks must be done in an environment where the whole point is automation and self-service. The three primary roles are an operations manager, with oversight for running and maintaining the Self-Service Layer; operators; and administrators. The key question is how many, if any, ongoing operational tasks there would be for operators and administrators to perform, given the service’s focus on automation and self-service.

In a traditional data center:

* Operating tasks are performed by operators or administrators. Operators generally execute preplanned tasks that are instruction-based. Administrators execute tasks that are not well-defined.
* Maintenance tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.
* Monitoring tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.

In a cloud environment:

* Most operating tasks for a self-service-focused Self-Service Layer will be automated, so there won’t be a lot of traditional tasks for operators and administrators. However, there will be some configuring/provisioning tasks—listed in the “Executing Operating Tasks for the Self-Service Layer” section. Most other operating tasks will be done by end users.
* Most monitoring and maintenance tasks will be done automatically.

#### Executing Operating Tasks for the Self-Service Layer

The VMM Self-Service Portal website component provides a role-based user interface to the Self-Service Portal that allows cloud tenants or authorized users to request, manage, and access services.

Some operating tasks that might be done by the following user roles—DCIT Admin, BUIT Admin, Advanced Operator, and Business Unit User—are:

* Configure the VMM Self-Service Portal, including bringing the Self-Service Portal into or out of maintenance mode.
* Import, configure, and provision virtual machine templates.
* Import virtual machines.
* Provision new or changed infrastructures, services, and service roles.
* Edit the properties of business units, or delete business units.

Data center administrators can use the VMM Self-Service Portal website component to do the following:

* Manage requests. Use standardized forms and follow a simple workflow for provisioning and approving or rejecting business unit requests.
* Configure and allocate data center resources. Store management and configuration information related to memory, network, and storage resources as assets in the VMM Self-Service Portal database.
* Customize virtual machine actions. Work with technology partners and hardware vendors to extend the default virtual machine actions; for example, adding scripts that interact with storage area networks (SANs) to support rapid provisioning of virtual machines.

#### Executing Maintenance Tasks for the Self-Service Layer

Some key maintenance tasks are:

* Tune the Self-Service Portal with global parameters.
* Back up the Self-Service Portal components.
* Ensure database availability.
* Troubleshoot the Self-Service Portal.

#### Executing Monitoring Tasks for the Self-Service Layer

Some key monitoring tasks are:

* Monitor active alerts.
* Monitor closed alerts.
* Monitor VMM Self-Service Portal service state.
* Monitor VMM Self-Service Portal helper service state.
* Monitor VMM state.
* Monitor VMM Self-Service Portal database component state.

### Conducting Operations in the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation. The goal of Operations is to run and maintain the Orchestration Layer so that it can effectively provide the IT process automation and workflow needed for the cloud without IT staff involvement.

Microsoft System Center 2012 - Orchestrator helps manage private clouds with a workflow designer that allows users to create runbooks to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operations Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager, Active Directory Domain Services, and third-party tools.

The primary people issue is determining which operating tasks must be done in an environment where the whole point is transforming repeatable tasks into workflow and automation. The three primary roles would be an operations manager, with oversight for running and maintaining the orchestration service; operators; and administrators. The key question is how many, if any, ongoing operational tasks would there be for operators and administrators to perform.

In a traditional data center:

* Operating tasks are performed by operators or administrators. Operators generally execute preplanned tasks that are instruction-based. Administrators execute tasks that are not well-defined.
* Maintenance tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.
* Monitoring tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.

In a cloud environment:

* Many low-value, repetitive tasks will be automated, which allows operators and administrators to focus on high-value work. However, there will be some runbook building and testing tasks—listed in the “Executing Operating Tasks for the Orchestration Layer” section. Many other operating tasks will be done by end users.
* Most monitoring and maintenance tasks will be done automatically.

#### Executing Operating Tasks for the Orchestration Layer

The Orchestration Layer’s focus is on runbooks. Some key examples of operating tasks are:

* Build a runbook.
* Test a runbook.
* Run a runbook.
* View Orchestrator data using PowerPivot.

#### Executing Maintenance Tasks for the Orchestration Layer

Some key examples of maintenance tasks are:

* Back up the Orchestrator components.
* Ensure Orchestrator availability.
* Troubleshoot Orchestrator.

#### Executing Monitoring Tasks for the Orchestration Layer

Some key examples of monitoring tasks are:

* Monitor event log.
* Monitor service.
* Get service status.
* Monitor process.
* Get process status.

### Conducting Operations in the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the Management Layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

The goal is to run and maintain the Management Layer so that it can effectively provide centralized administration and management of a virtual environment, without IT staff involvement.

The Management Layer tools that need to be operated, maintained, and monitored are:

* System Center 2012 - Virtual Machine Manager, which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the Virtual Machine Manager Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments; Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

Again, the primary people issue is determining which operating tasks must be done in an environment where the whole point is automation—in this case, automation of maintenance and monitoring of the cloud fabric. Fabric is an abstraction of the major resources needed to run a service—typically servers, networking, and storage.

The three primary roles would be an operations manager, with oversight for running and maintaining the management service; operators; and administrators. The key question is how many, if any, ongoing operational tasks would there be for operators and administrators to perform.

In a traditional data center:

* Operating tasks are performed by operators or administrators. Operators generally execute preplanned tasks that are instruction-based. Administrators execute tasks that are not well-defined.
* Maintenance tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.
* Monitoring tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.

In a cloud environment:

* Most operating tasks for an automated management service—one that monitors and maintains the cloud fabric—will be automated, so there won’t be a lot of traditional tasks for operators and administrators.
* Most monitoring and maintenance of the monitoring and maintenance tools will be done automatically.

#### Executing Operating Tasks for the Management Layer

Some key examples of operating tasks are:

* Create virtual machines.
* Place virtual machines on hosts.
* Manage virtual machines on different virtual software.
* Manage hosts in VMM.
* Manage the virtual machine library.
* Manage VMM.
* Configure virtual networks.

#### Executing Maintenance Tasks for the Management Layer

Some key examples of maintenance tasks are:

* Maintain each virtual machine that Virtual Machine Manager manages.
* Back up the Virtual Machine Manager database.
* Tune the performance of the Virtual Machine Manager database.
* Free storage space in the Virtual Machine Manager library.

#### Executing Monitoring Tasks for the Management Layer

Some key examples of monitoring tasks are:

* Check the health of each virtual machine that Virtual Machine Manager manages.
* Check connectivity to the Virtual Machine Manager server using the TCP port configured for database access.
* Check the health of Microsoft SQL Server®.
* Ensure that the backup successfully finished.

