

HP Server Automation

Software Version: 10.23

User Guide: Virtualization Management

Document Release Date: June 2016
Software Release Date: June 2016



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2001-2016 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: <http://h20230.www2.hp.com/selfsolve/manuals>

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: <http://h20229.www2.hp.com/passport-registration.html>

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: <http://www.hp.com/go/hpsupport>

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<http://h20229.www2.hp.com/passport-registration.html>

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Virtualization Management Help	7
Chapter 1: Benefits of Using SA for Virtualization Management	1
Visibility	1
Compliance	2
Control	3
Chapter 2: Managing Permissions	4
Virtualization User Groups	4
Virtualization Permissions	4
Setting Virtualization Container Permissions	7
Chapter 3: The SA Client Virtualization Tab	10
Virtualization Services	10
Virtualization Tab	10
Icons for Virtualization Items	14
Devices Tab	15
Managing Oracle Solaris Zones	16
Managing HP-UX Virtual Servers	16
Chapter 4: Virtual Machine and VM Template Life Cycle	17
Create VM Templates	17
Deploy VMs from VM Templates	20
Keep VMs in Compliance	20
VM Template Life Cycle	20
Modify Attached Policies	21
Modify Attached Policies and Create a New VM Template	22
Attach New Policies and Create a New VM Template	23
Chapter 5: Virtualization Service Tasks	25
Prerequisites	25
Virtualization Security	28
Supported Tasks	28
Add Virtualization Service	28

Reload Virtualization Service Data	30
Reload Virtualization Items Data	31
Edit Virtualization Service	31
Remove Virtualization Service from SA	32
Chapter 6: Virtual Machine and VM Template Tasks	34
Supported Tasks	34
Create and Provision a VM - vCenter	35
Create and Provision a VM - SCVMM	40
Deploy a VM from a VM Template - vCenter	44
Deploy a VM from a VM Template - SCVMM	50
Clone a VM - vCenter	54
Install the SA Agent on a VM	58
Prerequisites for OpenStack	59
Requirements for OpenStack Instance	59
Installing the SA Agent on the VM	59
Modify a VM - vCenter and SCVMM	60
Migrate a VM - vCenter	62
Migrate a VM - SCVMM	64
Deactivate the SA Agent on a VM	66
Delete a VM - vCenter and SCVMM	66
Power On/Off a VM - vCenter and SCVMM	67
Suspend a VM - vCenter and SCVMM	68
Pause a VM - SCVMM	68
Reset a VM - vCenter	69
Shut Down a VM Guest OS - vCenter and SCVMM	70
Restart a VM Guest OS - vCenter	70
Convert a VM to a VM Template - vCenter	71
Convert a VM to a VM Template - SCVMM	72
Modify a VM Template - vCenter and SCVMM	73
Delete a VM Template - vCenter and SCVMM	74
Chapter 7: Managing HP-UX Virtual Servers	76
Terms and Definitions	76
Requirements	76

Supported Platforms and Configurations	77
Not Supported	78
SA Permissions Required	78
Virtualization Service Management Permissions	78
Action Permissions Required	78
Folder Permissions Required	79
Resource Permissions Required	80
Server and Switch Status Icons	80
Quick Start vPars, HPVMs, and vSwitches	81
Launching the HP-UX Virtualization Manager	81
Saving ioscan Output	81
Viewing Summary, Hardware, and ioScan Information	82
Adding an HPVM Hypervisor/vPars Container	89
Configuring Server Timeouts	90
Custom Attributes that HP-UX Virtualization Manager Creates	91
Managing vPars Containers	92
Switching between nPars and vPars modes	92
Creating a vPar	93
Modifying a vPar	96
Starting a vPar	96
Shutting Down a vPar	96
Halting a vPar	97
Deleting a vPar	97
Managing HPVM Hypervisors	97
Creating an HPVM	97
Modifying HPVMs	101
Starting an HPVM	102
Halting an HPVM	102
Shutting Down an HPVM	102
Removing or Deleting an HPVM	103
Managing vSwitches	103
Creating a vSwitch	103
Modifying a vSwitch	104

Starting a vSwitch	105
Stopping a vSwitch	105
Deleting a vSwitch	105
Configuring VLAN Connections	106
Troubleshooting Issues	106
Checking Log Files	107
Example Log Messages	107
Chapter 8: Managing Oracle Solaris Zones	109
OS Provisioning and Agent Installation for Oracle Solaris Zones	109
Creating a Zone	110
Installing an Agent on an Existing Unmanaged Non-Global Zone	113
Modifying a Non-Global Zone	114
Starting or Stopping a Non-Global Zone	115
Deleting a Non-Global Zone	115
Reloading Oracle Solaris Zone Information	116
Chapter 9: Genealogy of VMs	117
Overview	117
How to Start Genealogy for a VM or Template	117
About the Genealogy Window	121
Management Permissions and Genealogy	126
Refresh Action from the Genealogy Window	128
Appendix A: Virtualization Concepts and Terms	130
Appendix B: Virtualization Security	133
Editing Secure Mode and Importing the CA Certificate	133
Removing a CA Certificate	134
Send Documentation Feedback	136

Virtualization Management Help

HP-supported integrations with virtualization vendors and cloud computing solutions are referred to collectively as virtualization services.

The virtualization vendors manage multiple hypervisors and VMs in a virtualization environment. HP supports integration with VMware vCenter Server, Microsoft System Center Virtual Machine Manager (SCVMM), and OpenStack.

OpenStack Support in Virtualization

Cloud computing solutions such as OpenStack offer Infrastructure as a Service (IaaS). HP SA supports limited integration with OpenStack.

Virtualization management in HP HP Server Automation provides:

Visibility into your datacenter and all your physical and virtual machines (VMs).

Compliance with all your regulatory and enterprise policies.

Control over your entire virtual environment so you can keep VM sprawl in check and detect and resolve problems quickly.

This help contains the following topics:

Benefits of Using SA for Virtualization Management

Managing Permissions

The SA Client Virtualization Tab

Virtual Machine and VM Template Life Cycle

Virtualization Service Tasks

Virtual Machine and VM Template Tasks

Managing HP-UX Virtual Servers

Managing Oracle Solaris Zones

Virtualization Concepts and Terms

Virtualization Security

Chapter 1: Benefits of Using SA for Virtualization Management

HP-supported integrations with virtualization vendors and cloud computing solutions are referred to collectively as virtualization services.

The virtualization vendors manage multiple hypervisors and VMs in a virtualization environment. HP supports integration with VMware vCenter Server and Microsoft System Center Virtual Machine Manager (SCVMM).

Cloud computing solutions such as OpenStack offer Infrastructure as a Service (IaaS). HP supports limited integration with OpenStack.

Virtualization management in HP Server Automation provides:

- **Visibility** into your datacenter and all your physical and virtual machines (VMs).
- **Compliance** with all your regulatory and enterprise policies.
- **Control** over your entire virtual environment so you can keep VM sprawl in check, and detect and resolve problems quickly.

Visibility

SA provides full visibility into your hybrid, heterogeneous, distributed datacenters:

- **Genealogy of VMs** - SA records how each VM was created and displays it in the Virtualization view of the SA Client. You can also perform searches on how VMs were created.
- **Search for VMs by Virtual Characteristics** - Advanced search allows you to locate VMs, VM templates, hypervisors, clusters, resource pools, and datacenters by cluster properties, resource pool properties, number of processors, datastore, hypervisor, memory, creation method, power state, and many other criteria.
- **One Tool, One Unified View** - SA Client's integrated view lets you see and manage your physical and virtual assets across virtualization technologies and in all your datacenters.
- **Support for Major Virtualization and Cloud Vendors** - You can view and manage virtual machines and virtual environments from VMware, Microsoft, Oracle, Hewlett-Packard, and

OpenStack. SA allows you to synchronize with these vendors' tools to ensure you have access to all changes and can update your data accurately.

- **Across Physical and Virtual Machines** - You can use the same processes to view, provision, install software and patches, configure, audit, and remediate your physical servers and VMs.
- **See All Virtual Assets** - SA provides comprehensive details about all your virtual assets, such as datacenters, resource pools, projects, clusters, hypervisors, virtual machines, folders, datastores, and network elements.
- **See Outside and Inside Servers** - SA gives you a view of both the outside of your servers – location, relationships with other servers – and inside your servers – hardware, software, and configurations:
 - **See Outside Your VMs** - SA provides a single view of your entire datacenter, across physical and virtual boundaries, across virtualization vendors, across networks, and across geographies.
 - **See Inside Your Servers** - SA lets you manage and provision the operating system, install and configure software, install patches, audit servers to detect compliance drift, and remediate servers to bring them back into compliance.
 - **Extensible** – You can store any custom information about your VMs in custom attributes. Then you can perform operations based on custom attribute values.
- **All Major Operating Systems** - You can provision, configure, and manage servers running on operating systems such as Microsoft Windows, Red Hat Enterprise Linux, Oracle Enterprise Linux, SuSE Linux Enterprise, VMware ESX, Oracle Solaris/SunOS, HP-UX, AIX, Ubuntu, and CentOS.
- **Storage** - SA gives you end-to-end visibility to your datastore inventory, physical and virtual disks, and DVDs.
- **Networks** - You can view detailed network information about physical servers and VMs, their network connections, and interfaces.

Compliance

With SA, you can keep your physical servers and VMs in compliance with your enterprise business, industry, and government IT requirements:

- **Create VM Templates from Baseline Servers** - VM templates contain everything needed to create standard, fully compliant, and fully manageable VMs – operating system, patches and patch

policies, and software and software policies.

- **Guest Customization** - After you create VMs, you can modify them to be network ready.
- **Audit Reports Detect Compliance Drift** – Regular audits identify servers that have been modified and are no longer in compliance.
- **Remediate Servers Back Into Compliance** – You can bring all your noncompliant servers back into compliance by installing required software and patches and reconfiguring your systems and software.

Control

SA provides users with the ability to create and manage VMs:

- **Full End-to-End VM Life Cycle** - You may create compliant, provisioned VMs from templates; monitor, modify, audit, and remediate them to keep them in compliance; and delete them when you no longer need them.
- **Discovery** - SA discovers the environment managed by a Virtualization Service (VS) to provide an inventory of VMs and associated networking and storage assets.
- **Create and Provision** - You may create, clone, and deploy VMs from templates. All VMs are provisioned with the operating system, application software, and configurations your users need and your IT standards require.
- **Place VMs** - SA provides you with full visibility and placement control.
- **Update Templates** - Keep your templates up to date with the latest patches, software, and configurations.
- **Detect Changes and Resolve Problems** - Detect changes and solve problems across all physical servers and VMs.
- **Power Controls** - With SA, you have full power controls over your VMs, including power on, power off, suspend, pause, reset, restart guest, and shut down guest.
- **Performance** - Allows you to detect overloaded and underutilized resources and move VMs from one host to another to balance resource usage.
- **Quick Access** - SA provides quick access to your servers with SA's Global Shell and remote login.

Chapter 2: Managing Permissions

This section describes how to set permissions in your virtualization environment. For more information on permissions, see the SA Administration Guide.

Virtualization User Groups

Permissions are granted through user groups. SA provides a set of user groups based on typical roles that are intended to help you set up your own user groups specific to your environment.

Make a copy of the HP-provided user groups listed in the following table and modify them to provide the permissions your staff needs. These user groups are provided as a starting point, and you should create your own user groups based on these user groups.

Virtualization User Groups

User Group Name	Description
Virtualization Administrators	Access to add, edit, and remove virtualization services, manage life cycle of VMs and VM templates, and administer permissions for your virtualization inventory.
VM Life Cycle Managers	Access to manage life cycle of VMs, including create, modify, migrate, clone, remove VMs, VM power controls, and deploy VMs from VM templates.
VM Template Deployers	Access to deploy VMs from VM templates, clone VMs, and VM power controls.
VM Template Managers	Access to manage life cycle of VMs and VM templates, including create, modify, migrate, clone, remove VMs, VM power controls, convert VMs to VM templates, deploy VMs from VM templates, and remove VM templates.

Virtualization Permissions

To perform virtualization actions, you need the following four types of permissions:

- **Action Permissions** allow you to perform specific tasks such as cloning a VM, deploying a VM from a VM template, converting a VM to a VM template, and so forth. Without action permissions, the corresponding menu items are not even displayed in the Actions menu of the SA Client. For a

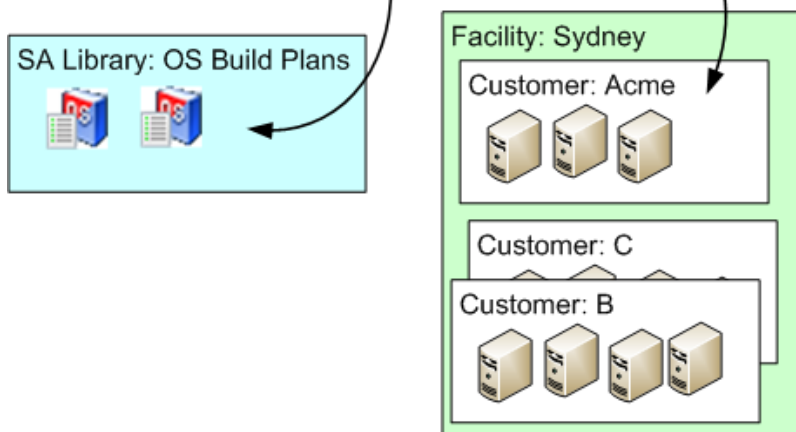
complete list of action permissions, see the SA Administration Guide.

- **Virtualization Container Permissions** give you access to the Virtualization Services and the containers under the VS. These containers can be datacenters, hypervisors, host groups, clusters, resource pools, folders, and projects under the Virtualization Service.
- **Server Resource Permissions** give you access to facilities, customers, and device groups where the VMs will run. For more information on server resource permissions, see the SA Administration Guide.
- **Folder Permissions** give you access to items in the SA Library needed by VMs, such as OS Build Plans, patches, and patch policies, software packages and software policies, application configurations, audit policies, and reports. For more information on folder permissions, see the SA Administration Guide.

The following figure shows some of the key permissions needed to create a VM for the customer Acme and provision it with an OS Build Plan.

Partial Permissions Needed to Create a VM

- ✓ Action Permission: *Manage VM Lifecycle: Create VM: Yes*
- ✓ VS Container Permission: *Hypervisor: Write*
- ✓ Server Resource Permission: *Customer Acme: Write*
- ✓ Folder Permission: *OS Build Plan: Execute*



Depending on your particular virtualization hierarchy, some or all of the following permissions are required for complete authorization to create a VM:

- **Action Permissions:** These action permissions are required to create and provision a VM.
 - **Manage VM Life Cycle: Create VM** - This is the basic action permission required to create a VM.
 - **Managed Servers and Groups** - This is the basic action permission required to view managed servers.
 - **View Virtualization Inventory** - This is the basic action permission required to view the virtualization inventory under the Virtualization tab in the SA Client. Without this permission, the Virtualization tab is not displayed in the SA Client.
 - **Allow Execute OS Build Plans** - This is the action permission required to provision a server using an OS Build Plan.
 - **Manage Package = Read** - This action allows you to select the boot image ISO in the SA client when performing an OS Build Plan without network boot, or PXE.
- **Virtualization Container Permissions:** These permissions depend on how your virtualization hierarchy is organized.
 - **Inventory Folder: Write** - This gives you write access to the virtualization inventory folder where the new VM will be stored.
 - **Hypervisor: Write** - This gives you write access to the hypervisor where the new VM will run.
 - **Resource Pool: Write** - This gives you write access to the resource pool where the new VM will run.
 - **Datacenter: Read** - This gives you write access on the datastores underlying that datacenter.
- **Server Resource Permissions:** Server resource permissions allow you to modify a limited set of specific VMs. For example, you may modify VMs assigned to Customer1, but not VMs assigned to Customer2.
 - **Facility: Write** - This gives you write access to the facility where managed servers are located.
 - **Customer: Write** - This gives you write access to the managed servers assigned to the customer. Every managed server is assigned to a customer, and you must grant access permissions to customers.
 - **Device Groups: Write** - This gives you write access to the device groups in which your VMs will be included automatically. For more information on device groups and customers, see the SA User Guide: Server Automation.

- **Folder Permissions:** These permissions give you access to items in the SA Library and depend on where (in which folder) these items are located in the SA Library.
 - OS Build Plan folder: Execute - This gives you permission to use the OS Build Plans in the folder.

Setting Virtualization Container Permissions

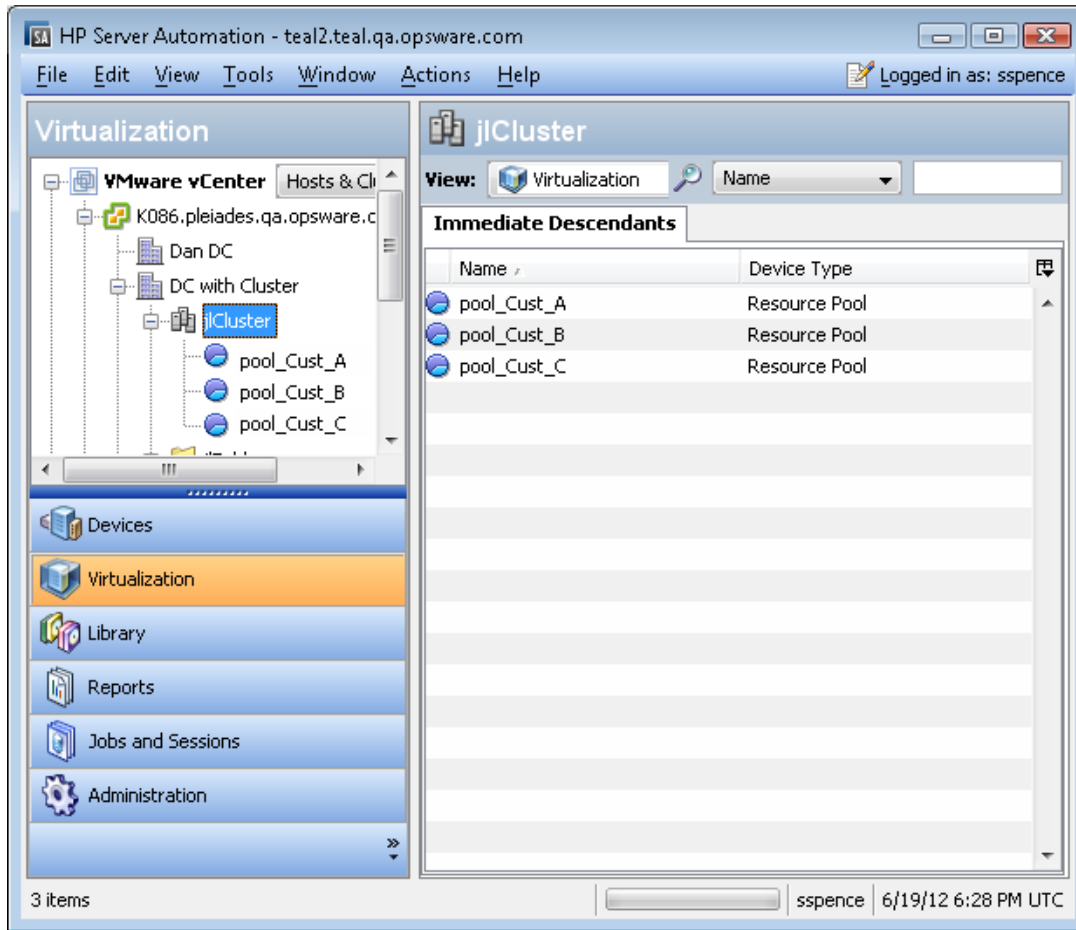
This section describes how to set virtualization container permissions. For information on the other types of permissions (action permissions, server resource permissions, and folder permissions), see the SA Administration Guide.

To perform any virtualization actions, including creating, deleting, modifying, or viewing items in your virtualization inventory, you must have virtualization container permissions, such as a datacenter, host, resource pool, and host cluster, on the container of the virtual resources.

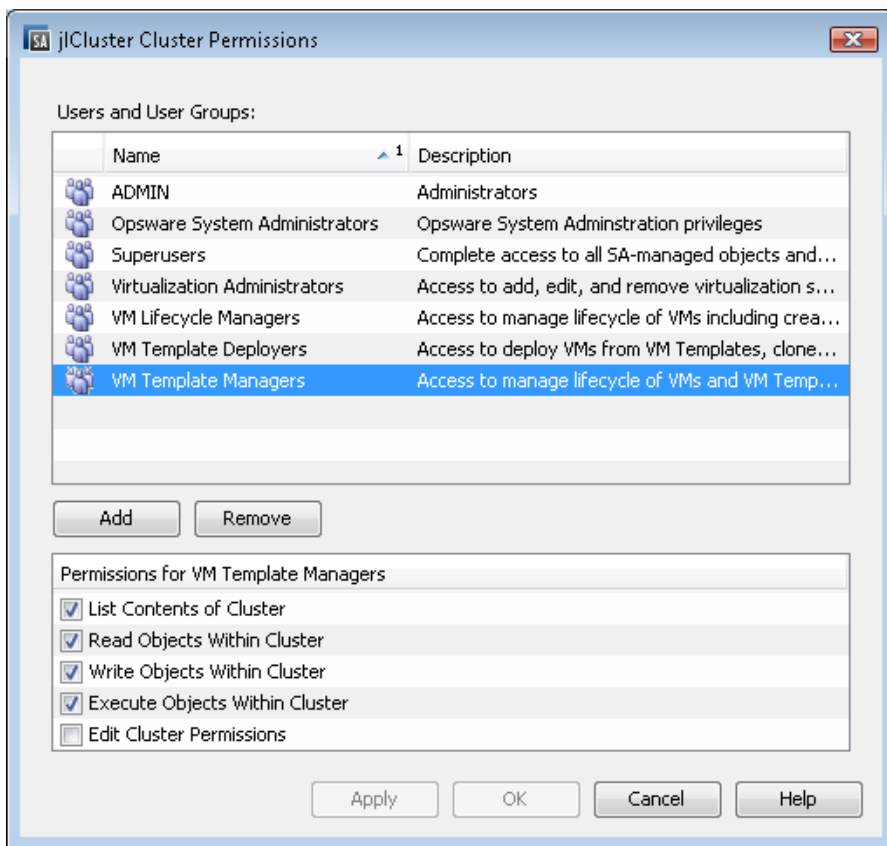
- All folders that reside above the targeted hypervisor and the inventory folder must have List permission.
- VMs and VM templates inherit permissions from their parent container.
 - In vCenter, you must have at least Read permission on a folder to view and manage the VMs and VM templates on that folder.
 - In SCVMM, you must have at least Read permission on a hypervisor to view and manage the VMs hosted by that hypervisor. To view all templates in SCVMM, you need at least Read rights on the “All VM Templates” folder.
 - In OpenStack, you must have at least Read permission on a project to view the VMs in that project.

To set access permissions on virtual resources:

1. In the SA Client, locate the virtual resource where you want to set permissions. For example, the following figure shows two datacenters, a cluster within a datacenter, and three resource pools within the cluster on the VS:



2. Select the virtual resource where you want to set permissions, then right-click and select **Permissions**. This displays the permissions window for that resource. The following figure shows the virtualization container permissions window for the cluster named j1Cluster.



3. Select the user or user group on which you want to set permissions. Use the Add and Remove buttons to add or remove user groups and users.

Grant permissions only to user groups, not to individual users. Granting permissions through user groups is recommended, because it is more manageable and maintainable than granting permissions to individual users. For more information on user groups, see the SA Administration Guide.

4. Select the check boxes to grant the desired permissions.
5. Select Apply or OK to save the permissions.
6. If the virtualization container is itself contained within other ancestor virtualization containers, you may be asked to grant List permissions on the ancestor containers.
If the virtualization container contains other children containers, you may be asked to grant the same permissions to the children containers.

If asked, select whether or not to propagate the permissions to the ancestor containers or the children containers.

7. Select Apply or OK to save the permissions.

Chapter 3: The SA Client Virtualization Tab

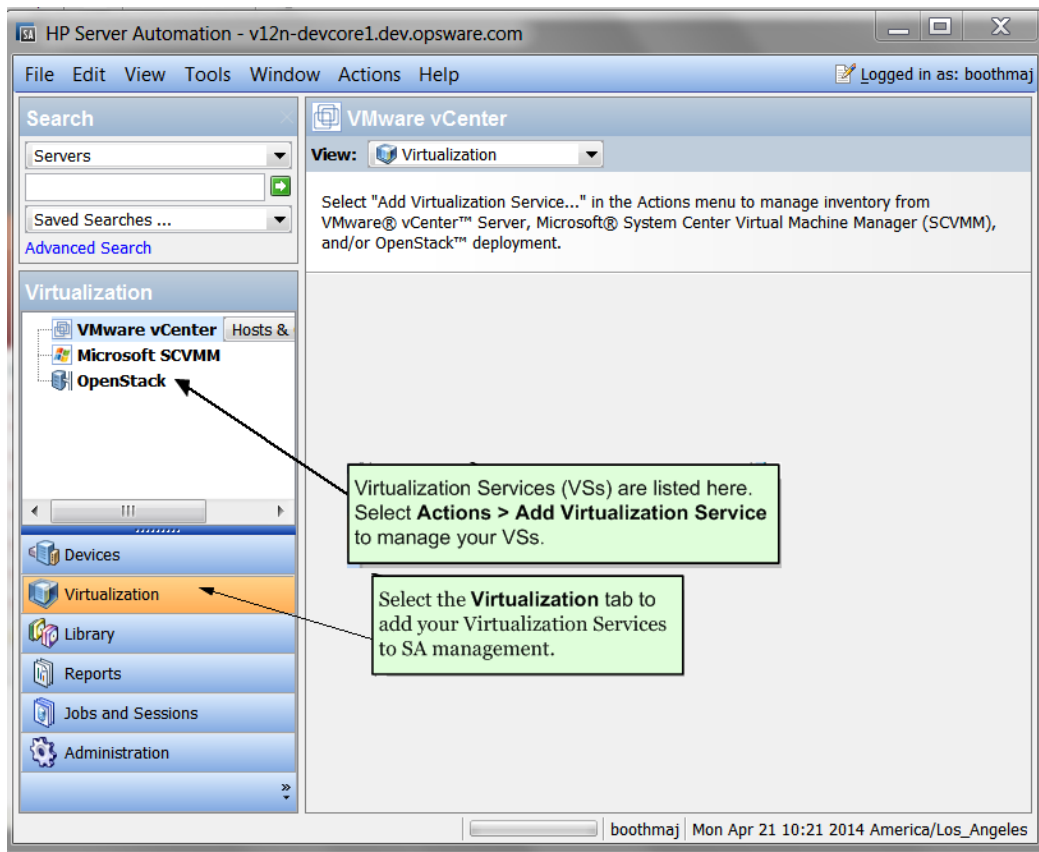
The SA Client allows you to manage your virtualization services (VSs) and create and manage VM templates and VMs. This section introduces you to the SA Client **Virtualization tab** and the **Devices tab** used to manage your VMs.

Virtualization Services

HP SA supports integration with VMware vCenter Server and Microsoft SCVMM. These virtualization vendors manage multiple hypervisors and VMs in a virtualization environment. SA also supports limited integration with on-premise OpenStack cloud deployments, which offer IaaS. We refer to this group of virtualization vendors and cloud computing solutions collectively as Virtualization Services.

Virtualization Tab

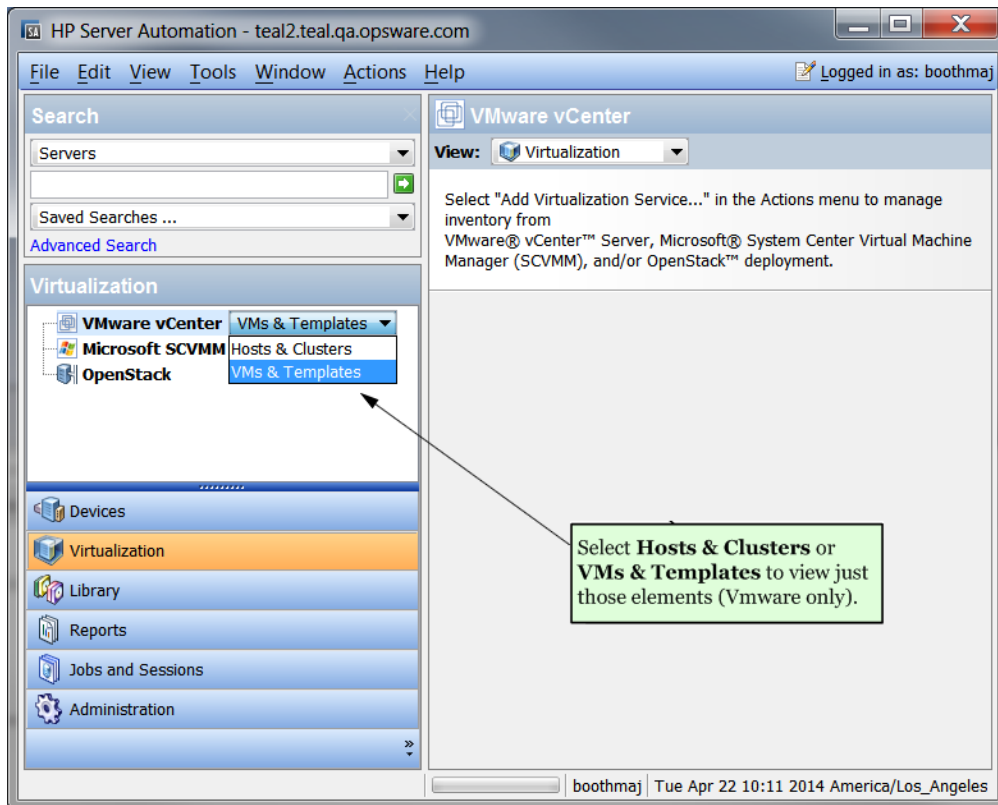
To start managing your VSs, select the Virtualization tab in the SA Client (see the following figure). This displays your virtualization inventory, including VMware vCenter, Microsoft SCVMM, and OpenStack servers.



To bring your VSs under SA management, select the **Actions** menu or right-click on VMware vCenter, Microsoft SCVMM, or OpenStack, and select **Add Virtualization Service**. For details, see ["Add Virtualization Service" on page 28](#).

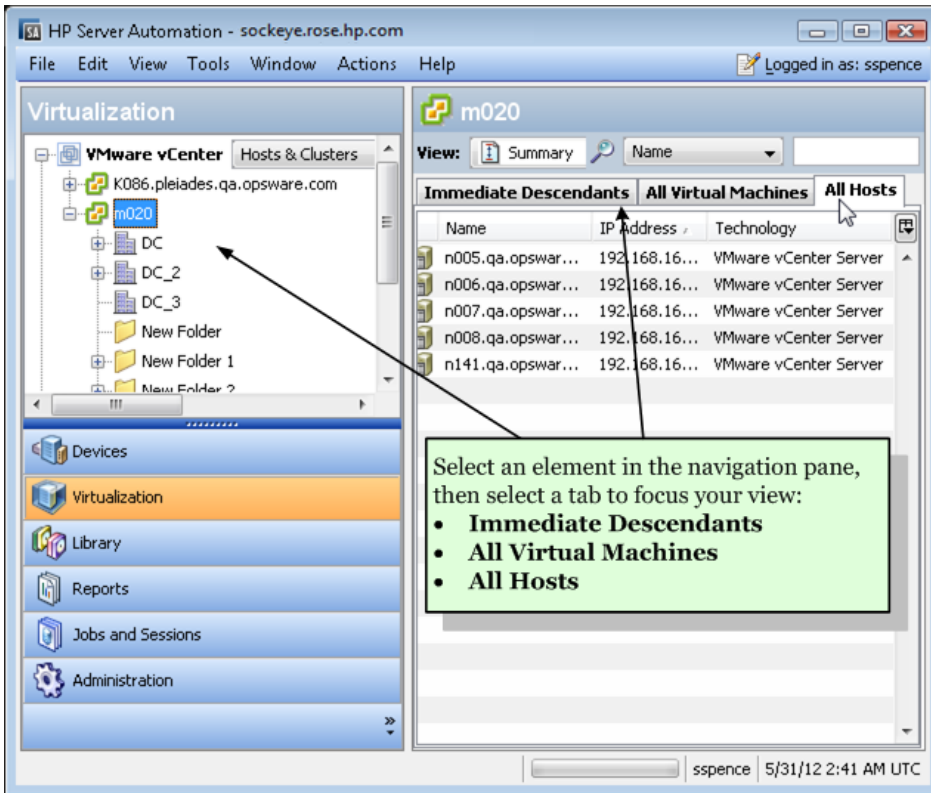
After adding the VS to SA, the SA Client displays the virtualization inventory under the VSs in the navigation pane. Locate the desired host, folder, or other element in the virtualization hierarchy.

