Microsoft® | Hyper-V Cloud

HYPER-V CLOUD DEPLOYMENT GUIDES

MODULE 3: OPERATIONS

INTRODUCTION

This document contains information about operating a virtualized Private Cloud environment on a day-to-day basis and managing change in the virtual environment.

This Operations Guide is one of five modules that are a part of the Microsoft Hyper-V Cloud Deployment Guides that are based on the framework that Microsoft Consulting Services has leveraged to deliver Server Virtualization for several years in over 82 countries.

The Hyper-V Cloud Deployment Guides from Microsoft can help IT Pros by:

- *Accelerating deployment by providing best practices for planning and delivering a Private Cloud solution based on Microsoft Virtualization technologies.*
- *Reducing training costs by providing methodologies for delivering Server Virtualization scenarios.*
- *Lowering risk by providing real-world examples of problems and solutions encountered by Microsoft architects and consultants.*

CONTENTS

OVERVIEW

An infrastructure that has virtualized, consolidated servers can fit into your current management model and infrastructure. Although the management of a virtual infrastructure can be simplified, a consolidated infrastructure has unique requirements. In addition, Private Cloud scenarios introduce some unique process management and sustainment challenges.

When planning for management, there are a number of important factors that must be considered:

- The differing management needs of hosts as compared to guests
- Additions to the management model to accommodate virtual machines
- Integrating Microsoft® Virtual Server Hosts and virtual machines into the management infrastructure
- Managing software updates to both host and guest servers
- Processes for management of the Private Cloud extensibility environment
- Capacity management of the Private Cloud infrastructure

The host computer becomes even more critical in a virtualized environment because it becomes the platform for many workloads. Server instability or hardware failure can affect multiple applications and workloads. It might be necessary to change the monitoring and alert levels for the host servers and to reevaluate the Service Level Agreements (SLAs) and response procedures around the virtual infrastructure.

One of the values of virtualization is that it offers organizations that might not have followed best practices around change and release management (due to hardware limitations) the opportunity to use the virtual infrastructure to properly test all changes before they are performed in the production environment.

The introduction of Private Cloud functionality which allows self-service may require some changes to the application of change and release management processes.

Microsoft® System Center Virtual Machine Manager 2008 R2 together with Microsoft® System Center Operations Manager and Microsoft® System Center Configuration Manager comprise the preferred suite of applications for managing the Windows®-based server infrastructure in general and the virtual infrastructure in particular.

This document serves as a general checklist of activities that focus on the following areas:

- Daily maintenance activities
- Weekly maintenance activities
- Monthly maintenance activities
- The Virtual Machine Manager administration console and views
- The Virtual Machine Manager Self-Service Portal 2.0 interface and tabs
- Backup strategies
- Change release strategies

VIRTUAL INFRASTRUCTURE MAINTENANCE ACTIVITIES

To ensure the availability and reliability of the virtual environment, there must be ongoing monitoring and maintenance of the virtual infrastructure and the services that support the virtual infrastructure. Preventive maintenance and ongoing support will help to identify potential errors before any of these errors becomes an issue that might cause downtime. Preventive maintenance combined with disaster recovery planning and regular backups will also help to minimize problems if they occur.

Monitoring the virtual infrastructure involves checking for problems with hosts, host groups, guests, services, server resources, and system resources. It is a best practice to set alerts to notify administrators when problems occur. The key advantages to daily monitoring are as follows:

- Helping to ensure that the performance requirements of the virtual infrastructure SLAs are being met
- Helping to ensure that specific administrative tasks, such as performing daily backup operations and checking server health, are being successfully completed
- Helping to enable the detection of and ability to address issues, such as a bottleneck in server performance or a need to add resources before productivity is affected

Daily Activities

The following table lists the daily maintenance tasks will help you to both establish baseline criteria for the normal operation of the virtual infrastructure environment and allow you to quickly detect any abnormal activity so that you can take action.

Daily activity	Comments
Ensure that all the services that are needed for the virtual environment are up and running.	Verify that all the services needed for the virtual environment hosts and guests are running as needed.
Ensure network connectivity to the virtual environment.	Verify that network connectivity is working.
Review outstanding incident tickets.	Review open/outstanding incident tickets daily to understand the impact of the incidents to the virtual environment and the SLAs.
Resolve open tickets, if possible.	Resolve open tickets as quickly as possible.
Monitor, at a minimum, the processor, disk, memory, and	Any agents used to monitor the physical computer or the host