### Conducting Operations in the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update, without IT staff involvement.

The goal is to run and maintain the Automation Layer so that it can provide these commands and scripts.

The Automation Layer contains three technical components. They are:

* Windows PowerShell, which can be used to write scripts and cmdlets that System Center 2012 - Orchestrator uses in its integration of the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

The primary people issue is determining which operating tasks must be done in an environment where the whole point is automation. The three primary roles would be an operations manager, with oversight for running and maintaining the automation service; operators; and administrators. The key question is how many, if any, ongoing operational tasks would there be for operators and administrators to perform.

In a traditional data center:

* Operating tasks are performed by operators or administrators. Operators generally execute preplanned tasks that are instruction-based. Administrators execute tasks that are not well-defined.
* Maintenance tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.
* Monitoring tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.

In a cloud environment:

* Most operating tasks for an Automation Layer will be automated, so there won’t be a lot of traditional tasks for operators and administrators.
* Most monitoring and maintenance tasks will be done automatically.

#### Executing Operating Tasks for the Automation Layer

Some key examples of operating tasks are:

* Start a virtual machine.
* Stop a virtual machine.
* Restart a server.
* Apply a software patch.

#### Executing Maintenance Tasks for the Automation Layer

Because PowerShell, WMI, and WS-Management are tools, there are no maintenance tasks for them.

#### Executing Monitoring Tasks for the Automation Layer

Because PowerShell, WMI, and WS-Management are tools, there are no monitoring tasks for them tools.

### Conducting Operations for Virtualization

Virtualization is key to a private cloud, in that it enables better management and distribution of workloads across the physical infrastructure. Additionally, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

The goal is to operate the Virtualization Layer, which abstracts computer resources for storage, network, and server, without IT staff involvement.

Operations is running and maintaining a service. It includes:

* Defining, documenting, and maintaining daily, weekly, monthly and ad-hoc tasks for running the service.
* Executing those tasks.
* Reporting on those tasks.

A key dependency is defining a health model for a service, and determining what monitoring and maintaining tasks are required to keep it healthy.

Virtualization has two technical components. They are:

* Microsoft Hyper-V Server 2008 R2: Hyper-V provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager:VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

In a traditional data center:

* Operating tasks are performed by operators or administrators. Operators generally execute preplanned tasks that are instruction-based. Administrators execute tasks that are not well-defined.
* Maintenance tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.
* Monitoring tasks are also performed by either operators or administrators, depending on whether the tasks are preplanned or not well-defined.

In a cloud environment:

* Most operating tasks for virtualization will be automated, so there won’t be a lot of traditional tasks for operators and administrators.
* Most monitoring and maintenance tasks will be done automatically.

The primary people issue is determining which operating tasks there are to do in an environment where the whole point is automation. The three primary roles would be an operations manager, with oversight for running and maintaining the virtualization service; operators; and administrators. The key question is how many, if any, ongoing operational tasks there would be for operators and administrators to perform.

#### Executing Operating Tasks for Virtualization with Hyper-V

Some key examples of operating tasks are:

* Create a virtualized server computing environment.
* Manage virtual machines remotely with Hyper-V Manager and Windows 7.
* Use an internal virtual network to move files to a virtual machine.
* Connect a virtual hard disk without shutting down the virtual machine.
* Connect a physical hard disk to a virtual machine.
* Create a virtual domain controller and connect a virtual machine to it.

#### Executing Operating Tasks for Virtualization with VMM

Some key examples of operating tasks are:

* Create virtual machines.
* Place virtual machines on hosts.
* Manage virtual machines on different virtual software.
* Manage hosts in VMM.
* Manage the VMM library.
* Manage VMM.
* Configure virtual networks.

#### Executing Maintenance Tasks for Virtualization with Hyper-V

Some key examples of maintenance tasks are:

* Restart the Hyper-V server if it does not respond remotely.
* Balance resources by migrating memory-intensive virtual machines to another Hyper-V server.
* Remove unnecessary roles from the management operating system.
* Prune accounts from the local Administrators group of the management operating system.
* Securely delete decommissioned virtual machines.

#### Executing Maintenance Tasks for Virtualization with VMM

Some key examples of maintenance tasks are:

* Perform maintenance tasks on each virtual machine that Microsoft System Center 2012 - Virtual Machine Manager manages.
* Back up the Virtual Machine Manager database.
* Tune the performance of the Virtual Machine Manager database.
* Free storage space in the Virtual Machine Manager library.

#### Executing Monitoring Tasks for Virtualization with Hyper-V

Some key examples of monitoring tasks are:

* Ensure that the Image Management service is running.
* Verify that the Hyper-V service is available.
* Verify memory capacity for current and expected workloads.
* Verify that the Hyper-V server is backed up.
* For each virtual machine, verify that each virtual hard disk is located on a physical disk not used by the parent partition.

#### Executing Monitoring Tasks for Virtualization with VMM

Some key examples of monitoring tasks are:

* Check the health of each virtual machine that System Center 2012 - Virtual Machine Manager manages.
* Check connectivity to the Virtual Machine Manager server using the TCP port configured for database access.
* Check the health of Microsoft SQL Server.
* Ensure that the backup successfully finished.

## Monitoring a Private Cloud

Monitoring a private cloud involves identifying the monitoring and maintenance tasks that are necessary for the health of the service. The tasks for monitoring and maintaining the service come from defining a health model for the cloud service, and defining the monitoring and maintenance tasks required to keep it healthy.

Defining a health model for a service—and determining what monitoring and maintenance tasks are required to keep it healthy—are part of Service Monitoring and Control. However, the execution of those tasks is Operations.

A more complete look at Service Monitoring and Control can be found in the MOF Service Monitoring and Control SMF.

### Monitoring and Maintaining the Self-Service Layer

The Self-Service Layer uses the System Center 2012 - Service Manager service catalog and Portal to allow groups within an organization, such as cloud tenants or authorized users, to request, manage, and access services.

The primary people issue is determining who is responsible for developing a health model for the Self-Service Layer. The likely role would be an operations manager, who would also have oversight for running and maintaining the Self-Service Layer; operators; and administrators.

#### Identifying What Needs to be Monitored and Maintained

In this case, the service to be monitored is the VMM Self-Service Portal. Part of that identification is creating a clear picture of the role of the Self-Service Portal and who its users are, and understanding its technical components and any dependencies it has on other technical services.