Select the **Hosts & Clusters** view or the **VMs & Templates** view to focus your view on just those elements of your VMware vCenter Server (as shown in the following figure).

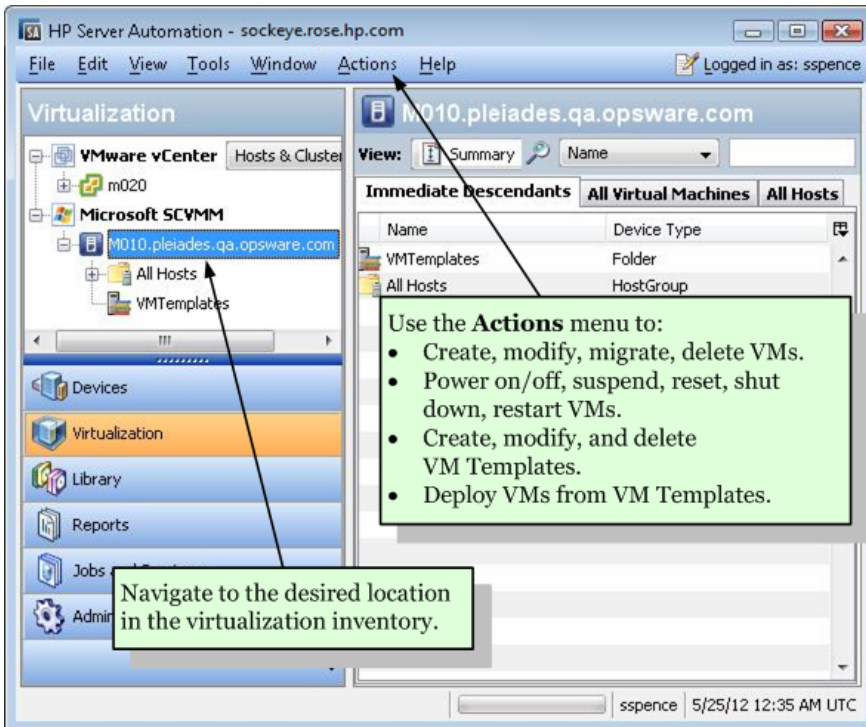


Select an item in the virtualization inventory, then select one of the following tabs:

- **Immediate Descendants** - Shows only items immediately under the selected item. Does not show the contents of any folders below the selected item.
- **All Virtual Machines** - Shows all VMs under the selected item, no matter how far down in the folder hierarchy (not applicable for OpenStack).
- **All Hosts** - Shows all hypervisors under the selected item, no matter how far down in the folder hierarchy (not applicable for OpenStack).



Right-click or use the **Actions** menu to perform a variety of operations on any item in the Virtualization inventory. For details, see "[Virtual Machine and VM Template Tasks](#)" on page 34.



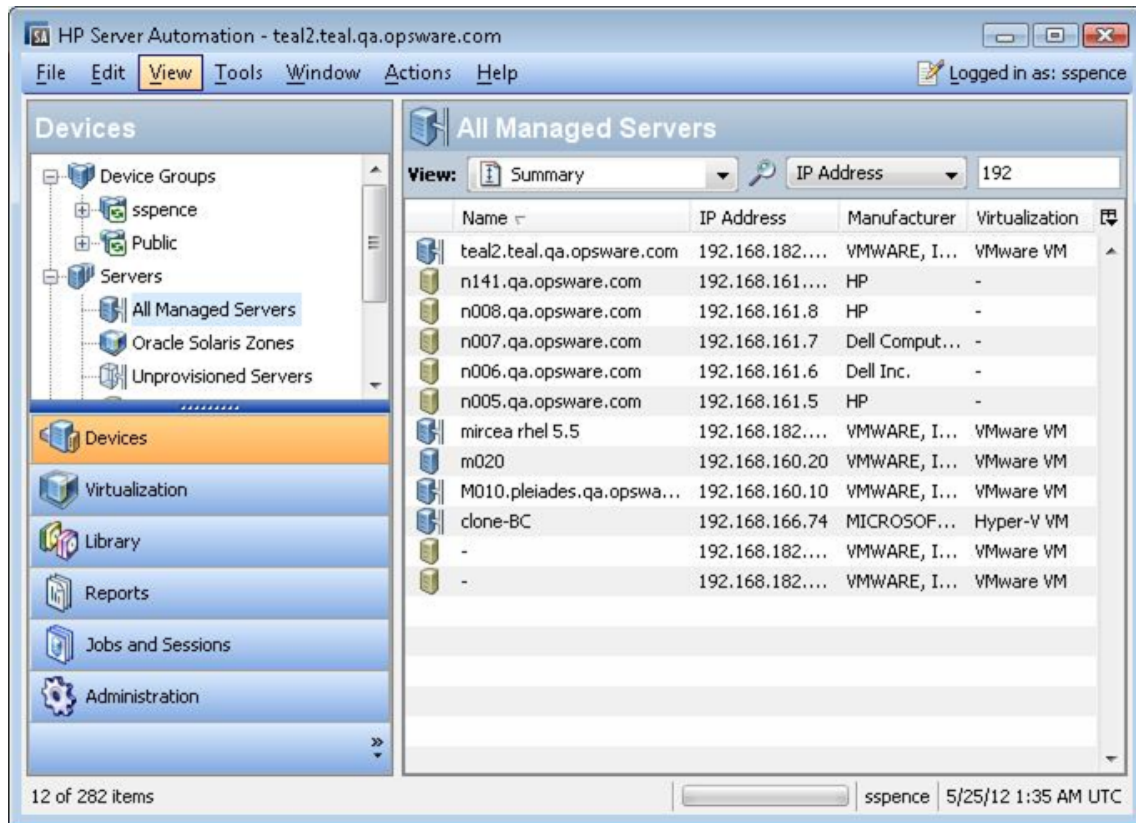
Icons for Virtualization Items

The following table shows the various icons for your virtualization inventory.

Icon	Description
	Hypervisor running the SA Agent and communicating with the SA core
	Hypervisor running the SA Agent and not communicating with the SA core
	Agentless hypervisor
	VM template, including the SA Agent
	Agentless VM template, not including the SA Agent
	VM running the SA Agent and communicating with the SA core
	VM running the SA Agent, not communicating with the SA core
	Agentless VM not running the SA Agent, not communicating with the SA core
	VMware Virtualization Service
	VMware datacenter
	VMware folder containing VMs and VM templates
	VMware folder containing hosts and clusters
	VMware cluster
	Microsoft host group
	Microsoft Virtualization Service
	Microsoft cluster
	Microsoft All VM Templates folder
	OpenStack Virtualization Service. Controller node running the SA Agent and communicating with the SA core.
	OpenStack project

Devices Tab

Select the **Devices** tab in the SA Client to manage your VMs, just as you would do for physical servers.



With SA you can provision, patch, install software, configure, audit, and generate reports for all your virtual and physical servers. For details, see the following guides:

- SA User Guide: Provisioning
- SA User Guide: Server Patching
- SA User Guide: Software Management
- SA User Guide: Application Configuration
- SA User Guide: Audit and Compliance
- SA Reports Guide
- SA User Guide: Server Automation

Managing Oracle Solaris Zones

You can manage Oracle Solaris Zones with SA:

1. In the SA Client, select the Devices tab.
2. Select **Servers > Oracle Solaris Zones**. This displays your Oracle Solaris Zones.

For more information, see "[Managing Oracle Solaris Zones](#)" on page 109.

Managing HP-UX Virtual Servers

For information on managing HP-UX virtual servers, see "[Managing HP-UX Virtual Servers](#)" on page 76.

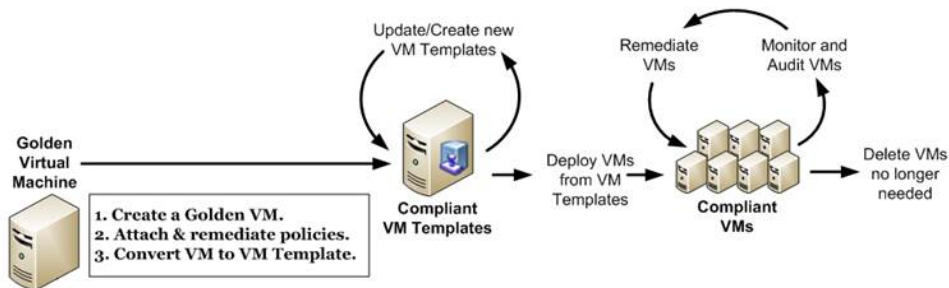
Chapter 4: Virtual Machine and VM Template Life Cycle

The information in this chapter does not apply to an OpenStack environment in HP SA Release 10.1.

By setting up a well-defined process of deploying, managing and deleting VMs and VM templates, you can control VM sprawl and VM compliance drift. This section describes and recommends processes for creating, managing, and deleting VMs and VM templates.

This section assumes you have added your Virtualization Service (VS) into SA and are managing your VS from SA, typically the SA Client. For more information, see ["Add Virtualization Service" on page 28](#).

The following figure summarizes the VM template and VM life cycle.



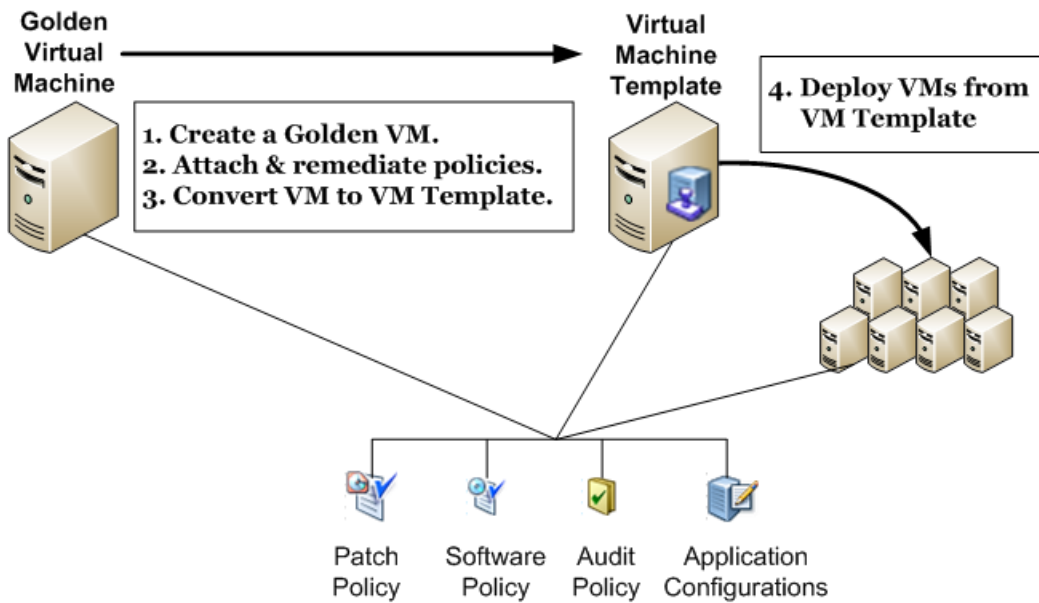
The following sections describe each part of the VM life cycle.

Create VM Templates

This section explains how to create VM templates. VM templates ensure your users deploy standard VMs that you can monitor, keep in compliance, and destroy efficiently so they do not waste your IT resources.

Create a limited number of VM templates. The fewer different templates you have to manage, the easier it will be to manage them and the VMs your users deploy from them.

The following figure summarizes the process of creating a VM template.



1. Determine the basic types of VMs your users will be deploying.
Each type of VM consists of the operating system, software applications, software and system configurations, patches to be installed, and audit rules that must be followed for compliance.

For example, you might have the following four basic types of VMs:

- Windows machine for administrative and managerial users.
- Windows machine for financial users.
- Linux machine for software developers and testers.
- Linux machine for production systems.

You could create two VM templates, one for the Windows servers and one for the Linux servers, and customize the VMs after deploying them from the templates. Or you could create four separate VM templates. Either method can work, but each has different trade-offs, benefits, and drawbacks. The following table lists some of the benefits and drawbacks of each strategy:

Comparing Two and Four VM Templates

	Benefits	Drawbacks
2 VM Templates - One for all Windows servers and one for all Linux servers	Fewer VM templates to maintain.	You must customize each VM for the intended user (administrative user or financial user for Windows, developer or production user for Linux) after deploying it.
4 VM Templates - Two for Windows servers and two for Linux Servers	No customization of VMs required after deploying them.	More VM templates to maintain.

2. For each type of VM your users will be deploying, create that VM as a “golden,” or baseline, VM:
 - a. Create the VM. The simplest way to do this is to clone an existing VM that represents the VM or is close to the VM, or deploy a VM from a VM template that is close to the desired VM.
 - b. Unless already done, install the operating system using an OS Build Plan. See the SA User Guide: Provisioning.
 - c. Create a patch policy for the VM that includes all the patches required by the VM. Attach the patch policy to the VM. See the SA User Guide: Server Patching.
 - d. Create a software policy for the software required for the VM. Attach the software policy to the VM. See the SA User Guide: Software Management.
 - e. Create application configurations for the VM. Attach the application configurations to the VM. See the SA User Guide: Application Configuration.
 - f. Create an audit policy for the VM. Attach the audit policy to the VM. See the SA User Guide: Audit and Compliance.
 - g. Remediate the VM to incorporate all policies into the golden VM.

3. From each golden VM, convert the VM to a VM template. For more information, see ["Convert a VM to a VM Template - vCenter" on page 71](#).
 When you convert a VM to a VM template, the VM no longer exists. If you want to keep the VM, clone the VM first, then convert the VM to a VM template. Or deploy a VM from the VM template immediately after creating the VM template.

4. Instruct your users to deploy VMs from your VM templates. These VMs will conform to your standard policies and be maintained by your standard processes for managed servers.

Deploy VMs from VM Templates

Ensure your users use your VM templates whenever they deploy VMs so they create standard VMs that you can manage. For instructions on deploying VMs from VM templates, see ["Deploy a VM from a VM Template - vCenter"](#) on page 44.

Keep VMs in Compliance

To keep your VMs in compliance, perform regular compliance checks and audits to determine which VMs are out of compliance with the attached policies. Remediate noncompliant VMs to bring them back into compliance.

This is the same process you use for keeping physical servers in compliance. For more information, see the SA User Guide: Server Patching, the SA User Guide: Software Management, and the SA User Guide: Audit and Compliance. For details about performing actions on a group of related VMs and VM templates, see ["Genealogy of VMs"](#) on page 117.

VM Template Life Cycle

This section explains how to update and maintain your VM templates while maintaining the connection between the VM template and the VMs deployed from them. It is important to update them methodically to keep your VMs in compliance efficiently.

Here are three ways to keep templates up to date:

- Modify the contents of the policies attached to the VM template (see ["Modify Attached Policies"](#) on the next page).
- Modify the contents of the policies attached to the VM template and create a new VM template (see ["Modify Attached Policies and Create a New VM Template"](#) on page 22).
- Attach one or more new policies to the VM template and to all VMs previously deployed from the VM template and create a new VM template (see ["Attach New Policies and Create a New VM Template"](#) on page 23).

Update your VM templates at regular intervals. For example, you might modify the attached policies weekly and create new VM templates monthly.

Modify Attached Policies

You can update your VM templates by modifying the contents of the policies attached to the VM template. This is the simplest method of updating VM templates.

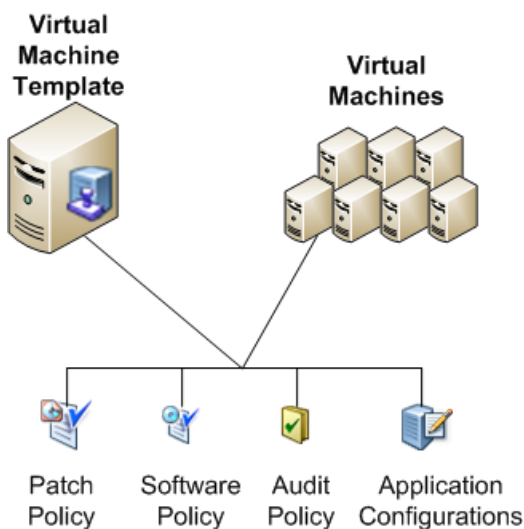
1. Modify the policies attached to your VMs and the VM template from which they were created.
2. Remediate the existing VMs previously created from the VM template. This brings them into compliance with the updated policies.
All VMs previously deployed from the VM template immediately become noncompliant and require remediation to be brought back into compliance.

For details about performing actions on a group of related VMs and VM templates, see ["Genealogy of VMs" on page 117](#).

3. Deploy new VMs from the updated VM template.
4. Scan and remediate the new VMs to bring them into compliance with the updated policies.
All new VMs deployed from the updated VM template immediately require a compliance scan and remediation, because the baseline VM template does not contain the new additions to the policies.

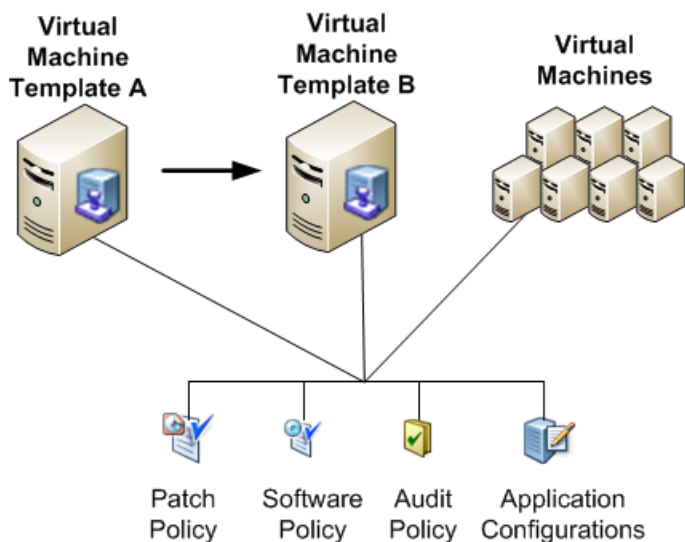
For details about performing actions on a group of related VMs and VM templates, see ["Genealogy of VMs" on page 117](#).

The following figure shows the VM template, the VMs created from it, and the attached policies.



Modify Attached Policies and Create a New VM Template

The following figure shows the old VM template (VM Template A), the new VM template (VM Template B), and the policies attached to both VM templates and to all the VMs deployed from them.



After updating the policies attached to your VM templates, you can create a new VM template from the old VM template with the same set of policies:

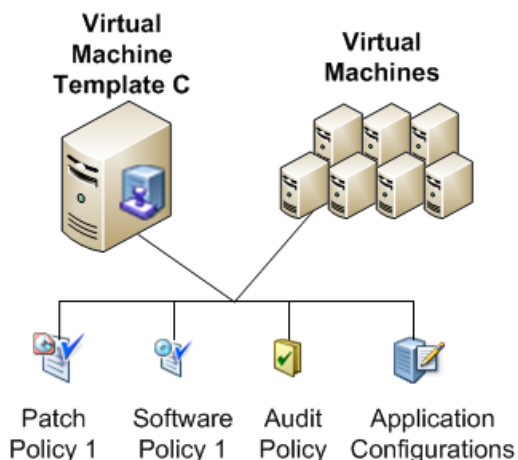
1. Deploy a VM from the VM template (VM Template A in the previous figure).
2. Remediate the VM.
3. Convert the VM to a new VM template (VM Template B in the previous figure). This incorporates the contents of all the policies into the baseline VM template (B).
4. Remediate all VMs previously deployed from the original VM template (A) to ensure they are in compliance.
After creating the new VM template (B), all VMs previously deployed from the VM template (A) immediately become noncompliant and require remediation to be brought into compliance.
5. Deploy new VMs from the new VM template (B).
All new VMs deployed from the new VM template (B) are compliant and do not need remediation. However, they do require a compliance scan.

For details about performing actions on a group of related VMs and VM templates, see ["Genealogy of VMs" on page 117](#).

Attach New Policies and Create a New VM Template

This section describes how you can add new policies and create a new VM template, and maintain compliance of all VMs previously created from the original VM template. The following figure shows this scenario before adding new policies.

VM Template C, Before Adding New Policies

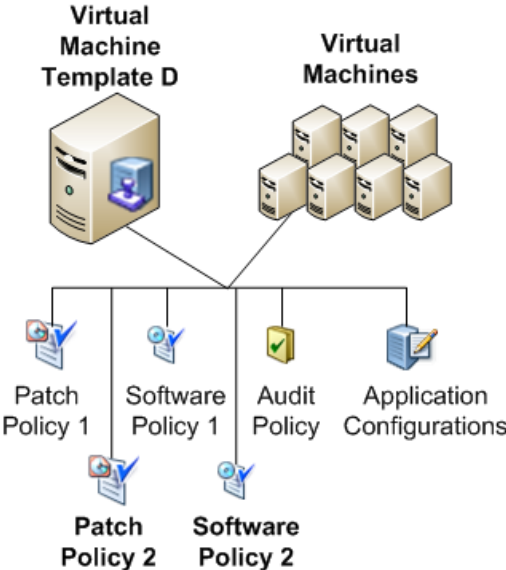


1. Deploy a VM from the VM template (VM Template C in the previous figure).
2. Attach new policies to the VM.
3. Remediate the VM to incorporate the new policies into the baseline VM.
4. Convert the VM to a new VM template (VM Template D in the previous figure).
5. Search for all VMs created from the original VM template (C).
All VMs previously deployed from the original VM template (C) will not have the new policies attached. You can search for all those VMs that were deployed from the original VM template (C), attach the new policies to those VMs, then remediate them to bring them into compliance with the new set of policies and the new VM template (D).
6. Attach the new policies to all the VMs deployed from VM templates (C).
7. Remediate all those VMs to bring them into compliance.
8. Instruct your users to use the new VM template (D) to create VMs. All VMs deployed from the new VM template are compliant and do not need remediation. However, they do require a compliance scan. This process is made easier by performing the Genealogy action for the original VM template, because all VMs previously deployed from the template are grouped together. For

details about performing actions on a group of related VMs and VM templates, see ["Genealogy of VMs" on page 117](#).

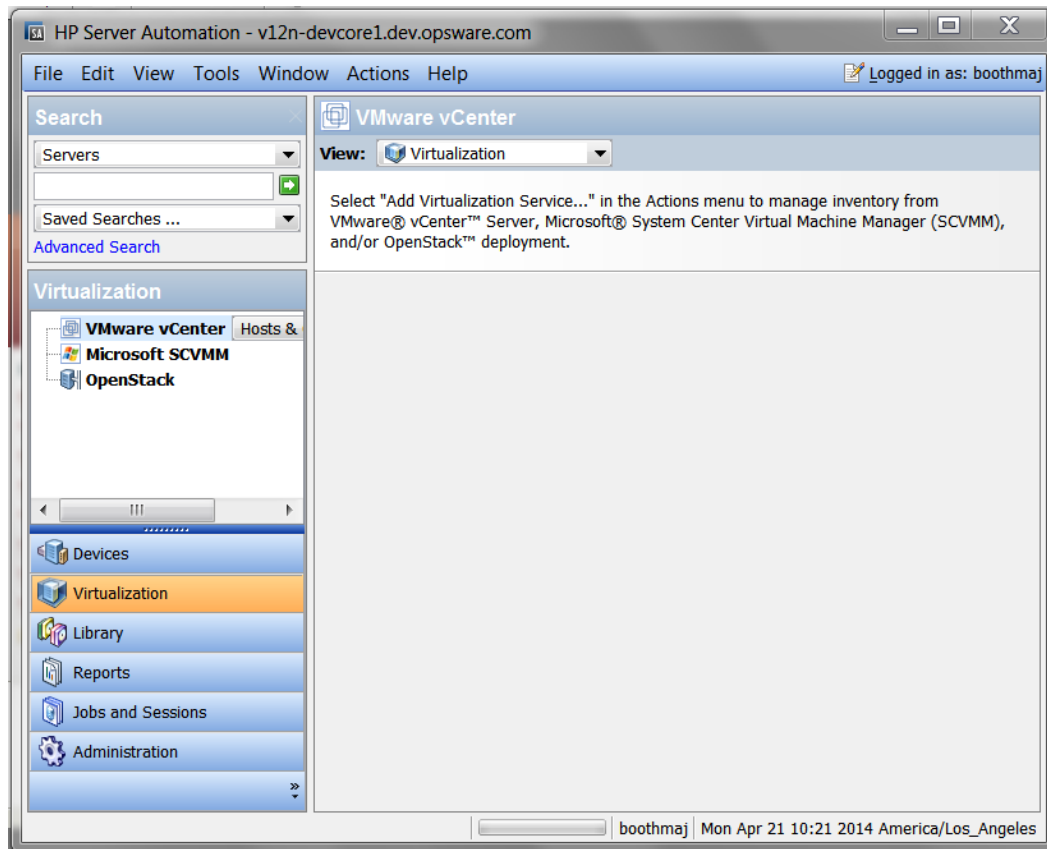
The following figure shows this scenario after all steps have been completed.

VM Template D, After Attaching Two New Policies



Chapter 5: Virtualization Service Tasks

This section describes how to add VMware vCenter, Microsoft SCVMM, or OpenStack as a Virtualization Service (VS). When you have added a VS, you can perform further tasks as shown in the Virtualization tab in the SA Client (see the following figure).

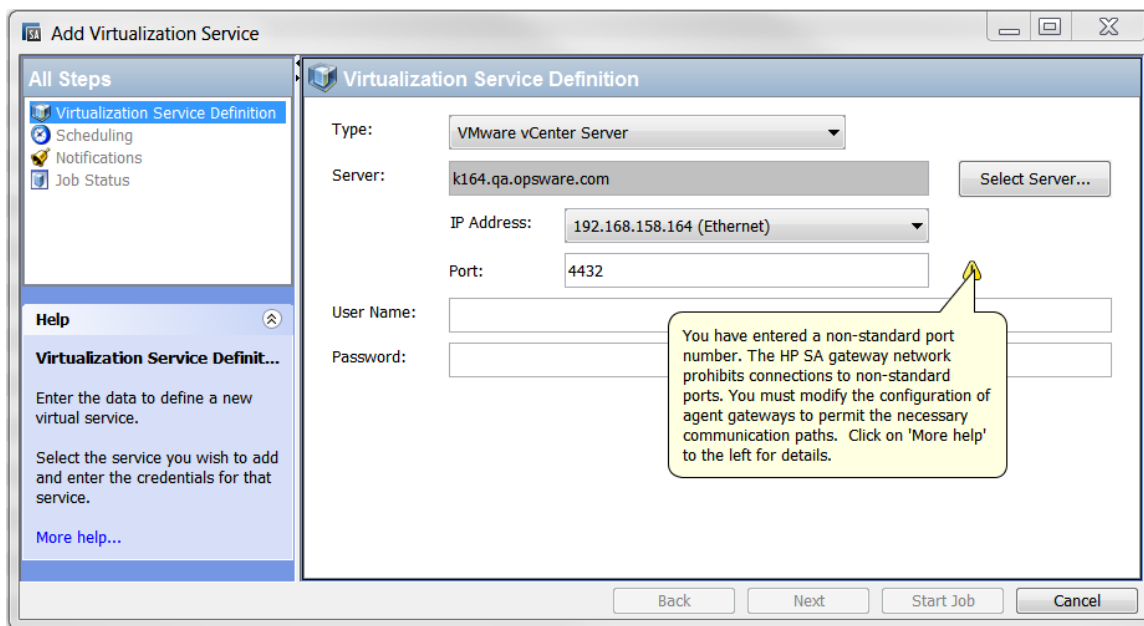


Prerequisites

- Any server running a VS managed by SA must be an agent-managed server. That is, it must have an SA Agent installed on it. Do not remove the SA Agent from servers running VSs managed by SA. The simplest way to ensure the server is a managed server running the SA Agent is to check the icon next to the server. A blue server icon indicates it is agent-managed (see ["Icons for Virtualization Items"](#) on page 14).

Alternatively, you can examine the server summary or the server properties in the SA Client. Select the Devices tab and locate the server under All Managed Servers. Select the server, then select the Summary View or the Properties View. Examine the agent status or the agent version. If this information does not appear, it is not an agent-managed server. For information about installing the SA Agent, see the SA User Guide: Server Automation.

- Ensure that a software registration has been performed on the server. For more information on running a software registration, see the SA User Guide: Server Automation.
- When adding a VS, specify a user with full permissions and privileges to the VS.
 - Any action done on the VS from SA is logged in the VS history as this user.
 - Enter the user with full permissions, and then apply SA user permissions within SA.
 - To ensure full discovery in OpenStack, the user must be a member of each Project to be discovered and managed in SA. We recommend that the user also has the Admin role for each project.
- When you add a VS with a non-default port, you must first configure agent gateways to allow communication with the port.
 - In vCenter, the Add VS wizard provides you with 443 as the default standard port. If you edit this field, the following window appears:



- To allow tunneling in OpenStack, SA Agent gateway communication must be configured as shown in the following table:

Port	Used to Communicate With
5000 - Or a custom port for your deployment	OpenStack controller node
8774 - Or a custom port for your deployment	OpenStack Nova service
8776 - Or a custom port for your deployment	OpenStack Cinder service

Use the following steps to configure your agent gateway in OpenStack. In this example, OpenStack is configured to listen on the default ports, and the agent gateway name is `example_gateway1`

- a. Identify the gateway host by opening the `/etc/opt/opsware/agent/opswgw.args` file from the OpenStack server.
- b. On the gateway host, open the `/etc/opt/opsware/example_gateway1/opswgw.custom` file.
- c. Add the following new lines:


```
opswgw.EgressFilter=tcp*:5000:*:*
opswgw.EgressFilter=tcp*:8774:*:*
opswgw.EgressFilter=tcp*:8776:*:*
```
- d. Save and close the file.
- e. Restart the agent gateway component on the gateway host from "[Identify the gateway host by opening the /etc/opt/opsware/agent/opswgw.args file from the OpenStack server.](#)" above by running the following command:

```
/etc/init.d/opsware-sas restart opswgw-agws
```

If you upgrade to Release 10.2 and enable IPv6 on a vCenter or OpenStack server, change the ":" to "@" on each line shown in step c and restart the agent gateway on each slice in each facility where IPv6 is enabled. For example:

For OpenStack:

```
opswgw.EgressFilter=tcp@@5000@@*@@*
```

For vCenter:

```
opswgw.EgressFilter=tcp@@8776@@*@@*
```

```
opswgw.EgressFilter=tcp@@8774@@*@@*
```

For more information on configuring the agent gateway, see the SA Installation Guide. For more information about OpenStack configuration, go to:

<http://www.openstack.org/>

Virtualization Security

For information regarding Virtualization Security prerequisites and tasks, see "[Virtualization Security](#)" on page 133.

