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 Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Support

Visit the HP Software Support Online website at:

https://softwaresupport.hp.com/

This website 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 website 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:

https://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

https://softwaresupport.hp.com/web/softwaresupport/access-levels

Support Matrices

For complete support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online website:

https://softwaresupport.hp.com/group/softwaresupport/support-matrices

You can also download the *HP Server Automation Support and Compatibility Matrix* for this release from the HP Software Support Online Product Manuals website:

https://softwaresupport.hp.com/

This site requires that you register for an HP Passport and sign in. After signing in, click the **Search** button and begin filtering documentation and knowledge documents using the filter panel.

Documentation Updates

All the latest Server Automation product documentation for this release is available from the SA Documentation Library:

https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417675

Use the SA Documentation Library to access any of the guides, release notes, support matrices, and white papers relevant to this release or to download the full documentation set as a bundle. The SA Documentation Library is updated in each release and whenever the release notes are updated or a new white paper is introduced.

How to Find Information Resources

You can access the information resources for Server Automation using any of the following methods:

Method 1: Access the latest individual documents by title and version with the new SA Documentation Library

Method 2: Use the complete documentation set in a local directory with All Manuals Downloads

Method 3: Search for any HP product document in any supported release on the HP Software Documentation Portal

To access individual documents:

1. Go to the SA 10.x Documentation Library:

   https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417675

2. Log in using your HP Passport credentials.
3. Locate the document title and version that you want, and then click **go**.

To use the complete documentation set in a local directory:

1. To download the complete documentation set to a local directory:
   a. Go to the SA Documentation Library:

   https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00417675

b Log in using your HP Passport credentials.

c Locate the All Manuals Download title for the SA 10.1 version.

d Click the **go** link to download the ZIP file to a local directory.

e Unzip the file.

2 To locate a document in the local directory, use the Documentation Catalog (docCatalog.html), which provides an indexed portal to the downloaded documents in your local directory.

3 To search for a keyword across all documents in the documentation set:

a Open any PDF document in the local directory.

b Select **Edit > Advanced Search** (or Shift+Ctrl_F).

c Select the All PDF Documents option and browse for the local directory.

d Enter your keyword and click Search.

To find additional documents on the HP Software Documentation Search Portal:

Go to the HP Software Documentation Search Portal:

https://softwaresupport.hp.com/

This site requires that you register for an HP Passport and sign in. After signing in, click the **Search** button and begin filtering documentation and knowledge documents using the filter panel.

To register for an HP Passport ID, click the **Register** link on the HP Software Support Online login page.

You can also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details. See Documentation Change Notes for a list of any revisions.

Product Editions

There are two editions of Server Automation:

- Server Automation (SA) is the Ultimate Edition of Server Automation. For information about Server Automation, see the SA Release Notes and the SA User Guide: Server Automation.
- Server Automation Virtual Appliance (SAVA) is the Premium Edition of Server Automation. For more information about what SAVA includes, see the SAVA Release Notes and the SAVA at a Glance Guide.

Contents

1 Introduction to Server Automation 9
Overview of Server Automation 9
SA Configurations 10
A Simple SA Configuration 10
The Oracle Database 11
Accessing SA Features 11
SA Client 11
SAS Web Client 12
Sample Use Cases and Tutorials 13

2 Overview of SA Features 15
SA Provisioning 16
Application Deployment 17
Script Execution 18
Agentless Server Discovery and Agent Installation 18
Device Explorer 18
Virtualization Management 19
Service Automation Visualizer (SAV) 19
Storage Visibility and Automation 19
Audit and Remediation 20
Compliance in the SA Client 20
Reports 21
Software Management 21
Patch Management for Windows 21
Patch Management for HP-UX 22
Patch Management for Solaris and Solaris 11 22
Patch Management for Ubuntu 23
Patch Management for UNIX 23
Application Configuration Management 24
Global Shell 24

3 Advanced SA Architecture 27
The SA Core 27
A Simple Single Host Installation 27
SA Server Agents 28
The Core Components 29
SA Core Component Bundling 29
Model Repository 30
The Core Component Bundles 31
Infrastructure Component Bundle 31