#### Deciding What to Monitor and Maintain

A health model defines what it means for a system to be healthy (operating within normal conditions) or unhealthy (failed or degraded) and the transitions in and out of such states. A service is healthy when it and all the components it depends on are behaving the way you need them to in order to meet your business needs.

Creating a health model is a matter of identifying the behaviors you want, and then quantifying them so you have a way to measure whether the service is delivering them.

#### Defining What Healthy Means

Defining health requires you to decide how important the service is and what you want it to do. That helps you set the boundaries for what healthy is for the service. The priorities or important behaviors will vary from service to service, but some are always important enough to keep an eye on. They are:

* **Availability.** Whether a service or application can be accessed when users need it. Availability is typically measured in percentage of uptime; downtime refers to periods of system unavailability.
* **Performance.** The responsiveness of the service or application. Performance is typically measured by how long it takes to complete a requested action.
* **Capacity.** Capacity management is the process used to ensure that current and future business IT needs are met in a cost-effective manner. It is generally measured in terms of whether a capacity plan is in place, whether there have been any capacity-related service disruptions, and whether a procurement/purchasing plan has been developed and followed.

#### Defining Notification Triggers Needed

Notification triggers should be based on the health model parameters you set. For example, if you set parameters around the percentage of uptime you want from the service—that is, availability—one trigger should be set to alert you when the service availability falls below that percent. Because you don’t want to wait until the service falls below your requirements to know something is wrong, your notification trigger is being defined for availability. You should use the health model to determine parameters, which are the limits of what is healthy. As you create the task list, use your definition of reliability to determine parameters. You should also set trend warning limits—alerts that indicate when a service is close to, but not at, failure. (For example, many photocopiers flash a warning sign when the paper is getting low—not just when it is empty.) Identifying these parameters and trend limits helps determine the amount of resources required to invest in maintenance activities.

#### Defining Who to Notify

Once you have decided what behavior will trigger an alert, you have to decide where that alert goes. In a traditional data center, alerts would likely go to the service owner—often an operator.

If you are using System Center 2012 - Operations Manager in your environment, you will have several management packs in place that will be monitoring the key elements of the private cloud. You’ll need to decide for each management pack which support team should receive an incident alert. For example:

* SQL alerts would go to the team responsible for managing SQL databases.
* AD Management Pack alerts would go to the people who support Active Directory in your private cloud.
* If you have distributed application alerts, the support team for that application would need to address incidents for it.

As your incident management process matures, you can build out automatic tasks/recovery tasks for incidents where the resolution is known and can be automated.

Key questions to ask are:

* Which groups or roles should be receiving alerts?
* Are other departments or resources working on the alerts/incident?
* Is automated event resolution applied and are some alerts automatically solved and closed?

#### Defining Historical Reporting Needs

This is a practice primarily for improving operational health. It is about producing reports that look at health over a period of time. The information gathered is used periodically to review operational health.

#### Adding Monitoring and Maintenance Tasks to Operations

Although the health model used to develop monitoring and maintenance tasks is developed as part of Service Monitoring and Control, the tasks themselves are operational tasks. They need to be added to the task list for whoever operates the VMM Self-Service Portal; ideally they should be automated.

### Monitoring and Maintaining the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation. System Center 2012 - Orchestrator helps manage private clouds with a workflow designer that allows users to create runbooks to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operations Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager, Active Directory Domain Services, and third-party tools.

The primary people issue is determining who is responsible for developing a health model for the orchestration service. The likely role would be an operations manager, who would also have oversight for running and maintaining the orchestration service; operators; and administrators.

#### Identifying What Needs to be Monitored and Maintained

In this case, the service to be monitored is System Center 2012 - Orchestrator. Part of that identification is creating a clear picture of the role of Orchestrator and who its users are, and understanding its technical components and any dependencies it has on other technical services.

#### Deciding What to Monitor and Maintain

A health model defines what it means for a system to be healthy (operating within normal conditions) or unhealthy (failed or degraded) and the transitions in and out of such states. A service is healthy when it and all the components it depends on are behaving the way you need them to in order to meet your business needs. Creating a health model is a matter of identifying the behaviors you want, and then quantifying them so you have a way to measure whether the service is delivering them.

#### Defining What Healthy Means

Defining health requires you to decide how important the service is and what you want it to do. That helps you set the boundaries for what healthy is for the service. The priorities or important behaviors will vary from service to service, but some are always important enough to monitor. They are:

* **Availability.** Whether a service or application can be accessed when users need it. Availability is typically measured in percentage of uptime; downtime refers to periods of system unavailability.
* **Performance.** The responsiveness of the service or application. Performance is typically measured by how long it takes to complete a requested action.
* **Capacity.** Capacity management is the process used to ensure that current and future business IT needs are met in a cost-effective manner. It is generally measured in terms of whether a capacity plan is in place, whether there have been any capacity-related service disruptions, and whether a procurement/purchasing plan has been developed and followed.

#### Defining Notification Triggers Needed

Notification triggers should be based on the health model parameters you set. For example, if you set parameters around the percentage of uptime you want from the service—that is, availability—one trigger should be set to alert you when the service availability falls below that percent. Because you don’t want to wait until the service falls below your requirements to know something is wrong, your notification trigger is being defined for availability. You should use the health model to determine parameters, which are the limits of what is healthy. As you create the task list, use your definition of reliability to determine parameters. You should also set trend warning limits—alerts that indicate when a service is close to, but not at, failure. (For example, many photocopiers flash a warning sign when the paper is getting low—not just when it is empty.) Identifying these parameters and trend limits helps determine the amount of resources required to invest in maintenance activities.

#### Defining Who to Notify

Once you have decided what behavior will trigger an alert, you have to decide where that alert goes. In a traditional data center, alerts would likely go to the service owner—often an operator.

If you are using Operations Manager in your environment, you will have several management packs in place that will be monitoring the key elements of the private cloud. You’ll need to decide for each management pack which support team should receive an incident alert. For example:

* SQL alerts would go to the team responsible for managing SQL databases.
* AD Management Pack alerts would go to the people who support Active Directory in your private cloud.
* If you have distributed application alerts, the support team for that application would need to address incidents for it.

As your incident management process matures, you can build out automatic tasks/recovery tasks for incidents where the resolution is known and can be automated.

Key questions to ask are:

* Which groups or roles should be receiving alerts?
* Are other departments or resources working on the alerts/incident?
* Is automated event resolution applied and are some alerts automatically solved and closed?