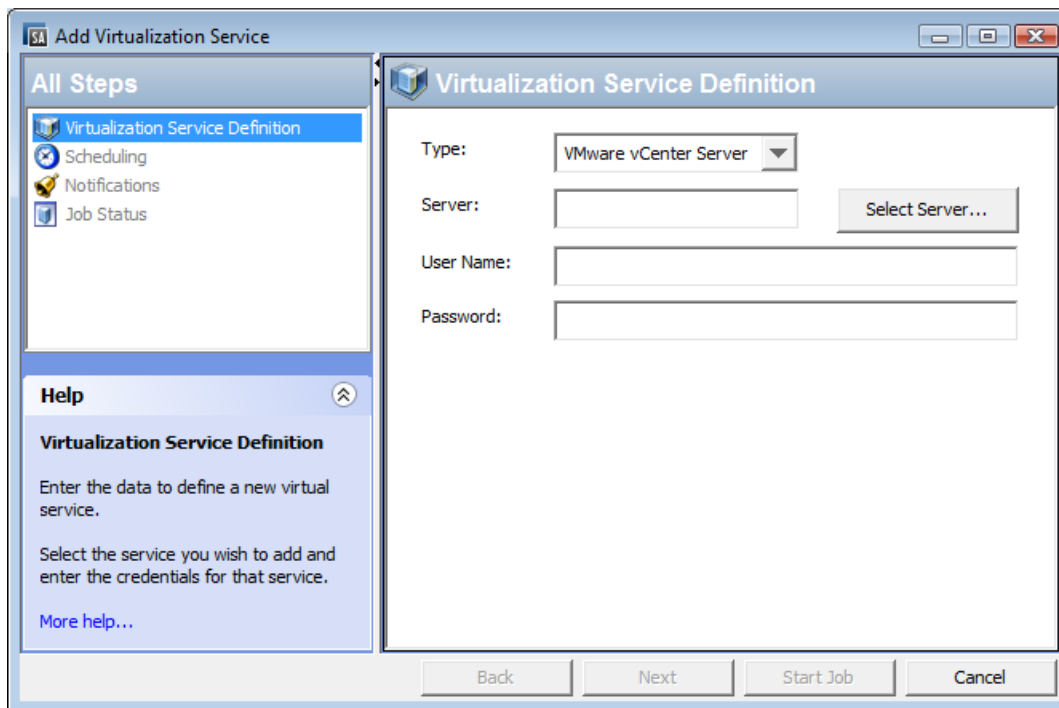
Supported Tasks

You can perform the following tasks with SA. Any tasks not listed must be performed with the native tools.

Add Virtualization Service

To make a VS visible to and managed by SA, you need to add it to SA.

1. In the SA Client, select the Virtualization tab. This displays all your registered VSs and the virtualization inventory under them.
2. In the navigation pane, select either **VMware vCenter**, **Microsoft SCVMM**, or **OpenStack**.
3. Right-click or select the **Actions** menu, and select **Add Virtualization Service**. This displays the Add Virtualization Service window (see the following figure).



4. **Virtualization Service Definition:** Enter the following information, then select Next. Or select Start Job to accept the remaining defaults and run the job.
 - Confirm that the type of VS you want to register appears in the Type field.
 - Click the Select Server button. This displays your available agent-managed servers running a VS of the selected Type; for example, if you select OpenStack Type, only OpenStack servers are displayed.
 - Select the server to be added as a VS, then click the Select button.
 - If the server has more than one IP address, select the IP address to use from the drop-down list.
 - Enter the port number to use to communicate with the VS (see ["Prerequisites" on page 25](#)).
 - Specify the *username* and password to the VS. If the user resides in a domain, provide the domain credentials, as shown:
domain1\username1
5. **Scheduling:** Enter when you want the VS to be added—immediately or in the future— then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.

7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.

When the job runs, it adds the VS to SA management and displays the results. Once the VS is under SA management, you will see the virtualization inventory of the VS in the SA Client.

If you change the IP address, port, or administrator password for a VS, the virtualization administrator must run Edit VS to update that VS's connection information.

Once the VS is under SA management, it is highly recommended that you make all its VMs agent-managed servers to have maximum visibility, control, and compliance for these VMs. For information about installing the SA Agent, see "[Install the SA Agent on a VM](#)" on page 58 the SA User Guide: Server Automation, and the SA Standard/Advanced Installation Guide.

Reload Virtualization Service Data

This section explains how to update SA information about the VS. Do this whenever something has changed outside of SA; for example, in the native VMware, Microsoft, or OpenStack tools.

If you modify elements of your virtualization inventory outside of SA, refresh the VS data in SA to ensure SA has complete and up-to-date information. Otherwise, the information in SA about your virtualization inventory may be inaccurate.

Schedule a recurring job that runs during non-peak hours and reloads the VS data in SA. This task synchronizes your data with any changes that occur outside of SA, such as distributed resource scheduler (DRS) migrations from VMware. The frequency you choose depends on how large your virtual inventory is and how much it changes outside of SA. The larger your virtual inventory, the longer the reload operation may take. One common frequency to use is every 24 hours.

To reload the VS data:

1. In the SA Client, select the Virtualization tab. This displays all your registered VSs.
2. Select a VS.
3. Right-click or select the **Actions** menu and select **Reload Data Now** or **Reload Data Scheduled**. This displays the Reload Data window.
If you selected Reload Data Now, the job begins and displays the status window.
4. **Preview:** If you selected Reload Data Scheduled, select Next. Or select Start Job to accept the remaining defaults and run the job.

5. **Scheduling:** Enter when you want the VS data to be reloaded, then select Next.
You can reload VS data immediately, once in the future, or set a recurring schedule.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it reloads all the data about the VS.

Reload Virtualization Items Data

You can reload virtualization service data on demand for all virtualization items (for example, VMs, templates, resource pools, and so on). However, you cannot perform a scheduled reload on any virtualization item other than the VS.

Edit Virtualization Service

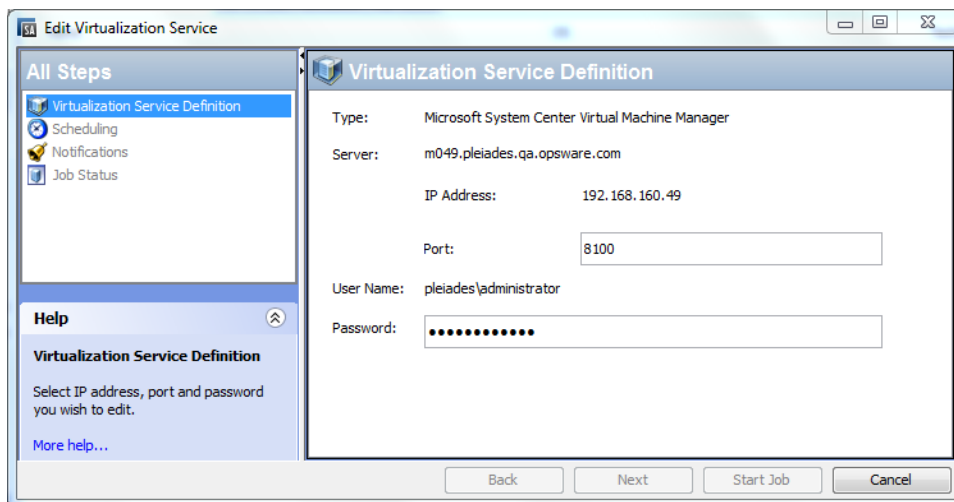
In vCenter and OpenStack, Edit VS lets you update the IP address (when the server has multiple IP addresses), port number, and administrator password for the VS. If you change the port number for vCenter or OpenStack, be sure to configure the port in the agent gateway (see ["Prerequisites" on page 25](#)).

In SCVMM, you can edit the port number and password for the VS. The IP address is the SA management IP used to connect to SCVMM.

If the IP address for a VS is changed, the virtualization administrator must run Edit VS to update that VS's IP connection information.

To edit the VS:

1. In the SA Client, select the Virtualization tab. This displays all your registered VSs.
2. Select a VS.
3. Right-click or select the **Actions** menu and select **Edit Virtualization Service**. This displays the Virtualization Service Definition window.
4. **Virtualization Service Definition:** Modify the IP address or the port number used to communicate with the VS, or the password of the VS user, then select Next. Or you can select Start Job to accept the remaining defaults and run the job (see the following figure).



5. **Scheduling:** Select when you want the job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it modifies the VS and displays the results.

Remove Virtualization Service from SA

SA does not permit you to remove a VS if there are any other jobs running against it.

When you no longer need to manage a VS from SA Management, you can remove it using the following process. This process removes all the VMs and hypervisors from SA management that are only managed by the VS. That is, any VMs and hypervisors managed by the VS that are also agent-managed will still be managed by SA.

1. In the SA Client, select the Virtualization tab. This displays all your registered VSs.
2. Select a VS.
3. Right-click or select the **Actions** menu and select **Remove Virtualization Service**. This displays the Remove Virtualization Service window.
4. **Confirmation:** Confirm that the VS displayed is the one you want to remove, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.

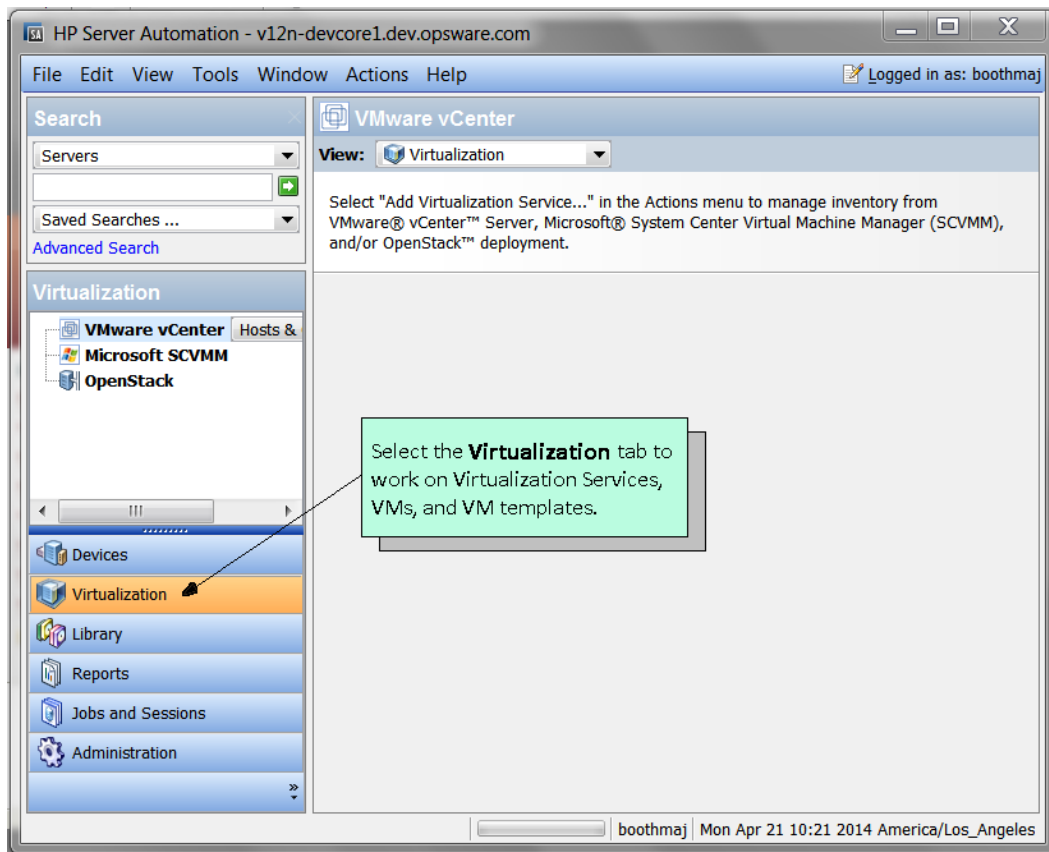
5. **Scheduling:** Select when you want the VS to be removed—immediately or in the future—then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it removes the VS and displays the results.

Once the VS has been removed from SA management, the virtualization inventory of the VS will not be displayed in the SA Client under the Virtualization tab. All hypervisors or virtual machines that are agent-managed or iLO-managed will still be displayed under the Devices tab.

Chapter 6: Virtual Machine and VM Template Tasks

This section describes the tasks you can do with VMs and VM templates using the Virtualization tab in the SA Client, as shown in the following figure.

You can also view and manage VMs using the Devices tab. For more information, see the SA User Guide: Server Automation.



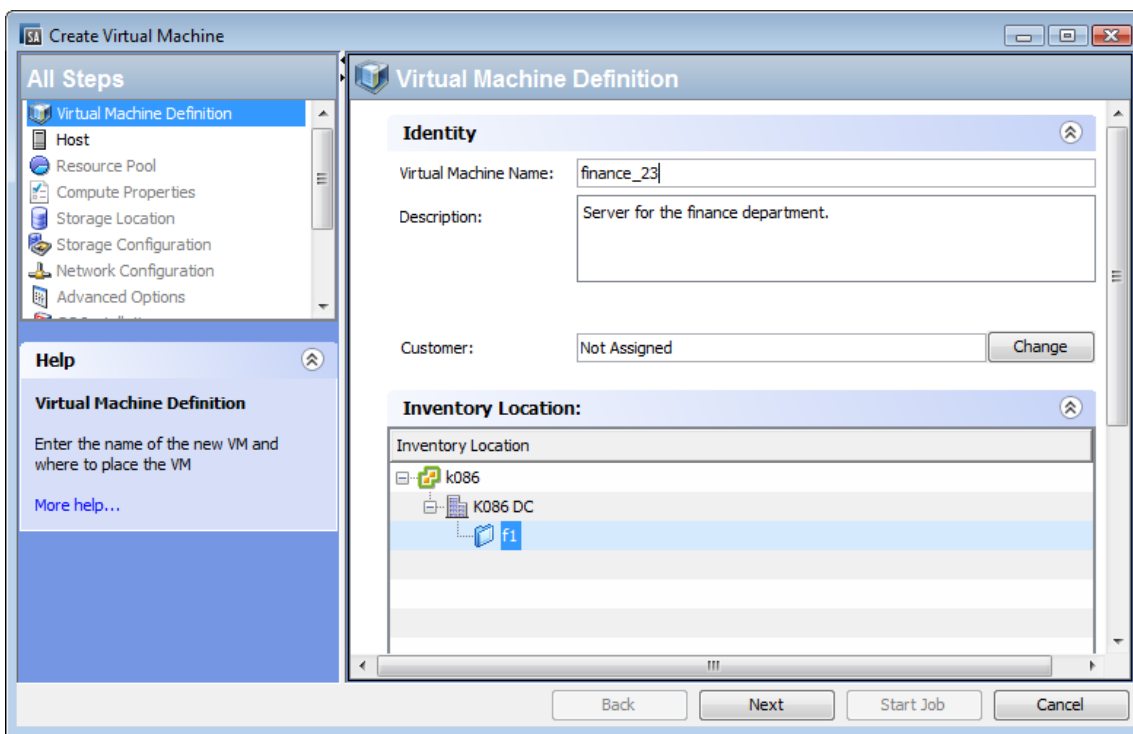
Supported Tasks

You can perform the VM and VM template tasks described in this chapter with SA. Any other VM or VM template tasks not listed here must be performed with the native tools. For more information, see also ["Virtualization Service Tasks" on page 25.](#)

Create and Provision a VM - vCenter

This section describes how to create and provision a VM under a VMware vCenter Server. You can also deploy a VM from a VM template or clone a VM from another VM. See ["Deploy a VM from a VM Template - vCenter"](#) on page 44 and ["Clone a VM - vCenter"](#) on page 54 for more information.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the desired location where you want to place the new VM. VMs must be created under a datacenter. VMs can also be placed under clusters, hypervisors, or resource pools or in folders under these virtualization containers.
3. Select the desired location and right-click or select the **Actions** menu. Select **Create VM...** to display the Virtual Machine Definition window (see the following figure).

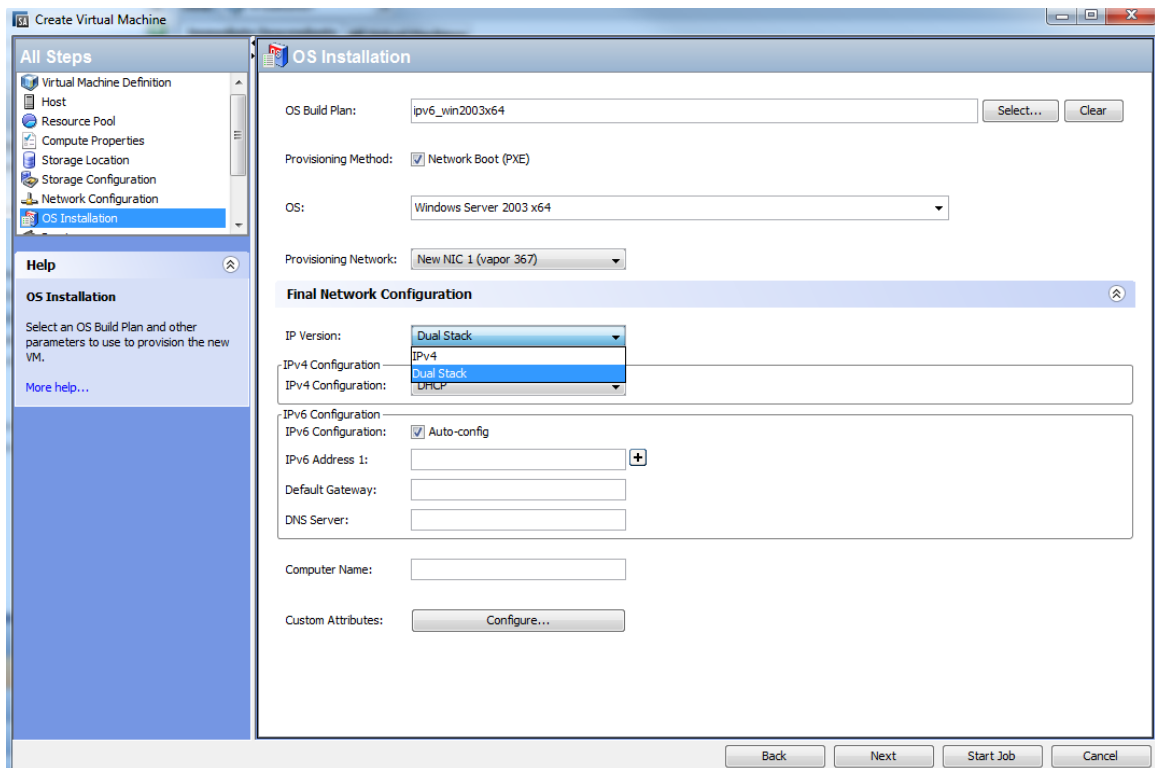


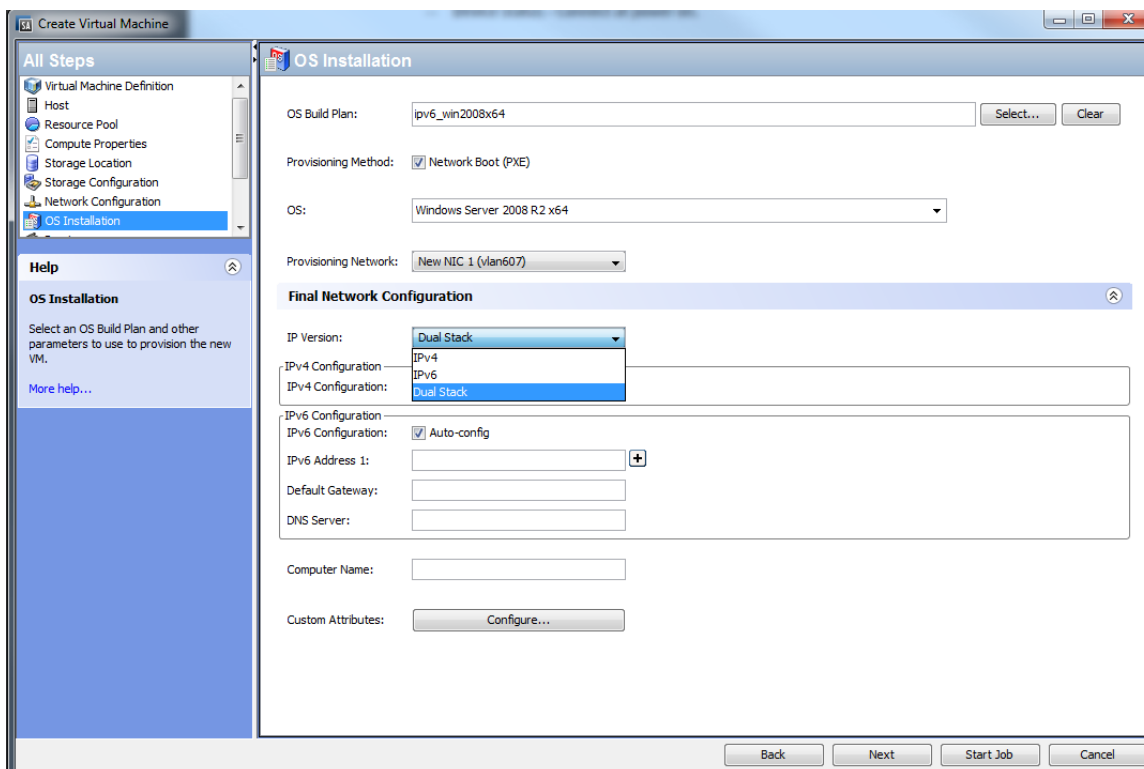
4. **Virtual Machine Definition:** Enter the following information, then select Next.
 - The VM name.
 - A VM description.
 - A customer to assign the VM to. The default is "Not Assigned."

- Verify or change the location in the virtualization inventory where you want to place the new VM.
5. **Host:** Navigate to and select the server that you want to host the VM. Verify that the host is compatible, then select Next.
 6. **Resource Pool:** If the host or cluster has resource pools defined, navigate to and select the resource pool where you want to place the new VM. Select Next.
 7. **Compute Properties:** Enter the following information, then select Next.
 - Enter the amount of memory for the VM.
 - Enter the number of virtual processors for the VM.
 - Select the guest operating system that you will install on the VM.
 8. **Storage Location:** Select the datastore with sufficient free space in which to store the VM configuration file, then select Next.
 9. **Storage Configuration:** Your first virtual hard disk (VHD) is added automatically. Use this window to specify the details for this VHD:
 - Type: Select IDE or SCSI (default) from the drop-down list.
 - Allocated Size: Select the amount of GB (the default is 20).
 - Disk Provisioning Type: Thin (default) or thick.
 - Location: Select Store with the virtual machine (default) or select a datastore from the list. Optionally, you can add and configure more storage devices. The maximum number of IDE devices you can add is 4. Specify the storage details, then select Next.
 10. **Network Configuration:** The first Network Interface Card (NIC) for your new VM is added automatically. Configure the following, then select Next:
 - Network name
 - Adapter type
 - MAC address: Automatic (default) or manual
 - Device status - Connect at power on.

It is recommended that you create the VM with a single network adapter to ensure that the job completes. However, if you must create a VM with multiple adapters, ensure that the NIC on the provisioning network is specified first.

11. **OS Installation:** Specify the following to provision an OS on the VM, then select Next (see the next two figures).





- **OS Build Plan** - Select the OS Build Plan you want to install. For more information on OS Build Plans, see the SA User Guide: Provisioning. To run an OS Build Plan, you must have adequate action permissions and adequate resource permissions on the OS Build Plan. For information on permissions, see the SA Administration Guide.
SA no longer integrates Create VM with OS sequences. Contact your OS Provisioning administrator to create a custom OS Build Plan for your needs.
- **Provisioning Method** - Select the provisioning method to use:
 - **Network boot (PXE)** - Network-based installation.
 - **CD/DVD boot** - Uncheck Network Boot (PXE) to install the OS from virtual media on an attached CD/DVD drive.
- **Operating System** - Use the OS selector to choose the OS that the OS Build Plan will install.
- **Provisioning Network** - Select the NIC to be used for provisioning.
- **Final Network Configuration** - From the drop-down list, select the IP version to be used to configure the VM. Depending on the OS you select, you can use IPv4 only; IPv4 and IPv4/IPv6 dual-stack; or IPv4, IPv6, and IPv4/IPv6 dual-stack.

- For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
- For IPv6:
 - With Autoconfig - Optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.
- For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 with scenarios as described above.

For more information about IPv6, see the SA Administration Guide. For more information about DHCP configuration, see the SA User Guide: Provisioning.

- **Custom Attributes** - Optionally specify custom attributes. For more information on custom attributes, see the SA User Guide: Server Automation.
- **Preview:** Verify all your VM settings. Use the Back button or select any step to make changes, then select Next.
- **Scheduling:** Select when you want the job to run, then select Next.
- **Notifications:** Optionally enter a notifier, then select Next.
- **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.

When the job runs, it creates the VM and displays the results. Once the VM is created, you will see it in the virtualization inventory of the VS in the SA Client and in the Devices All Managed Servers view.

It is highly recommended that you make all VMs agent-managed servers to have maximum visibility, control, and compliance for these VMs. The easiest way is to install the OS using an OS Build Plan, which automatically installs the SA Agent. For more information about installing the SA Agent, see ["Install the SA Agent on a VM" on page 58](#) and the SA User Guide: Server Automation. For more information about OS Build Plans, see the SA User Guide: Provisioning

Create and Provision a VM - SCVMM

This section describes how to create and provision a VM on a Microsoft SCVMM Server. You can also deploy a VM from a VM template. See ["Deploy a VM from a VM Template - SCVMM" on page 50](#) for further details.

If you install Ubuntu with a single or multiple CPUs, or any other Linux VM with multiple CPUs, you must exclude the `irqbalance` package from your installation media, or the VM's networking will not work.

To modify the Ubuntu OS Build Plan to exclude `irqbalance`, copy the default Ubuntu OS Build Plan and create a new one. In the new OS Build Plan, modify step 3 to add the following line:

```
d-i preseed/late_command string \  
    in-target apt-get -y remove irqbalance
```


1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the location where you want to place the new VM.
3. Select the desired location and right-click or select the **Actions** menu. Select **Create VM** to display the Virtual Machine Definition window.
4. **Virtual Machine Definition:** Enter the following information, then select Next.
 - The VM name.
 - A VM description.
 - A customer to assign the VM to. The default is "Not Assigned."
 - Amount of memory for the VM.

- Number of virtual processors for the VM.
- The guest operating system for the VM.

To create a Linux VM on SCVMM, you must select “Other Linux (64-bit)” or “Other Linux (32-bit).”

5. **Storage Configuration:** Your first VHD is added automatically. Use this window to specify the details for this VHD (see the following figure):

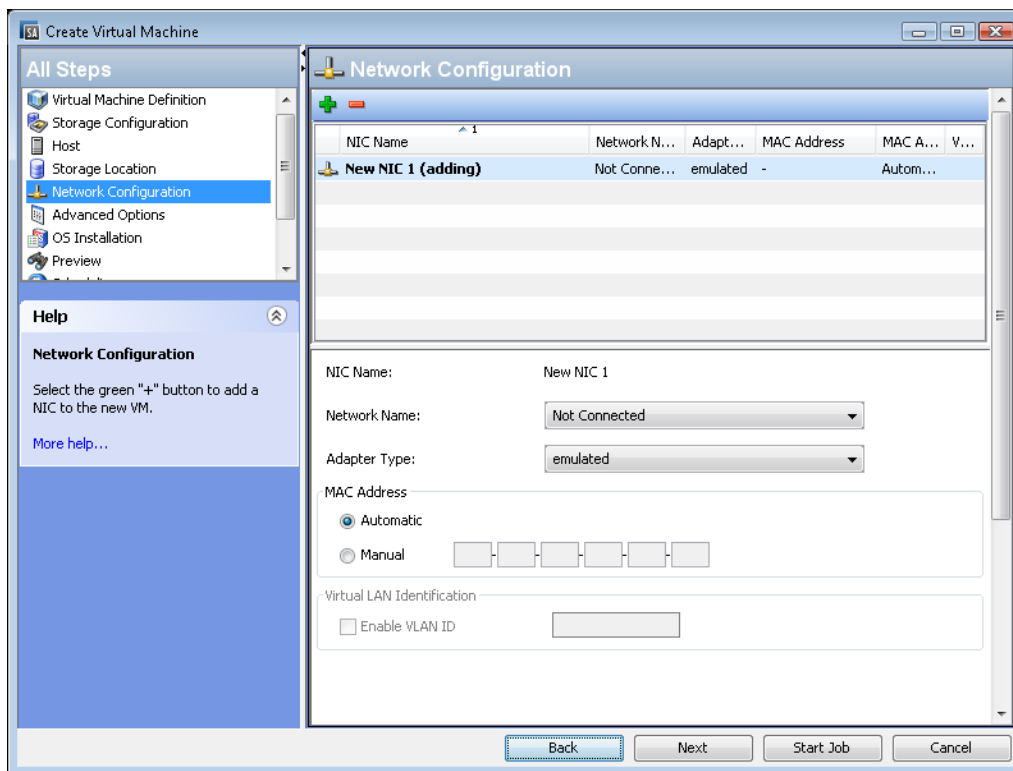
- Type: Select IDE from the drop-down list. Do not select the SCSI option.
- Allocated Size: Select the amount of GB (the default is 20).
- Disk Provisioning Type: Dynamic (default) or Fixed.
- File Name: Accept the default file name for the VHD, or modify it.

Optionally, you can add and configure more storage devices. Select the  button to add a virtual hard disk or CD/DVD drive to the VM. The maximum number of IDE devices you can add is 3. Specify the storage details, then select Next.

6. **Host:** Select the hypervisor that you want to host the VM. Verify the host ratings, then select Next.

7. **Storage Location:** Select from the default paths configured on the hypervisor or enter a valid path that exists on the host.

8. **Network Configuration:** The first NIC for your new VM is added automatically. Configure the following, then select Next (see the following figure).



- Network name
- Adapter type
- MAC address: Automatic (default) or manual
- Virtual LAN identification: Enable VLAN ID, then specify the VLAN ID.

It is recommended that you create the VM with a single network adapter to ensure that the job completes. However, if you must create a VM with multiple adapters, ensure that the NIC on the provisioning network is specified first.

9. **Advanced Options:** Select the action you want to perform on the VM when the hypervisor stops and starts, select the boot order, and then select Next.
10. **OS Installation:** Specify the following to provision an OS on the VM, then select Next.
 - **OS Build Plan** - Select the OS Build Plan you want to install. For more information on OS Build Plans, see the SA User Guide: Provisioning. To run an OS Build Plan, you must have adequate action permissions and adequate resource permissions on the OS Build Plan. For

information on permissions, see the SA Administration Guide.

SA no longer integrates Create VM with OS sequences. Contact your OS Provisioning administrator to create a custom OS Build Plan for your needs.

- **Provisioning Method** - Select the provisioning method to use:
 - **Network boot (PXE)** - Network-based installation.
 - **CD/DVD boot** - Uncheck Network Boot (PXE) to install the OS from physical media on an attached CD/DVD drive.

To create a 64-bit Linux VM using PXE provisioning with a 64-bit Linux OS Build Plan, choose the 32-bit version of the OS from the OS selector.

- **Operating System** - Use the OS selector to choose the OS that the OS Build Plan will install.
- **Provisioning Network** - Select the NIC to be used for provisioning.
- **Final Network Configuration** - From the drop-down list, select the IP version to be used to configure the VM. Depending on the OS you select, you can use IPv4 only; IPv4 and IPv4/IPv6 dual-stack; or IPv4, IPv6, and IPv4/IPv6 dual-stack.
 - For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
 - For IPv6:
 - With Autoconfig - Optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the

address, provided that no other valid prefix (an integer between 1 and 128) has been given.

- For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 with scenarios as described above.

For more information about IPv6, see the SA Administration Guide. For more information about DHCP configuration, see the SA User Guide: Provisioning.

- **Custom Attributes** - Optionally specify custom attributes. For more information on custom attributes, see the SA User Guide: Server Automation.
11. **Preview:** Verify all your VM settings. Use the Back button or select any step to make changes, then select Next.
 12. **Scheduling:** Select when you want the create VM job to run, then select Next.
 13. **Notifications:** Optionally enter a notifier, then select Next.
 14. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it creates the VM and displays the results. Once the VM is created, you will see it in the virtualization inventory of the VS in the SA Client and All Managed Servers.

It is highly recommended that you make all VMs into agent-managed servers to have maximum visibility, control, and compliance for these VMs. The easiest way is to install the OS using an OS Build Plan, which automatically installs the SA Agent. For information about installing the SA Agent, see ["Install the SA Agent on a VM" on page 58](#) and the SA User Guide: Server Automation. For more information about OS Build Plans, see the SA User Guide: Provisioning.