Slice Component Bundle 32
SA Provisioning Components Bundle 34
Satellite Installations 34
SA Gateways 34
Multimaster Master Gateway Backup Routes 35
SA Topologies 36
Single Host Core 36
Multimaster Mesh (Multiple Cores) 37
Benefits of Multimaster Mesh 38
Facilities and Realms 38
Facilities 38
Realms 39
Multimaster Mesh Topology Examples 40
SA Satellites 41
Satellite Topology Examples 42
A Simple Single Core to Satellite Link 42
A Two Satellite to Single Core Link 43
A Cascading Satellite Link 43
Satellites in a Multimaster Mesh 44
Satellite With Multiple Gateways in a Multimaster Mesh 45
SA Product Options 46
Service Automation Visualizer (SAV) 47
Storage Visibility and Automation 47
Reports 47
SA Utilities 47
Script Execution 47
Network Automation (NA) Integration 48

1 Introduction to Server Automation

Overview of Server Automation

This section provides a description of basic Server Automation (SA) features and architecture. For more detailed information about SA, see Chapter 3, Advanced SA Architecture.

SA is data center automation software that centralizes and streamlines many data center functions and automates critical areas of your data center's server management:

- **Server Discovery**

  SA scans your network for servers that it does not yet manage and displays them in an agentless server list. You then bring these servers under SA management by installing an SA Agent on each server. After the servers are under SA management, you can perform management tasks on them, including the following:

  — **Operating System Provisioning**

  SA Provisioning enables you to provision bare metal and virtual servers with a preconfigured operating system and bring them into the SA Managed Server Pool, after which SA can centrally manage the newly provisioned servers.

  — **Operating System Patching**

  SA provides an automated, centralized, and flexible method of applying the required operating system patches for Windows, Linux, and Solaris-based managed servers. You can compare required patches against operating system vendor approved lists. You can customize the patching process to omit patches that are incompatible with a server's environment.

  — **Software Provisioning**

  After a server is part of the managed server pool, you can install and configure software applications using templates called Software Policies. A software policy specifies the software to be installed, the configurations to be applied, and the scripts to be run during installation. Software policies allow you to establish a baseline configuration for your servers which you can then enforce using SA's Software Compliance feature. For example, you can install an baseline version of an Apache server on all or a subset of your SA managed servers.

  — **Audit and Compliance**

  SA Audit and Remediation allows you to define server configuration policies to help you ensure that your SA managed servers meet your policy standards. When servers are found to be out of compliance—not configured the way you want them to be—you can remediate them (force them into compliance). You can base your compliance policy on a snapshot of a base server that you have configured as you want all servers to be configured.

  SA's audit trail data helps you establish strict accountability in your data center environment—an increasingly urgent topic in the age of Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act (GLB Act), and the Health Information Portability and Accountability Act (HIPAA).

- **Application Configuration**

  You can design application configuration templates and push those configurations to all SA managed servers. For example, if you have an Apache web server, you might want to ensure that its configuration files are standardized on all servers on which it is deployed. Application configuration allows you to do that. For more information, see the *SA User Guide: Application Configuration*.

- **Application Deployment**

  Using SA Application Deployment, you can quickly and easily move your complex, custom, multi-tier applications from the development team to the quality assurance team for testing, to preproduction, staging and finally to production. For more information, see the *SA User Guide: Application Deployment Manager*.

- **Software Compliance**

  SA's Software Policy Compliance Scan determines whether a Managed Server's software configuration is compliant with the specifications in the software policies attached to that server.

- **Reporting**

  SA provides an extensive set of comprehensive and configurable reports that you can use to present data about the state of your managed servers for various audiences.

SA allows you to make changes more safely and consistently, because you can model and validate changes before you actually commit the changes to a managed server. SA also provides methods to ensure that modifications you plan for your managed servers work on the first time because they have been tested before being applied, thereby reducing downtime.

SA Configurations

A simple SA installation consists of an SA Core, its components, and an Oracle database hosted on single server. More advanced installations can add Secondary Cores (cores that supplement a Primary SA Core and enhance its server management capacity), SA Satellites (similar to an SA Core but smaller and with more limited capabilities used for data centers/branches with limited requirements/resources), and Multimaster Mesh, which allows two separate SA Core installations to communicate and co-manage servers. For more information, see Chapter 3, Advanced SA Architecture.