#### Defining Historical Reporting Needs

This is a practice primarily for improving operational health. It is about producing reports that look at health over a period of time. The information gathered is used periodically to review operational health.

#### Adding Monitoring and Maintenance Tasks to Operations

Although the health model used to develop monitoring and maintenance tasks is developed as part of Service Monitoring and Control, the tasks themselves are operational tasks. They need to be added to the task list for whoever operates the Self-Service Portal; ideally they should be automated.

### Monitoring and Maintaining the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the Management Layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

Its goal is to ensure the reliability of the Management Layer so that it can effectively provide centralized administration and management of a virtual environment, without IT staff involvement. The Management Layer uses the following tools:

* System Center 2012 - Virtual Machine Manager, which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the Virtual Machine Manager Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments. Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

The primary people issue is determining who is responsible for developing a health model for the orchestration service. The likely role would be an operations manager, who would also have oversight for running and maintaining the management service; operators; and administrators.

#### Identifying What Needs to be Monitored and Maintained

In this case, the services to be monitored are:

* System Center 2012 - Virtual Machine Manager
* System Center 2012 - Operations Manager
* System Center 2012 Configuration Manager
* System Center 2012 - Data Protection Manager

Part of that identification is creating a clear picture of the roles of those services and who their users are, and understanding their technical components and any dependencies they have on other technical services.

#### Deciding What to Monitor and Maintain

A health model defines what it means for a system to be healthy (operating within normal conditions) or unhealthy (failed or degraded) and the transitions in and out of such states. A service is healthy when it and all the components it depends on are behaving the way you need them to in order to meet your business needs. Creating a health model is a matter of identifying the behaviors you want, and then quantifying them so you have a way to measure whether the service is delivering them.

#### Defining What Healthy Means

Defining health requires you to decide how important the service is and what you want it to do. That helps you set the boundaries for what healthy is for the service. The priorities or important behaviors will vary from service to service, but some are always important enough to monitor. They are:

* **Availability.** Whether a service or application can be accessed when users need it. Availability is typically measured in percentage of uptime; downtime refers to periods of system unavailability.
* **Performance.** The responsiveness of the service or application. Performance is typically measured by how long it takes to complete a requested action.
* **Capacity.** Capacity management is the process used to ensure that current and future business IT needs are met in a cost-effective manner. It is generally measured in terms of whether a capacity plan is in place, whether there have been any capacity-related service disruptions, and whether a procurement/purchasing plan has been developed and followed.

#### Defining Notification Triggers Needed

Notification triggers should be based on the health model parameters you set. For example, if you set parameters around the percentage of uptime you want from the service—that is, availability—one trigger should be set to alert you when the service availability falls below that percent. Because you don’t want to wait until the service falls below your requirements to know something is wrong, your notification trigger is being defined for availability. You should use the health model to determine parameters, which are the limits of what is healthy. As you create the task list, use your definition of reliability to determine parameters. You should also set trend warning limits—alerts that indicate when a service is close to, but not at, failure. (For example, many photocopiers flash a warning sign when the paper is getting low—not just when it is empty.) Identifying these parameters and trend limits helps determine the amount of resources required to invest in maintenance activities.

#### Defining Who to Notify

Once you have decided what behavior will trigger an alert, you have to decide where that alert goes. In a traditional data center, alerts would likely go to the service owner—often an operator.

If you are using System Center 2012 - Operations Manager in your environment, you will have several management packs in place that will be monitoring the key elements of the private cloud. You’ll need to decide for each management pack which support team should receive an incident alert. For example:

* SQL alerts would go to the team responsible for managing SQL databases.
* AD Management Pack alerts would go to the people who support Active Directory in your private cloud.
* If you have distributed application alerts, the support team for that application would need to address incidents for it.

As your incident management process matures, you can build out automatic tasks/recovery tasks for incidents where the resolution is known and can be automated.

Key questions to ask are:

* Which groups or roles should be receiving alerts?
* Are other departments or resources working on the alerts/incident?
* Is automated event resolution applied and are some alerts automatically solved and closed?

#### Defining Historical Reporting Needs

This is a practice primarily for improving operational health. It is about producing reports that look at health over a period of time. The information gathered is used periodically to review operational health.

#### Adding Monitoring and Maintenance Tasks to Operations

Although the health model used to develop monitoring and maintenance tasks is developed as part of Service Monitoring and Control, the tasks themselves are operational tasks. They need to be added to the task list for whoever operates the management service; ideally they should be automated.

### Monitoring and Maintaining the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update, without IT staff involvement. Monitoring and maintaining the layer ensures its reliability.

The Automation Layer uses three tools. They are:

* Windows PowerShell, which can be used to write scripts and cmdlets that Orchestrator uses in its integration of the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

The primary people issue is determining who is responsible for developing a health model for the automation tools. The likely role would be an operations manager, who would also have oversight for running and maintaining the management service; operators; and administrators.

#### Identifying What Needs to be Monitored and Maintained

In this case, there are three services to be monitored:

* Windows PowerShell, which can be used to write scripts and cmdlets that Orchestrator uses in its integration of the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

Part of that identification is creating a clear picture of the roles of those services and who their users are, and understanding their technical components and any dependencies they have on other technical services.

#### Deciding What to Monitor and Maintain

A health model defines what it means for a system to be healthy (operating within normal conditions) or unhealthy (failed or degraded) and the transitions in and out of such states. A service is healthy when it and all the components it depends on are behaving the way you need them to in order to meet your business needs. Creating a health model is a matter of identifying the behaviors you want, and then quantifying them so you have a way to measure whether the service is delivering them.

#### Defining What Healthy Means

Defining health requires you to decide how important the service is and what you want it to do. That helps you set the boundaries for what healthy is for the service. The priorities or important behaviors will vary from service to service, but some are always important enough to keep an eye on. They are:

* **Availability.** Whether a service or application can be accessed when users need it. Availability is typically measured in percentage of uptime; downtime refers to periods of system unavailability.
* **Performance.** The responsiveness of the service or application. Performance is typically measured by how long it takes to complete a requested action.
* **Capacity.** Capacity management is the process used to ensure that current and future business IT needs are met in a cost-effective manner. It is generally measured in terms of whether a capacity plan is in place, whether there have been any capacity-related service disruptions, and whether a procurement/purchasing plan has been developed and followed.