network.	operating system, such as Operations Manager agents, should provide monitoring support.
Check Operations Manager alerts and reports.	Operations Manager can contain reports and alerts on various items in the virtual environment and can tell you what is occurring in the virtual infrastructure.
Perform a backup of the host systems.	A daily backup of the virtual host systems should be performed.
Perform a backup of the guest systems.	A daily backup of the guest systems should be performed.
Perform a backup of the Virtual Machine Manager library, VHDs, ISO images, and scripts.	A daily backup of the Virtual Machine Manager library should be performed for the VHDs, ISO images, and scripts contained in the library.
Perform a backup of the Microsoft® SQL Server® database for Virtual Machine Manager and of the Virtual Machine Manager job history.	The SQL Server database for Virtual Machine Manager 2008 and the job history for Virtual Machine Manager should be backed up daily.
Perform backups of the Self Service Portal 2.0 Microsoft® SQL Server® database	The Microsoft® SQL Server® database for the Self Service Portal 2.0 must be backed up daily
Backup of all Self Service Portal 2.0 Extensibility custom ActionXML segments	All custom ActionXML segments in the Self Service Portal 2.0 must be backed up daily
Review the backup status and results.	Review the backup status and results for each backup performed on a daily basis.
Check security news for the	Identify service packs, hotfixes,

latest viruses, worms, and other vulnerabilities.	or updates that may need to be applied. Test the fixes and use the change control procedures identified by you organization to apply these fixes to the specified environments.
Check Self Service Portal 2.0 requests page for outstanding requests	The Self Service Portal 2.0 requests page should be checked daily for requests the Administrator needs to action

Weekly Activities

The following table lists the weekly maintenance tasks will help you to both establish baseline criteria for the normal operation of the virtual infrastructure environment and allow you to quickly detect any abnormal activity so that you can take action.

Weekly activity	Comments
Review the SLA performance figures for the virtual environment.	Verify that the SLA performance figures for the hosts and guests are within the required ranges. Note any values above the stated thresholds so that further investigation can be performed to resolve the discrepancies.
Review Operations Manager or other monitoring reports and alerts.	Review the reports and alerts from Operations Manager or another monitoring tool with the administration team.
Review the weekly performance of the virtual environment.	Review the weekly performance reports and alerts from Operations Manager or another monitoring tool to help ensure the proper performance of the

	system over the period.
Monitor and review any updates made to the virtual environment over the last week.	Monitor and review any changes or updates made to the system over the last week. Note any changes to the performance or availability of the virtual infrastructure since the changes were applied.
Check Operations Manager alerts and reports.	Operations Manager can contain reports and alerts on various items in the virtual environment and can tell you what is occurring in the virtual infrastructure.
Perform a weekly operations management review.	Review the items listed in this table with the team.
Monitor Self Service Portal 2.0 infrastructure consumption reports	Use the dashboard reports in Self Service Portal 2.0 monitor business unit infrastructure consumption

Monthly Activities

The following table lists the monthly maintenance tasks will help you to both establish baseline criteria for the normal operation of the virtual infrastructure environment and allow you to quickly detect any abnormal activity so that you can take action.

Monthly activity	Description/Comment
Review the security checks.	Depending on the level of security that you require, it might be appropriate to perform regular audits of security, including firewall rules, user rights, group memberships, delegate rights, and so on to

	help ensure that the appropriate security levels are applied and maintained for hosts, guests and the virtual infrastructure.
Perform capacity planning.	Check capacity and performance against the SLAs. Review the SLA requirements and the capacity of the previous month. Produce and implement an upgrade path based on projected growth data. Review the Self Service Portal 2.0 infrastructure consumption reports and track consumption trends
Review and update the internal documentation and guidance for administrators.	Check that internal documentation and guidance for creating new virtual machines and maintaining the virtual infrastructure are up to date. Have a process in place to verify that the internal documentation for administrators is up to date. Audit Self Service Portal 2.0 extensibility documentation and version control. Versions of ActionXML segments must be up to date and have accurate documentation
Perform a disaster recovery test. (This test can be performed quarterly.)	Perform a disaster recovery test to verify that the process is up to date and works as expected. This can be a quarterly process.
Monitor and review the updates made to the virtual environment over the last	Monitor and review any changes or updates made to the system over the last week. Note any

week.	changes to performance or availability of the virtual infrastructure since the changes were applied. Maintain a running log of all maintenance activities. These should be reviewed weekly and monthly, and any impacts to the virtual infrastructure should be noted.
Investigate any new service packs that are available to see whether there is a need to test and apply them.	Review and investigate the service packs to see whether there is a need to test and apply them.