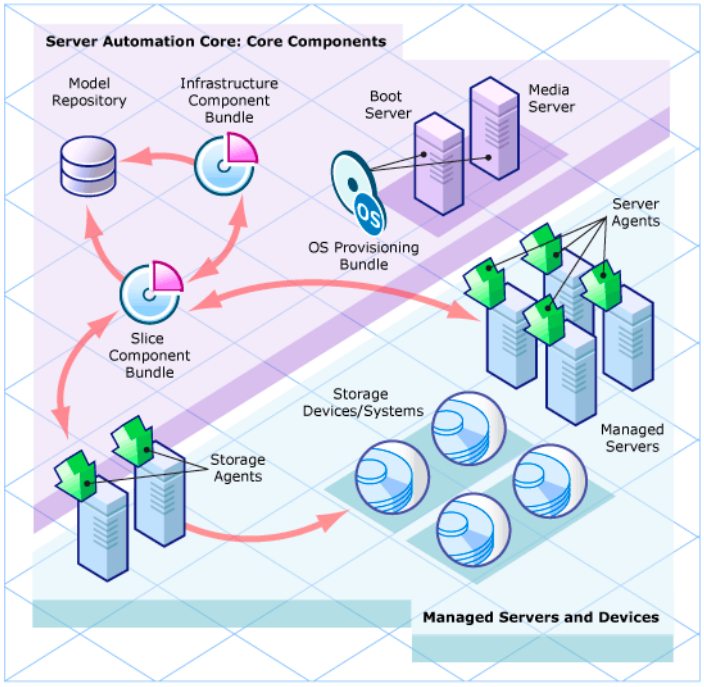
SA supports customer installation in eight specific configurations. These configurations are listed in the *SA Standard/Advanced Installation Guide*. Other configurations are not supported for customer installation and require HP Professional Services.

A Simple SA Configuration

SA installs a number of components that provide its server management capabilities. If you have no need to customize your SA installation, you can choose a SA Single-Host installation. If you need to customize your core installation (for example, distribute SA Core Components to different servers for performance reasons,) you will need to use HP Professional Services or certified HP consultants.

Figure 1 shows the simplest SA installation for a single data center/facility. It consists of all SA components installed on a single host managing servers on a single network.

figure 1 A Simple SA Installation



The Oracle Database

All SA installations require an Oracle database that is configured specifically for SA and is used by an SA component called the Model repository (see Model Repository on page 30) to store information about your network, storage devices, managed servers and the operating systems and applications installed on them, and so on. This database is provided as part of the SA installation, or you can use an existing Oracle installation that has been configured for use with SA (see Appendix A: "Oracle Setup for the Model Repository" in the *SA Standard/Advanced Installation Guide*.

Accessing SA Features

There are two ways you typically access SA functions:

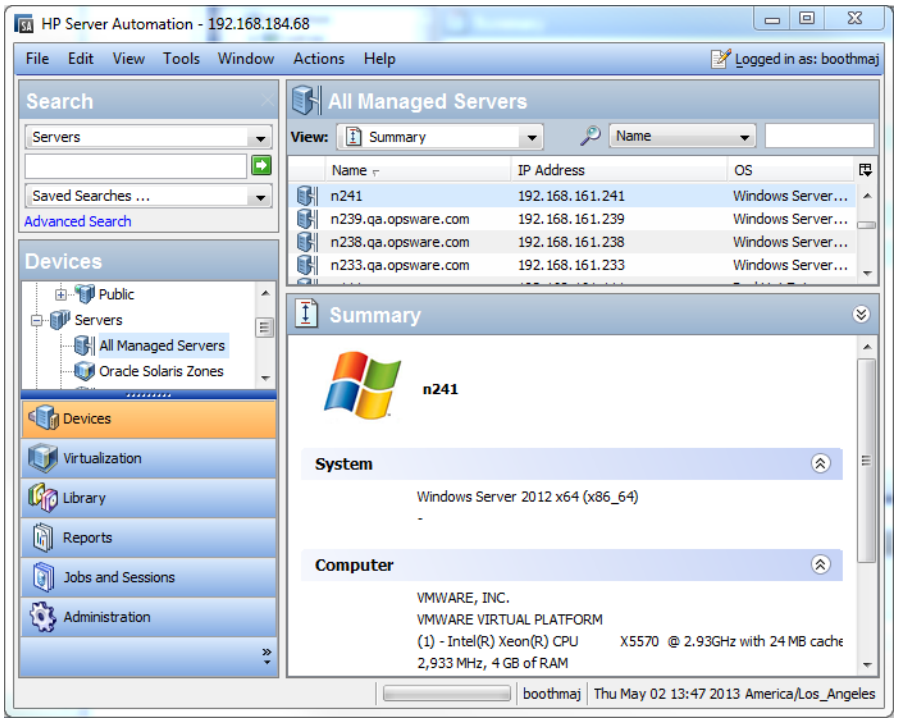
SA Client

SA Client is a Windows application that you install after SA is installed. It provides an interface to SA functions.