#### Defining Notification Triggers Needed

Notification triggers should be based on the health model parameters you set. For example, if you set parameters around the percentage of uptime you want from the service—that is, availability—one trigger should be set to alert you when the service availability falls below that percent. Because you don’t want to wait until the service falls below your requirements to know something is wrong, your notification trigger is being defined for availability. You should use the health model to determine parameters, which are the limits of what is healthy. As you create the task list, use your definition of reliability to determine parameters. You should also set trend warning limits—alerts that indicate when a service is close to, but not at, failure. (For example, many photocopiers flash a warning sign when the paper is getting low—not just when it is empty.) Identifying these parameters and trend limits helps determine the amount of resources required to invest in maintenance activities.

#### Defining Who to Notify

Once you have decided what behavior will trigger an alert, you have to decide where that alert goes. In a traditional data center, alerts would likely go to the service owner—often an operator.

If you are using Operations Manager in your environment, you will have several management packs in place that will be monitoring the key elements of the private cloud. You’ll need to decide for each management pack which support team should receive an incident alert. For example:

* SQL alerts would go to the team responsible for managing SQL databases.
* AD Management Pack alerts would go to the people who support Active Directory in your private cloud.
* If you have distributed application alerts, the support team for that application would need to address incidents for it.

As your incident management process matures, you can build out automatic tasks/recovery tasks for incidents where the resolution is known and can be automated.

Key questions to ask are:

* Which groups or roles should be receiving alerts?
* Are other departments or resources working on the alerts/incident?
* Is automated event resolution applied and are some alerts automatically solved and closed?

#### Defining Historical Reporting Needs

This is a practice primarily for improving operational health. It is about producing reports that look at health over a period of time. The information gathered is used periodically to review operational health.

#### Adding Monitoring and Maintenance Tasks to Operations

Although the health model used to develop monitoring and maintenance tasks is developed as part of Service Monitoring and Control, the tasks themselves are operational tasks. They need to be added to the task list for whoever operates the management service; ideally they should be automated.

### Monitoring and Maintaining Virtualization

Service Monitoring and Control is the real-time monitoring of how healthy an IT system is, and the real-time alerting when a system is not healthy. That also includes the maintenance of systems to keep them healthy.

Virtualization is key to a private cloud, in that it enables better management and distribution of workloads across the physical infrastructure. Additionally, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

The goal is to ensure reliability of the Virtualization Layer so that it effectively abstracts computer resources for storage, network, and server, without IT staff involvement.

Virtualization uses two tools. They are:

* Microsoft Hyper-V Server 2008 R2: Hyper-V provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager: VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

The primary people issue is determining who is responsible for developing a health model for the virtualization service. The likely role would be an operations manager, who would also have oversight for running and maintaining the orchestration service; operators; and administrators.

#### Identifying What Needs to be Monitored and Maintained

In this case, the services that need to be monitored and maintained are:

* Hyper-V Server
* VMM

#### Deciding What to Monitor and Maintain

A health model defines what it means for a system to be healthy (operating within normal conditions) or unhealthy (failed or degraded) and the transitions in and out of such states. A service is healthy when it and all the components it depends on are behaving the way you need them to in order to meet your business needs. Creating a health model is a matter of identifying the behaviors you want, and then quantifying them so you have a way to measure whether the service is delivering them.

#### Defining What Healthy Means

Defining health requires you to decide how important the service is and what you want it to do. That helps you set the boundaries for what healthy is for the service. The priorities or important behaviors will vary from service to service, but some are always important enough to monitor. They are:

* **Availability.** Whether a service or application can be accessed when users need it. Availability is typically measured in percentage of uptime; downtime refers to periods of system unavailability.
* **Performance.** The responsiveness of the service or application. Performance is typically measured by how long it takes to complete a requested action.
* **Capacity.** Capacity management is the process used to ensure that current and future business IT needs are met in a cost-effective manner. It is generally measured in terms of whether there is a capacity plan in place, whether there have been any capacity-related service disruptions, and whether a procurement/purchasing plan has been developed and followed.

#### Defining Notification Triggers Needed

Notification triggers should be based on the health model parameters you set. For example, if you set parameters around the percentage of uptime you want from the service—that is, availability—one trigger should be set to alert you when the service availability falls below that percent. Because you don’t want to wait until the service falls below your requirements to know something is wrong, your notification trigger is being defined for availability. You should use the health model to determine parameters, which are the limits of what is healthy. As you create the task list, use your definition of reliability to determine parameters. You should also set trend warning limits—alerts that indicate when a service is close to, but not at, failure. (For example, many photocopiers flash a warning sign when the paper is getting low—not just when it is empty.) Identifying these parameters and trend limits helps determine the amount of resources required to invest in maintenance activities.

#### Defining Who to Notify

Once you have decided what behavior will trigger an alert, you have to decide where that alert goes. In a traditional data center, alerts would likely go to the service owner—often an operator.

If you are using Operations Manager in your environment, you will have several management packs in place that will be monitoring the key elements of the private cloud. You’ll need to decide for each management pack which support team should receive an incident alert. For example:

* SQL alerts would go to the team responsible for managing SQL databases.
* AD Management Pack alerts would go to the people who support Active Directory in your private cloud.
* If you have distributed application alerts, the support team for that application would need to address incidents for it.

As your incident management process matures, you can build out automatic tasks/recovery tasks for incidents where the resolution is known and can be automated.

Key questions to ask are:

* Which groups or roles should be receiving alerts?
* Are other departments or resources working on the alerts/incident?
* Is automated event resolution applied and are some alerts automatically solved and closed?

#### Defining Historical Reporting Needs

This is a practice primarily for improving operational health. It is about producing reports that look at health over a period of time. The information gathered is used periodically to review operational health.

#### Adding Monitoring and Maintenance Tasks to Operations

Although the health model used to develop monitoring and maintenance tasks is developed as part of Service Monitoring and Control, the tasks themselves are operational tasks. They need to be added to the task list for whoever operates the Virtualization Layer; ideally they should be automated.

## Servicing Private Cloud Customers

Customer Service focuses on providing a positive experience for IT service users by meeting their IT needs and addressing complaints and issues that arise during the normal course of using an IT service.

### Conducting Customer Service for the Self-Service Layer

The Self-Service Layer provides an interface that allows cloud tenants or authorized users to request, manage, and access services. Its goal is to ensure that Hyper-V cloud tenants or authorized users are able to request, manage, and access services, such as virtual machines, as well as get service-related questions answered and incidents managed. Customer Service should also ensure that any requests, questions, or incidents relating to provisioning tools can be resolved.

The System Center 2012 - Service Manager service catalog and Portal serve as the provisioning user interface that allows groups within an organization to manage their own IT needs.