VIRTUAL MACHINE MANAGER ADMINISTRATOR CONSOLE

The administrator console is used to perform all the administrative tasks in Virtual Machine Manager, allowing for the centralized management of virtual hosts, virtual machines, and Virtual Machine Manager libraries. There are five main views:

- **Hosts** view
- **Virtual Machines** view
- **Library** view
- **Jobs** view
- **Administration** view

These views are briefly described in the following subsections.

Hosts View

Windows Server® Hyper-V™ hosts are managed in the Hosts view. Most of the configuration tasks are available from the Hosts view. In addition, host groups can be created and self-service policies defined.

Host Groups

Host groups are custom groups of virtual machine hosts that exist for the ease of monitoring and managing hosts and virtual machines. Host groups are represented by folders in the navigation pane of Hosts view and Virtual Machines view.

A host group's most basic function is to act as a container that can be used to group hosts and virtual machines in a meaningful way. Host groups can also be used to set aside resources on the hosts for the use of the host operating system, to provide hosts for self-service users, and to enable the automatic placement of virtual machines on the best host in a group of hosts.

Host groups are hierarchical. A child host group of an existing host group can be created for general management purposes, to override the host reserves that are inherited from the parent group, or to amend or add to the virtual machine permissions that are inherited from a parent host group.

A child host group can inherit the host reserve settings and self-service policies from its parent. However, property inheritance works differently for the following features:

- **Host reserves**. When the host reserves for a host group change, an administrator selection determines whether these changes will flow to all of its child groups. If inheritance is selected, all the host reserve settings for the parent host group will overwrite all the previous settings for all the child groups.
- **Self-service policies**. If a parent host group is used for virtual machine self-service, each of its child host groups will automatically inherit the self-service policies from the parent host group. A self-service policy can be added for the same user or group to both a parent and a child host group. In this manner, the same users can be assigned different templates, virtual machine permissions, and quotas on a subset of hosts within the parent host group.
  NOTE: This does not apply to the VMMSSP. The Self-Service polices apply to the self-service portal included with SCVMM.

Self-Service Portal 1.0 Policies

A self-service policy can be used to grant a user the ability to perform the following activities through the virtual machine self-service portal:

- Create a virtual machine
- Operate a virtual machine
- Manage a virtual machine
- Store a virtual machine
- Create checkpoints
- Connect to his or her own virtual machine

Virtual machine permissions that are set in the self-service policy determine the actions that a user or group can take on the individual virtual machines. The administrator can grant any of the following permissions:

- **Create**. Allows the user to create new virtual machines by using virtual machine templates that the administrator provides. The administrator can limit the number of virtual machines that the user can have deployed at one time by setting a virtual machine quota.
- **Full control**. Grants all the following management permissions for the virtual machines that the user owns:
  - **Start virtual machine**.
  - **Stop virtual machine**.
  - **Remove virtual machine**. Allows the user to remove the virtual machine and delete the configuration files.
  - **Pause and resume virtual machine**.
  - **Shut down virtual machine**. Allows the user to shut down the operating system on a virtual machine that has Virtual Machine Additions installed.
  - **Local administrator on virtual machine**. Allows the user to set the local administrator password when creating a virtual machine through the Virtual Machine Manager self-service portal.
  - **Virtual Machine Remote Control (VMRC) access to virtual machine**.
  - **Create and manage checkpoints on virtual machine**.

Allows the user to create and merge checkpoints and to restore a virtual machine to a previous checkpoint.

- **Store in library**. Allows the user to store virtual machines in the library when they are not in use. Stored virtual machines do not count against the user's virtual machine quota. The user's virtual machines are stored on the library share that is specified in the self-service policy. The user will have no knowledge of the physical location of a stored virtual machine.

For self-service users who are allowed to create their own virtual machines, the number of virtual machines that the users can deploy at one time can be limited by setting a quota on the self-service policy.

Since virtual machines can vary in the amount of disk space and resources they consume, a different number of quota points can be assigned to different virtual machines. This is configured through templates that the users employ to create their virtual machines.

Quota points apply only to virtual machines that are deployed to a host. If users are allowed to store their virtual machines when they are not in use, the virtual machines that are stored will not count against the quota.

Note: Section 3.1.1.2 refers to the Self Service Portal 1.0 (included with Virtual Machine Manager). Management for Self Service Portal 2.0 is different, as permissions are controlled via the Self Service Portal web portal and not from the Virtual Machine Manager console.