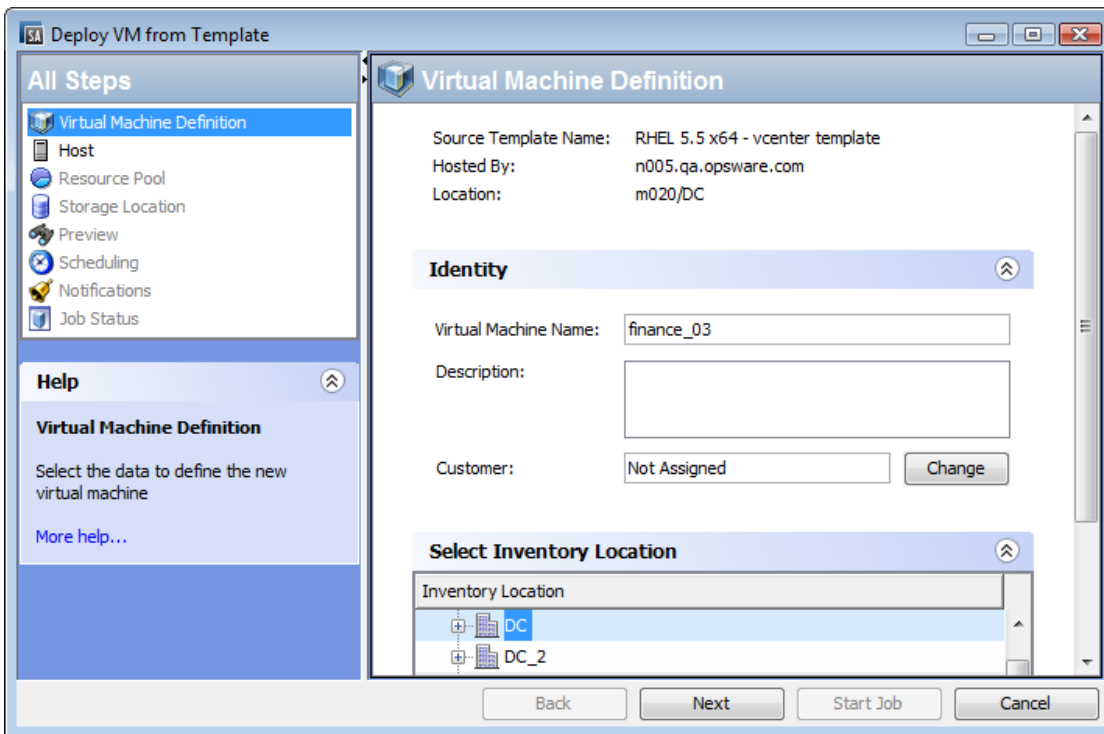
Deploy a VM from a VM Template - vCenter

This section describes how to deploy a VM from a VM template. You can also create and provision a VM or clone a VM from another VM (see ["Create and Provision a VM - vCenter" on page 35](#) and ["Clone a VM - vCenter" on page 54](#)).

Use an agent-managed template.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM template.

3. Select the VM template and right-click or select the **Actions** menu. Select **Deploy VM** to display the Deploy VM from VM Template window (see the following figure).



4. **Virtual Machine Definition:** Enter the following information, then select Next.
 - The VM name.
 - Select a customer to assign the VM to. You can select the customer; the default option is the customer assigned to the template. The defaults for customer, inventory location, host, resource pool, and storage location are the same as the source.
 - Verify or change the location in the virtualization inventory where you want to place the new VM.
5. **Host:** Navigate to and select the server that you want to host the VM. Verify that the host is compatible, then select Next.
6. **Resource Pool:** If the host or cluster has resource pools defined, navigate to and select the resource pool where you want to place the new VM. Examine the Compatibility Details to make sure the resource pool can support the new VM, then select Next.

7. **Storage Location:** Select the datastore in which to store the VM configuration file and the VM disk files.
- Use the drop-down list to select a virtual disk format.
 - In Basic mode, select the datastore where all the VM related files will go (the VM configuration file and the VM disk files).
 - In Advanced mode, you can select different datastores for the VM configuration file and for each of the VM disk files. Select the VM configuration file or any disk, then select the datastore from the drop-down list of available datastores.

Verify that the specified storage location is compatible with the VM you are creating, then select Next.

8. **Guest Customization:** Guest customization is strongly recommended so that your new VM does not have any network conflicts with the source VM and to ensure HPSA agent connectivity. Guest customization is available on agent-managed VMs and templates.

Guest customization can be used on the following platforms:

- CentOS 5.8 and above
- Microsoft Windows Server 2008 (32-bit)
- Microsoft Windows Server 2008 (64-bit)
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows Server 2012 (64-bit)
- Microsoft Windows Server 2012 R2 (64-bit)
- Microsoft Windows 7 (64-bit)
- Microsoft Windows 8.1 (64-bit)
- Oracle Enterprise Linux 5.8 and above
- Red Hat Enterprise Linux 5 and above
- SuSE Linux Enterprise Server 11
- Ubuntu Linux Server 12.04
- Ubuntu Linux Server 12.04 x86_64

For Microsoft Windows Server 2008 (64-bit), Microsoft Windows Server 2008 R2 (64-bit), and Microsoft Windows 7 (64-bit), use only source VMs with IPv4 DHCP or autoconfiguration IPv6 when cloning to a target that will have an IPv6 autoconfiguration address (DHCPv6).

Do the following to guest-customize the new VM:

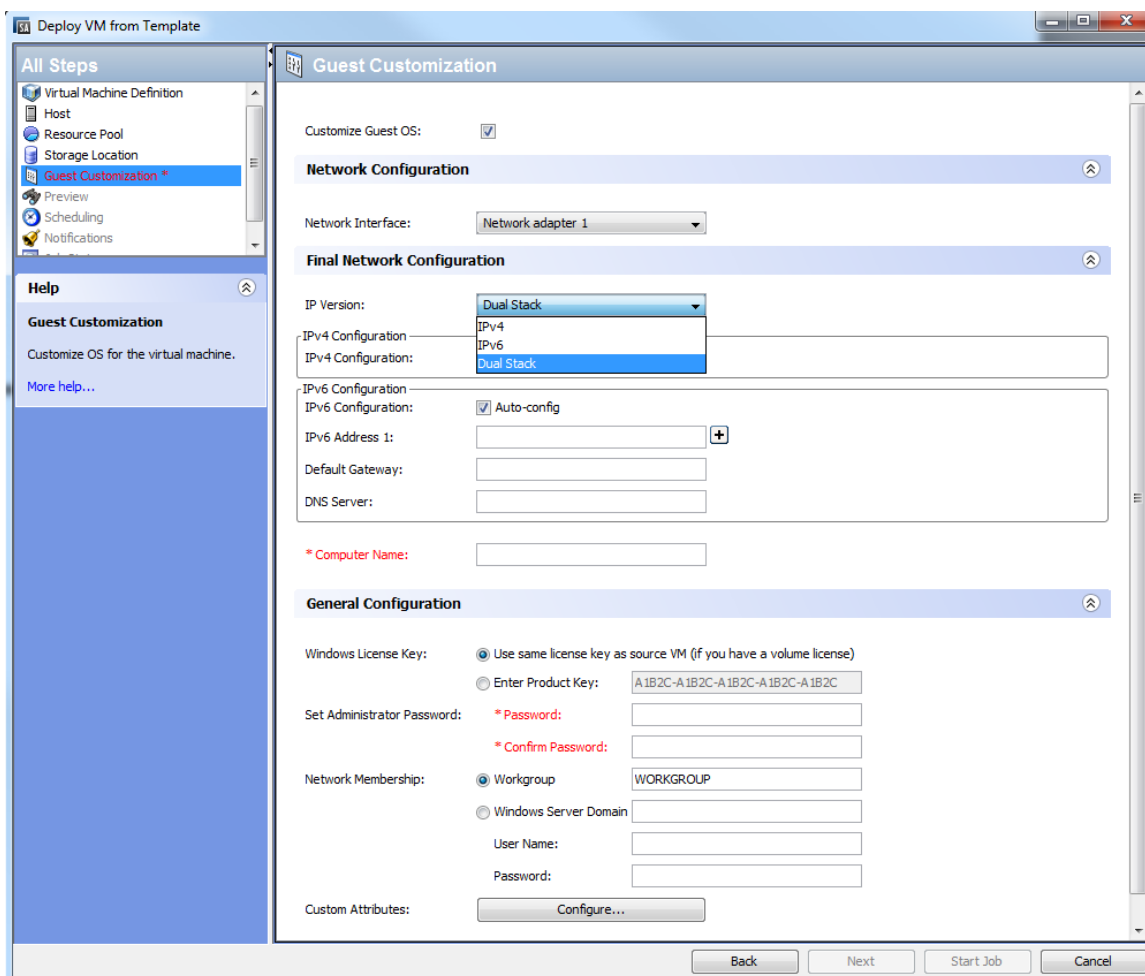
On Windows:

- From the drop-down list, select the IP version to be used to configure the VM.

Depending on the OS you select, you can use IPv4 only; IPv4 and IPv4/IPv6 dualstack; or IPv4, IPv6, and IPv4/IPv6 dual-stack.

- For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a static IP as the final network configuration for PXE-boot, although DHCP must be enabled for you to PXE-boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
 - For IPv6:
 - With Autoconfig - You can optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name, and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.
 - For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 addresses as described.
- Enter the Computer Name for the new VM.
 - Use the source volume license key, or optionally enter the product key as XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, in which each X represents a letter or number.
 - Set the Administrator Password.
 - Select Network Membership for the new VM.
 - If you select Workgroup, enter the Workgroup name for the new VM.
 - If you select Windows Server Domain, enter the domain. You must then enter your User Name and Password for that domain.

- To add optional Customer Attributes, press the Configuration button (see the following figure):

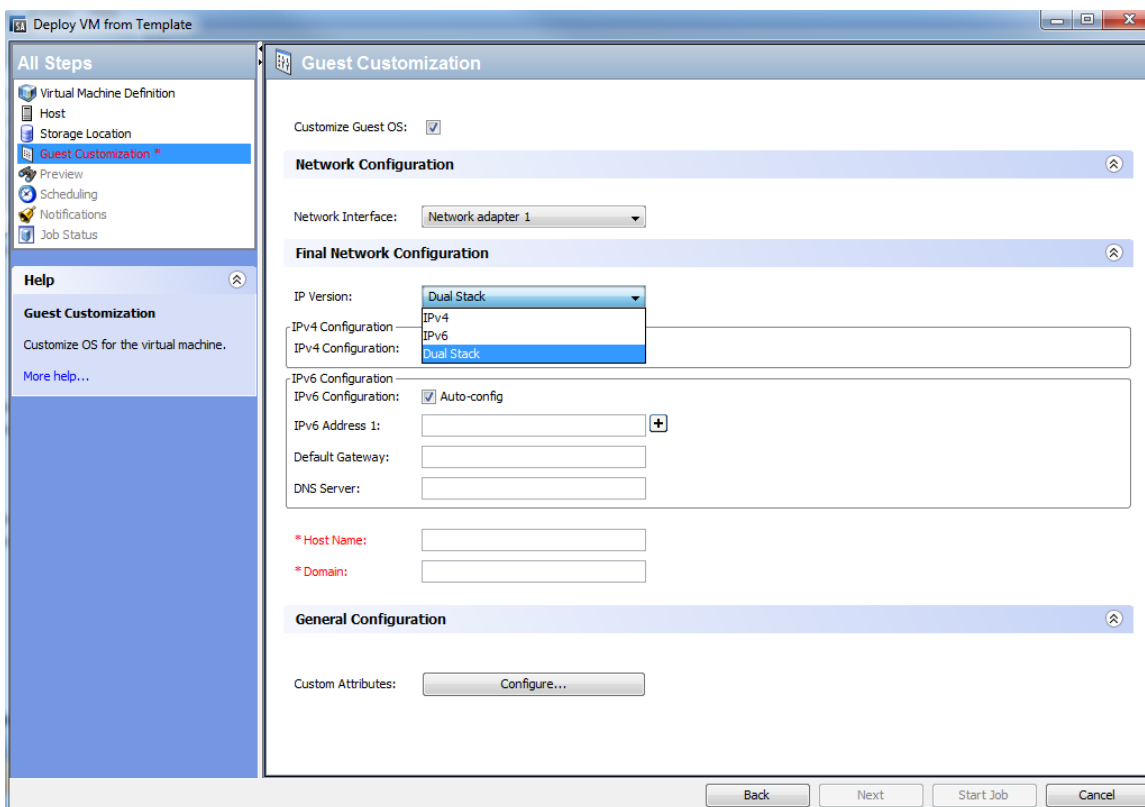


Tip: Determine which drive the system partition is using. If the Source Windows VM has more than one partition (for example, a “Reserved Partition,” which default Windows installations have), you must set a custom attribute called “SystemPartition” on the source to specify the partition in which the system files reside. For example, if you have two partitions (Reserved and OS), set the “SystemPartition” drive custom attribute to D.

On Linux:

- Select the desired IP Version for the VM from the drop-down list. Depending on the platform there are one, two or three options available (IPv4 only, IPv4 and DualStack or IPv4, IPv6 and DualStack).

- For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
- For IPv6:
 - With Autoconfig - Optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.
- For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 addresses as described.
- Enter the Host Name and Domain for the new VM.
- Optionally set custom attributes for the new VM (see the following figure):



9. **Preview:** Verify the information about the VM to be deployed. Use the Back button or select a previous step to make changes, then select **Next**.
10. **Scheduling:** Select when you want the deploy VM job to run, then select **Next**.
11. **Notifications:** Optionally enter a notifier, then select **Next**.
12. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it deploys the VM and displays the results. Once the VM is deployed, you will see it in the virtualization inventory of the VS in the SA Client and All Managed Servers.

Deploy a VM from a VM Template - SCVMM

This section describes how to create a VM from a VM template. You can also create and provision a VM using ["Create and Provision a VM - SCVMM" on page 40](#).

Use an agent-managed template.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM template.
3. Select the VM template and right-click or select the **Actions** menu and select **Deploy VM** to display the Deploy VM from VM Template window.
4. **Virtual Machine Definition:** Enter the following information, then select Next.
 - The VM name.
 - A description of the VM.
 - Assign a customer to the VM. You can select the customer; the default option is the customer assigned to the template.
5. **Host:** Select the server that you want to host the VM. Verify the host ratings, then select Next.
6. **Storage Location:** Select from the default paths configured on the host or enter a valid path that exists on the host.
7. **Network Configuration:** Select the network and optionally configure the VLAN ID for each NIC.
8. **Guest Customization:** Guest customization is strongly recommended so that your new VM does not have any network conflicts with the source VM and to ensure HPSA agent connectivity. Guest customization is available on agent-managed VMs and templates.

Guest customization is supported on the following platforms:

 - CentOS 5.8 and above
 - Microsoft Windows Server 2008 (32-bit)
 - Microsoft Windows Server 2008 (64-bit)
 - Microsoft Windows Server 2008 R2 (64-bit)
 - Microsoft Windows Server 2012 (64-bit)
 - Microsoft Windows Server 2012 R2 (64-bit)
 - Microsoft Windows 7 (64-bit)
 - Microsoft Windows 8.1 (64-bit)
 - Oracle Enterprise Linux 5.8 and above
 - Red Hat Enterprise Linux 5 and above
 - SuSE Linux Enterprise Server 11
 - Ubuntu Linux Server 12.04
 - Ubuntu Linux Server 12.04 x86_64

For Microsoft Windows Server 2008 (64-bit), Microsoft Windows Server 2008 R2 (64-bit), and Microsoft Windows 7 (64-bit), use only source VMs with IPv4 DHCP or autoconfiguration IPv6 when cloning to a target that will have an IPv6 autoconfiguration address (DHCPv6).

Do the following to guest-customize the new VM:

On Windows:

- From the drop-down list, select the IP version to be used to configure the VM. Depending on the OS you select, you can use IPv4 only; IPv4 and IPv4/IPv6 dual-stack; or IPv4, IPv6, and IPv4/IPv6 dual-stack.
 - For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
 - For IPv6:
 - With Autoconfig - You can optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.
 - For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 addresses as described.
- Enter the Computer Name for the new VM.
- Use the source volume license key, or optionally enter the product key as XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, in which each X represents a letter or number.
- Set the Administrator Password.

- Select Network Membership for the new VM.
 - If you select Workgroup, enter the Workgroup name for the new VM.
 - If you select Windows Server Domain, enter the domain. You must then enter your User Name and Password for that domain.
- To add optional Custom Attributes, press the Configure button.

Determine which drive the system partition is using. If the Source Windows VM has more than one partition (for example, a “Reserved Partition,” which default Windows installations have), you must set a custom attribute called “SystemPartition” on the source to specify the partition in which the system files reside. For example, if you have two partitions (Reserved and OS), set the “SystemPartition” drive custom attribute to D.

On Linux:

- Select the IP version to be used to configure the VM.
 - For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
 - For IPv6:
 - With Autoconfig - Optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.
 - For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 addresses as described.

- Enter the Host Name and Domain for the new VM.
- Optionally set custom attributes for the new VM.

Windows or Linux: When configuring the network interfaces, if there are multiple NICs, only one can be configured with a Static IP.

9. **Preview:** Verify the information about the VM to be deployed. Use the Back button or select a previous step to make changes, then select Next.
10. **Scheduling:** Select when you want the deploy VM job to run, then select Next.
11. **Notifications:** Optionally enter a notifier, then select Next.
12. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it deploys the VM and displays the results. Once the VM is deployed, you will see it in the virtualization inventory of the VS in the SA Client and All Managed Servers.

Clone a VM - vCenter

Cloning a VM creates an exact copy of the original VM. It is recommended that you primarily use VM templates to create VMs to ensure the VMs are consistent and maintainable.

To clone a VM, the source VM must be agent-managed. For information about installing the SA Agent, see ["Install the SA Agent on a VM" on page 58](#) and the SA User Guide: Server Automation.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to clone.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Manage > Clone** to display the Virtual Machine Definition window.
4. **Virtual Machine Definition:** Enter the following information, then select Next.
 - The VM name.
 - Select a customer to assign the VM to. You can select the customer; the default option is the customer assigned to the source VM.

- The defaults for customer, inventory location, hypervisor, resource pool, and storage location are the same as the source.
 - Verify or change the location in the virtualization inventory where you want to place the new VM.
5. **Host:** Navigate to and select the Host where you want the new VM to run. Examine the Compatibility Details to make sure the host can support the new VM. Note that compatibility can be checked only if the VM being cloned is powered off.
 6. **Resource Pool:** If the host has resource pools defined, select the resource pool where you want to place the new VM. Examine the Compatibility Details to make sure the resource pool can support the new VM, then select Next. Note that compatibility can be checked only if the VM being cloned is powered off.
 7. **Storage Location:** Select the datastore in which to store the VM configuration file and the VM disk files.
 - Use the drop-down list to select a virtual disk format.
 - In Basic mode, select the datastore where all the VM related files will go (the VM configuration file and the VM disk files).
 - In Advanced mode, you can select different datastores for the VM configuration file and for each of the VM disk files. Select the VM configuration file or any disk, then select the datastore from the drop-down list of available datastores.

Verify that the specified storage location is compatible with the VM you are creating, then select Next.

8. **Guest Customization:** Guest customization is strongly recommended so that your new VM does not have any network conflicts with the source VM and to ensure HPSA agent connectivity. Guest customization is available on agent-managed VMs and templates. Guest customization can be used on the following platforms:
 - CentOS 5.8 and above
 - Microsoft Windows Server 2008 (32-bit)
 - Microsoft Windows Server 2008 (64-bit)
 - Microsoft Windows Server 2008 R2 (64-bit)
 - Microsoft Windows Server 2012 (64-bit)
 - Microsoft Windows Server 2012 R2 (64-bit)
 - Microsoft Windows 7 (64-bit)
 - Microsoft Windows 8.1 (64-bit)

- Oracle Enterprise Linux 5.8 and above
- Red Hat Enterprise Linux 5 and above
- SuSE Linux Enterprise Server 11
- Ubuntu Linux Server 12.04
- Ubuntu Linux Server 12.04 x86_64

For Microsoft Windows Server 2008 (64-bit), Microsoft Windows Server 2008 R2 (64-bit), and Microsoft Windows 7 (64-bit), use only source VMs with IPv4 DHCP or autoconfiguration IPv6 when cloning to a target that will have an IPv6 autoconfiguration address (DHCPv6).

Do the following to guest-customize the new VM:

On Windows:

- From the drop-down list, select the IP version to be used to configure the VM. Depending on the OS you select, you can use IPv4 only; IPv4 and IPv4/IPv6 dual-stack; or IPv4, IPv6, and IPv4/IPv6 dual-stack.
 - For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
 - For IPv6:
 - With Autoconfig - You can optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.
 - For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 with scenarios as described above.

For more information about IPv6, see the SA Administration Guide. For more information about DHCP configuration, see the SA User Guide: Provisioning.

- Enter the Computer Name for the new VM.
- Use the source volume license key, or optionally enter the product key as XXXXX–XXXXX–XXXXX–XXXXX–XXXXX, in which each X represents a letter or number.
- Set the Administrator Password.
- Select New Membership for the new VM.
If you select Workgroup, enter the Workgroup name for the new VM.

If you select Windows Server Domain, enter the domain. You must then enter your User Name and Password for that domain.

- To add optional Custom Attributes, press the Configure button.

On Linux:

- From the drop-down list, select the IP version to be used to configure the VM. Depending on the OS you select, you can use IPv4 only; IPv4 and IPv4/IPv6 dual-stack; or IPv4, IPv6, and IPv4/IPv6 dual-stack.
 - For IPv4, you can select DHCP to configure your network using your HPSA DHCP-enabled environment, or choose Static to configure your network settings manually. For more information about an HPSA DHCP-enabled environment, see the SA User Guide: Provisioning.
 - You can specify a Static IP as the final network configuration for PXE boot, although DHCP must be enabled for you to PXE boot.
 - For static IP, you are required to enter the IP address, subnet mask, default gateway, and DNS server.
 - For IPv6:
 - With Autoconfig - You can optionally specify one or more IPv6 address, the default gateway, the DNS server, the host name and the domain.
 - Without Autoconfig - You are required to enter a IPv6 address and the host name. Optionally, you can specify the default gateway, the DNS server, and the domain.
 - When an IPv6 address is specified, the default prefix (64) is added at the end of the address, provided that no other valid prefix (an integer between 1 and 128) has been given.

- For IPv4/IPv6 dual-stack configuration - Configure both IPv4 and IPv6 with scenarios as described above.
For more information about IPv6, see the SA Administration Guide. For more information about DHCP configuration, see the SA User Guide: Provisioning.
 - Enter the Host Name and Domain for the new VM.
 - Optionally set custom attributes for the new VM.
9. **Preview:** Verify the selections listed. Use the Back button or select any previous step to make changes, then select Next.
 10. **Scheduling:** Select when you want the clone VM job to run, then select Next.
 11. **Notifications:** Optionally enter a notifier, then select Next.
 12. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it clones the VM and displays the results. Once the VM is created, you will see it in the virtualization inventory of the VS in the SA Client and All Managed Servers.

Install the SA Agent on a VM

To gain the most benefit from SA, you should always install the SA Agent on all managed servers, both VMs and physical servers.

If you created the VM from an agent-managed server or an agent-managed VM template, the SA Agent is already installed on the VM. You only need to install the SA Agent if you created a VM without an SA Agent.

To determine if the SA Agent is running on a VM (or any server), locate the VM or server in the SA Client and hover your mouse pointer over the icon for the server. The SA Client will display the agent status of the server, either agentless or agent managed. You can also select or open the server in the SA Client, and select the Summary view. This view gives the status of the SA Agent. To ensure connectivity, you can run a Communication test by selecting the Actions menu, then selecting Run > Communication Test.

For more information about the SA Agent, agent-managed servers, and installing the agent on multiple servers, see the SA User Guide: Server Automation.

Prerequisites for OpenStack

The OpenStack instance must have a user name and password set up on the VM. Enable SSH on the server to allow remote logins.

Requirements for OpenStack Instance

An OpenStack instance must have:

- A working username/password login.
- A routable IP (typically a floating IP) that the SA core can reach.

Installing the SA Agent on the VM

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM on which you want to install the SA Agent.
3. Select the desired VM and right-click or select the **Actions** menu. Select **Install SA Agent** to display the Install SA Agent window.
4. Select the IP address for the VM from the drop-down list. Select the IP the SA core can reach.
5. Select Scan. SA attempts to establish communications with the VM and determines the best protocol to use to install the SA Agent. If the scan fails, check the power status and network settings of the VM.
6. Select a network protocol to connect to the VM from the drop-down list.
In most cases, you should choose Select Automatically to allow SA to select an appropriate protocol for the VM.
7. Enter a user name and password to use for logging into the VM.
For Windows-based systems, specify the Windows administrator user name and password.

For UNIX systems, specify a root user and password.

- If you are unable to deploy the agent to a UNIX server by logging in as root, the system you are deploying to may be configured to disallow direct root logins. In such cases, SA allows you to log in as a non-root user and escalates your privileges using either the `su` or `sudo` command.

To deploy agents as non-root users:

- Enter the non-root user name in the Username field to log into the server.
- Enter the non-root password in the Password field.
- Select the Become root (UNIX) checkbox. Select “Supply root password” and enter the password or select “Use sudo.” If you use sudo, the non-root account must be able to run any command as root.

In OpenStack, you must enable “Security Group Rule” on a project to allow required port 1002 through. If this is not open, installing an agent will not work.

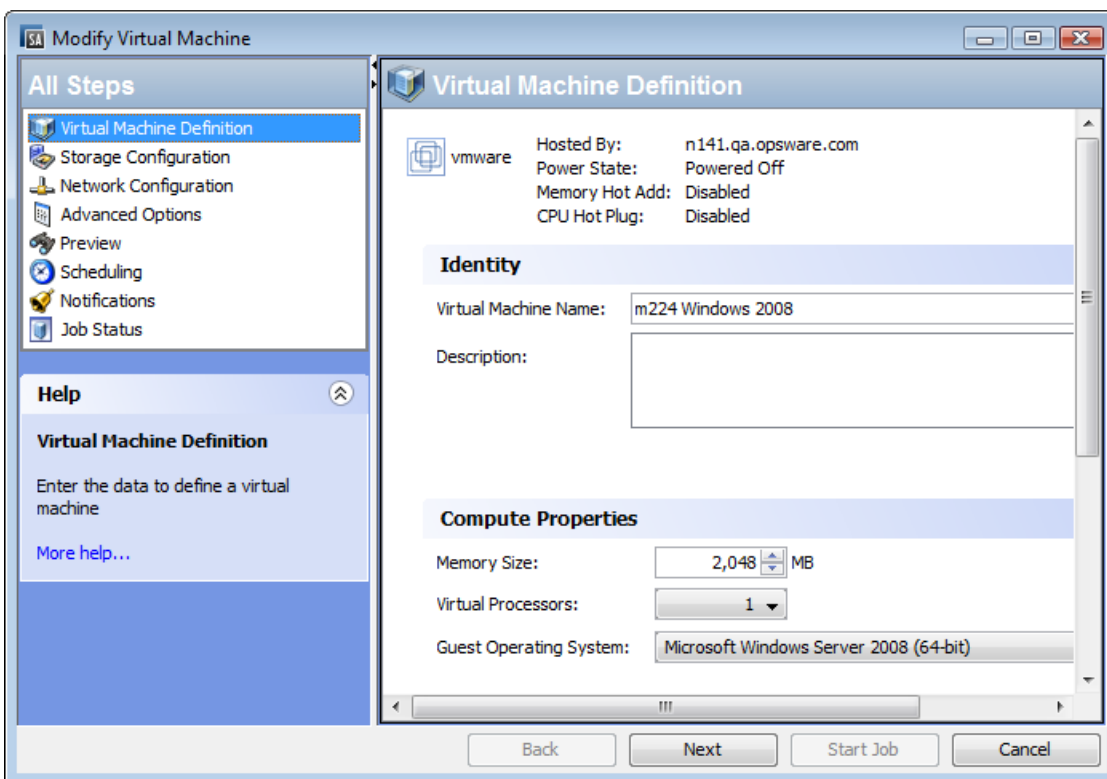
8. Select one of the following deployment actions:
 - Verify installation prerequisites.
Checks for sufficient disk space for agent installation on the VM, verifies that no other applications are using port 1002, and verifies that ports to the SA gateway are accessible.
 - Verify prerequisites and copy agent installer to servers.
Copies the agent installer to the VM.
 - Verify prerequisites, copy installer, and install agent.
Installs the SA Agent on the VM.
9. Optionally specify the agent installer options and advanced options to control the way the agent is installed on a server. See the SA User Guide: Server Automation for more information.
10. Select OK to perform your selected actions.
11. After the deployment action is completed, the SA Client displays the results and updates the status icons for the VM.

For more information on agent installation status and troubleshooting, see the SA User Guide: Server Automation.

Modify a VM - vCenter and SCVMM

A VM must be powered off before it can be modified. For more information, see ["Power On/Off a VM - vCenter and SCVMM " on page 67.](#)

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to modify. Make sure it is powered off.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Manage > Modify** to display the Virtual Machine Definition window, as shown below.



4. **Virtual Machine Definition:** Change the VM name, description, memory size, number of virtual processors, or the guest operating system setting, then select Next.
5. **Storage Configuration:** Use the **+** and **-** buttons to add or remove storage for the VM. Select any storage item to modify its settings, then select Next.
6. **Network Configuration:** Use the **+** and **-** buttons to add or remove NICs. Select a NIC to change its settings, then select Next.
 After modifying the network configuration, make sure that the network adapter selected for cloning or deploying from template is seen by the operating system and that an SA Agent hardware registration was performed on the VM. Failure to do so may cause cloning jobs or deploy VM from template jobs to fail. This is because full network configuration discovery is done by the SA Agent.
7. **Integration Services:** For SCVMM, select the desired services for the VM, then select Next.

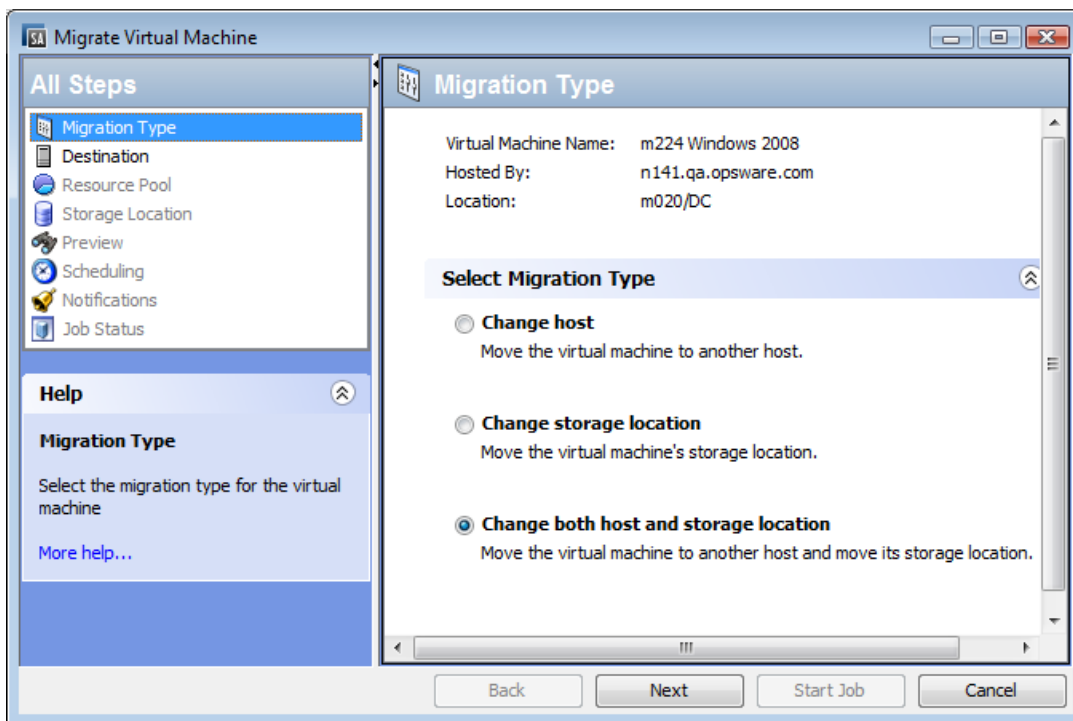
8. **Advanced Options:** Set the following, then select Next.
 - vCenter - Set the power on boot delay time, if desired.

 - SCVMM - Set the start and stop options and the boot order, if desired.
9. **Preview:** Verify the information about the VM. Use the Back button or select a previous step to make changes, then select Next.
10. **Scheduling:** Select when you want the modify VM job to run, then select Next.
11. **Notifications:** Optionally enter a notifier, then select Next.
12. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it modifies the VM and displays the results.