The primary people issue is that in the private cloud, customer service will move from a people-intensive activity to a largely automated one. In a traditional data center, a customer service manager might be in charge of customer service, and there might be a variety of roles for taking calls, answering questions, and resolving incidents.

In a private cloud environment, it’s more likely that someone will have oversight of how customers’ requests, questions, and incidents are resolved, but that the resolutions will be done without direct IT involvement.

As much as possible, customer service tasks in a private cloud should be handled automatically. At the Self-Service Layer, most customer service requests will be made through the Self-Service Portal. The following are the primary customer service tasks:

* Receive and record requests from users or systems. Most requests will be from tenants or authorized users requesting a virtual machine, although some might be for information or to report an issue.
* Classify the request, to determine whether it is informational, an issue, or a request for a service.
* Determine whether the request is supported.
* Prioritize the request based on its impact and urgency.
* Resolve the request directly or with escalation assistance. Again, most requests should be resolved automatically through the portal.
* Record metrics/reports.

### Conducting Customer Service for the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation. Its goal is to ensure that any requests relating to the Orchestration Layer, or reporting issues with it, are resolved so that it can provide the IT process automation and workflow needed for the cloud, without IT staff involvement.

System Center 2012 - Orchestrator helps manage private clouds with a workflow designer that allows users to create runbooks to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operations Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager, Active Directory Domain Services, and third-party tools.

The primary people issue is that in the private cloud, customer service will move from a people-intensive activity to a largely automated one. In a traditional data center, a customer service manager might be in charge of customer service, and there might be a variety of roles for taking calls, answering questions, and resolving incidents.

In a private cloud environment, it’s more likely that someone will have oversight of how customers’ requests, questions, and incidents are resolved, but that the resolutions will be done without direct IT involvement.

### Conducting Customer Service for the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the Management Layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

Its goal is to ensure that that requests relating to the Management Layer, or reporting issues with it, are resolved so that it can effectively provide centralized administration and management of a virtual environment, without IT staff involvement.

The primary tools for the Management Layer are:

* System Center 2012 - Virtual Machine Manager, which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the System Center Virtual Machine Manager Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments; Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

The primary people issue is that in the private cloud, customer service will move from a people-intensive activity to a largely automated one. In a traditional data center, a customer service manager might be in charge of customer service, and there might be a variety of roles for taking calls, answering questions, and resolving incidents.

In a private cloud environment, it’s more likely that someone will have oversight of how customers’ requests, questions, and incidents are resolved, but that the resolutions will be done without direct IT involvement.

### Conducting Customer Service for the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update, without IT staff involvement.

Ensure that any requests relating to the Automation Layer, or reporting issues with it, are resolved.

The Automation Layer contains three components. They are:

* Windows PowerShell, which can be used to write scripts and cmdlets that Orchestrator uses in its integration of the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

The primary people issue is that in the private cloud, customer service will move from a people-intensive activity to a largely automated one. In a traditional data center, a customer service manager might be in charge of customer service, and there might be a variety of roles for taking calls, answering questions, and resolving incidents.

In a private cloud environment, it’s more likely that someone will have oversight of how customers’ requests, questions, and incidents are resolved, but that the resolutions will be done without direct IT involvement.

### Conducting Customer Service for Virtualization

Virtualization is key to a private cloud in that it enables better management and distribution of workloads across the physical infrastructure. Additionally, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

Ensure that any requests relating to the Virtualization Layer, or reporting issues with it, are resolved so that it can effectively abstract computer resources for storage, network, and server, without IT staff involvement.

The technology components that make up the Virtualization Layer are:

* Microsoft Hyper-V Server 2008 R2: Hyper-V Server provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager:VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

The primary people issue is that in the private cloud, customer service will move from a people-intensive activity to a largely automated one. In a traditional data center, a customer service manager might be in charge of customer service, and there might be a variety of roles for taking calls, answering questions, and resolving incidents.

In a private cloud environment, it’s more likely that someone will have oversight of how customers’ requests, questions, and incidents are resolved, but that the resolutions will be done without direct IT involvement.

## Managing Private Cloud Problems

Problem Management focuses on identifying underlying problems to prevent incidents before they occur. Typically, the focus of Problem Management is on complex problems that are beyond the scope of a request for incident resolution.

Problem Management is an effort to reduce the occurrence of failures with IT services by looking for common, underlying issues. It is related to customer service in that it tries to resolve large numbers of incidents, or prevent them, by analyzing their causes.

Problem Management generally involves these tasks:

* Document, classify, and prioritize the problem.
* Research the problem.
* Apply the fix or workaround if one is found; communicate the resolution so related incidents can be closed.
* Update processes if necessary to prevent future recurrence.

### Identifying Problems in the Self-Service Layer

The Self-Service Layer provides an interface that allows cloud tenants or authorized users to request, manage, and access services. Problem Management’s goal is to find patterns, uncover and resolve root causes to fix current problems and prevent future ones with the Self-Service Layer so that Hyper-V cloud tenants or authorized users are able to request, manage, and access services, such as virtual machines.

The System Center 2012 - Service Manager service catalog and Portal serve as the provisioning user interface that allows groups within an organization to manage their own IT needs.

Problem Management is likely to be the least-changed IT process in a private cloud. It is by design a labor-intensive effort. Although it’s possible to automate some aspects of gathering information about incidents and their causes, most of the analysis will likely be done by people. Most Problem Management in the Self-Service Layer would be resolving issues with the Self-Service Portal.

The primary role type is a problem resolver; a customer service manager would likely be involved in deciding which incidents are analyzed.

### Identifying Problems in the Orchestration Layer

The Orchestration Layer is the interface between the IT organization and its infrastructure and should help transform repeatable tasks into workflow and automation. The goal of Problem Management for the layer is to find patterns, uncover and resolve root causes to fix current problems, and prevent future ones with the Orchestration Layer so that it can provide the IT process automation and workflow needed for the cloud, without IT staff involvement.

System Center 2012 - Orchestrator helps manage private clouds with a workflow designer that allows users to create runbooks to help automate data center workloads. It automatically shares data and initiates tasks in System Center 2012 - Operations Manager, System Center 2012 Configuration Manager, System Center 2012 - Service Manager, System Center 2012 - Virtual Machine Manager, Active Directory, and third-party tools.