Virtual Machines View

Virtual Machines view provides a tabular and graphical overview of the status of the virtual machines that are managed by Virtual Machine Manager. From here, the administrator can perform the following actions against a virtual machine:

- Start
- Stop
- Pause
- Save state

- Discard a saved state
- Shut down a guest operating system
- Connect (through VMRC)
- Migrate a virtual machine
- Create a checkpoint
- Manage checkpoints
- Disable undo disks
- Repair a virtual machine
- Clone a virtual machine
- Store a virtual machine in the library
- Remove a virtual machine
- Change the properties of a virtual machine

Library View

The Library view shows a graphical summary or a tabular view of the recourse options that are available in the Virtual Machine Manager library. From within the Library view, new library servers can be added along with templates, hardware profiles, and guest operating-system profiles. Virtual machines that have been created with other virtualization solutions, such as VMware, can be converted and added to the library from this view.

Jobs View

Each unit of work in Virtual Machine Manager is tracked as a job. These jobs are created as actions are taken on the objects that are managed by Virtual Machine Manager. For example, creating a virtual machine is a single job. Stopping or starting that same machine is also a job that can be monitored, canceled, or restarted. These jobs are displayed in Jobs view and can be searched, sorted, filtered, and grouped.

Virtual Machine Manager can report the following job information:

- Status
- Applicable Windows PowerShell™ command
- Start date
- End date
- Progress

- Resulting object name
- Result type
- Owner

Administration View
The Administration view provides the access to create and manage the following:

- **Managed computers**. Manage Virtual Machine Manager agents on managed hosts and library servers: update the agent, remove agent roles, and re-associate agents with the current Virtual Machine Manager server.
- **Self-service**. Add and remove Web servers that are used in virtual machine self-service.
- **Settings**. Configure the system-wide settings for joining or leaving the Customer Experience Improvement Program (CEIP); for configuring library refreshes, virtual machine intelligent placement defaults, and system-wide VMRC settings; for specifying the administrative contact for self-service users; and for backing up Virtual Machine Manager.

SCVMM SELF-SERVICE PORTAL 2.0 MANAGEMENT INTERFACE

All user actions and Management tasks for the Self Service Portal 2.0 are performed through the web interface. The web UI is security context trimmed, so only administrators can see all functions. There are six function tabs in the Self Service Portal 2.0.

- Requests
- Infrastructure
- Virtual Machines
- Jobs
- User Roles
- Settings

The tabs are explained in the following section.

Requests

This tab is where Business Unit administrators make requests. There are three types of requests that can be made:

- Business Unit registration
- Infrastructure creation
- Change Request to existing infrastructure

From the administrator view, all requests are presented on this tab. From the 'Requests' tab the administrator enters required information into the requests and can approve or reject them.

Infrastructure

The infrastructure tab displays all infrastructures configured in the system. An infrastructure in Self Service Portal is defined as a collection of environment settings and virtual machine quotas. Limits of RAM and Storage are assigned to infrastructures, which are broken down into sub-groups called 'Services'. Business Units can create Virtual Machines at will as long as the limits assigned to the infrastructure are not exceeded.

Business Unit admins can only see their own infrastructures, whereas Self Service Portal Administrators can see all infrastructures in the system.

Virtual Machines

The Virtual Machines tab is used to view and interact with the Virtual Machines created by the portal.

The following functions can be made available to users:

- Connect to VM
- Create VM
- Delete VM
- Deploy VM (from Virtual Machine Manager Library)
- Pause VM
- Resume VM
- Shutdown VM
- Start VM

- Stop VM (In Virtual Machine Manager Library)

Which functions are available will depend on the permissions assigned to users.

Jobs

The jobs tab will display the status of jobs initiated by the Self Service Portal. In most cases, equivalent jobs can be seen in the Virtual Machine Manager console ‘Jobs’ view. However, some differences must be noted:

- Jobs in the Self Service Portal cannot be restarted
- Not all Jobs seen in Virtual Machine Manager Console are reflected in the Self Service Portal. Self Service Portal only displays jobs initiated by the Self Service Portal
- Self Service Portal job also display the status of all ActionXML tasks within an activity.

User Roles

All access to the Self Service Portal is controlled from the ‘User Roles’ tab. When a Business Unit is approved, the nominated administrator of that Business Unit has full control over access controls for all infrastructures assigned to that Business Unit.

An infrastructure is broken down into sub-groups called Services. Services can then be broken down into Service Roles. Virtual Machine access can be controlled at the infrastructure, Service and Service Role levels. For example, the Business Unit Administrator can assign access to Virtual Machines in Service ‘A’, but not Service ‘B’ within an infrastructure.

There are five default User Roles within the Self Service Portal:

- DCIT (Data Center Administrator)
- BUIT (Business Unit Administrator)
- Business Unit Advanced Operator
- Business Unit User
- Custom User

DCIT

The Data Center Administrator has full control over all aspects of the Self Service Portal including:

- All configuration settings
- Device Configuration (SAN and Load Balancer)
- Network Configuration
- Virtual Machine Manager Template Import
- Approval/Rejection of all requests
- Creation of Custom User Roles

BUIT

The Business Unit Administrator has full control over the Business Unit to which they have been designated Administrator. An individual or group can be administrators of more than one Business Unit.