Migrate a VM - vCenter

You can migrate a VM to run on a different host, migrate a VM's storage to a different storage location, or migrate the VM to a different resource pool. To migrate a VM, it must be powered off or suspended. For more information, see "[Power On/Off a VM - vCenter and SCVMM](#) " on page 67 and "[Suspend a VM - vCenter and SCVMM](#) " on page 68.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to migrate. If the VM is powered on, power it off or suspend it.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Manage > Migrate** to display the Migration Type window, as shown in the following figure.



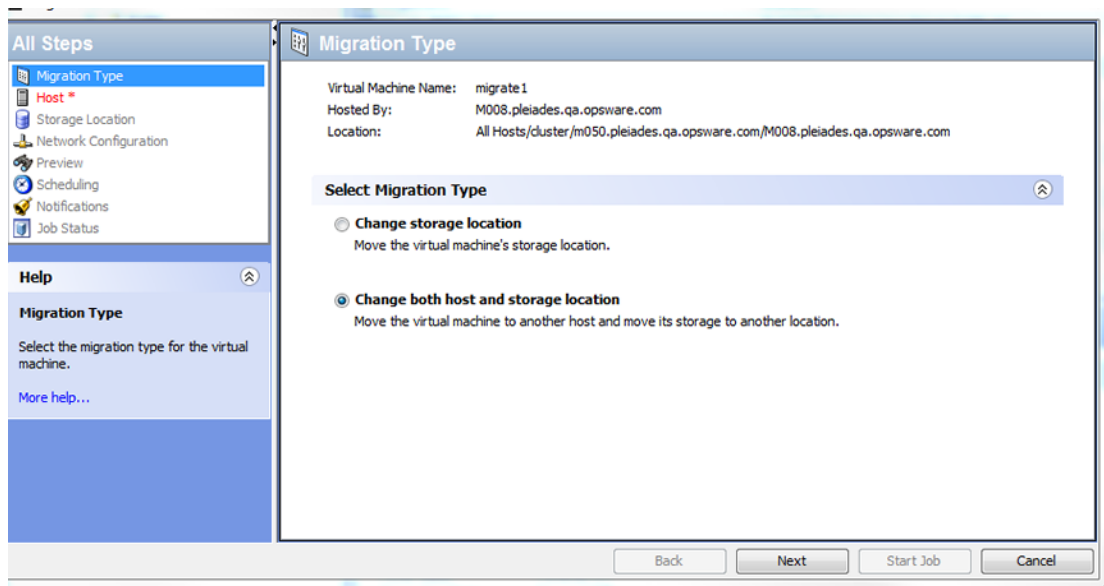
4. **Migration Type:** Select the type of migration you want, then select Next. You can change the VM host, or the VM storage, or both. The next window or windows depend on the type of migration you selected. Check all of the following windows that apply to your situation:
5. **Destination:** Change the host where you want to migrate the VM. Examine the Compatibility Details to make sure the selected location can support the VM, and select Next.
6. **Resource Pool:** Change where you want to place the VM. Examine the compatibility details to make sure the resource pool can support the VM, and select Next.
7. **Storage Location:** Select the datastore in which you want to store the VM configuration file and the VM disk files. Verify that the specified storage location is compatible with the VM you are migrating, and select Next.
 - Select the format for the virtual disk. You can specify the same format as the source disk, thin provisioned, or thick provisioned with lazy zeroing. If the VM has multiple disks, this setting applies only to disks being migrated to another datastore. It will not change the format for disks not being migrated to another datastore.
 - In Basic mode, select the datastore where all the VM related files will go (the VM configuration file and the VM disk files).

- In Advanced mode, you can select different datastores for the VM configuration file and for each of the VM disk files. Select the VM configuration file or any disk, then select the datastore from the drop-down list of available datastores.
8. **Preview:** Verify the changes. Use the Back button or select a previous step to make changes, then select Next.
 9. **Scheduling:** Select when you want the migrate VM job to run, then select Next.
 10. **Notifications:** Optionally enter a notifier, then select Next.
 11. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it migrates the VM and displays the results.

Migrate a VM - SCVMM

You can migrate a VM to run on a different host or you can migrate a VM's storage to a different storage location. To migrate a VM, it must be powered off or suspended. For more information, see "[Power On/Off a VM - vCenter and SCVMM](#) " on page 67 and "[Suspend a VM - vCenter and SCVMM](#) " on page 68.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to migrate. If the VM is powered on, power it off or suspend it.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Manage > Migrate** to display the Migration Type window, as shown in the following figure.



4. **Migration Type:** Select the type of migration you want, then select Next. The next window or windows depend on the type of migration you selected. Check all of the following windows that apply to your situation:
5. **Host:** Select the host to which you want to migrate the VM. Check the host rating details to verify the destination host is compatible, and select Next.
6. **Storage Location:** Enter the path on the host where you want to place the VM file and the VM disk files, then select Next. You can specify a different location for each disk.
7. **Network Configuration:** For each NIC, use the drop-down menu to select the network to which you want to connect the VM, and select Next.
8. **Preview:** Verify the changes listed. Use the Back button or select a previous step to make changes, then select Next.
9. **Scheduling:** Select when you want the migrate VM job to run, then select Next.
10. **Notifications:** Optionally enter a notifier, then select Next.
11. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it migrates the VM and displays the result.

Deactivate the SA Agent on a VM

Deactivating the SA Agent on a virtual machine is the same as deactivating the agent on a physical machine: it makes the server no longer agent-managed. Virtual servers that are not agent-managed can still be managed by a Virtualization Service.

This is the same process used for physical servers, which are accessed under the Devices tab. For more information about the SA Agent and agent-managed servers, see the SA User Guide: Server Automation.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the agent-managed VM you want to deactivate.
3. Select the desired VMs and right-click or select the **Actions** menu and select **Deactivate SA Agent**.
4. Verify that you want to deactivate the agent on the VM and select Deactivate.

Delete a VM - vCenter and SCVMM

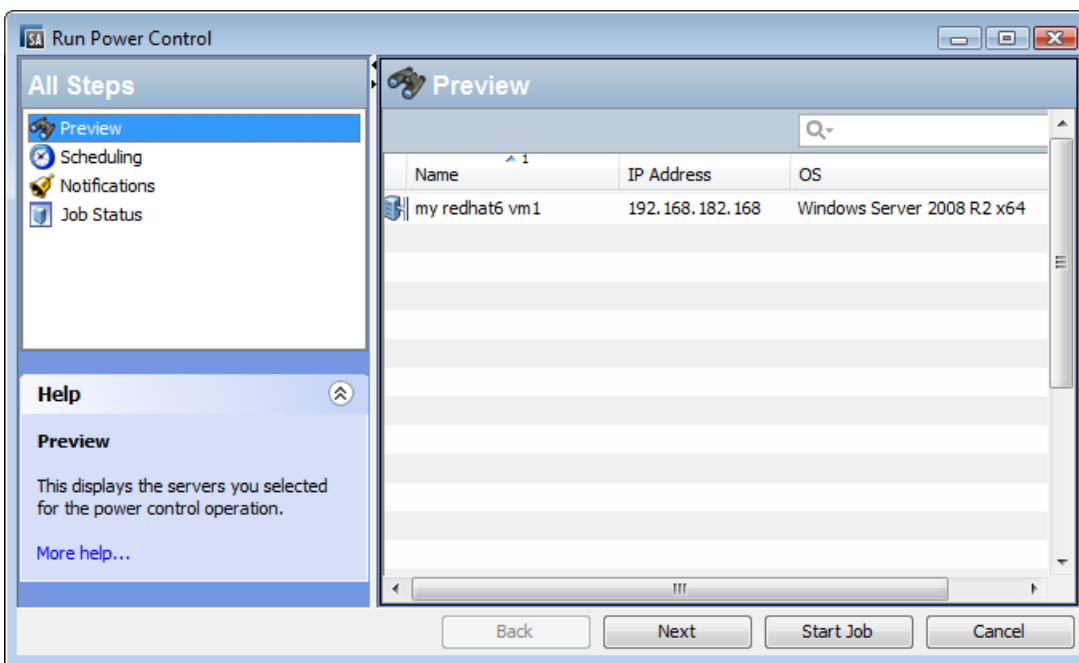
To delete a VM, the SA Agent on the VM must be deactivated, and the VM must be powered off. You can delete several VMs at once. For more information, see ["Deactivate the SA Agent on a VM "](#) above and ["Power On/Off a VM - vCenter and SCVMM "](#) on the next page.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to delete. If the VM is agent-managed, deactivate the agent. If the VM is powered on, power it off.
3. Select the desired VM and right-click or select the **Actions** menu and select **VM Manage > Delete** to display the Delete Virtual Machines window.
4. **Delete Virtual Machines:** Verify the VM that you want to delete, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the delete VM job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.

7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab. When the job runs, it deletes the VM and displays the results.

Power On/Off a VM - vCenter and SCVMM

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to power on or off.
3. You can power on or power off several VMs at once. Select the desired VM(s) and right-click or select the **Actions** menu. Select **VM Power > Power On** or **Power Off** to display the Run Power Control window, as shown in the following figure.



4. **Run Power Control:** Verify the VM you want to power on or off, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the power control job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.

7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it powers the VM on or off and displays the results.

Suspend a VM - vCenter and SCVMM

Suspending a VM pauses the virtual machine activity. All transactions are frozen until you power on the VM. Consumed host memory and CPU are released back to host.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to suspend.
3. Select the desired VM and right-click or select the **Actions** menu and select **VM Power > Suspend** to display the Run Power Control window.
4. **Run Power Control:** Verify the VM you want to suspend, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the suspend job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it suspends the VM and displays the results.

Use Power On to restart a suspended VM. For more information, see "[Power On/Off a VM - vCenter and SCVMM](#)" on the previous page.

Pause a VM - SCVMM

Pausing a VM suspends execution of the VM and keeps all VM state in memory.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to pause.

3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Power > Pause** to display the Run Power Control window.
4. **Run Power Control:** Verify the VM you want to pause, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the pause job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it pauses the VM and displays the results.

Use Power On to resume a paused VM. For more information, see ["Power On/Off a VM - vCenter and SCVMM " on page 67.](#)

Reset a VM - vCenter

Resetting a VM stops the VM and restarts (reboots) it.

Use care when resetting a VM, because it performs a hard shut down.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to reset.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Power > Reset** to display the Run Power Control window.
4. **Run Power Control:** Verify the VM you want to reset, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the reset job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it resets the VMs and displays the results.

Shut Down a VM Guest OS - vCenter and SCVMM

To shut down the guest operating system of the VM, the guest tools must be installed on the VM. For more information on guest tools, see the virtualization vendor's documentation.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VMs you want to shut down.
3. Select the desired VMs and right-click or select the **Actions** menu. Select **VM Power > Shut down guest** to display the Run Power Control window.
4. **Run Power Control:** Verify the VM you want to shut down, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the shut down job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it shuts down the VM operating system and displays the results.

Use Power On to restart a VM that has been shut down. For more information, see "[Power On/Off a VM - vCenter and SCVMM](#)" on page 67.

Restart a VM Guest OS - vCenter

To stop and restart the guest operating system of the VM, the guest tools must be installed on the VM. For more information on guest tools, see the virtualization vendor's documentation.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VMs you want to restart.
3. Select the desired VMs and right-click or select the **Actions** menu. Select **VM Power > Restart guest** to display the Run Power Control window.

4. **Run Power Control:** Verify the VM you want to restart, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the restart job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it stops and restarts the VM operating system and displays the results.

Convert a VM to a VM Template - vCenter

You can convert VM information to a VM template and then deploy VMs from the VM template. For more information, see ["Deploy a VM from a VM Template - vCenter" on page 44](#).

To convert a VM to a VM template, the VM must be agent-managed and powered off. For more information, see ["Install the SA Agent on a VM" on page 58](#) and ["Power On/Off a VM - vCenter and SCVMM" on page 67](#).

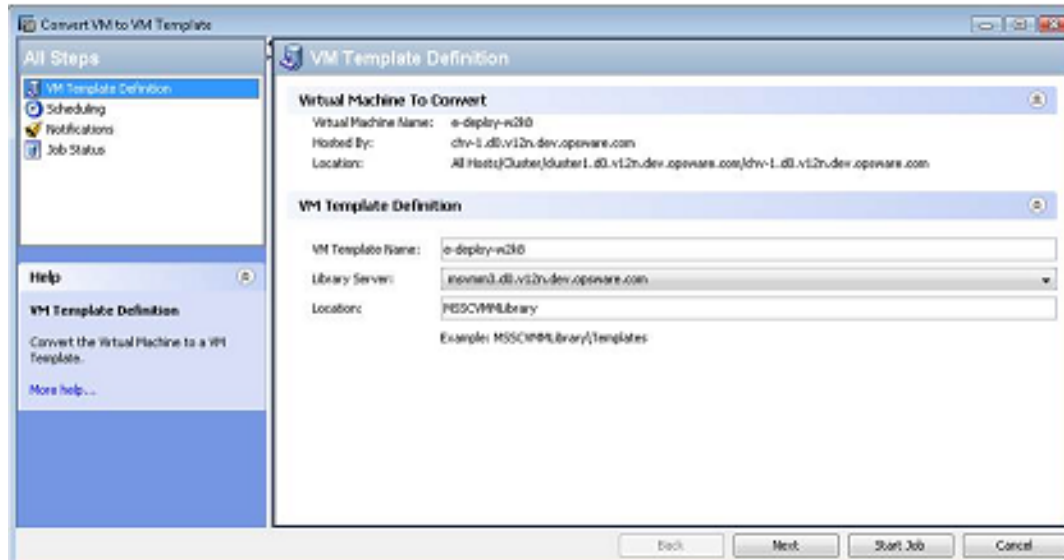
1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to convert to a VM template. If the VM is powered on, power it off.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Manage > Convert to VM Template** to display the Convert VM to VM Template window.
4. **Convert VM to VM Template:** Verify the VM you want to convert to a VM template, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it converts the VM to a VM template and displays the results.

Convert a VM to a VM Template - SCVMM

You can convert VM information to a VM template and then deploy VMs from the VM template. For more information, see ["Deploy a VM from a VM Template - SCVMM" on page 50](#).

To convert a VM to a VM template, the VM must be agent-managed and powered off. For more information, see ["Install the SA Agent on a VM" on page 58](#) and ["Power On/Off a VM - vCenter and SCVMM " on page 67](#).

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM you want to convert to a VM template. If the VM is powered on, power it off.
3. Select the desired VM and right-click or select the **Actions** menu. Select **VM Manage > Convert to VM Template** to display the Convert VM to VM Template window.
4. **Convert VM to VM Template:** Verify the VM you want to convert to a VM template. Specify the Library Server to which you want to store the template and enter the location, which must be an existing path. Then select Next or Start Job to accept the remaining defaults and run the job.



5. **Scheduling:** Select when you want the job to run, then select Next.
6. **Notifications:** Optionally enter a notifier, then select Next.

- Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
 When the job runs, it converts the VM to a VM template and displays the results.

Modify a VM Template - vCenter and SCVMM

This section describes how to modify certain aspects of a VM template. The following table shows the actions you can perform with an agent-managed VM template and an agentless VM template.

To modify other aspects of the VM template, you must deploy a VM from the VM template, modify the VM, and convert the modified VM to a new VM template. For more information, see ["Deploy a VM from a VM Template - vCenter" on page 44](#) and ["Convert a VM to a VM Template - vCenter" on page 71](#).

VM Template Action	Agent-Managed	Agentless
Open the VM template	✓	✓
Modify the name and description	✓	✓
Modify the customer with which the VM template is associated	✓	✓
Modify the Server Use setting	✓	✓
Add, modify, and delete custom attributes	✓	✓
Create a snapshot specification with the VM template	✗	✗
Deactivate the SA Agent on the VM template	✓	✗
Deploy a VM from the VM template	✓	✓
Delete the VM template	✓	✓
Reload data about the VM template	✓	✓
View event history for the VM template	✓	✓
Add the VM template to a device group	✓	✓
Attach software policies to the VM template	✓	✗
Attach patch policies to the VM template	✓	✗

VM Template Action	Agent-Managed	Agentless
Attach patch policies to the VM template	✓	✗
Attach application configurations to the VM template	✓	✗
Create an audit with the VM template		✗
Export patch information from the VM template	✓	✗
Open the VM template with HP Service Automation Visualizer	✓	✗

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM template you want to modify.
3. Select the VM template and right-click or select the **Actions** menu. Select **Open** to display the VM template in a separate window.
4. Navigate to the desired view of the VM template by selecting one of the tabs labeled Information, Relationships, and Inventory.
5. Use the navigation pane on the left to locate the elements of the VM template you want to change, and make your changes.
6. Select the **File > Revert** menu to discard your changes.
Select the **File > Save** menu to save your changes.

Delete a VM Template - vCenter and SCVMM

Performing the Delete a VM Template action deletes a template or templates permanently. You can delete several VM templates at once.

1. In the SA Client, select the Virtualization tab to display your virtualization inventory.
2. Navigate to the VM template you want to delete.
3. Select the desired VM template and right-click or select the **Actions** menu. Select **Delete VM Template** to display the Delete VM Templates window.
4. Verify the VM templates that you want to delete, then select Next. Or you can select Start Job to accept the remaining defaults and run the job.
5. **Scheduling:** Select when you want the delete VM template job to run, then select Next.

6. **Notifications:** Optionally enter a notifier, then select Next.
7. **Job Status:** Select the Start Job or Schedule Job button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the Jobs and Sessions tab.
When the job runs, it deletes the VM template and displays the results.

Chapter 7: Managing HP-UX Virtual Servers

This section describes how to use the SA web extension to create and manage HP-UX VMs, HP-UX Virtual partitions, and HP Integrity Virtual machines.

Terms and Definitions

- **HP-UX Virtual Partitions (vPars containers)** - vPars containers enables you to run multiple instances of HP-UX simultaneously on one hard partition by dividing that hard partition further into virtual partitions. Each virtual partition is assigned its own subset of hardware, runs a separate instance of HP-UX, and hosts its own set of applications. Because each instance of HP-UX is isolated from all other instances, vPars provides application and operating system (OS) fault isolation. Each instance of HP-UX can have different patches and a different kernel.
- **HPVM Hypervisors** - HPVM hypervisors are soft partitioning and virtualization technologies that provides operating system isolation, with sub-CPU allocation granularity and shared I/O. HPVM hypervisors can be installed on an Integrity server, Integrity server blade, or hardware partition (nPartition) running HP-UX. The HPVM hypervisor environment consists of two types of components:
 - HPVM Host
 - VMs (also called guests)
- **HPVM Hypervisor Host (Host)** - The HPVM hypervisor host virtualizes physical processors, memory, and I/O devices, allowing you to allocate them as virtual resources to each virtual machine.
- **HPVM** - Individual VMs, components of the HPVM Hypervisor.
- **vPars** - Individual vPars, components of the vPars Container.
- **vSwitches** - Virtual switches.

Requirements

The following are requirements for HP-UX virtualization:

- For both vPars and HPVM hypervisors:
 - Make all host servers (HP-UX servers) managed servers on HP Server Automation. For more information, see the SA User Guide: Server Automation.

- For vPars:
 - Install the Virtual Partitions product on the host server. See “Virtual Partitions” in <http://docs.hp.com/hpux/11iv3>.

- For HPVM hypervisors:
 - Install the HP Integrity Virtual Machine product on the host server. See “HP Integrity Virtual Machines and Online VM Migration” in: <http://docs.hp.com/hpux/11iv3>.

Supported Platforms and Configurations

Managing HP-UX virtual servers using SA supports the following platforms and configurations:

Supported Platforms and Configurations

Platform or Configuration	Support
Virtualization platforms	vPars A.5.06 and later versions HPVM hypervisors 4.2 and later versions
HP-UX guest OS	11iV3
HP-UX host OS for IVM and first vPars on physical server	11iV3
Processor architecture	Itanium
SA version	9.04 CORD release
SA platform	RHEL AS4 – 64-bit
Satellite and multimaster support	RHEL AS4 – 64-bit
Integrity platform support	As defined by the vPars and HPVM support matrix.

Not Supported

Cloning and migration of VMs are not supported by the HP-UX Virtualization Manager. However, they are supported by HP Integrity Virtual Machines.

SA Permissions Required

This section describes the SA permissions required for HP-UX use. For complete information on permissions, see the SA Administration Guide.

Virtualization Service Management Permissions

The SA Administration Guide provides details on permissions required for HP-UX use. Not all of these permissions apply to HP-UX; check these tables for more detailed information.

Action Permissions Required

To manage HP-UX VMs, your SA user must either belong to an SA user group that has the following action permissions or have the permissions:

Action Permissions Required for Managing HP-UX VMs

Permission Tab	Setting	User Action Enabled
System Administration: Managed Servers and Groups	Yes	View managed servers and device groups
Virtualization: View Virtualization Inventory	Yes	View HPVM hypervisors, HPVMs, vPars containers, vPars, and vSwitches Discover and refresh HPVM hypervisors

Permission Tab	Setting	User Action Enabled
Virtualization: Manage VM Lifecycle: Create VM Manage VM Lifecycle: Modify VM Manage VM Lifecycle: Delete VM	Yes	Create, modify, and remove HPVM hypervisors, vPars containers, vPars, vSwitches, and HPVMs
Virtualization: Manage VM Power State	Yes	Shut down, halt, and start HPVMs, vPars, and vSwitches

Folder Permissions Required

You need access to the SA Library folder containing the HP-UX Virtualization Manager web extension to manage HP-UX VMs and run the web extension. This web extension is located in the SA Library folder `/Opware/Tools/Virtualization Programs`. For complete information on folder permissions, refer to the SA Administration Guide.

Use the following procedure to assign the required folder permissions to a user:

1. Log in to the SA Client as an administrative user that has permission to set folder permissions.
2. In the SA Client, select the Library tab.
3. Select the By Folder tab to display the SA Library folder structure.
4. Navigate to the folder: `/Opware/Tools/Virtualization Programs`.
5. Right-click Virtualization Programs and select the Folder Properties menu. This displays the Folder Properties window.
6. In the Folder Properties window, select the Permissions tab. This displays the user groups that have some permissions to the folder.
7. Select the user group you want to grant access to. If the user group does not appear, select the Add button to add it.
8. Select Execute Objects Within Folder.
9. Select OK.

Resource Permissions Required





As with all server management tasks, you need access to the HP-UX servers. Grant access to the facility, customer and at least one device group of your HP-UX managed servers. For complete information on resource permissions, see the SA Administration Guide.

Server and Switch Status Icons

This section describes the icons associated with HPVM hypervisors and vPars containers.



The following table describes the vPar container and HPVM hypervisor status icons (displayed in the HP-UX Virtualization Manager web extension) and their meaning:

Status Icons

Icon	Icon Meaning for vPars Containers	Icon Meaning for HPVM Hypervisor
	Agent-managed 1 or more vPars reachable	Agent-managed and reachable
	Agent-managed Unreachable	Agent-managed but unreachable
	Agentless (or HP-UX Virtualization Manager web extension not run while the server in nPars mode) 1 or more nPars reachable	Not applicable
	Agentless (or HP-UX Virtualization Manager web extension not run while the server in vPars mode) Unreachable	Not applicable

The following table shows the vSwitch icons displayed in the HP-UX Virtualization Manager web extension and their meanings.

vSwitch Icons

Icon	Icon Meaning for vSwitches
	Status is Up
	Status is not Up

Quick Start vPars, HPVMs, and vSwitches

This section describes prerequisites for using HP-UX Virtualization Manager web extensions:

1. Make sure that your HP-UX servers are agent-managed by SA and visible in the SA client under Devices > All Managed Servers. For more information, see the SA User Guide: Server Automation.
2. Make sure that your SA user has adequate permissions. For details, see ["SA Permissions Required" on page 78](#).

Prerequisites for managing vPars, HPVMs, or vSwitches:

1. Manage your vPars as described in ["Managing vPars Containers" on page 92](#).
2. Manage your HPVMs as described in ["Managing HPVM Hypervisors" on page 97](#).
3. Manage your vSwitches as described in ["Managing vSwitches" on page 103](#).

Launching the HP-UX Virtualization Manager

To launch the HPVM manager:

1. In the SA Client, in the left panel, choose **Library > Extensions > Web**.
2. In the Web panel, double-click the HP-UX Virtualization Manager icon to display the HP-UX Virtual Servers window, which lists HPVM hypervisors and vPars containers.

Saving ioscan Output

For vPars, `ioscan` output can only be obtained when the nPar or physical server is in nPars mode.

The following procedure saves a copy of the `ioscan` output, makes the output viewable, and simplifies the process of creating and modifying vPars. You will need to repeat these steps to refresh the `ioscan` output if you add or remove input/output information.

1. Boot the server to nPars mode.
2. Follow the steps in ["Launching the HP-UX Virtualization Manager" on the previous page](#) to display the HP-UX Virtual Servers window.
3. If the server is already displayed on the main page, the `ioscan` output has been saved.
4. If the server is not displayed, add the server to the main page (see ["Adding an HPVM Hypervisor/vPars Container" on page 89](#)).

The saved `ioscan` output can now be viewed at any time. However, if I/O on the server is added or removed, you must repeat steps 1 through 4 to refresh the `ioscan` output.

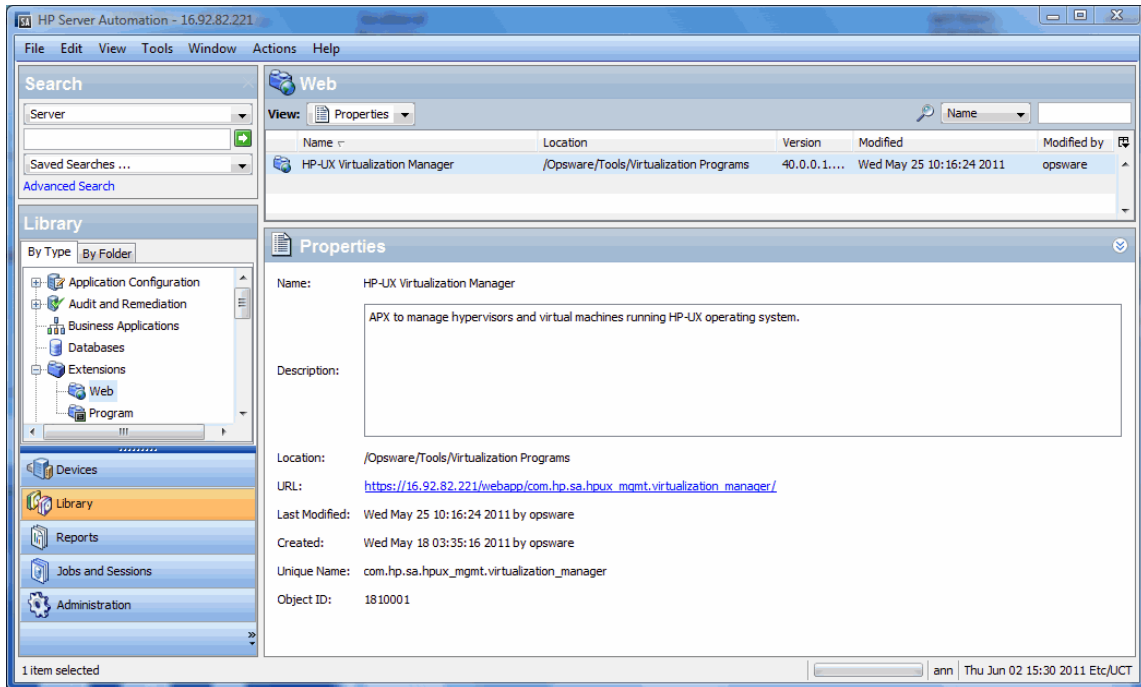
The `ioscan` output displayed in this view can also be used to simplify the creation and modification of vPars.

Viewing Summary, Hardware, and ioScan Information

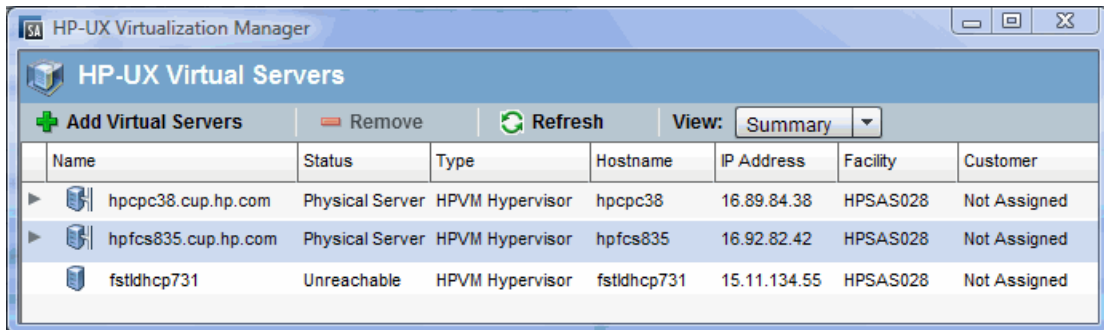
This section describes how to view information for HPVM hypervisors/vPars containers/HPVMs/vPars, and vSwitches.

To view information:

1. Follow the steps in ["Launching the HP-UX Virtualization Manager" on the previous page](#) to display the HP-UX Virtual Servers window (see the following figure).



2. Double-click HP-UX Virtualization Manager to display the HP-UX Virtual Servers window, which contains a list of HPVM hypervisors/vPars containers associated with that manager (see the following figure).



To view individual HPVMs/vPars/vSwitches, click the arrow to the left of the HPVM hypervisor/vPars container associated with that individual component (see the following table).

HPVM Hypervisor/vPars Containers/HPVMs/vPars/vSwitches Information

Property	Description
Name	Name, as designated when the HPVM hypervisor/vPars container was added to the HP-UX Virtualization Manager

Property	Description
Status	<p>Status (whether the HPVM hypervisor/vPars container is reachable from the SA Client core or not)</p> <p>Status = Unreachable or</p> <p>Status = vPars (for vPars mode); Physical Server (for nPars mode or HPVM)</p> <p>For individual vPars and vSwitches, status = Up/Down</p> <p>For individual HPVMs, status = On/Off</p>
Type	Whether the HPVM hypervisor or vPars container is running the vPars or HPVM software
Hostname	<p>Host name of:</p> <p>HPVM hypervisor or vPars container</p> <p>HPVM or vPars that has become a managed server in the SA Client</p> <p>Note: Host name = - (dash) if HPVM or vPars is not a managed server</p>
IP Address	<p>Individual HPVM hypervisor/vPars container /HPVM/vPars IP address</p> <p>Note: Value is blank if HPVM is not an SA-managed server</p>
Facility	Physical location of the HPVM hypervisor/vPars container host machine
Customer	Assigned customer

- To display summary information for a selected HPVM hypervisor/vPars container/HPVM/vPars/vSwitch, choose View > Summary and then select the HPVM hypervisor/vPars container/HPVM/vPars/vSwitch to display its summary information in the bottom summary panel (see the following figure).

HP-UX Virtual Servers							
+ Add Virtual Servers		- Remove		Refresh		View: Summary	
Name	Status	Type	Hostname	IP Address	Facility	Customer	
hpcpc38.cup.hp.com	Physical Server	HPVM Hypervisor	hpcpc38	16.89.84.38	HPSAS028	Not Assigned	
hpfc835.cup.hp.com	Physical Server	HPVM Hypervisor	hpfc835	16.92.82.42	HPSAS028	Not Assigned	
fstdhcp731	Unreachable	HPVM Hypervisor	fstdhcp731	15.11.134.55	HPSAS028	Not Assigned	

Summary	
ID:	350001
Status:	Physical Server
Lifecycle:	MANAGED
Manufacturer:	HP
Model:	IA64 HP SERVER RX6600
OS Version:	HP-UX 11.31
Serial:	USE4720HWW

Summary information includes:

Summary Information

Property	Description
ID	Identification number in the SA Client
Status	Status (whether the HPVM hypervisor/vPars container/HPVM/vPars/vSwitch is reachable from the SA Client core or not) Status = Unreachable or Status = vPars (for vPars mode); Physical Server (for nPars mode or HPVM) For individual vPars and vSwitches, status = Up/Down For individual HPVMs, status = On/Off
Lifecycle	Managed by the SA Client or not
Manufacturer	Name of the manufacturer
OS Version	Version
Serial	Serial number

To display hardware information for a selected HPVM hypervisor/vPars container/HPVMs/vPars, choose **View > Hardware** (see the following figure).