To install the SA Client, you must download and install the SA Client by opening the home page of your core and clicking the **Download Server Automation Client** button.

Figure 2 shows the SA Client main screen. You can find more detailed information about the SA Client in the *User Guide: Server Automation*.

figure 2 The SA Client Main Screen



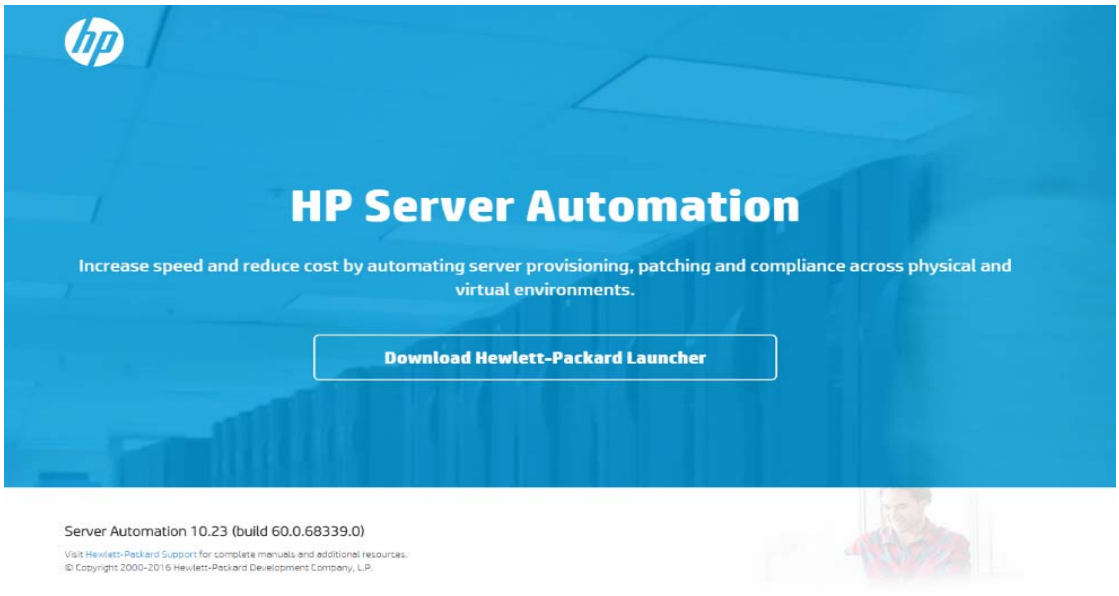
SAS Web Client

The SAS Web Client is deprecated. Certain SA functions are still provided through the SAS Web Client; however, you should use the SA Client when possible.

The SA Web Client is the web-based user interface to SA through which you can download the SA Client launcher. Instructions for starting the SAS Web Client in your browser are in the *User Guide: Server Automation*. After you start the SAS Web Client, you can download and install the SA Client Launcher executable.

Figure 3 shows the SAS Web Client home page.

figure 3 The SAS Web Client Home Page



Sample Use Cases and Tutorials

Chapter 2, Overview of SA Features, provides an overview of using SA features. HP also provides interactive tutorials in the *SA Getting Started* guide that walk you through performing certain tasks such as installing an operating system on a server, creating a software policy, applying Windows/Solaris patches, and more. The SA Client also provides interactive tutorials accessible through the online help.

2 Overview of SA Features

SA automates data center processes, replacing ad hoc, error-prone, manual processes. For example, by using SAProvisioning, you can set standards for different types of servers and automatically provision the servers, saving time and ensuring that operating system builds are consistent.

You can establish patch polices to install and maintain patches for supported operating systems running on managed servers in your IT environment.

By using Compliance, you have visibility across your managed servers to see which servers are out of compliance. You can then remediate noncompliant servers to bring them back into compliance, based on the policies you created.

SA provides the following capabilities:

- SA Provisioning
- Application Deployment
- Script Execution
- Agentless Server Discovery and Agent Installation
- Device Explorer
- Virtualization Management
- Service Automation Visualizer (SAV)
- Storage Visibility and Automation
- Audit and Remediation
- Compliance in the SA Client
- Reports
- Software Management
- Patch Management for Windows
- Patch Management for HP-UX
- Patch Management for UNIX
- Patch Management for Solaris and Solaris 11
- Patch Management for Ubuntu
- Application Configuration Management
- Global Shell

SA supports cross-platform environments and is designed to automate both new and existing data center environments.