The BUIT is able to undertake the following actions on behalf of a Business Unit:

- Request Infrastructures (Requires DCIT approval)
- Request changes to Infrastructures (Requires DCIT Approval)
- Assign permissions to Virtual Machine access to an Infrastructure, Service(s) and Service Role(s)
- All Virtual Machine Tasks

Business Unit Advanced Operator

The Business Unit Advanced Operator can only manage Virtual Machines and is given access to the following Virtual Machine functions:

- Connect to VM
- Create VM
- Delete VM
- Deploy VM (from Virtual Machine Manager Library)
- Pause VM
- Resume VM
- Shutdown VM
- Start VM
- Stop VM
- Store VM (in Virtual Machine Manager Library)

Business Unit User

The Business Unit User is given access to the following subset of Virtual Machine actions:

- Connect to VM
- Deploy VM (from Virtual Machine Manager Library)
- Resume VM
- Shutdown VM
- Start VM
- Stop VM
- Store VM (in Virtual Machine Manager Library)

Custom User

Custom User Roles can be created by the DCIT. The Custom User Role can be assigned any combination of Virtual Machine actions. Once a Custom Role has been created by the DCIT, it will be available to all BUITs.

Settings

The Settings tab is where all Self Service Portal configurations are performed. The Settings Tab is separated into three main areas:

- Data Center Management
- Virtual Machine Templates
- Virtual Machine Actions

Data Center Management

The Data Center configuration is where the Self Service Portal connections are configured.

SCVMM Server – The FQDN of the Virtual Machine Manager server is specified in this section. The Self Service Portal can only be associated with a single Virtual Machine Manager server. The Service Account running the Self Service Portal Engine service must have administrator rights within Virtual Machine Manager.

Device Configuration – Connection parameters to SAN and Load Balancer devices are configured in this section. The Device name is supplied with the script connection string to be used for device connection.

Network Configuration – Networks are added in this sectionthe following parameters can be assigned on a per network basis:

- Domain Join – If selected, all Virtual Machines on this network will be joined to a specified domain. Multiple domains can be listed for selection.
- VLAN – A VLAN ID can be assigned to all VMs assigned to a network.
- IP addressing – Dynamic or static can be selected. If Static is configured, the Administrator can enter scope details and the Virtual Machines will be assigned the next free address in the specified range.

Active Directory – All Domains Virtual Machines are able to join are listed here. If Domains are listed and the Domain Join option is checked in the network configuration the user will be presented with a list of Domains to select from when a Virtual Machine is created.

Quota – Default Value units are assigned for RAM (per GB/Day) and Storage (per GB/Day). These values can be overridden at the 'Service' level within an infrastructure. These unit values are used in chargeback calculations.

Environment – The environment setting is supplied as a choice when users create Virtual Machines. Environment is a free from text field and can be any value. There must be at least one value for environment in place for Virtual Machines to be created. The environment value can be used as a variable in execution scripts to undertake particular actions.

SCVMM Templates

This section is where Templates are imported from Virtual Machine Manager for use by the Self Service Portal. By Default the template must be a syspreped image to be deployed by the standard scripts. Value units are assigned to the template in this section, which are used in chargeback calculations. The value will be charged as

Units/Day for any Virtual Machine provisioned from a template.

Virtual Machine Actions

Custom ActionXML segments are created in this section. Custom ActionXML scripts are used to undertake additional provision actions that may be required. For example, a custom segment could create a LUN on storage equipment or configure a Load Balancer with IP details of the VM being created. The custom segment can also be used to deploy applications/services to the Virtual Machine by integrating with the organizations software distribution system.

The ActionXML segment is made up of a collection of tasks. Each task represents a script, which can be; PowerShell, VBScript or Batch (command line). For example, the CreateVM action under the Custom ActionXML segment might contain three distinct tasks, Configure the Load Balancer, Create the VM and Deploy and application to the VM.

Use of the Custom ActionXML segments allows end-to-end automation for the creation of Virtual Machines. The actions undertaken are transparent to the user; they simply request a Virtual Machine Service Role. The Service Role is tied to a particular ActionXML segment that undertakes the required actions.