The screenshot shows the 'HP-UX Virtual Servers' management interface. At the top, there are buttons for 'Add Virtual Servers', 'Remove', and 'Refresh', along with a 'View:' dropdown menu set to 'Summary'. Below this is a table with columns: Name, Status, Type, Hostname, IP Address, Facility, and Customer. Three servers are listed: hpcpc38.cup.hp.com (Physical Server, HPVM Hypervisor, hpcpc38, 16.89.84.38, HPSAS028, Not Assigned), hpfc835.cup.hp.com (Physical Server, HPVM Hypervisor, hpfc835, 16.92.82.42, HPSAS028, Not Assigned), and fstldhcp731 (Unreachable, HPVM Hypervisor, fstldhcp731, 15.11.134.55, HPSAS028, Not Assigned). Below the table, a 'Hardware' section displays the following information:

Available CPUs:	8
Available CPU speed for a VM:	1595 MHZ
Total Physical Memory:	65504 MB
Available memory for a VM:	52228 MB
Model:	IA64 HP SERVER RX8600
OS Version:	HP-UX 11.31
Serial:	USE4720HWW

Hardware information includes:

HPVM Hypervisor Hardware Information

Property	Description
Available CPUs	Number of CPUs assigned
Available CPU speed for an HPVM	CPU speed available for HPVMs associated with that HPVM hypervisor/vPars container
Total Physical Memory	Total physical memory associated with the HPVM hypervisors/vPars container
Available memory for a HPVM	Memory available for a particular HPVM associated with the HPVM hypervisors/vPars container

vPars Container Hardware Information

Property	Description
Available CPUs	Number of CPUs assigned

Property	Description
Available Interleaved Memory	Amount of non-cached memory available to the vPars container
Available Cell - Memory	Amount of memory available per cell (series of comma-separated <cell number>:<memory size>)
Available Cell - CPU	Indicates the number of CPUs available per cell (a series of comma-separated <cell number>:<number of CPUs>)

vPars Hardware Information

Property	Description
Assigned CPUs	Number of CPUs assigned to vPars
Assigned Total Memory	Amount of assigned memory for vPars
Cell - CPU	Number of available cell CPUs
Cell - Memory	Amount of cell memory available
Primary Boot Disk	Name of the primary boot disk
Alternate Boot Disk	Name of the alternate boot disk
Number of Local Bus Adapter(s)	Number of local bus adapters for vPar
Local Bus Adapter(s)	Name of the local bus adapters

HPVM Hardware Information

Property	Description
Assigned CPUs	Number of CPUs assigned to HPVM
Assigned Memory	Amount of memory assigned to HPVM
Assigned vSwitches	vSwitches assigned to HPVM, in a list of comma-separated <port> - <HPVM> associated with the vSwitch
Assigned Storage	Amount of storage assigned to the HPVM

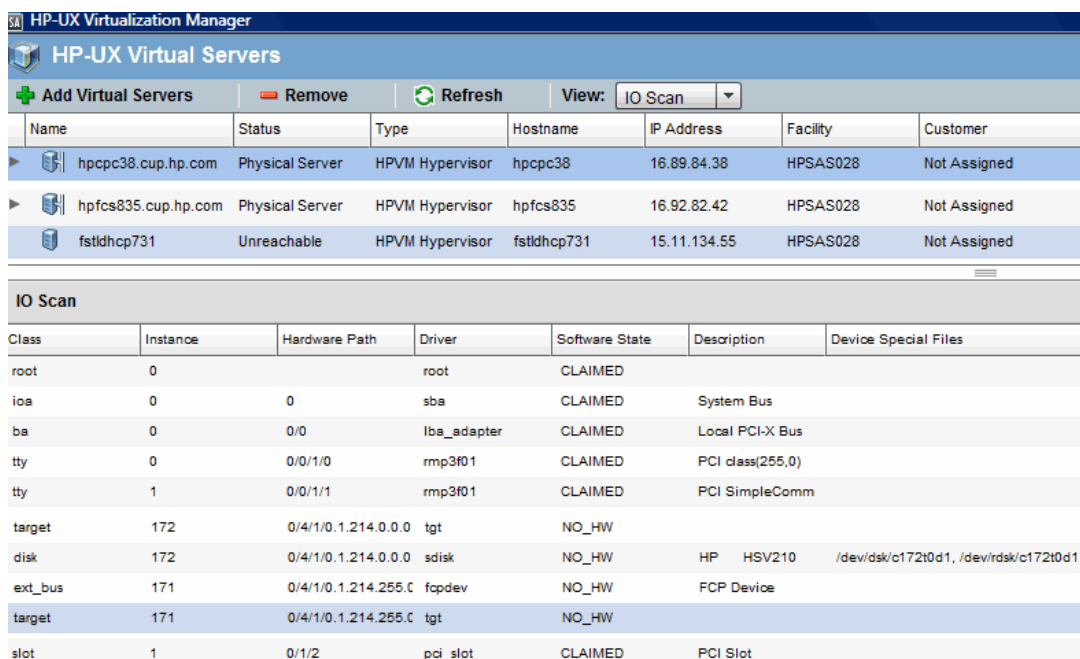
vSwitch Hardware Information

Property	Description
Assigned LAN interface	LAN interface assigned to the vSwitch
Assigned Ports	Ports assigned exclusively to the vSwitch

To display information about the devices connected to a selected HPVM hypervisors/vPars container/HPVM/vPars machine, such as storage, disk, memory, and processor information, choose View > IO Scan (see the figure below).

The IO Scan view shows the output from the HP-UX ioscan (1M) command for the selected vPars container or HPVM.

To rearrange ioScan output columns, drag and drop them. To sort by column, select the column header. To sort by additional columns, hold down the Ctrl key while selecting the column header.



IOscan information (which is applicable only to HPVM hypervisors and vPars containers) includes:

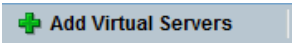
IO Scan Information

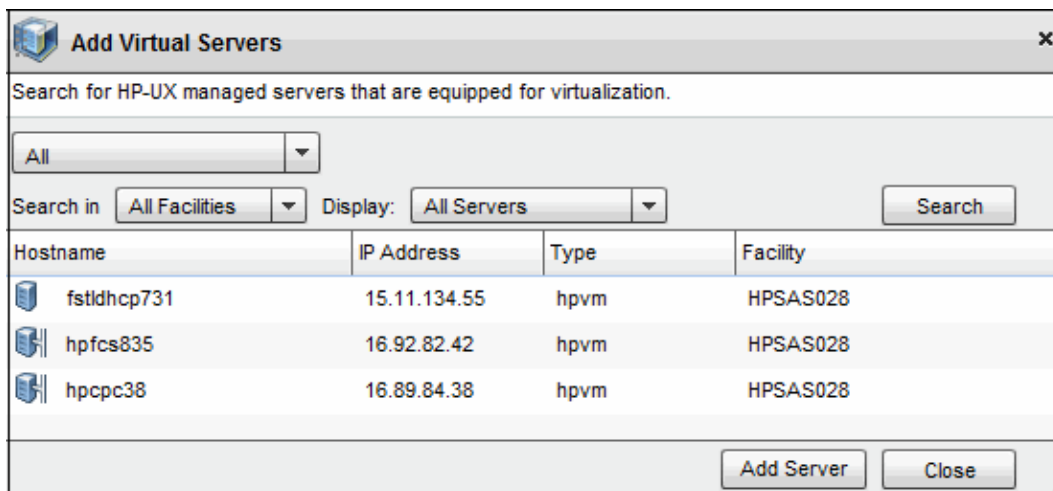
Property	Description
Class	Device class
Instance	Instance
Hardware Path	Hardware path to the device

Property	Description
Driver	Driver associated with the device
Software State (of devices attached to the machine)	CLAIMED = device software bound successfully NO-HW = device hardware is no longer responding
Description	Device description (for example, whether it is an adapter or processor)
Device Special Files	Device filename (as identified by the system)

Adding an HPVM Hypervisor/vPars Container

To add an HPVM hypervisor or vPars container to HP-UX Virtualization Manager management:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81 to display the HP-UX Virtual Servers window.
2. In the HP-UX Virtual Servers window, select the HPVM hypervisor to associate with the new HPVM.
3. Click . The Add Virtual Servers window is displayed (see below).



- In the Virtual Servers window, choose the following HPVM search criteria (you can use wild cards to search):

Add Virtual Servers Search

Field	Choice	Displays
Main field		
	All	All servers (including managed and virtual)
	Explicit IPs/Hostname	HPVM hypervisors by their IP address or host name
	Supply IP Address Range	HPVMs within an IP address range
Search in	All Facilities	HPVMs at all facilities
	<specific facility choice>	HPVMs at the specified facility
Display	Virtual Servers only	Only HPVMs
	All Servers	

- Click Search.
- In the results field, select the HPVM(s) to be added.
- Click Add Server to add the HPVM.
The new HPVM is added as a managed server in the list below its associated HPVM hypervisor/vPars container.

Configuring Server Timeouts

SA verifies connectivity with HP-UX virtual servers by pinging them. If a server is offline, the ping will time out, and the server will be considered offline. By default, the ping timeout value is 15 seconds. You can reduce the ping timeout and improve responsiveness on networks with low latency by setting the value of the custom attribute `hpux_v12n_timeout`.

You can configure the timeout value by setting a custom attribute named `hpux_v12n_timeout`. The default value is 15 seconds. You can set it to any integer from 1 to 120.

For each server, SA searches the following objects in order for the custom attribute:

1. Server
2. Device group
3. Customer
4. Realm
5. Facility
6. OS
7. Software policy

For example, if you add the `hpux_v12n_timeout` custom attribute to the device group named “HP-UX 11.31,” all HP-UX 11.31 servers inherit that timeout value unless the custom attribute is set explicitly at the server level.

To change the timeout value for all the servers that reside in a particular facility, add the custom attribute to that facility.

For more information on custom attributes, see the SA User Guide: Server Automation.

Custom Attributes that HP-UX Virtualization Manager Creates

The HP-UX Virtualization Manager creates the custom attributes shown below for internal management:

HP-UX Virtualization Manager Custom Attributes

vPars/HPVM	Attribute	Value	Description
vPars	<code>ioscan</code>	String (JSON format)	<code>ioscan</code> command output (enables server to be displayed in vPars mode)
vPars	<code>nPar</code>	True	True = server reboots while in nPars mode
vPars HPVM	<code>partition_</code> <code>ident:</code> <code><value></code>	True	Partition identifier (identifies which servers are on the same partition)

vPars/HPVM	Attribute	Value	Description
vPars	sa_vPars_hypervisor	True	True = server displayed on the HP-UX Virtualization Manager main page
vPars	vpar_name	String	Server's vPars name.

Managing vPars Containers

You can only create, use, and manage vPars containers on managed servers. See the SA User Guide: Server Automation for instructions on how to make a server a managed SA server.

Your HP-UX server must be in nPars mode or in vPars mode to use the HP-UX Virtualization Manager. You must use HP-UX commands and tools to switch between nPars mode and vPars mode. For more information, see the HP-UX Virtual Partitions documentation.

The following sections describe how to manage HP-UX virtual partitions. You can perform any of these operations on any vPars as long as at least one vPar in the vPar container is a managed server and is online.

Switching between nPars and vPars modes

To switch between nPars and vPars from the HP-UX shell:

Set the mode for the next nPartition reboot:

```
# vparenv [-m mode]
```

where mode has the value of either vPars or nPars. This action might take a few minutes to process.

For example:

1. Set the mode:


```
# vparenv -m vPars
```
2. Manually reboot the nPartition:


```
# shutdown -r
```

...

```
Shell> fs0:
```

```
fs0:\> hpux/stand/vpmon
```

...

MON>

To switch between nPars and vPars from the vPars monitor:

Reboot the nPartition into the *mode* mode:

```
reboot [mode]
```

where mode is either vPars or nPars.

If any virtual partitions are up, issuing this command causes them to be shut down ungracefully.

To switch from the EFI, issue the following command:

```
Shell> fs0:
```

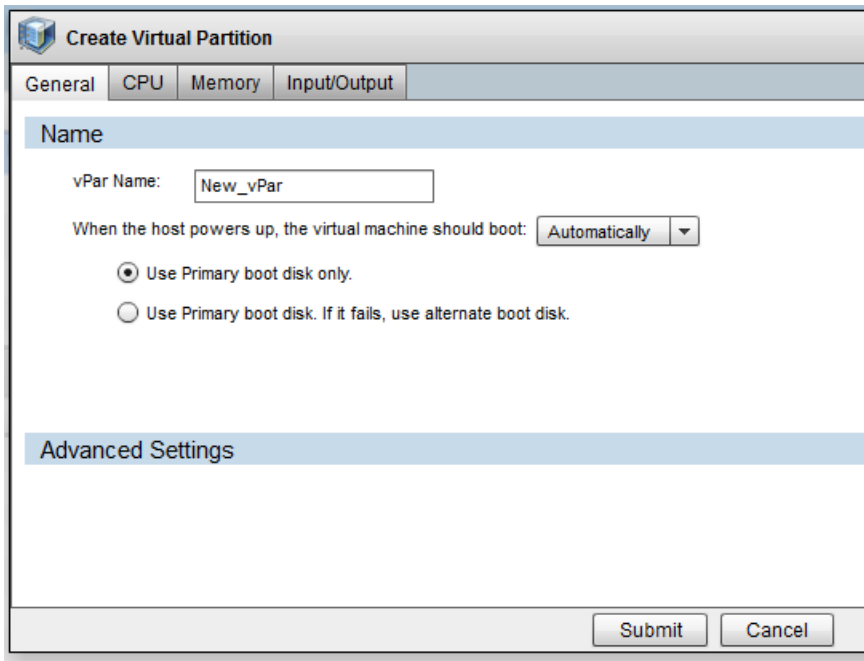
```
fs0:\. vparconfig reboot [mode]
```

where mode is either vPars or nPars.

Creating a vPar

To create an HP-UX vPars virtual partition:

1. Run the HP-UX Virtualization Manager as described in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. Select an HP-UX server that is a vPars Container.
3. Right-click on the HP-UX server, and select Create vPar. This displays the Create Virtual Partition window (see below).



4. Select the General tab, and enter the vPars General settings:

vPars General Settings

Property	Description
vPars name	Name, as designated when the vPars container was added to the HP-UX Virtualization Manager
vPar Boot Disk Setting	Setting to automatically or manually boot the disk Use the primary boot only or have alternate boot available.
Advanced Settings - Kernel path and Kernel Boot Options	Full kernel path and kernel boot options (optional)

5. Select the CPU tab, and enter the CPU settings:

vPars CPU Settings

Property	Description
CPU	<p>Number of CPUs to be allocated to the vPars</p> <p>If the server is in nPars mode, the total available CPUs, remaining CPUs, number of cells and the default maximum number of CPUs are unknown.</p> <p>The number of allocated CPUs must fall within the 'CPU Minimum'/'CPU Maximum' range.</p> <p>A total of 16 cells will always be displayed in the table.</p>
Minimum Number of CPUs	Minimum number of CPUs to allocate to the vPars
Maximum Number of CPUs	Maximum number of CPUs to allocate to the vPars (default: 256)

Select the Memory tab, and enter the memory settings:

vPars Memory Settings

Property	Description
Base Memory	<p>Amount of base memory to allocate to the vPars</p> <p>If the server is in nPars mode, the Remaining Available memory and the number of cells are unknown.</p> <p>A total of 16 cells will always be displayed in the table.</p>
Floating Memory	Amount of floating memory to allocate to the vPars
Cell Local Memory	Amount of cell local memory to allocate to the first vPars (optional)
Inter Leaved Memory	Amount of inter-leaved memory to allocate to the first vPars (optional)

Select the Input/Output tab, and set the I/O settings for the vPar:

vPars Input/Output Settings

Property	Description
Primary boot disk	Path to the primary boot disk (You must type in the full hardware path of the disk or logical box [LBA].)
Alternate boot disk	Path to the alternate boot disk (optional) (You must type in the full hardware path of the disk or logical box [LBA])
Local bus adapter	Name of the local bus adapter
Advanced setting: Kernel Path	Kernel path
Advanced setting: Kernel Boot	Kernel boot options

If ioScan data is not available, the Available Hardware Inventory panel will be blank.

- Click Submit to create the vPar virtual partition.

Modifying a vPar

To modify a vPar, right-click on a vPar and select Modify vPar. The Modify vPar window is generally the same as the Create vPar, except the current values of the vPar are filled in, and the memory and I/O settings cannot be modified if the vPar's status is Up.

Note: This APX will make multiple calls to the `vparmodify` command to modify the vPar as needed. So, although the `vparmodify` command has restrictions on the number of things that can be modified per command invocation, this APX does not.

Starting a vPar

To start a vPar, right-click on the vPar and select Start vPar. (Starting a vPar invokes the `vparboot` command, which always attempts to boot an OS from the primary boot disk regardless of the autoboot settings.)

Shutting Down a vPar

To shut down a vPar gracefully, right-click the vPar and select Shutdown vPar. This runs the HP-UX shutdown (1M) command on the vPar. This operation is only available when the vPar is an SA

managed server, and the status is Up.

Halting a vPar

To halt a vPar forcefully, right-click the vPar and select Halt vPar. This runs the HP-UX `vparreset -f -h` command to halt the vPar. This operation is only available when the vPar status is Up.

Deleting a vPar

A vPar that is not in Up status can be deleted. To delete a vPar, right-click on the vPar and select Delete vPar. This option is also available on the right-click menu of a vPar.

Managing HPVM Hypervisors

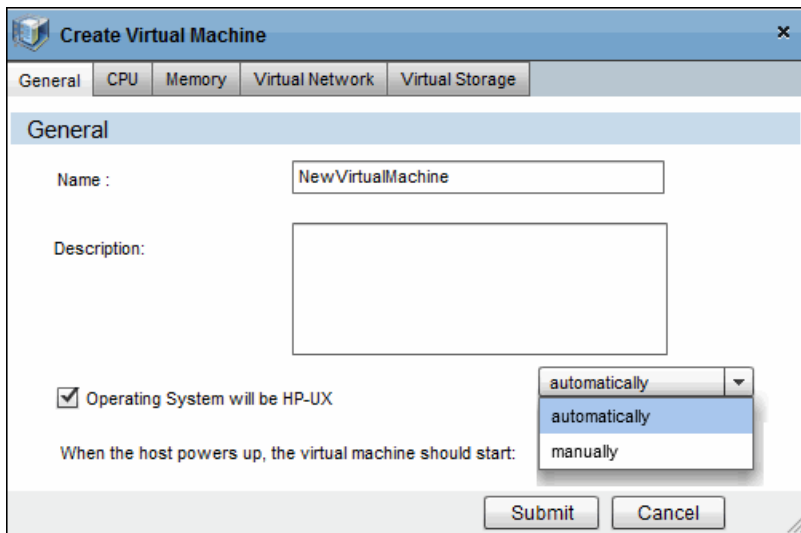
This section describes how to create, add, delete, and modify HPVM hypervisors and HPVMs using the HP-UX Virtualization Manager.

To manage HPVMs using the web extension, the HPVM host must be a managed server in Server Automation. For instructions on how to convert HPVMs into managed servers, see the SA User Guide: Server Automation.

Creating an HPVM

To create an HPVM:


1. Follow the instructions in ["Launching the HP-UX Virtualization Manager" on page 81](#).
2. In the HP-UX Virtual Servers window, right-click an HPVM hypervisor.
3. Choose Create VM to display the Create Virtual Machine window (see below).




4. Enter the following information for the new HPVM. You can create a new HPVM simply by entering a name and accepting the defaults:

Create VM

Tab and Section	Field or Button	Choice	Description and Default Setting
General			
General	Name		HPVM name (Can include up to 256 upper or lower case alphanumeric characters; dash (—); underscore (_), and period (.)) Note: Cannot start with a dash (Required) Default: NewVirtualMachine.
	Description		HPVM description. (Can include up to 256 upper or lower case alphanumeric characters; dash (—); underscore (_), and period (.))

Tab and Section	Field or Button	Choice	Description and Default Setting
	Operating System will be HP-UX		Whether the HP-UX operating system be installed on this VM Note: Installing the HP-UX operating system is not part of creating an HPVM. Default: Not selected.
	When the host machine powers up, the HPVM should start:	Automatically	Starts when host powers up Default: Automatically.
		Manually	Start HPVM manually
CPU			
Desired CPUs	Number of CPUs	1 - 256	Number of CPUs dedicated to the HPVM Default: 1
Entitlement (click  to display choices)	Specify Processing Power	%Utilization: Minimum Maximum	% of each CPU to be used for the HPVM % Utilization maximum must be >= % utilization minimum Defaults: Minimum: 10; Maximum: 100
		CPU Cycles Minimum Maximum	Number of CPU cycles (Megahertz or Gigahertz)
Memory			
Desired Memory	Memory		MegaBytes (MB) of memory allocated to HPVM Default: 512

Tab and Section	Field or Button	Choice	Description and Default Setting
Dynamic Memory Control (click  to display choices)	Use dynamic memory control		Required: Checked Dynamic Memory Control box Default: Disabled
	Initial Target Memory Size		Initial memory that dynamic memory driver tries to access when guest starts Required: Checked Dynamic Memory Control box
	Minimum Memory Size		Minimum memory available to be dynamically allocated to guest Required: Checked Dynamic Memory Control box
	Maximum Memory Size		Maximum memory available to be dynamically allocated to guest Required: Checked Dynamic Memory Control box
Virtual Networks			List of vSwitches associated with HPVM
Defined Virtual Network - Add Virtual Switch (click Add Virtual Switch to display choices)			vSwitch information for existing vSwitches
	Network Adapter Type	LAN AVIO-LAN	LAN or AVIO-LAN to associate with the vSwitch Default: LAN

Tab and Section	Field or Button	Choice	Description and Default Setting
	Network Interface Card	Any available PCI Bus (0 - 7) PCI Device (0-7)	Type of interface card to associate with the vSwitch Default: Any available PCI bus or device (recommended choice)
	Select a vSwitch		vSwitches available to associate with the HPVM Note: Select the switch and click Done to add the switch to the list.

5. Click Submit to create the HPVM and add it to the list.

Modifying HPVMs

To modify HPVM information:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. In the HP-UX Virtual Servers window, right-click an HPVM.
3. Choose Modify VM.
4. Change HPVM settings (see "[Creating an HPVM](#)" on page 97 for more information on the settings).

Note: Modify VM has a setting that is not available in the Creating HPVM function:

Advance Settings > Forced Configuration.

Choosing this setting will force the system to make configuration changes and suppress all resource conflict checks and associated warning messages.

Note: If you choose this setting, there will be no notification of potential resource problems for a virtual machine that is modified with this option.

5. Click Submit to save the modifications.

Starting an HPVM

To start an HPVM:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. In the HP-UX Virtual Servers window, right-click an HPVM.
3. Choose Start VM.

For information about operating system installation, go to the *HP Integrity Virtual Machines Installation, Configuration, Administration Guide* at: <http://docs.hp.com/hpux/11iv3>, then choose: HP Virtualization Software > HP Integrity Virtual Machines and Online VM Migration.

Halting an HPVM

To halt an HPVM:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. In the HP-UX Virtual Servers window, right-click an HPVM.
3. Choose Halt VM.

Halting an HPVM temporarily stops it from performing its functions and allows the manager to reallocate resources assigned to it.

Shutting Down an HPVM

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. In the HP-UX Virtual Servers window, right-click an HPVM.
3. Choose Shutdown HPVM.
Choosing shutdown means that the HPVM shuts down within 30 seconds. If the time-out period expires before the shutdown occurs, a hard stop occurs.

Note: Shutting down an HPVM takes the machine offline and allows the manager to reallocate resources assigned to it.

Removing or Deleting an HPVM

1. To remove or delete an HPVM from HP-UX Virtualization Manager control:
2. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
3. In the HP-UX Virtual Servers window, right-click an HPVMs to delete.
4. Choose Delete VM, and click OK when asked to confirm the deletion.
5. The HPVM is removed from the list of managed servers.

Managing vSwitches

This section describes how to create, modify, and delete a vSwitch.

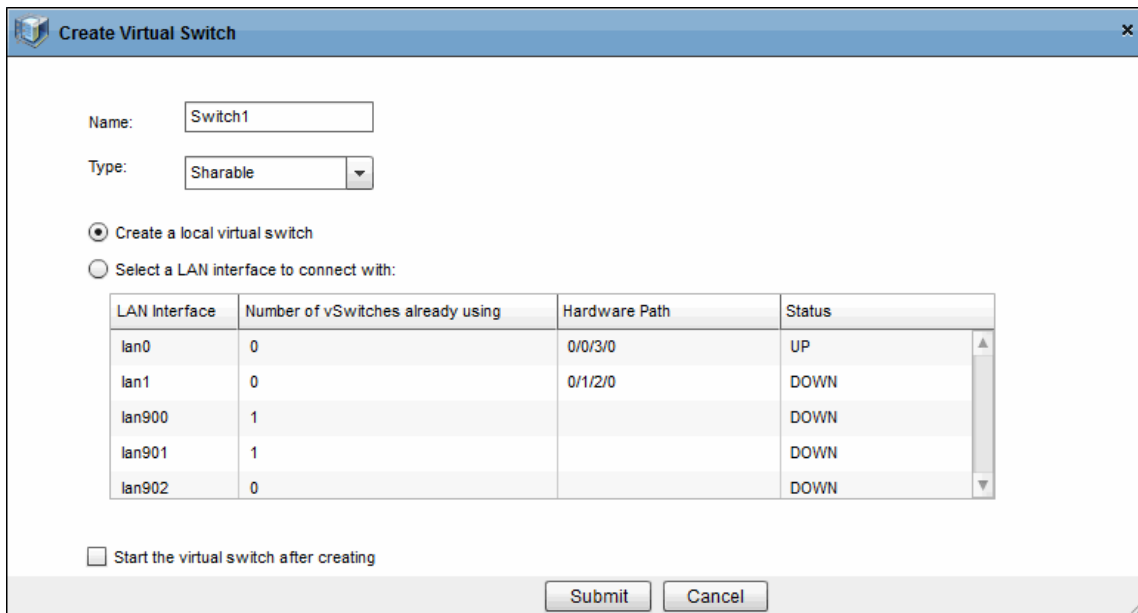
HP-UX Virtualization Manager manages vSwitches. To view HPVM/vSwitch settings, go to the *HP Integrity Virtual Machines Installation, Configuration, Administration Guide* at:

<http://docs.hp.com/hpux/11iv3>, then choose: HP Virtualization Software > HP Integrity Virtual Machines and Online VM Migration. For instructions on how to configure LANs and VLANs, see LAN/VLAN documentation.

Creating a vSwitch

To create a vSwitch:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. In the HP-UX Virtual Servers window, right-click an HPVM hypervisor.
3. Choose Create vSwitch to display the Create vSwitch window (see below).



4. Enter the following information for the new vSwitch:

Create vSwitch

Field/Button	Description
Name	Choose a name for the vSwitch that does not exceed eight (8) characters. Default: Switch1
Type	Sharable (shared with other HPVMs) or dedicated (associated only with this HPVM) Default: Shareable
Create a local virtual switch, OR Select a LAN interface to connect to (must select the LAN from the list)	Local switch that is not connected to another device. LAN to connect to (Default)
Start the virtual switch after creating	Starts the vSwitch immediately after it is created. Default: Not selected

Modifying a vSwitch

To modify vSwitch information:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81 to access the HP-UX Virtual Servers window.
2. In the HP-UX Virtual Servers window, right-click a vSwitch.
3. Choose Modify vSwitch.
4. Change vSwitch settings.
The fields that cannot be modified will not be enabled.

Starting a vSwitch

To start a vSwitch:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81 to access the HP-UX Virtual Servers window.
2. In the HP-UX Virtual Servers window, right-click a vSwitch.
3. Choose Start vSwitch.

Stopping a vSwitch

To stop or halt a vSwitch:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81 to access the HP-UX Virtual Servers window.
2. In the HP-UX Virtual Servers window, right-click a vSwitch.
3. Choose Stop vSwitch.

Halting or stopping a vSwitch temporarily stops it from performing its functions and allows the manager to reallocate resources assigned to it.

Deleting a vSwitch

To delete a vSwitch from HP-UX Virtualization Manager control:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81 to access the HP-UX Virtual Servers window.

2. In the HP-UX Virtual Servers window, right-click a vSwitch to delete.
3. Choose Delete vSwitch, and click OK when asked to confirm the deletion.

Configuring VLAN Connections

To configure VLAN connections:

1. Follow the instructions in "[Launching the HP-UX Virtualization Manager](#)" on page 81.
2. In the HP-UX Virtual Servers window, right-click a vSwitch.
3. Choose Configure VLAN.
4. For each HPVM, choose the corresponding VLAN ID.

Troubleshooting Issues

Problem: The HP-UX Virtualization Manager extension is not displayed in the SA Library.

- Make sure your user has permission to view and execute the web extension. For details, see "[Folder Permissions Required](#)" on page 79.

Problem: When adding virtual servers, an HP-UX server does not appear in the search results. Or, when searching all servers, the server displays, but when searching for specific IP addresses, it does not.

- Set the Display drop-down list to All Servers, and search again.
- Ensure the server is a managed server. For more information, see the SA User Guide: Server Automation.
- Perform a hardware registration. On the managed server, run the following SA command:
`/opt/opsware/agent/pylibs/cog/bs_hardware`

Problem: When adding virtual servers, a particular server only shows in the results when display is set to All Servers.

- Ensure either Virtual Partition or HP VM software is installed on the server
- Perform a software registration. On the managed server, run the following SA command:
`/opt/opsware/agent/pylibs/cog/bs_software`

Problem: The Summary view for a server does not display all information about the server.

- If the server is not managed by SA, some information may not be displayed. Bring the server under SA management. For instructions, see the SA User Guide: Server Automation.
- If the server is a managed server, perform a hardware registration. On the managed server, run the following SA command:
`/opt/opsware/agent/pylibs/cog/bs_hardware`

Checking Log Files

Log files are stored in the user's `/tmp` directory in the Global File System (OGFS). To access them, log in to the OGSH and change directory to `/tmp`.

The name of the log file for HP-UX virtualization is `hpuxvirtlog`. This is a rotating log file, so over time you will see `hpuxvirtlog.1` and `hpuxvirtlog.2` up to a maximum of 3 log files. The current log file is always `hpuxvirtlog`. The file rotates when the size reaches 5Mb.

The log file shows informative messages, warnings, and errors. The informative messages show the vPars and HP VM commands that are executed on the managed servers.

Nearly all errors and warnings are displayed in the HP-UX Virtualization manager, so checking the log files is usually not necessary.

Example Log Messages

Here are example log messages:

```
2011-05-31 10:53:59 INFO HPUX-V12N(127): Requested operation: modify_virtual_
machine
```

```
2011-05-31 10:54:00 INFO HPUX-V12N.vpar(416): dhcp-184-241: scanning
```

```
2011-05-31 10:54:03 INFO HPUX-V12N.vpar(462): /usr/sbin/vparmodify -p vpar2 -m
cell:1:cpu::1
```

```
Returned: 0
```

```
2011-05-31 10:54:03 INFO HPUX-V12N.vpar(462): /usr/sbin/vparmodify -p vpar2 -B
search
```

Returned: 0

The messages include the date, time, log level (INFO), module (HPUX-V12N and HPUX-V12N.vpar), and the message text. The lines above show a modify operation performed on a vPar (vpar2). The modify commands were executed on server dhcp-184-241 and both commands returned 0, meaning they were successful.

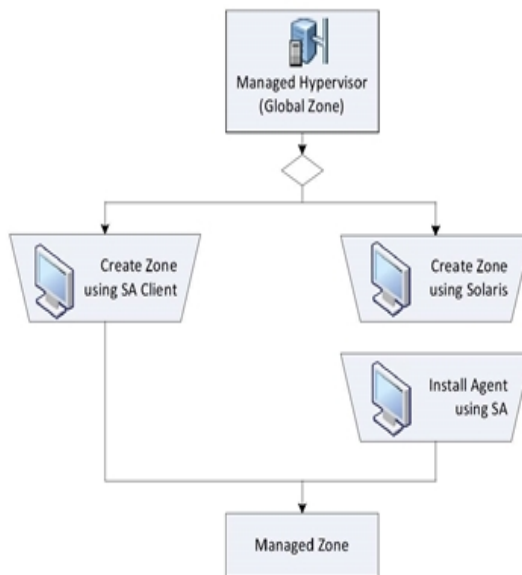
Chapter 8: Managing Oracle Solaris Zones

This section describes how to manage Oracle Solaris Zones with the SA Client.