SA Provisioning

SA Provisioning provides the ability to to install (or *provision*) pre-configured operating system baselines onto bare metal and virtual servers quickly, consistently, and with minimal manual intervention. Bare metal and virtual server SA Provisioning is a key part of the overall process of getting a server into production.

SA Provisioning ensures that each server in your facility has a standardized, default operating system configuration that you control. For detailed information about SA Provisioning, see the *SA User Guide: Provisioning*.

Benefits of SA Provisioning include:

- **Integration with other SA functionality**

  Because SA Provisioning is integrated with the suite of SA automation capabilities, including patch management, software management, and distributed script execution, hand-offs between IT groups are seamless. SA ensures that all IT groups are working with a shared understanding of the current state of the environment, which is an essential element of delivering high-quality operations and reliable change management.

- **Update server baselines without re-imaging**

  Unlike many other provisioning solutions, systems provisioned with SA can be easily changed after provisioning to adapt to new requirements. The key to this benefit is the SA use of templates and an installation-based approach to provisioning.

- **Flexible architecture designed to work in many environments**

  SA Provisioning supports many different types of servers, networks, security architectures, and operational processes. SA works well in CD (Linux provisioning) or network-boot environments (both DHCP and non-DHCP environments), with scheduled or on-demand workflows, and across a large variety of hardware models. This flexibility ensures that you can provision operating systems to suit your organization's needs.

You can perform SA Provisioning functions from the SA Client. SA automates the entire process of provisioning a comprehensive server baseline, which typically consists of the following tasks:

- Preparing the hardware for OS installation using an OS installation profile (required only for OS Sequences).
- Defining OS Build Plans which are a list of tasks to be performed on a server before and after operating system installation. OS Build Plans are more powerful than and can be used in place of OS Sequences.
- Defining OS Sequences which are a list of tasks to be performed on a server during installation. OS Sequences can include application, patch, and remediation policies. SA recommends that you use the more flexible OS Build Plans.
- Installing a base operating system and default OS configuration using an OS Build Plan or OS Sequence.
- Applying the latest set of OS patches. The exact list depends on the applications running on the server.
- Executing pre-installation or post-installation scripts that configure the system with values such as a root password.
- Installing system agents and utilities such as SSH, PC Anywhere, backup agents, monitoring agents, or anti-virus software.
- Installing widely shared system software such as Java Virtual Machines.

SA Provisioning supports:

- Windows, Solaris, and Linux.
- Network or CD/DVD-based installations.
- Separation of duties between data center staff and systems administrators.
- A model-based approach — in which you create a *standard build* in SA which can then be installed on many systems.

SA Provisioning integrates with your operating system vendors' native installation technology, specifically:

- Windows setup answer files: `unattend.txt, unattend.xml, sysprep.inf`
- Red Hat Kickstart
- SuSE YaST (Yet another Setup Tool)
- Solaris Jumpstart
- WINPE/WIN-BCOM/UNDI

You can provision an operating system on:

- A server in SA's agentless server pool that does not have an operating system installed (*bare metal sever*)
- A virtual server
- A server in SA's *unmanaged server pool* with an installed operating system
- A server in SA's *managed server pool* with an installed operating system (*reprovisioning*)

Application Deployment

With Application Deployment, you can create, test, and deploy your custom software applications to target servers in your data centers. For example, you can move applications from the development team to the quality assurance team for testing. Once testing is complete, you can move the application to other phases such as preproduction, staging, and finally to production. The Application Deployment tool reduces the complex communications necessary to deploy applications by providing a single point of access where everyone involved can view or enter data that is relevant to them and to their role.

With Application Deployment, you can:

- Model your application components such as code, scripts, configuration files, and tiers such as application servers, web servers, and databases.
- Manage multiple concurrent releases and versions of your applications.
- Deploy, roll back, and undeploy your applications on target servers.
- Model your target servers that are running the tiers required by your applications. These target servers are managed servers in Server Automation.
- Provide clear, concise communication between software application developers, Quality Assurance, and testing, systems administrators, and other operations personnel.
- Model and implement life cycles from application development to QA to preproduction to staging to production. You can customize SA to match your enterprise life cycle.

For complete information, see the *SA User Guide: Application Deployment Manager*.

Script Execution

SA Script Execution enables you to share and run ad-hoc or saved scripts across an entire farm of SA-managed servers.