Problem Management is likely to be the least-changed IT process in a private cloud. It is by design a labor-intensive effort. Although it’s possible to automate some aspects of gathering information about incidents and their causes, most of the analysis will likely be done by people. Most Problem Management in the Orchestration Layer would be resolving issues with Orchestrator and the technical services it relies on.

The primary role type is a problem resolver; a customer service manager would likely be involved in deciding which incidents are analyzed.

### Identifying Problems in the Management Layer

The Management Layer is responsible for providing centralized administration and management of a virtual environment, which includes the following:

* Infrastructure deployment

**Note** Deployment is assumed done for the purposes of this document.

* Infrastructure provisioning and deprovisioning

**Note** These processes are done through the Service Manager Portal or self-service interface; the Management Layer underpins that.

* Infrastructure monitoring
* Infrastructure maintenance
* Resource optimization
* Backup and disaster recovery
* Reporting

The goal of Problem Management for this layer is to find patterns, uncover and resolve root causes to fix current problems, and prevent future ones with the Management Layer so that it can effectively provide centralized administration and management of a virtual environment, without IT staff involvement.

The primary tools for the Management Layer are:

* System Center 2012 - Virtual Machine Manager, which provides centralized administration and management of the entire virtual environment.
* System Center 2012 - Operations Manager, which monitors the health and availability of the VMM management server, database server, library servers, and self-service web servers, and provides diagram views of the virtualized environment in the Virtual Machine Manager Administrator Console.
* System Center 2012 Configuration Manager, which assesses and deploys servers across physical and virtual environments; Configuration Manager also helps assess variation from desired configuration, does hardware and software inventory, and helps remotely administer computers.
* System Center 2012 - Data Protection Manager, which provides comprehensive backup capability.

Problem Management is likely to be the least-changed IT process in a private cloud. It is by design a labor-intensive effort. Although it’s possible to automate some aspects of gathering information about incidents and their causes, most of the analysis will likely be done by people. Most Problem Management in the Management Layer would be resolving issues with the technical services that support it.

The primary role type is a problem resolver; a customer service manager would likely be involved in deciding which incidents are analyzed.

### Identifying Problems in the Automation Layer

Automation provides a series of single-purpose commands and scripts that perform such operations as starting or stopping a virtual machine, restarting a server, and applying a software update, without IT staff involvement.

The goal of Problem Management for this layer is to find patterns, uncover and resolve root causes to fix current problems and prevent future ones with the Automation Layer.

The Automation Layer contains three components. They are:

* Windows PowerShell, which can be used to write scripts and cmdlets that Orchestrator uses in its integration of the rest of System Center, for such automated system administration tasks as managing the registry, services, processes, and event logs.
* Windows Management Instrumentation (WMI), which offers a consistent way to access comprehensive system management information, including information from across networks.
* Web Services for Management (WS-Management), which can use WMI to collect data about resources or to manage resources on Windows-based computers.

Problem Management is likely to be the least-changed IT process in a private cloud. It is by design a labor-intensive effort. Although it’s possible to automate some aspects of gathering information about incidents and their causes, most of the analysis will likely be done by people. Most Problem Management in the Automation Layer would be resolving issues with Windows PowerShell, WMI, and WS-Management.

### Identifying Problems with Virtualization

Virtualization is key to a private cloud in that it enables better management and distribution of workloads across the physical infrastructure. Additionally, virtualization helps lower costs (through server consolidation and redundancy), improve service availability, allow for hardware isolation, and facilitate testing.

The goal of Problem Management in this layer is to find patterns, uncover and resolve root causes to fix current problems and prevent future ones with the Virtualization Layer so that it can effectively abstract computer resources for storage, network, and server, without IT staff involvement.

Virtualization is enabled by:

* Microsoft Hyper-V Server 2008 R2: Hyper-V Server provides software infrastructure and basic management tools that you can use to create and manage a virtualized server computing environment.
* System Center 2012 - Virtual Machine Manager:VMM provides centralized administration and management of the entire virtual environment. The VMM management server runs the Virtual Machine Manager service, which runs commands, transfers files, and controls communications with other VMM components and with all virtual machine hosts and VMM library servers, collectively referred to as managed computers.

Problem Management is likely to be the least-changed IT process in a private cloud. It is by design a labor-intensive effort. Although it’s possible to automate some aspects of gathering information about incidents and their causes, most of the analysis will likely be done by people. Most Problem Management in the Virtualization Layer would be resolving issues with Hyper-V and VMM.

The primary role type is a problem resolver; a customer service manager would likely be involved in deciding which incidents are analyzed.

## Reviewing Operations

One primary management review plays a role in the Operate Phase. It is the Operational Health Management Review, which:

* Evaluates whether the cloud is operating efficiently.
* Evaluates whether the cloud is meeting expectations.
* Remediates if change is needed.

Outcomes of the Operational Health Management Review might include change requests for the continuous improvement of both processes and technology.

### Conducting an Operational Health Management Review for the Self-Service Layer

The goal of this review is to ensure that IT is effectively maintaining, monitoring, and supporting the Self-Service Layer.

Attendees should include:

* IT management.
* Key personnel from the Self-Service Layer.

The review should address the following:

* **Reports/inputs:**
* Action items/outcomes from previous Operational Health Management Review meetings for the Self-Service Layer.
* Percent of service requests being completed on time.
* Percent of tasks for requests that are manual.
* Number of new requests.
* Number of decommissions.
* Number of incidents affecting the portal.
* Portal availability.
* **Analysis/decisions:**
* Are service requests being completed as outlined in SLAs?
* Are SLAs being met?
* Are SLAs being overachieved? (This could mean SLA targets are set too low.)
* Are SLAs not being met at all? (Could be a case of overselling and underdelivering.)
* What is the number of new requests this period? YTD? Are things growing exponentially?
* Is the number of decommissions realistic?
* Is there virtual machine sprawl?
* Is portal availability sufficient?
* What number and types of service requests are manual?
* **Tools to provide data:**
* System Center 2012 - Service Manager
* **Outcomes/outputs:**
* Revisit SLA targets if exceeding or not meeting SLAs for service requests/incidents.
* Identify manual service requests that need to be automated.
* Review incidents affecting the portal and assign these to Problem Management to find the root cause.
* Review all action items at the next Operational Health MR meeting to get updates on status.
* Ensure that all action items have an owner and a due date.

### Conducting an Operational Health Management Review for the Orchestration Layer

The goal of this review is to ensure that IT is effectively maintaining, monitoring, and supporting the Orchestration Layer.

Attendees should include:

* IT management.
* Key personnel from the Orchestration Layer.