To perform any of these tasks, the zone must be reachable by SA.

OS Provisioning and Agent Installation for Oracle Solaris Zones

The following figure shows the process for creating a non-global zone and bringing it under Agent management by SA. You can create a zone using either the SA Client or the Solaris commands. When you use the SA Client to create a zone, SA also installs an Agent on the zone, which allows you to manage the zone using SA.



To find out more about the tasks shown in the above figure, see the documentation referenced in the following table.

Documentation for Zone OS Provisioning and Agent Installation

Task Shown In Previous Figure	Where to Get More Information
Create a Zone using the SA Client	"Creating a Zone" below
Create a Zone using Solaris	Solaris documentation
Install an Agent using the SA Client	"Installing an Agent on an Existing Unmanaged Non-Global Zone" on page 113

Creating a Zone

The SA Client enables you to create a fully operable, non-global zone on a Solaris global zone (hypervisor).

Before a non-global zone can be created with the SA Client for the first time, the global zone's hardware must be registered with SA. The hardware registration must occur each time the hardware from the Solaris machine is updated (e.g., when a network interface is added or removed). Creating a non-global zone also installs an Agent on the zone, bringing the zone under Agent management by SA. After Agent installation, the non-global zone appears in the **All Managed Servers** and the **Virtual Servers** lists in the SA Client.

To create a non-global zone:

1. In the SA Client, from the navigation pane, select the **Devices** tab.
2. Expand **Servers** and select **Oracle Solaris Zones**.
3. In the content pane, right-click the global zone that will host the new zone, and select **Oracle Solaris Zones > Create Zone**.
4. In the Zone Definition Method step of the Create Virtual Zone window, select one of the following methods:
 - **Manual (Fill out data form)**: Using this method, you must manually enter the zone configuration parameters in the fields provided on the Zone Definition dialog.
 - **Zone Creation Command Script**: Using this method, you provide a command script that contains the zone creation and configuration commands. When using a script, if IPv6 addresses are provided, then the local link addresses also need to be specified (Solaris does not generate them).

The local link addresses provided as part of the script will not be visible in the modify step and cannot be updated. This command script has the same syntax as the *command_file* specified by the following Solaris command:

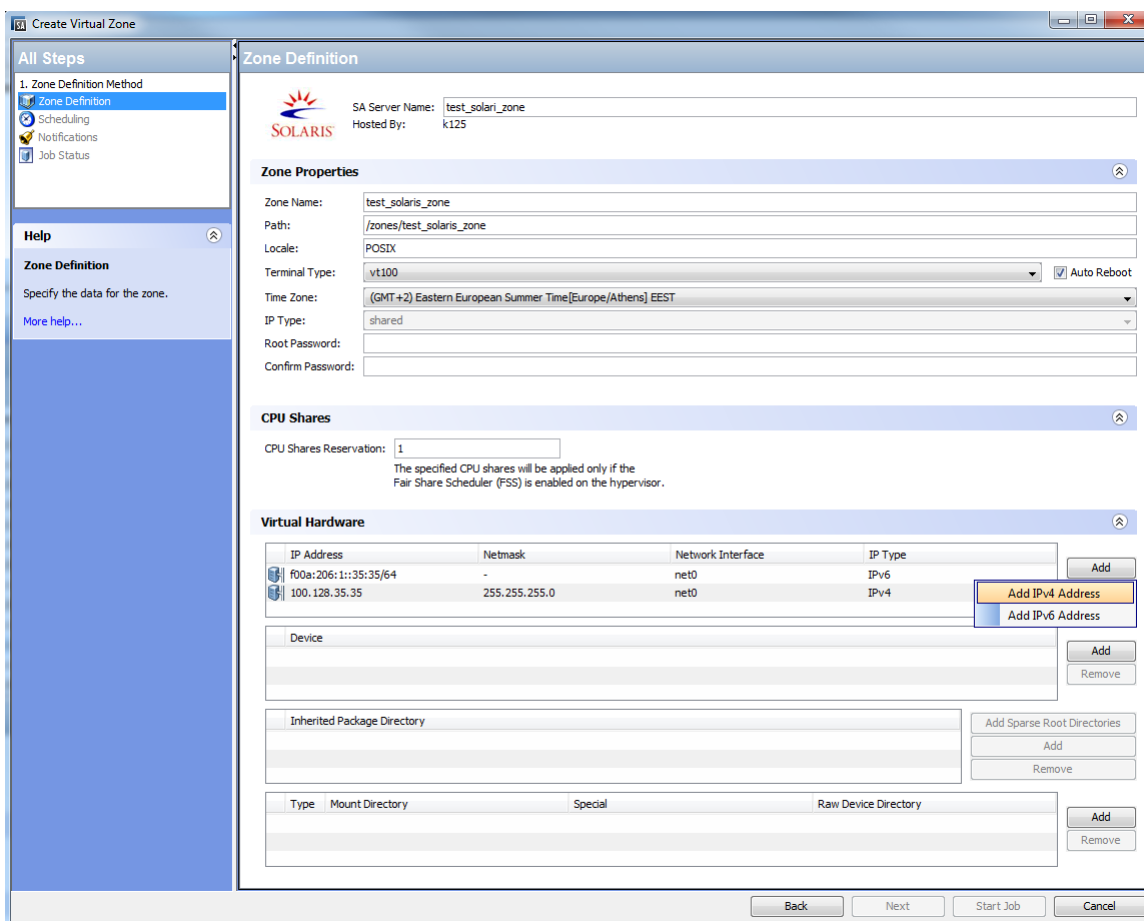
```
zonectfg -z zone_name -f command_file
```

SA does not validate the contents of the zone creation command script, so ensure that your script works. For the syntax of the commands allowed in the script, see the Solaris 10/Solaris 11 documentation on `zonectfg`.

5. Click **Next** to proceed to the Zone Definition step.
6. If you are using a Zone Creation Command script, skip to **step 7**. If you chose the manual method in **step 4** above, complete the following fields:
 - **Server**: Enter the SA server name for the new virtual server. (The global zone (hypervisor) that will host the new non-global zone is displayed below this field.)
 - **Zone Name**: Enter an appropriate name for the new non-global zone.
 - **Locale**: Enter the language code for the non-global zone.
 - **Terminal Type**: Specify the terminal client that the SA Client uses for Remote Terminal sessions on the non-global zone.
 - **Auto Reboot**: Specifies whether to automatically reboot the non-global zone if the physical server running the hosting Global zone is rebooted.
 - **Time Zone**: Specify a time zone for the non-global zone.
 - **Root Password**: Enter the root password for the non-global zone.
 - **Confirm Password**: Enter the root password again for verification.
 - **CPU Shares Reservation**: Enter an integer that allocates the shares of the CPU resource.

For the CPU Shares Reservation to take effect, the Fair Share Scheduler (FSS) must be enabled on the Solaris hypervisor server on which you are creating the new zone. By default, the FSS is not enabled.

- IP Address:** It is possible to add IPv4 and IPv6 addresses (as shown in the following figure):



- If you add an IPv4 address, enter the IP address and select the virtual network interface. A zone that requires network connectivity must have one or more dedicated IP addresses. These addresses are associated with the physical network interface of the global zone.
- If you add an IPv6 address, the default prefix (64) is added at the end of the address, provided that no valid prefix (an integer between 1 and 128) has been given. In this case, the *netmask* value is set to null by default and cannot be changed.

For IPv6, one does not need to manually add the local-link addresses, as they are generated by SA.

- Device:** (Optional) Click **Add** to enter a path name to a device, for example, `/dev/pts*`, on the global zone hypervisor. This action gives the new zone access to a device on the global zone.

- **Inherited Package Directory:** (Optional) Click Add to enter a path name to the package directory you want the zone to inherit. These package directories are read-only. Or, click **Add Sparse Root Directory** to enter a default package directory inherited by the new zone from the global zone.

The **Add Sparse Root Directory** is disabled in Solaris 11. See Solaris 11 documentation for further details.

- **Mount Directory:** (Optional) Click Add to mount a file system type and path for the zone. This action grants the zone access to a physical disk or file system of the non-global zone. A `ufs` file system creates a file system mount within the zone; the `lofs` type is a loopback file system mount to the global zone.
7. If you are using a Zone Creation Command Script, you will see the Zone Configuration Commands section. Here you can manually enter the contents of the zone creation command script, cut-and-paste from another file, or select **Import File** to import the script directly from another file, then select **Next**.
 8. **Scheduling:** Select when you want the create zone job to run, then select **Next**.
 9. **Notifications:** Enter email addresses to receive notifications when the job finishes. Select the type of notifications you want. Optionally enter a ticket identifier to be associated with the job, then select **Next**.
 10. **Job Status:** Select the **Start Job** or **Schedule Job** button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the **Jobs and Sessions** tab.
When the job runs, it creates the zone and displays the results.

Installing an Agent on an Existing Unmanaged Non-Global Zone

To bring a zone under agent management by SA, you must first install an SA Server Agent. Before installing an Agent, verify that the following requirements are met:

- The non-global zone is running.

- All *services* on the non-global zone are up and running. If they are not, the zone may not have the necessary `sysconfig` information that is provided when the non-global zone is booted for the first time. See the Sun Solaris 10/Solaris 11 documentation on zone configuration for more information.

You can install an Agent on an unmanaged Oracle Solaris Zone in two ways:

- Using SA as described in “Installing and Managing User Agents” in the *SA User Guide: Server Automation*.
- Using the SA zone management interface.

To install an Agent on an unmanaged non-global zone through the SA zone management interface:

1. In the navigation pane, select **Devices**.
2. Expand **Servers**, and then select **Oracle Solaris Zones**.
3. In the content pane, expand the Global zone that hosts the unmanaged non-global zone you want to modify.
4. Right-click the non-global zone and select **Oracle Solaris Zones > Install Agent**.

Modifying a Non-Global Zone

You can modify a subset of the zone parameters that were defined when you created the non-global zone. For example, if an HTTP server running on a zone is sluggish because of increased usage, you can increase the CPU Share Reservation parameter for the zone. After you modify a zone with the SA Client, the zone is automatically restarted.

To modify the parameters of a non-global zone:

1. In the SA Client, from the navigation pane, select the **Devices** tab.
2. Expand Servers and select **Oracle Solaris Zones**.
3. In the content pane, expand the global zone that hosts the zone you want to modify.
4. Right-click the non-global zone and select **Oracle Solaris Zones > Modify Zone**.
The Modify Virtual Zone window appears. In the Zone Definition step of the Modify Virtual window, edit the parameters you want to change, then select **Next**.

Link-link addresses are not visible in the IP list for the **Modify** action. After zone creation, these addresses are managed by SA.

5. **Scheduling:** Select when you want the modify zone job to run, then select **Next**.
6. **Notifications:** Enter email addresses to receive notifications when the job finishes. Select the type of notifications you want. Optionally enter a ticket identifier to be associated with the job, then select **Next**.
7. **Job Status:** Select the **Start Job** or **Schedule Job** button. This runs the job or schedules it to be run in the future and displays the Job ID number in the window banner. You can use the Job ID number to look up the job under the **Jobs and Sessions** tab.
When the job runs, it modifies and restarts the zone and displays the results.

Starting or Stopping a Non-Global Zone

1. In the navigation pane, select the **Devices** tab.
2. Expand **Servers** and select **Oracle Solaris Zones**.
3. In the content pane, expand the global zone that hosts the non-global zone.
4. Right-click the zone and select **Oracle Solaris Zones > Start Zone** or **Stop Zone**.
Or
5. In the **Oracle Solaris Zones** list, open the hypervisor. In the **Virtualization** view, select the zone and click either **Start** or **Stop**.

Note: If a non-global zone is not running, the state displayed is **Installed**.

Deleting a Non-Global Zone

This action deletes the non-global zone permanently and removes it from the SA.

1. In the SA Client, from the navigation pane, select the **Devices** tab.
2. Expand **Servers** and select **Oracle Solaris Zones**.
3. In the content pane, expand the global zone that hosts the zone you want to delete.

4. Right-click the non-global zone and select **Oracle Solaris Zones > Remove Zone**. This action is available only if the **Zone** is stopped.

Reloading Oracle Solaris Zone Information

Because Oracle Solaris Zones can be created and managed outside of SA, SA automatically reloads the virtual server information every 24 hours.

To reload Oracle Solaris Zone information manually:

1. In the SA Client navigation pane, select the **Devices** tab, then select **Servers > Oracle Solaris Zones**. This action displays all your Oracle Solaris Zones being managed by SA.
2. Locate the hypervisor whose information you want to reload. Right-click or select the **Actions** menu and select **Oracle Solaris Zones > Reload Data**.

Chapter 9: Genealogy of VMs

This chapter describes the Genealogy of VMs. SA records how a VM or a VM template was created. This information can be used to discover all VMs and VM templates that are created from a given source; that is, the VM or VM template's genealogy.

The VM or VM template for which we invoke the Show Genealogy Tree action is the source VM or VM template. A VM or VM template derived from the source VM or VM template is created from the source VM or VM template, or from one of its descendants.

Genealogy in SA provides:

- Complete visibility on VMs and VM templates that have the same parent.
- A group view of all related VMs and VM templates, without having to perform additional searches or operations.
- Remediation for descendant VMs and VM templates when the parent VM or VM template is updated.
- The ability to perform actions such as power control and patch or software management on a group of related VMs and VM templates.

Overview

The **Genealogy** window allows you to manage the VMs and VM templates derived from a selected source.

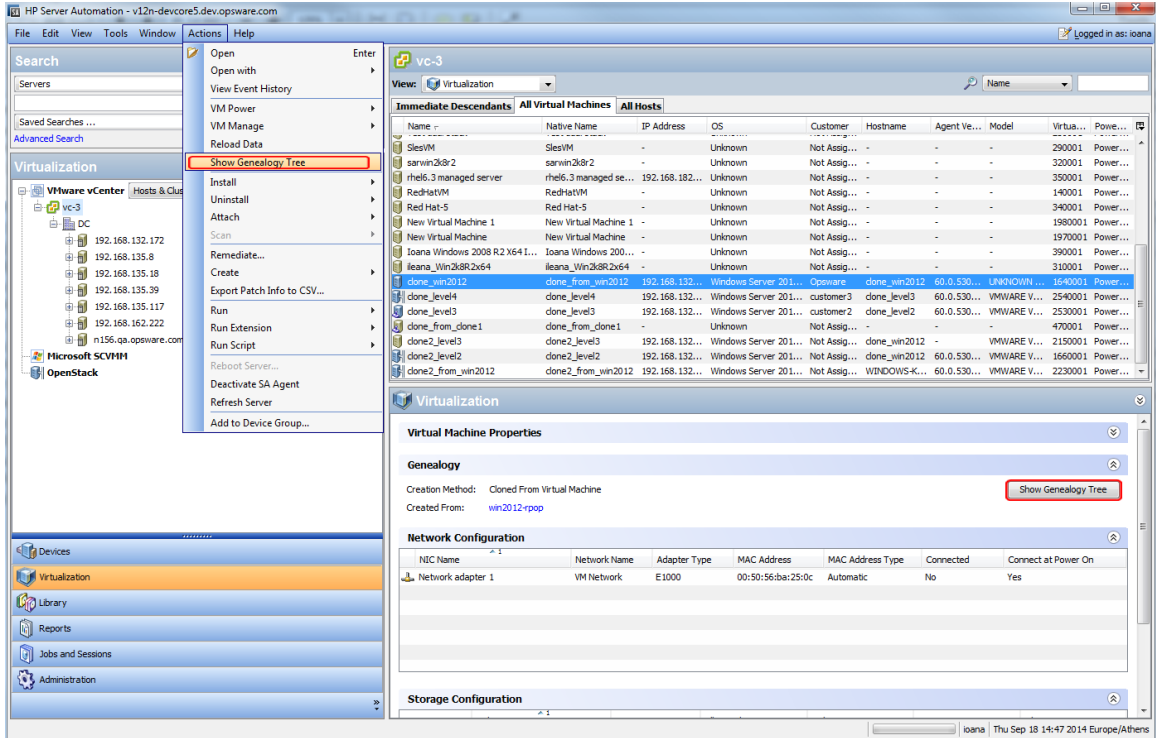
How to Start Genealogy for a VM or Template

To start the Genealogy window, navigate to the Virtualization tab in the SA Client. Choose a Virtualization Service from the left tree. From the **Immediate Descendants** or **All Virtual Machines** tab, select a VM or a VM template. For the selected VM or VM template, launch Genealogy from any of the following options:

1. The **Show Genealogy Tree** option from the **Actions** menu (see **Figure 1**).
2. Select **Virtualization from View**. Under Genealogy, press the Show Genealogy Tree button (see

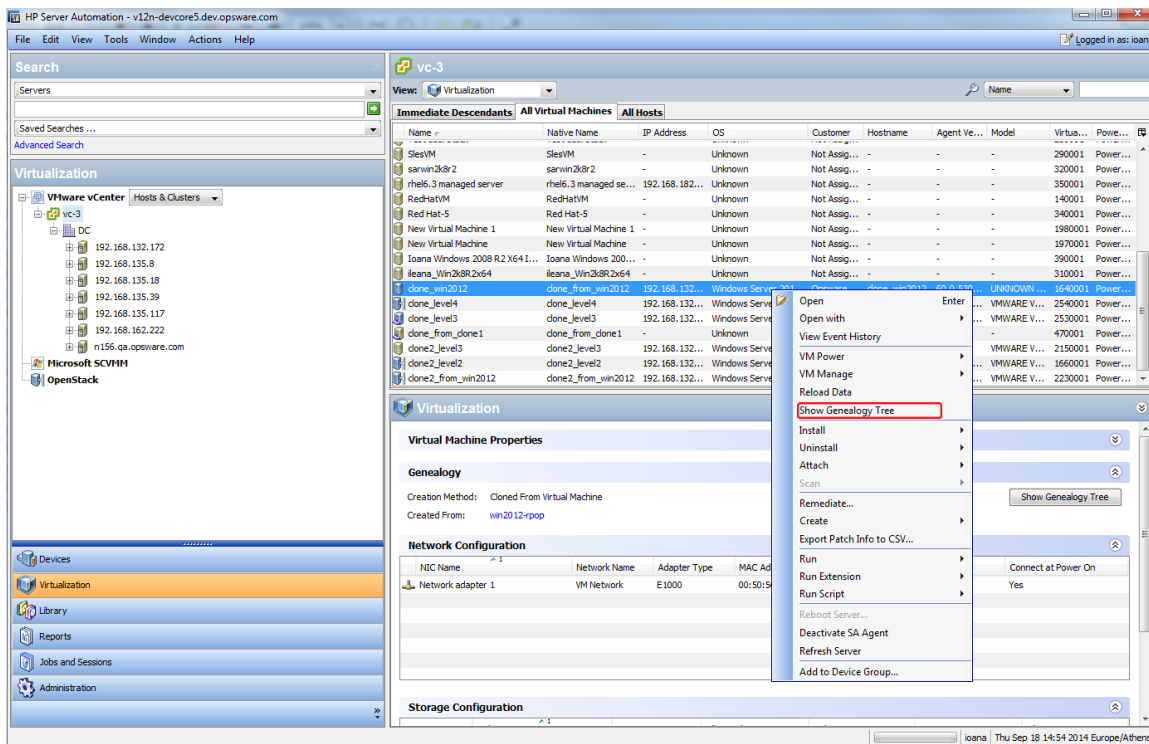
Figure 1).

Figure 1. Start Genealogy from Virtualization Tab, Actions Menu, or Genealogy Pane



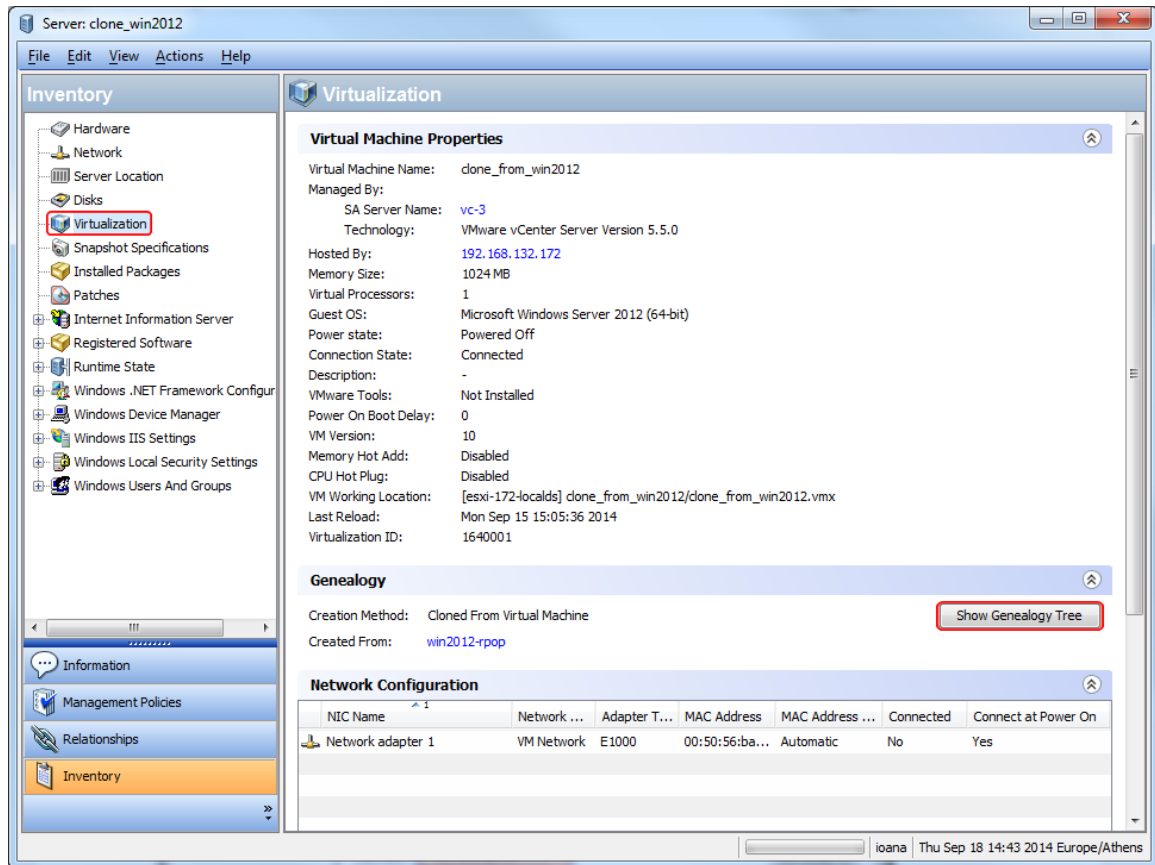
3. Right-click the selected item. The Actions drop-down list appears. Select the Show Genealogy tree from the Actions popup and click on the selected item (see Figure 2):

Figure 2. Start Genealogy from Virtualization Tab using right-click



- Open the Object Browser for the selected VM or VM template and select **Inventory > Virtualization**. Under Genealogy, press the Show Genealogy Tree button (see Figure 3).

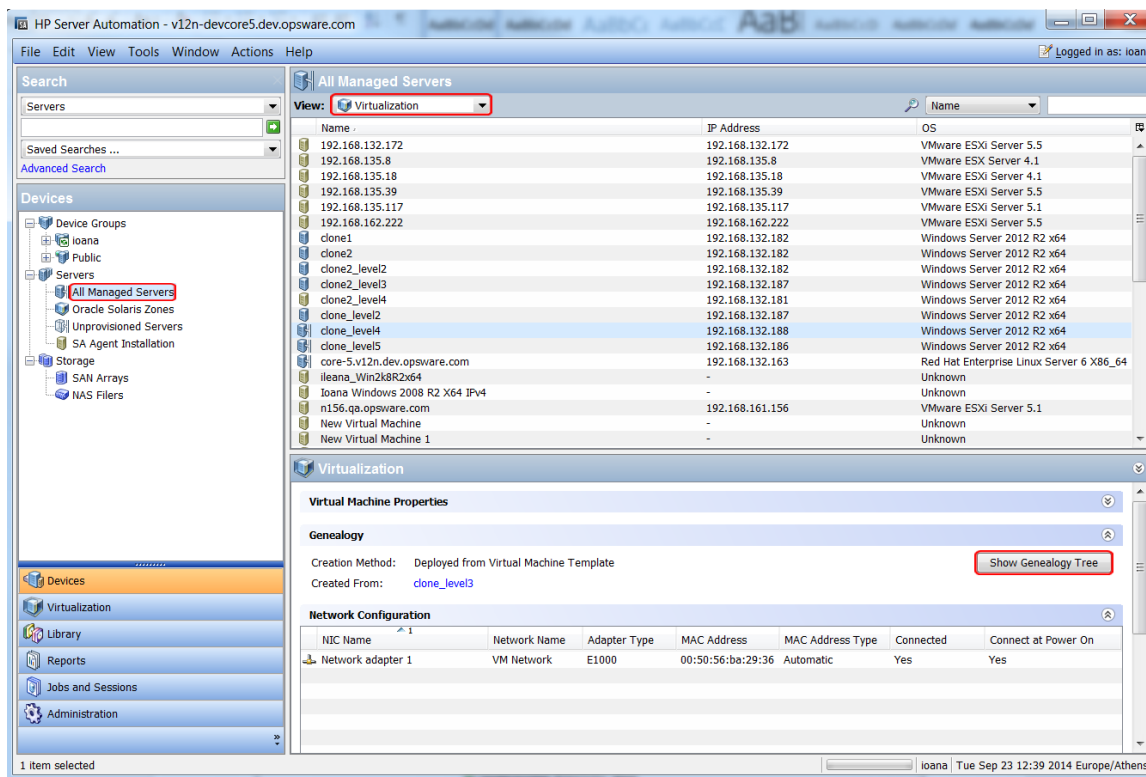
Figure 3. Start Genealogy from Virtualization Tab using Object Browser



Alternatively, you could start Genealogy as follows:

1. From the Devices tab, select All Managed Servers.
2. Select Virtualization from View.
3. Choose a VM or VM template. Under Genealogy, press the Show Genealogy Tree button (see **Figure 4**).

Figure 4. Start Genealogy from the Devices Tab



About the Genealogy Window

- The name of the source VM or VM template used to start Genealogy is displayed in the window's title (see **Figures 5 and 6**).

Figure 5. Genealogy for a VM (WINDOWS-KCBSKM8) with Descendants and without Ancestors

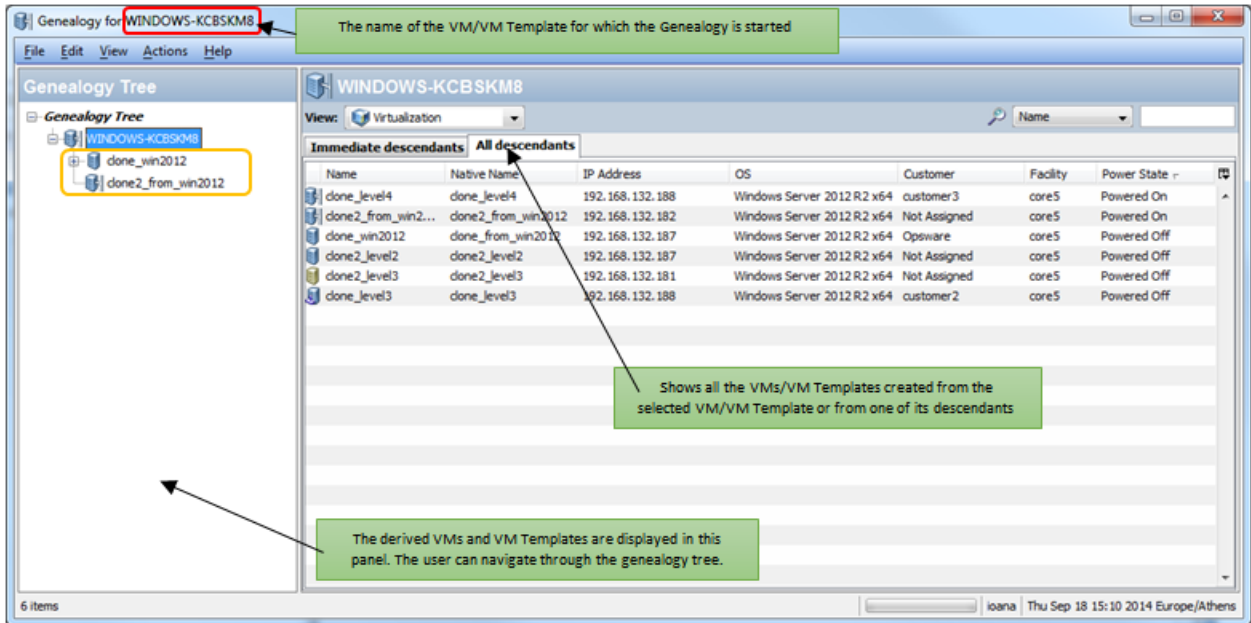
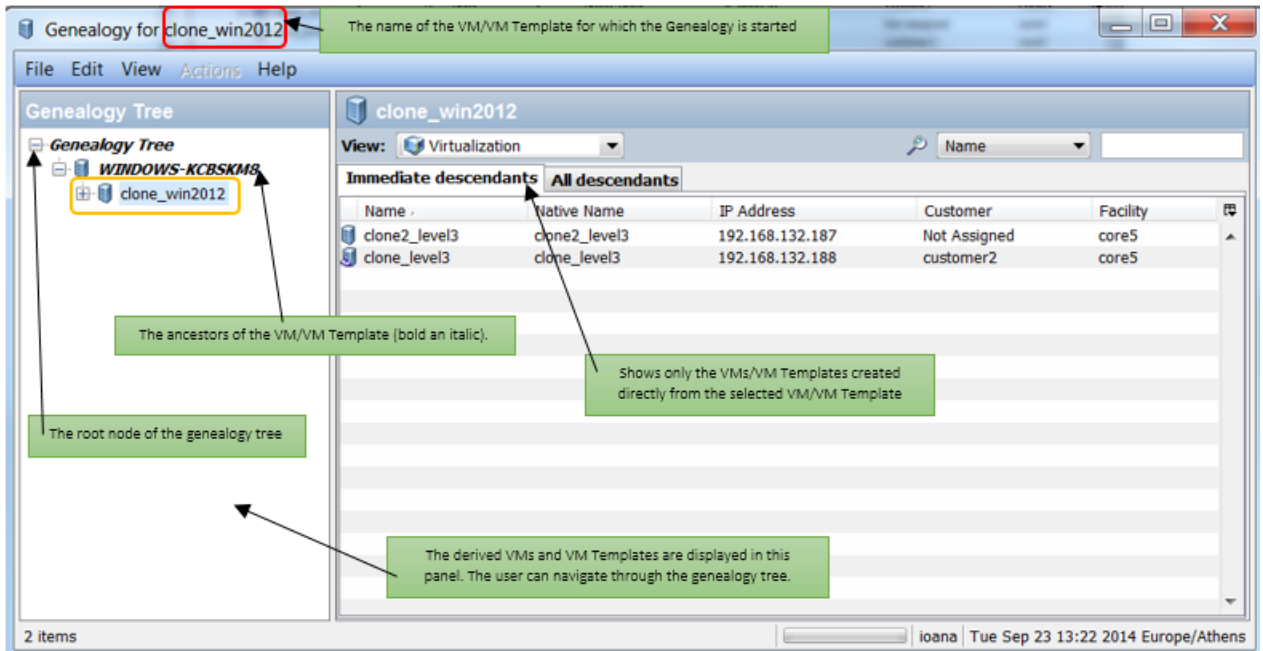
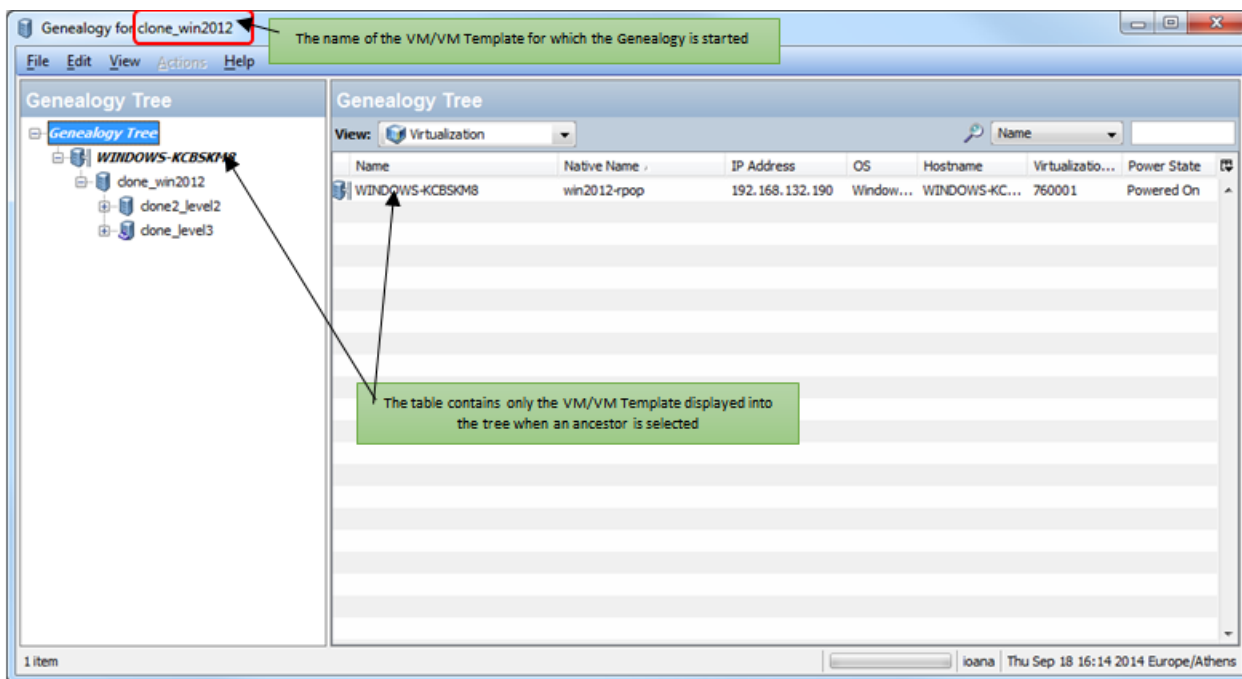


Figure 6. Genealogy of a VM (clone_win2012) with Descendants and an Ancestor



- The window name is not changed when you navigate through the tree (see **Figure 7**).