By executing scripts with SA instead of manually, administrators benefit from:

- Parallel script execution across many UNIX and/or Windows servers, saving time and ensuring consistency.
- Role-based access control, ensuring only authorized administrators can execute scripts on hosts to which they have access.
- The ability to control access to scripts by storing them in private or in public libraries.
- The ability to see and download script output one server at a time or in a consolidated report, which captures output from all servers in a single place.
- The ability for scripts to be mass-customized. Administrators can access information in SA about the environment and the state of servers. This is critical to ensuring that the right scripts are executed on the right servers.
- A comprehensive audit trail that reports who, what, when, and where a particular script was executed.

Because Script Execution is an integrated part of SA, administrators can take advantage of unique benefits when compared to standalone script execution tools:

- Using known system state and configuration information to customize script execution, users can tailor each script by referencing and accessing the rich store of information in SA, such as the customer or business that owns the server, whether the server is a staging or production server, which facility the server is located in, and custom name-value pairs.
- By sharing scripts without compromised security, users can share scripts with each other without compromising security because SA maintains strict controls on who can execute scripts on which servers and generates a comprehensive audit trail of script execution.

Agentless Server Discovery and Agent Installation

Agentless server discovery and agent installation allows you to deploy Server Agents to a large number of servers in your facility and place them under SA management.

You can perform the following tasks:

- Scan your network for agentless servers.
- Select servers for SA Agent installation.
- Select a communication tool and provide user/password combinations.
- Choose agent installation options and deploy agents.

Device Explorer

The Device Explorer lets you view information about servers in your managed environment.

From the Server Explorer, you can perform the following tasks:

- Create a server snapshot, perform a server audit, audit application configurations, create a package, and open a remote terminal session on a remote server.

— Browse a server's file system, registry, hardware inventory, software and patch lists, and services.

— Browse SA information such as properties, configurable applications, and even server history.

From the Groups Browser, you can perform the following tasks:

— Audit system information, take a server snapshot, and configure applications.

— View and access group members (servers and other groups).

— View group summary and history information.

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 Automationprovides:

- 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.

Service Automation Visualizer (SAV)

Service Automation Visualizer (SAV) is designed to help you optimally understand and manage the operational architecture and behavior of distributed business applications in your IT environment. Since these applications are complex collections of services that typically run across many servers, as well as network and storage devices, it can become increasingly difficult to understand (or remember) what is connected to what, where performance problems originate, how to troubleshoot and resolve problems, and what result would occur if you make a change in your environment.

SAV helps you see (visualize) this type of information through physical and logical drawings.

Storage Visibility and Automation

Storage Visibility and Automation offers storage management capabilities by enabling end-to-end visibility and management of the entire storage supply chain. Storage Visibility and Automation helps server administrators day-to-day tasks by providing tools that increase cost savings through application storage, dependency and visibility, storage audits, storage capacity and utilization trending, and scripting and automation. See the Storage Visibility and Automation User's Guide for more information.

Audit and Remediation

Audit and Remediation allows you to identify which objects you want checked, where you want to check for them, and when you want to check them in your IT environment.

- *Audit policies* define what to check—such as files, directories, configuration values, and so on.
- *Audits* define where to check—such as servers and server groups.
- *Audit schedules* define when to check—such as one time or as a recurring job.

These capabilities help you understand how to make your managed server environment compliant and how to keep your servers compliant. In SA, you can define server configuration policies to ensure that servers in your facilities meet policy standards. When servers are found to be *out of compliance*—not configured the way you want them to be—you can remediate them to comply with your organization's standards.

Using the SA Client, you can audit server configuration values based on a live server or a server snapshot, based on your own custom values, or based on pre-configured audit policies. You can also take server configuration snapshots to capture the current state of a system, so that you can compare other servers against a known baseline.

Audit policies allow you to define company or industry-wide compliance and security standards, which can then be used inside of audits, snapshot specifications, and other audit policies. Referencing audit policies in your audits or snapshot specifications helps verify that you are up to date with the latest compliance definitions in your organization.

Using Audit and Remediation, you can perform the following tasks:

- Compare servers or snapshots to reference servers or snapshots
- Create audits for repeated use
- Create audit policies that define compliance and security standards for your organization
- Associate audits with individual servers or dynamic server groups
- Remediate problems at multiple levels, including files, directories, patches, registry keys, and packages

Compliance in the SA Client

In the SA Client, the Compliance view allows you to see the overall compliance levels for all servers and groups of servers in your facility. From this view, which is commonly known as the *compliance dashboard*, you can remediate servers that are *out of compliance*. You can view compliance for an individual server, multiple servers, groups of servers, or for all servers under SA management.