MANAGING VIRTUAL INFRASTRUCTURE BACKUPS

It is important to develop and implement a comprehensive backup plan for protecting Virtual Machine Manager and the Self Service Portal data, including the Virtual Machine Manager server, hosts, virtual machines, library servers, the Self Service Portal Database and ActionXML Segments

> **Important**
>
> Virtual machine checkpoints should not be considered backups for disaster recovery. Checkpoints do not create full duplicates of the hard disk contents, nor do they copy data to a separate

> volume. A checkpoint can serve as temporary backup before an operating system is updated so that it can be rolled back. A backup application should be used to back up and recover your data in case of catastrophic data loss.

Creating a Backup Plan

The principal factor to consider when planning data backups is the ability to quickly recover the environment if data is lost or corrupted. Key candidates for protection are files that change frequently or are frequently accessed. Backup plans will be needed for:

- The Virtual Machine Manager server
  - The SQL Server database (user accounts and configuration data)
  - The job history
- Hosts
  - Virtual machines
- Library server data
  - VHDs
  - ISO images
  - Scripts
- Self Service Portal 2.0 data
  - Self Service Portal 2.0 Database
  - Custom ActionXML segments

Backing Up Virtual Machine Manager Servers

A Virtual Machine Manager server contains the SQL Server database that holds the Virtual Machine Manager configuration information. The SQL Server database can be backed up through the Virtual Machine Manager administrator console, or a system state backup of the Virtual Machine Manager server can be performed.

It is recommended that when a Virtual Machine Manager server is backed up, a system state backup is created so that the Virtual Machine Manager server can be rebuilt with the same security identifier (SID) in the event of catastrophic data loss.

Backing Up Hosts and Library Servers

A virtualized environment requires the same attention to backup planning as the physical environment does. Unlike a physical server, for which the internal system resource usage does not impact other workloads, a virtual machine shares hardware resources with other virtual machines. Therefore, the virtual machine backup schedule must minimize the impact on performance and application availability.

It is recommended that you use Microsoft® System Center Data Protection Manager or a third-party backup suite that takes advantage of the Volume Shadow Copy Service (VSS) to make a copy of the host and library data for backup.

Hyper-V™ provides new functionality with its VSS writer interface. The Hyper-V VSS writer provides the following functionality:

- The backup and recovery of Virtual Server and all configuration settings.
- The online backup of Windows Server® 2003 (or later) virtual machines.
- The offline backup of all supported guest operating systems.
- The ability of users to initiate a backup from a parent partition, which provides a seamless backup of the virtual machines that have Integration Services installed
- Using Windows Server Backup requires that you register Hyper-V as a supported application before you initiate the volume backup. Backing up and recovering child partitions and machines from the parent is not a supported scenario for Windows Server Backup. Windows Server Backup can be used to individually protect each guest operating system.
- The recovery of individual virtual machines to the same or a different host.

For library servers, much of the library data actually resides in the Virtual Machine Manager database. Templates, hardware profiles, and guest operating-system profiles are not represented as files on the library share. Therefore, this information is backed up with the Virtual

Machine Manager database. Library resources that are represented by files can be backed up by using the customer's backup suite.

Backing up Self Service Portal Data

The bulk of the important Self Service Portal data, including Virtual Machines in service, infrastructure information and chargeback data are stored in the Microsoft SQL Server database. This database must be backed up via an approved method for the database and transaction logs.

The ActionXML segments are broken up into two areas:

- Task name and execution order
- Task content (script and assigned variables)

All aspects of a Custom ActionXML should be versioned and fully documented.

VIRTUAL INFRASTRUCTURE PATCH MANAGEMENT

Patch management is a critical component of operating any infrastructure. There are many software suites that can be used to manage updates on virtual machines, such as Windows Server Update Services, Microsoft® Systems Management Server 2003 and System Center Configuration Manager 2007, and third-party applications.

In most instances, virtual hosts and virtual machines can be treated in much the same manner for patch management. However, there are some patch management challenges that are unique to the virtual environment:

- **Host updates**. A Hyper-V host that requires a restart after update installation affects the availability of all of its guests.
- **Isolated guests**. Virtual machines may be connected to an internal network and inaccessible to the patch management solution.
- **Powered-off guests**. A virtual machine that is either used for testing or stored in the Virtual Machine Manager library

may be powered off for extended periods of time.

- **Performance**. Updating all the guests on a particular host can have a significant performance impact on all the machines.

Virtual Server Host Updates

When the host machine requires a restart to complete the installation of an update or service pack, all the virtual machines that are assigned to that host will be unavailable during the reboot period.

If the guest applications are critical, consider using Hyper-V host clustering with quick migration to minimize the service interruption for mission-critical guests.

Otherwise, coordinate the time of the updates to the virtual infrastructure so that the virtual machines are updated first and then restarted, if necessary. After that is complete, shut down the running guests and update the host. After the host restart is complete, all the guests can be returned to service.