Figure 7. Genealogy Window when an Ancestor is selected



- The VM or VM template used to start the Genealogy process is selected by default.
- The Immediate descendants tab is selected by default.
- The ancestors of the VM or VM template used to start the Genealogy process are shown.

The Genealogy tree contains the following elements:

- The source VM and VM template used to start the Genealogy process.
- The ancestors of the source VM or VM template used to start the Genealogy process.
- The VMs or VM templates derived from the source VM or VM template used to start the Genealogy process.

For ancestors, the Genealogy shows only the direct path from the source VM or VM template used to start the Genealogy to the root VM or VM template. As such, for each ancestor only one child is displayed, even if an ancestor has more than one child.

The ancestors of the source VM or VM template are recursively searched. First the parent of the source VM or VM template is found, then the parent of the parent, and so on, until no more ancestors are found.

If an ancestor is selected (including in the root of the **Genealogy Tree**), a table appears on the right side of the Genealogy window. The table contains the VM or VM template displayed in the Genealogy Tree under the selected ancestor. The root of the Genealogy Tree is a node created artificially to display the

root VM or VM template in the right pane. Select the root VM or VM template to see its properties and to perform available actions.

Special tooltips are displayed for the ancestors and for the root of the tree (see **Figures 8 and 9**).

Figure 8. Tooltip for an Ancestor

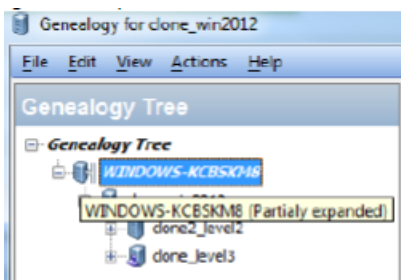
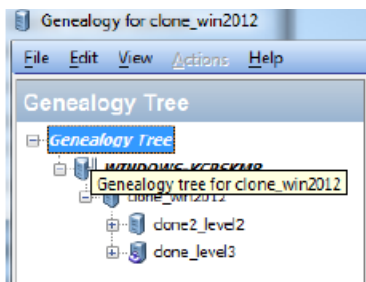


Figure 9. Tooltip for Genealogy Tree Node

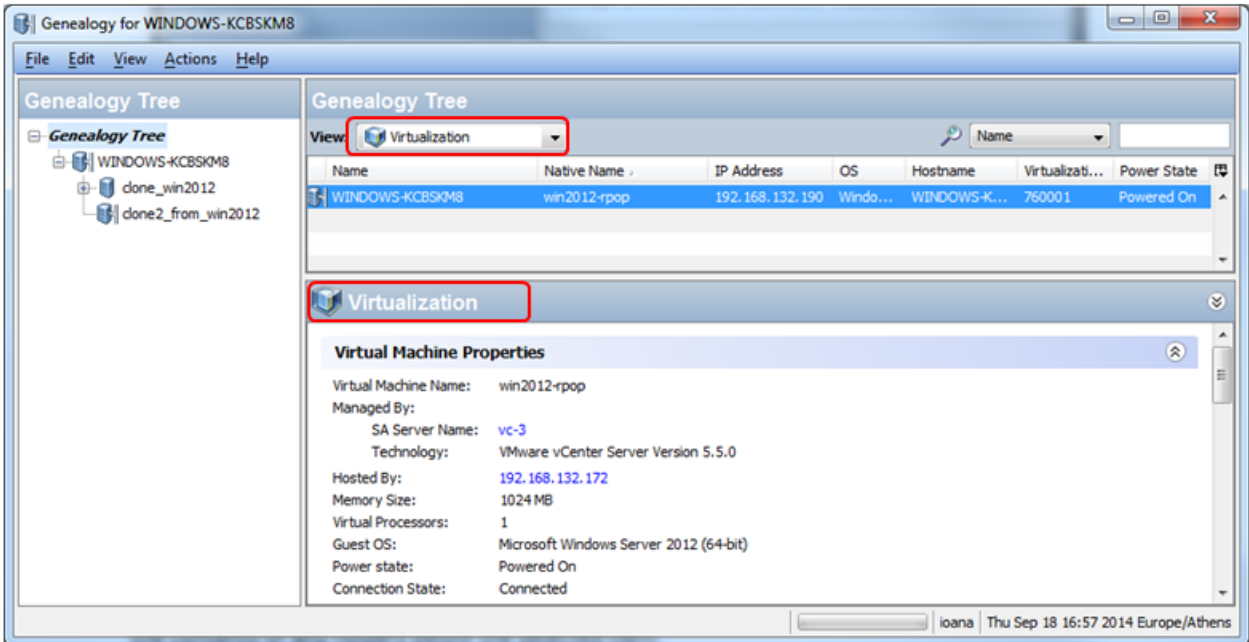


If the source VM or VM template or one of its descendants is selected, the Genealogy window contains two tabs:

- Immediate descendants: Shows VMs and VM templates immediately under the selected item in the tree (see **Figure 6**).
- All descendants: Shows all VMs and VM templates under the selected item in the tree, regardless of their place in the hierarchy (see **Figure 5**).

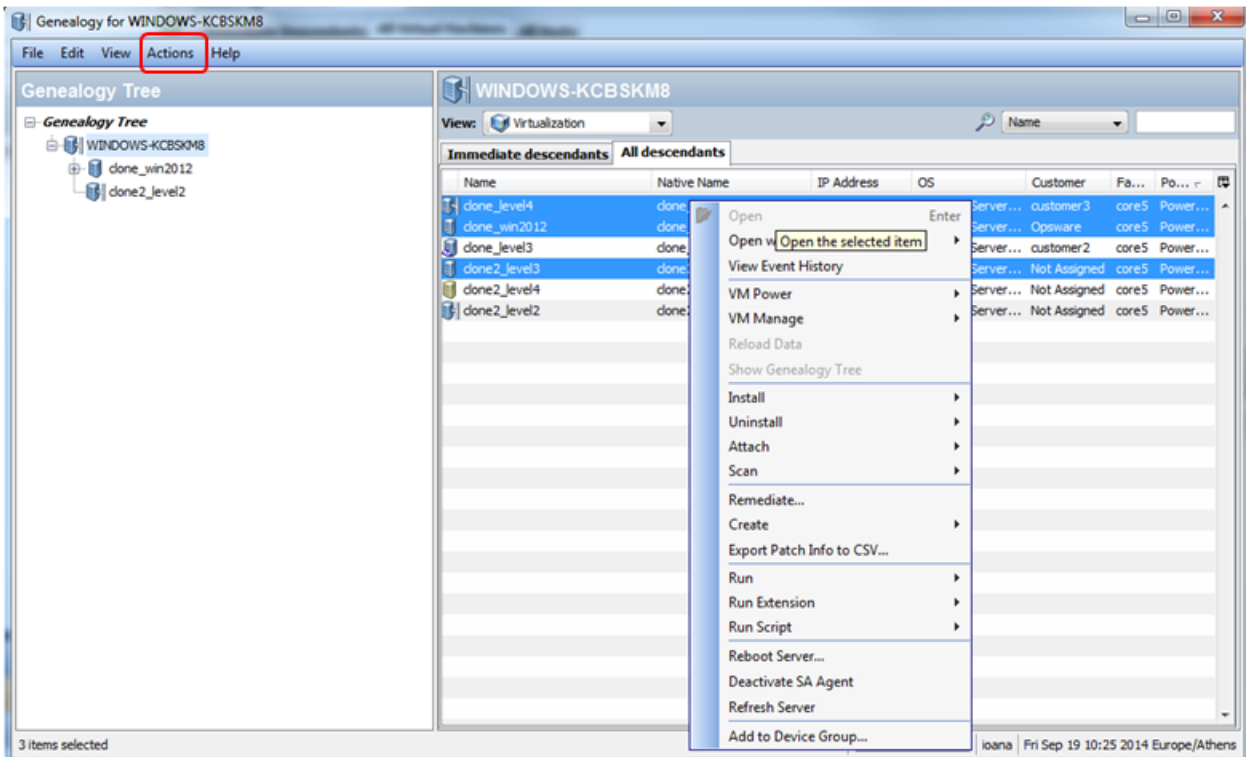
If a single tree item, ancestor or descendant, is selected in the right pane of the Genealogy window, the Preview pane appears. The Preview pane shows properties for the selected VM or VM template (see **Figure 10**). For more details about the Preview window, see ["Virtual Machine and VM Template Tasks" on page 34](#).

Figure 10. Preview Pane for the selected VM or VM Template



You can perform actions on one or more descendants from the Action menu or by right-clicking on the VM or VM template (see **Figure 11**). For details about these actions, see ["Virtual Machine and VM Template Tasks"](#) on page 34.

Figure 11. Genealogy Window, VM Actions

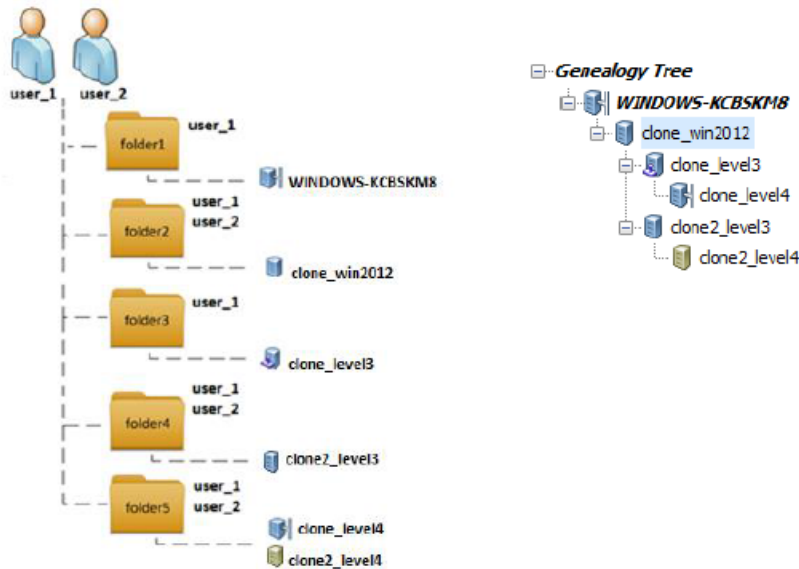


Management Permissions and Genealogy

To view the full hierarchy of VMs and VM templates in the Genealogy window, the user must have Read permission on the folders where these VMs and the VM templates are located. Without Read permission, only part of the Genealogy Tree is displayed. When you navigate through the tree, user permissions on the VMs and VM template folders are updated. For details about user groups and permissions, see ["Managing Permissions" on page 4](#).

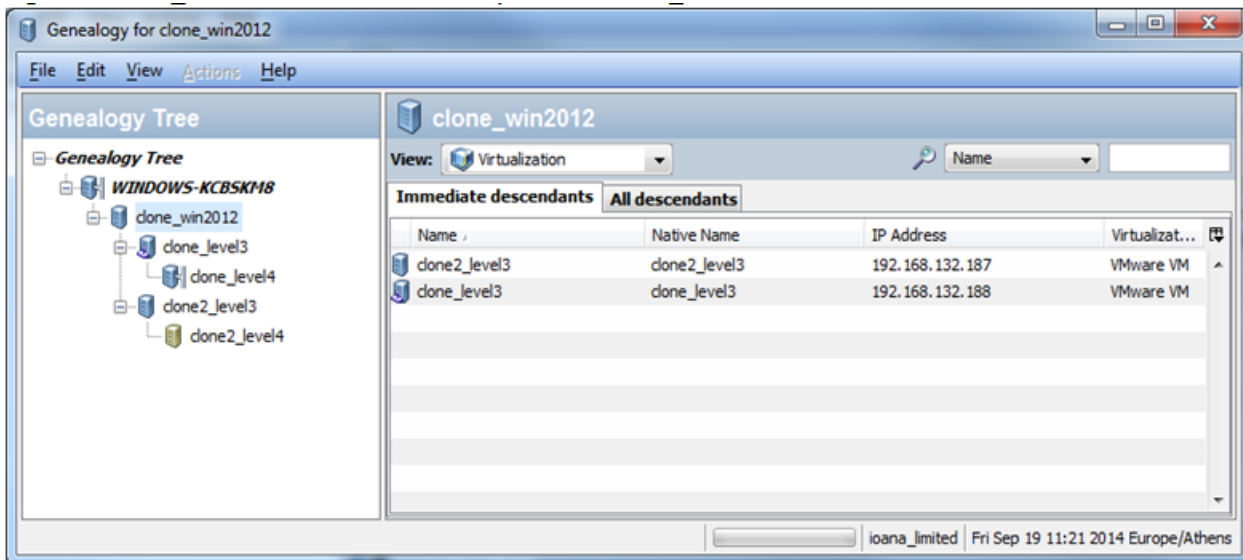
Example: Create two users with different folder permissions.

- user_1 has Read permission on all folders (folder1, folder2, folder3, folder4, folder5) where VMs and VM templates are located.
- user_2 has Read permission on some folders (folder2, folder4, folder5) and List permission on others (folder1 and folder3).



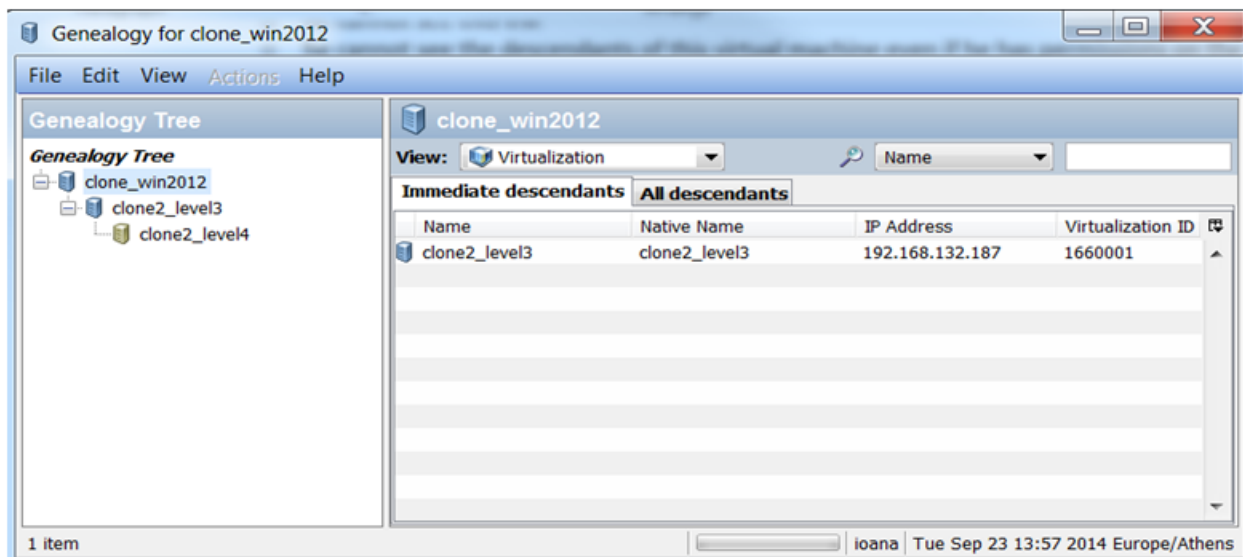
user_1 can see the full hierarchy, or Genealogy Tree (see **Figure 12**):

Figure 12. Full Genealogy Tree View of VM clone_win2012



user_2 can see only part of the hierarchy (see **Figure 13**):

Figure 13. Partial Genealogy Tree View of VM clone_win2012



- user_2 does not have permissions on the folder where the ancestor WINDOWS-KCBSKM8 is located, so this VM is not displayed in the tree.
- user_2 does not have permissions on the folder where the VM clone_level3 is located.
 - The VM is not visible.
 - The descendants of this VM are not visible even if the user has permissions on the folders where the descendants are located.

Refresh Action from the Genealogy Window

SA data can change while the Genealogy window is displayed for a VM or VM template. Some possible changes are:

- Folder permissions can be added or removed on or from some folders where VMs and VM templates from the Genealogy Tree are located.
- VMs and VM templates from the Genealogy Tree can be deleted.
- VMs can be created (cloned or deployed from a VM or VM template).
- VMs can be converted to templates.
- VMs can be modified (e.g., powered on or off, SA Agent deactivated).

The **View > Refresh** action updates the Genealogy window with all SA user changes, providing up-to-date information. The Refresh action:

- Rebuilds the Genealogy Tree.
- Retains the last selected node.
 - If the selected node is deleted, then only the root node Genealogy Tree is displayed.
- Updates each deleted VM or VM template so its descendants become descendants of its parent.
- Updates the window display.

Example: **Figures 14** and **15** show the Genealogy window before and after the Refresh action when a VM (VM to_delete) is removed.

Figure 14. Genealogy for WINDOWS-KCBSKM8 Before Refresh

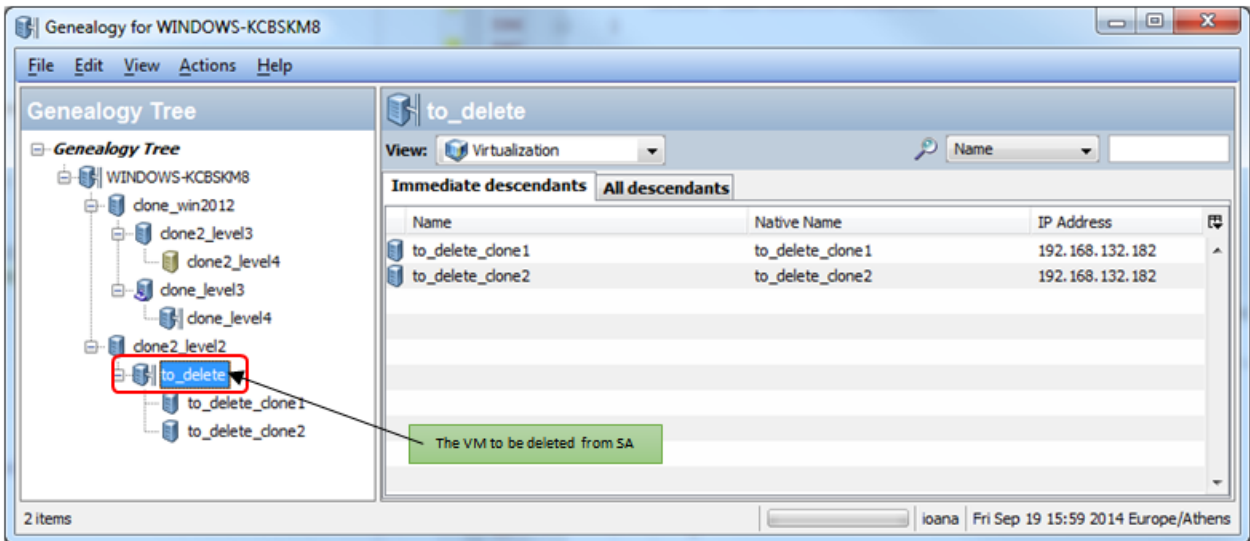
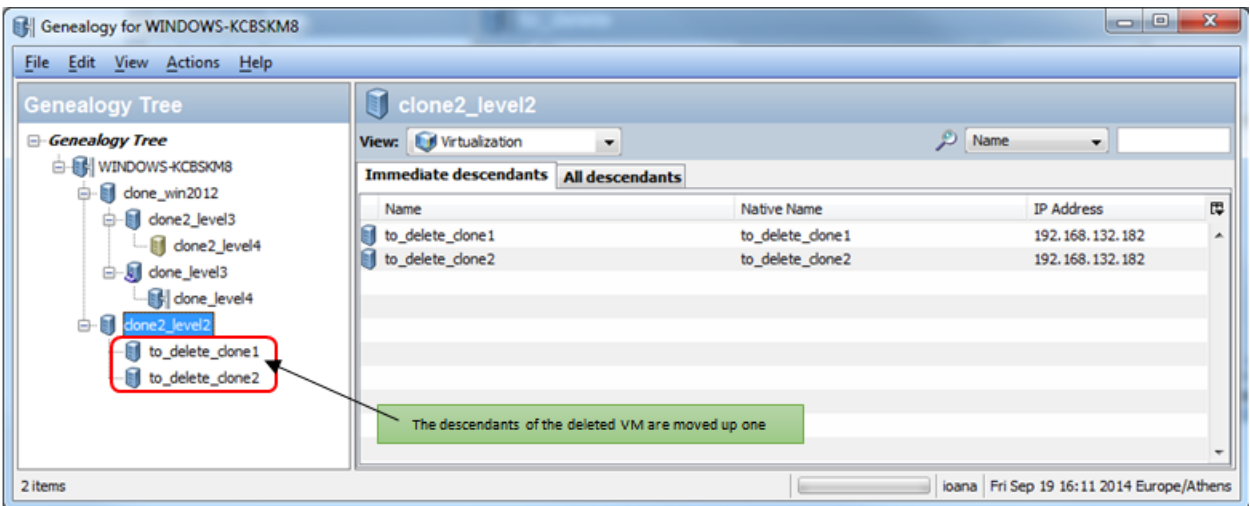


Figure 15. Genealogy for WINDOWS-KCBSKM8 After Refresh



It is not possible to display two Genealogy windows for the same source VM or VM template.

Appendix A: Virtualization Concepts and Terms

This section defines terms in this guide. For more information, also refer your virtualization vendor's documentation.

Agent – The SA Agent is software that runs on a server and enables SA to manage the server. The SA Agent must be installed on physical and virtual servers for full management capabilities on servers.

Clone – (n.) A virtual machine created by copying another virtual machine. The clone is identical to the original machine in that it has the same operating system, software, patches as well as CPU, memory and network resources. (vb.) The action of making a copy of a virtual machine.

Cluster – A group of hosts that share resources and can be managed as a unit. You can create virtual machines that run on and share the resources of the cluster. When you add a host to a cluster, that host's resources become part of the cluster's resources. The cluster provides a way to manage the resources of the hosts within it. Clusters also enable high availability and load balancing.

Datacenter – The top level container for a set of VMware virtualization resources. A datacenter contains hosts, clusters, resource pools, datastores, and virtual machines. These items can also be organized in folders.

Datastore – A VMware container of storage elements used to allocate storage to virtual machines.

Folder – A location and a container in the virtualization inventory where virtualization objects are stored and accessed. Folders also provide access control based on permissions. The SA Library also uses folders to organize and control access to other items such as patches, patch policies, software packages, and so forth.

Guest Customization – The process of modifying a new virtual machine to make it unique. This may include setting the host name, domain name, time zone, and static IP address. Guest customization is typically one step in deploying a VM from a VM template or in cloning a VM.

Guest Operating System – The configuration setting indicating the operating system running on the virtual machine. Note that this setting may be different from the actual operating system running on the VM.

Guest Tools – The virtualization vendor's software that runs on a virtual machine and improves integration and performance of the VM. Guest tools perform operations such as synchronizing system clocks and providing a heart beat back to the Virtualization Service. Also called **VMware Tools** in VMware and **Virtual Machine Additions** in SCVMM.

Best Practice: Always install the guest tools on all your VMs for best integration.

Host – A server that uses virtualization software to run VMs. A host provides CPU and memory resources, and access to storage and networks for VMs.

Host Groups – In SCVMM, containers you can create to group a set of virtual machine hosts for easier management. Host groups are hierarchical and can contain other host groups.

Hypervisor – A software program that provides the ability to run VMs and typically runs on physical server. May also be called a host.

IaaS - Infrastructure as a Service is a provisioning model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Management Path – The method by which SA manages a server. Three management paths are available: agent managed, VS managed and iLO managed. Servers can be managed by more than one management path.

- **Agent Managed** - Servers managed by the SA Agent. The SA Agent provides the most management capabilities.
- **VS Managed** - Servers managed by a Virtualization Service such as VMware vCenter Server or Microsoft SCVMM.
- **iLO Managed** - Servers managed by HP Integrated Lights Out. For more information, see www.hp.com/go/iLO.

NIC – Network interface card.

OpenStack - OpenStack is a cloud computing project aimed at providing IaaS. It is free and open-source software released under the terms of the Apache License. The project is managed by the OpenStack Foundation, a non-profit corporate entity established in September 2012 to promote OpenStack software and its community.

OpenStack controller node - Server on which you have installed your OpenStack controller and keystone services.

Project – In OpenStack, a project is a logical grouping of VMs that defines quotas and access to VM images.

PXE - The Preboot Execution Environment, or PXE, is an environment in which to boot computers using a network interface independently of data storage devices or installed operating systems.

Resource Pool – In VMware, a way to divide the resources of a host or a cluster into smaller pools. A resource pool contains a set of CPU and memory resources that all the VMs running in the resource pool share. Resource pools provide the ability to balance workloads across the resource pool.

SCVMM – System Center Virtual Machine Manager, Microsoft’s management tool for managing hypervisors and virtual machines.

vCenter Server – VMware’s Virtualization Service for managing ESX and ESXi hypervisors, and virtual machines.

Virtualization Containers – Any container of virtualization resources including clusters, datacenters, folders, host groups, hypervisors, resource pools, and virtualization services.

Virtualization Service – A platform for centrally managing virtual resources such as hypervisors and virtual machines. Examples are VMware vCenter Server and Microsoft System Center Virtual Machine Manager (SCVMM).

Virtual Machine (VM) – A software version of a computer, consisting of an operating system, storage, networking and applications, just like a physical computer. In OpenStack, a VM may be called an “instance.”

VM Template – A specification for a virtual machine. You can create a virtual machine from a VM template and you can create a VM templates from a virtual machine. A VM template typically includes an OS Build Plan for installing an operating system, patch policies that specify patches to be installed, software policies that specify software to be installed, application configurations that specify how the software should be configured, and the SA Agent for managing the virtual machine. VM templates allow you to control what type of virtual machines get created and they allow you to keep your virtual machines in compliance.

Appendix B: Virtualization Security

If your architecture includes a master core and one or more secondary cores, follow the steps in this section for the master core and for each of the secondary cores. Similarly, if your SA computer has a sliced-core installation with one or more slices, repeat the steps for each slice.

HP Server Automation (SA) complies with the Federal Information Processing Standards (FIPS) publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules.

Secure Mode in SA Virtualization allows you to upload CA Certificates for secure communication to the VS. When Secure Mode is enabled, it secures the communication with the VS by authenticating the certificate that the customer uploads to the non-FIPS keystore. Secure Mode is enabled (or True) by default in a new SA 10.1 installation and disabled (or False) on an upgrade to SA 10.1.

- If FIPS is enabled, it overrides Virtualization Secure Mode. In this case, you need to upload the VS certificate to the FIPS keystore.
- If FIPS is disabled, then Secure Mode can be True or False.
 - If Secure Mode is True, you must upload the certificate to the non-FIPS keystore. This will use SSL to communicate with the VS and also validate the certificate.
 - If False, you do not need to upload any certificates.

For more information about FIPS, see Chapter 5, “SA Core Installation” and Appendix G, “HP SA FIPS 140-2 Compliance Statement” in the SA Standard/Advanced Installation Guide.

Editing Secure Mode and Importing the CA Certificate

Note: FIPS-enabled OpenStack can be used only in a properly secured SA environment. For more information, see Chapter 5 in the SA Standard/Advanced Installation Guide.

1. Select the **Administration** tab in the SA Client.
2. Select System Configuration in the navigation pane.
3. In the list of SA components, select Server Automation Web Services Data Access Engine. This displays the system configuration parameters for this component.

4. Locate the Secure Mode flag, which is called `twist.v12n.ssl.secure`, and change the Value to True or False.
5. Import your root CA Certificate onto each core and slice:
`/opt/opsware/twist/importV12nCert.sh ~/<srcCertFile> <type> <certAlias>`

where

- `<type>` is either `vmware` or `openstack`.
- `<certAlias>` is a unique alias name you provide to identify the CA Certificate.

For example:

```
/opt/opsware/twist/importV12nCert.sh ~/tmp/rui.crt vmware vcenter_cert
```

The import function automatically imports your CA Certificate to both the FIPS NSS store and the Virtualization non-FIPS store.

6. Restart the Web Services Data Access Engine (Twist) on all servers on the core where the certificate was imported:
`/etc/init.d/opsware-sas restart twist`

Removing a CA Certificate

To remove a CA Certificate from the Virtualization FIPS keystore, perform the following steps:

1. Enter the following command to view a list of CA Certificates. The certificates are listed by randomly generated alias names:

```
export LD_LIBRARY_PATH=/opt/opsware/nss/lib/;/opt/opsware/nss/bin/certutil
-d /var/opt/opsware/crypto/nss/twist/db -L
```

2. To view details about your certificate, enter your unique alias name:

```
export LD_LIBRARY_PATH=/opt/opsware/nss/lib/;/opt/opsware/nss/bin/certutil
-d /var/opt/opsware/crypto/nss/twist/db -L -n <certAlias>
```

For example:

```
export LD_LIBRARY_PATH=/opt/opsware/nss/lib/;/opt/opsware/nss/bin/certutil
-d /var/opt/opsware/crypto/nss/twist/db -L -n vcenter_cert
```

3. To remove the certificate, enter the following command:

```
/opt/opsware/nss/bin/certutil -d /var/opt/opsware/crypto/nss/twist/db -D -n  
<certAlias>
```

For example:

```
/opt/opsware/nss/bin/certutil -d /var/opt/opsware/crypto/nss/twist/db -D -n  
vcenter_cert
```

To remove CA Certificates from the Virtualization non-FIPS keystore, perform the following steps:

1. Enter the following command to view a list of imported certificates and identify your certificate alias:

```
/opt/opsware/twist/v12nCertUtil.sh <type> list
```

Where:

<type> is either vmware or openstack.

2. Enter the following command to remove the certificate:

```
opt/opsware/twist/v12nCertUtil.sh <type> delete <certAlias>
```

Where:

<type> is either vmware or openstack.

<certAlias> is your certificate alias.

For example:

```
opt/opsware/twist/v12nCertUtil.sh vmware delete vcenter_cert
```

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on User Guide: Virtualization Management (Server Automation 10.20)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to sa-docs@hp.com.

We appreciate your feedback!