The review should address the following:

* **Reports/inputs:**
* Number of jobs executed by runbook, per period, YTD.
* Number of activities with associated runbooks.
* Number of incidents involving workflows/runbooks.
* Number of incidents where workflows/runbooks do not achieve expected results.
* Number of automated service requests completed successfully.
* Percent of tasks that require manual intervention.
* Upcoming plans for automation.
* **Analysis/decisions:**
* Is there a large number of errors with runbooks?
* Is the number of incidents with runbooks on the rise?
* Is the number of jobs run by runbooks on the rise?
* Is there a cost savings in labor due to the creation of runbooks?
* **Tools to provide data:**
* System Center 2012 - Orchestrator
* System Center 2012 - Service Manager
* **Outcomes/outputs:**
* Plan for new automation of runbooks.
* Review incidents with runbooks or the ports and assign these to Problem Management to find root cause.
* Review all action items at next Operational Health MR meeting to get updates on status.
* Ensure that all action items have an owner and a due date.

### Conducting an Operational Health Management Review for the Management Layer

The goal of this review is to ensure that IT is effectively maintaining, monitoring, and supporting the Management Layer.

Attendees should include:

* IT management.
* Key personnel from the Management Layer.
* Others could be added for expertise; for example, VMM expertise and Operations Manager expertise.

The review should address the following:

* **Reports/inputs:**
* Number of infrastructure alerts reported as Service Manager incidents.
* Number of maintenance tasks performed this period.
* Fabric management reporting.
* Storage management reports.
* Network capacity reports.
* Host density reports.
* Host-to-guest resource utilization.
* Backup reporting.
* Virtual machine health report—use Performance and Resource Optimization (PRO).
* SQL Database health report.
* Number of active versus closed alerts by period and YTD.
* Cloud component availability reports.
* **Analysis/decisions**:
* Are there a large number of errors with runbooks?
* Is the number of incidents with runbooks on the rise?
* Is the number of jobs run by runbooks on the rise?
* Is there a cost savings in labor due to the creation of runbooks?
* How well is fabric management being performed?
* Are private cloud resources being underconsumed/overconsumed?
* **Tools to provide data:**
* System Center 2012 - Operations Manager
* System Center 2012 - Service Manager
* System Center 2012 - Virtual Machine Manager
* **Outcomes/outputs:**
* Plans for new automation of runbooks.
* Review incidents with runbooks or the portal and assign these to Problem Management to find root cause.
* Identify service requests that require automation.
* Improvement plans for storage/network provisioning using VMM.
* Is additional capacity required?
* Review all action items at next Operational Health MR meeting to get updates on status.
* Ensure that all action items have an owner and a due date.

### Conducting an Operational Health Management Review for the Automation Layer

The goal of this review is to ensure that IT is effectively maintaining, monitoring, and supporting the Automation Layer.

Attendees should include:

* IT management.
* Key personnel from the Automation Layer.

The review should address the following:

* **Reports/inputs:**
* Run System Center 2012 - Orchestrator history reports on runbooks.
* Review event logs for Orchestrator runbooks.
* **Analysis/decisions**:
* Are there a large number of errors with runbooks?
* Is the number of incidents with runbooks on the rise?
* Is the number of jobs run by runbooks on the rise?
* Is there a cost savings in labor due to the creation of runbooks?
* **Tools to provide data:**
* System Center 2012 - Orchestrator
* **Outcomes/outputs:**
* Plans for new automation of runbooks.
* Review incidents with runbooks or the ports and assign these to Problem Management to find root cause.
* Review all action items at next Operational Health MR meeting to get updates on status.
* Ensure that all action items have an owner and a due date.

### Conducting an Operational Health Management Review for Virtualization

The goal of this review is to ensure that IT is effectively maintaining, monitoring, and supporting Virtualization.

Attendees should include:

* IT management.
* Key personnel from Virtualization.

The review should address the following:

* **Reports/inputs:**
* Number of virtual machines moved to an underutilized host.
* Number of new virtual machine templates created.
* Number of virtual machine templates retired.
* Number of service templates created.
* Number of updates per service.
* Monitoring and reporting on virtual machine and host health.
* Software updates applied to virtual machines and hosts.
* Insight to Problem Management for common incidents within the environment.
* SAN storage provisioned per period/YTD.
* Host density reports.
* Network capacity reports.
* **Analysis/decisions**:
* How well are we performing fabric management?
* Are resources under- or overconsumed?
* Do we need to plan for capacity upgrades?
* How efficient is this layer?
* **Tools to provide data:**
* System Center 2012 - Virtual Machine Manager
* System Center 2012 - Operations Manager
* **Outcomes/outputs:**
* Identification of areas where capacity needs to be addressed.
* Improvement plans for storage/network provisioning using VMM.

# Conclusion

Use this guide to manage and operate a Microsoft private cloud. It shows you how to apply the service management processes of the Microsoft Operations Framework (MOF). MOF is an IT service management framework that helps translate service management principles to everyday IT tasks and activities. Its goal is to align IT with business needs.

You can read this document as a guide, or as a reference document.

# Version History

|  |  |  |
| --- | --- | --- |
| **Version** | **Description** | **Date** |
| 1.0 | First release. | July 2012 |

# Acknowledgments

The Microsoft Operations Framework team acknowledges and thanks the people who produced *Managing and Operating a Microsoft Private Cloud*. The following people were either directly responsible for or made a substantial contribution to the writing, development, and testing of this paper.

**Lead Writer and Program Manager**

* Jerry Dyer *–* Microsoft

**Reviewers**

* Kathleen Wilson *–* Microsoft
* Shawn LaBelle *–* Microsoft
* Sean Christensen *–* Microsoft
* Rob Van der Burg *–* Microsoft
* Nigel Cain *–* Microsoft
* John Clark *–* Microsoft
* Clare Henry *–* Microsoft
* Michael Kaczmarek *–* Microsoft
* Mike Lewis *–* Microsoft
* Tomasz Makara *–* Microsoft
* Kaisa Selkokari *–* Microsoft
* Klaas Zweepe *–* Microsoft
* Melissa Stowe *–* Microsoft
* David Pultorak – Pultorak & Associates

**Editors**

* Jude Chosnyk *– GrandMasters*
* Laurie Dunham *– Xtreme Consulting Group*

## Feedback

Please direct questions and comments about this guide to [mofpm@microsoft.com](mailto:mofpm@microsoft.com?subject=MOF%20-%20Managing%20and%20Operating%20a%20Microsoft%20Private%20Cloud).