Offline Virtual Machine Servicing

The Offline Virtual Machine Servicing Toolkit is a complimentary Solution Accelerator. Solution Accelerators are authoritative resources that help IT pros plan, deliver, operate, and manage IT systems that address real-world scenarios. Solution Accelerators provide free, prescriptive guidance and automation to accelerate cross-product integration, core infrastructure development, and other enhancements.

Self Service Portal Patching Requests

When an infrastructure is requested by a Business Unit in the Self Service Portal, there is a section to specify backup and patching requirements.

This must be taken into account when designing a patching infrastructure. A Business Unit may be provisioning Virtual Machines in an isolated test environment where a constant state is required. In such and environment, patching may not be desirable.

ADDITIONAL CHANGE MANAGEMENT CONSIDERATIONS

Change management focuses on a variety of change-related issues that can follow the deployment of the virtual infrastructure. The organizational changes subject to the change management process include those regarding hardware, software, system components, documents, and processes—anything deliberately introduced into the virtual environment that could affect its functioning as reflected in the SLAs between the IT department and the business that it serves. When considering a process for change management for the virtual infrastructure, the following activities should be considered or included as part of that process:

- **Making a change request**. Formally initiating a change by submitting a request for change (RFC).
- **Classifying a change**. Aassigning a priority and category to the change, using its urgency and impact on the infrastructure or users as criteria. This assignment affects the implementation speed and route.
- **Authorizing a change**. Considering and approving or disapproving the change by the Change Manager, and if one exists, the Change Advisory Board (CAB)—a board that contains IT and business representatives.
- **Developing a change**. Planning and developing the change, a process that can vary immensely in scope and that includes reviews at key interim milestones.
- **Releasing a change**. Rreleasing and deploying the change into the production environment.
- **Reviewing a change**. Conducting a post-implementation process that determines whether the change has achieved the goals established for it and whether the change should

be kept in effect.

At a minimum, determine and document the change management policies regarding the how, when, and who elements of the patch management process. Some questions to consider:

- Are changes managed (identified, tested, and deployed)?
- Do users or the operations staff perform the changes?
- What tools are used? Are they automated? In what way?

Private Cloud Agility

With the Private Cloud scenarios enabled by the Self Service Portal 2.0, a different application of Change Management theory needs to be employed.

The concept behind Private Cloud includes the dynamic provisioning of Virtual Machines on demand from Business Units. This activity should not attract the full change management approval process. Rather the provision of the underlying infrastructure would attract the change approval process.

The workflow in Self Service Portal has been designed for the approval stages to be set at the Business Unit registration, Infrastructure request and Infrastructure change request stages. Once an Infrastructure request has passed change and release management controls, the Infrastructure can be considered 'Live'. At this point the Administrator can approve the Infrastructure request in the Self Service Portal. The Creation and Removal of Virtual Machines from that Infrastructure are the responsibility of the Business Unit and should not attract additional processes.

CONFIGURATION MANAGEMENT CONSIDERATIONS

Configuration management is the critical process responsible for identifying, controlling, and tracking all the versions of hardware, software, documentation, processes, procedures, and other critical components of the IT organization. The key benefit that configuration management provides is the modeling of relationships in the environment. Change management uses this information to evaluate the impact of a change and so depends on the accuracy of the configuration data to ensure that such an impact can be understood and communicated appropriately.

It is especially important that environments running Hyper-V follow configuration management best practices for the host systems. Insufficient or incorrect configuration information can lead to poor decisions that negatively impact the environment. Host system information that could be included in the configuration management system includes the following configuration items and attributes:

- Name
  - Network interfaces
  - Operating system
  - Memory
- Processor
  - Manufacturer
  - Speed
  - Cores
- Network interfaces
  - Name
  - Subnet
  - IP address
  - Internet Small Computer System Interface (iSCSI)
- Applications
  - Microsoft patches
  - Antivirus software
  - Application versions
  - Backup software
  - And so on
- Storage controller
  - Additional CIs and attributes
- Cluster

- Additional CIs and attributes

Documentation includes SLAs, the disaster recovery plan, the build documentation, and so on.

For more information about configuration management and the Microsoft Operations Framework (MOF), visit http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx.

Self Service Portal Custom ActionXML version control and documentation

The Self Service Portal Custom ActionXML segments are capable of very powerful automation actions, when integrating with SAN and Load Balancer equipment in particular. Due to the powerful nature of the feature, it is critical to keep very tight version controls on the Custom ActionXML segments to provision Virtual Machines. Changes to any segments must be documented and subject to change and release management.