The compliance dashboard displays the results of all compliance statuses on servers or groups of servers for audits, audit policies, software policies, patch policies, and application configurations. A server's compliance status is based on a *compliance policy.* A compliance policy defines unique server configuration settings or values to ensure that your IT environment is configured as it should be.

A compliance policy is typically created and defined by a *policy setter.* In some environments, a system administrator might be required to create an ad-hoc policy. The policy setter creates compliance policies and then attaches them to servers to ensure that servers are compliant with your organization's standards and policies.

For example, a policy setter can create a software policy that defines a standard set of patches and packages that must be installed on a server. The policy setter can also define the manner in which certain application files must be configured on a server. A server or group of servers is considered *compliant* if its configuration matches the rules, defined by the policy setter, in the compliance policy.

The compliance dashboard allows you to determine whether the server's actual installed software, packages, patches, and configuration files settings match the configuration defined in the *software policy*. The Compliance view allows you to view compliance for groups of servers, showing a compliance status rollup for all members and sub-group members of a group. From the Compliance view, you can discover servers and groups of servers that are *out of compliance* and then remediate any problems.

Reports

SA Reports provide comprehensive, real-time information about managed servers, network devices, software, patches, customers, facilities, operating systems, compliance policies, and users and security in your environment. These reports are presented in graphical and tabular format, and are actionable—where you can perform appropriate actions on objects, such as a policy or an audit, within the report. These reports are also exportable to your local file system (in `.html` and `.xls` formats) to facilitate use within your organization.

Software Management

SA Software Management provides a powerful mechanism to model software by using software policies and to automate the process of deploying software and configuring applications on a server in a single step. In addition, SA Software Management provides a structure to organize your software resources in folders and define security permissions around them. SA Software Management allows you to verify the compliance status of a server and remediate non-compliant servers.

SA Software Management provides the following capabilities:

- Creating an organizational structure for software
- Defining security boundaries for folders
- Defining a model-based approach to manage the IT environment in your organization
- Enabling sharing of software resources among user groups
- Deploying and configuring applications simultaneously
- Deploying multiple application instances on one server
- Establishing a software deployment process
- Verifying compliance status of servers to software policies
- Generating reports
- Comprehensively searching for software resources and servers

See Software Management Quick Start of the *SA User Guide: Software Management*.

Patch Management for Windows

Patch Management for Windows enables you to identify, install, and remove Microsoft® Windows patches, and maintain a high level of security across managed servers in your organization. You can identify and install patches that protect against security vulnerabilities for Windows operating systems.

See the *Server Automation Compatibility Matrix* for more information.

Because Windows patches are often released to address security threats, an organization must be able to roll out patches quickly, before systems are compromised. However, at the same time, patches themselves can cause serious problems, from performance degradation to server failures.

While patch management allows you to react quickly to newly discovered threats, it also provides support for strict testing and standardization of patch installation. And, if patches cause problems, even after being tested and approved, Windows patch management allows you to uninstall the patches in a safe and standardized way.

See Quick Start to Patch Management of the *SA User Guide: Server Patching*.

Patch Management for HP-UX

SA automates HP-UX Patch Management by enabling you to:

- Define HP-UX software policies that provide a model-based approach to managing your HP-UX servers. Server Automation enables you to create a model of your IT environment using HP-UX software policies. These software policies specify patches and scripts that can be installed on the managed servers.
- Install HP-UX patches and patch bundles on your managed servers.
- Establish a patch installation process.
- Schedule the stages of patch management: analysis, download, and installation. You can also set up email notification for each stage and associate a ticket ID for each job.
- Verify the compliance status of servers, based on software policies.
- Display the Compliance view to see whether servers are configured according to the software policy and to remediate non-compliant servers.
- Search for software resources and servers.
- Use the SA Library to search for HP-UX packages, patches, and software policies using powerful and flexible search criteria, such as availability, architecture, operating system, reboot options, version, and so on. You can also search for HP-UX software policies by name, folder name, availability, and operating system.
- View patch dependencies and patch applicability analysis while previewing patch installation.

See Quick Start to Patch Management of the *SA User Guide: Server Patching*.

Patch Management for Solaris and Solaris 11

Server Automation patch management for Solaris enables you to identify, install, and remove Solaris patches, and maintain a high level of security across managed servers in your organization.