RELEASE MANAGEMENT CONSIDERATIONS

One of the greatest values of virtualization is the ability of organizations that have not performed full release management activities in the past to now use the technology to help ensure that all approved changes are properly vetted before being introduced into the production environment. Release management is responsible for deploying changes into an IT environment. After one or more changes are developed, tested, and packaged into releases for deployment, release management is responsible for introducing these changes and managing their release.

The challenge many organizations face is that they have insufficient hardware to fully test releases. If test environments do exist, it is often time consuming and difficult to test the changes on exact replicas of the production environment. Virtualization technology, along with effective change management, configuration management, and release management processes, allow organizations to better ensure that releases do not cause disruption or outages when introduced into production. Hyper-V provides the ability to easily create copies of guest systems and test the releases and changes.

For more information about release management and Microsoft Operations Framework 4.0, visit http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfrelmg.mspx.

APPENDIX A: PORTS AND PROTOCOLS

Virtual Machine Manager uses various ports and protocols to pass data and commands among Virtual Machine Manager components:

- The Virtual Machine Manager server communicates with Virtual Machine Manager agents by using Windows Remote Management (WinRM) and transfers data to and from the managed computers by using the Background Intelligent Transfer Service (BITS).
- The Virtual Machine Manager administrator console communicates with the Virtual Machine Manager server by using Windows Communication Foundation services.
- The Virtual Machine Manager self-service portal communicates with the Virtual Machine Manager server by using Windows Communication Foundation services, and self-service users connect to the portal by using HTTP.
- A self-service user connects to and interacts with the virtual machines by using VMRC.

The following table provides the default port settings that are used by Virtual Machine Manager. These are configurable to suit the needs of the customer.

Connection type	Protocol	Port
Virtual Machine Manager server to managed computers (control channel)	WinRM	TCP 80

Virtual Machine Manager server to managed computers (data transfer)	BITS	TCP 443
Virtual Machine Manager administrator console to Virtual Machine Manager server	WCF	TCP 8100
Virtual Machine Manager self-service portal to Virtual Machine Manager server	WCF	TCP 8100
Self-service users to Virtual Machine Manager self-service portal (1.0)	HTTP	80
Self-Service users to VMMSSP 2.0	HTTP	Admin nominated (80 by default)
VMMSSP Web server to Engine Server for queue service	WCF	Admin nominated (TCP 8100 and 8000 by default)
VMMSSP Web and Engine Server connection to SQL database	TCP	Admin nominated (1433 by default)
VMMSSP Dashboard reporting website	TCP	Admin nominated (specified at installation)

ADDITIONAL RESOURCES

Below are several other resources available to accelerate a successful Server Virtualization deployment.

Microsoft Solution Accelerators

Microsoft provides tools and guidance to help you solve your deployment, planning, and operational IT problems. They are free and fully supported.

Microsoft Assessment and Planning (MAP) Toolkit
Download this network-wide inventory and assessment tool to determine the virtualization candidates for Windows Server 2008 R2 Hyper-V and Application Virtualization. If your customer is currently running VMware, the toolkit now includes a VMware discovery feature that identifies already-virtualized servers running under VMware that can be managed with System Center Virtual Machine Manager or which can be migrated to Hyper-V.

Learn more at: http://technet.microsoft.com/en-us/solutionaccelerators/dd537570.aspx?SA_CE=VIRT-MAP-WEB-SAT-2009-07-13

Offline Virtual Machine Servicing Tool 2.1
The Offline Virtual Machine Servicing Tool 2.1 has free, tested guidance and automated tools to help keep offline virtualized machines updated, without introducing vulnerabilities into your IT infrastructure. The tool combines the Windows Workflow programming model with the Windows PowerShell™ interface to automatically bring groups of virtual machines online, service them with the latest security updates, and return them to an offline state.

Learn more at: http://technet.microsoft.com/en-us/library/cc501231.aspx?SA_CE=OVMST21-Release-VIRTPROD-2009-

12-07

Infrastructure Planning and Design Guides for Virtualization

Streamline your virtualization-infrastructure design processes with planning guidance from Infrastructure Planning and Design Guides for Virtualization. Each guide addresses a unique virtualization-infrastructure technology or scenario, provides critical architectural decisions to be addressed with available options, and supplies the means to validate design decisions to ensure that solutions meet the requirements of both business and IT stakeholders.

Learn more at: http://technet.microsoft.com/en-us/solutionaccelerators/ee395429.aspx

Microsoft.com

In addition to the resources above, please visit http://www.microsoft.com to find resources for delivering Microsoft Server Virtualization technologies.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document and its contents are provided AS IS without warranty of any kind, and should not be interpreted as an offer or commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented. The information in this document represents the current view of Microsoft on the content. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.