Server Automation patch management for Solaris allows you to automate the process of installing and uninstalling Solaris patches and patch clusters on Sun Solaris using patch policies. In addition, SA analyzes the dependency, supersedence, and applicability relationships between patches in the policy and displays an updated and ordered list of patches that should be installed on the server. This feature allows you to verify the compliance status of a server and remediate non-compliant servers and automatically download the Solaris patches into SA and organize them into patch policies.

SA automates Solaris patching by enabling you to:

- Determine which patches your managed servers need.
- Create Solaris patch policies.
- Download Solaris patches, patch clusters, and patch bundles, and then store them, and related vendor information, in the SA Library.

- Resolve all dependent patches for Solaris patches.
- Install Solaris patches and patch clusters on managed servers.
- Install Solaris patches in single-user mode.
- Install patches by Oracle Solaris zones.
- Establish a patch installation process.
- Verify the compliance status of servers with patch policies.
- Search for software resources and servers.

See Quick Start to Patch Management of the *SA User Guide: Server Patching*.

Patch Management for Ubuntu

HP Server Automation (SA) patch management for Ubuntu enables you to identify, install, and remove Ubuntu Debian package updates, and maintain a high level of security across managed servers in your organization. You can identify and install Ubuntu packages that protect against security vulnerabilities for the SA-supported Managed Server platforms.

SA automates the key aspects of patch management while offering a fine degree of control over how and under what conditions Ubuntu packages are installed. By automating the patching process, patch management can reduce the amount of downtime required for patching. SA also allows you to schedule patch activity, so that patching occurs during off-peak hours.

Best Practice: With Ubuntu patching in SA, you can import the metadata before importing the binary packages. You can run the Ubuntu scanner with only the metadata downloaded to determine the server vulnerabilities. Then you can run the Ubuntu package importer to import only those packages that are required by managed servers. This practice saves you storage space as well as scan and remediation processing time.

The Ubuntu Patch Management documentation contains information about how to import Ubuntu metadata and packages, scan for vulnerabilities, and install Ubuntu package updates using patch policies.

SA automates Ubuntu patching by providing the following features and capabilities:

- **A central repository** where packages are stored and organized in their native formats.
- **A database** that stores information about every package that has been applied.
- **Dynamic Patch Policies** that analyze platform vulnerabilities based on the latest metadata from the vendor.
- **Advanced search** abilities that identify servers that require package updates.
- **Auditing abilities** for tracking the deployment of important package updates.

See Quick Start to Patch Management of the *SA User Guide: Server Patching*.

Patch Management for UNIX

Patch Management for UNIX enables you to identify, install, and remove patches, to maintain a high level of security across managed servers in your organization. Using the SA Client, you can identify and install patches that protect against security vulnerabilities for AIX operating systems.

SA allows you to react quickly to newly discovered security threats and also provides support for strict testing and standardization of patch installation. If patches cause problems after being tested and approved, SA allows you to uninstall the patches in a safe and standardized way.

SA stores patch information in the SA Library that includes detailed information about every server under management, the patches and software installed on the servers, and the patches and software available for installation. You can use this data to determine the severity of your exposure to a newly discovered threats, and to help assess the benefits of rolling out a patch versus the costs in downtime and testing requirements.

By automating the patching procedure, SA can reduce the amount of downtime required for patching. SA also allows you to schedule patch activity, so that patching occurs during off-peak hours.

Patch Management for UNIX provides the following capabilities that enable you to browse patches by a certain operating system, schedule patch downloads and installations, set up email notifications, preview a patch installation, use software policies and remediation to install and uninstall patches, and export patch information to a reusable file format:

- The SA Library where patches are stored and organized in their formats
- A database that includes information on every patch that has been applied
- Customized scripts that can be run before and after a patch is installed
- Advanced search abilities that identify servers that require patching
- Auditing abilities that enable security personnel to track the deployment of important patches

See Quick Start to Patch Management of the *SA User Guide: Server Patching*.

Application Configuration Management

Application Configuration Management (ACM) allows you to create templates so you can modify and manage application configurations associated with server applications. ACM enables you to manage, update, and modify those configurations from a central location, ensuring that applications in your facility are accurately and consistently configured.

Using ACM, you can perform the following tasks:

- Manage configurations based on files and objects, such as Windows registry, IIS metabase, WebSphere, COM+, and more.
- Preview configuration changes before applying them.
- Edit and push configuration changes to individual servers or server groups.
- Use information in the SA data model to set configuration values.
- Manage configurations of any application by building configuration templates.
- Audit the Application Configurations on a server to determine if any of the configuration files on the server are out of sync with the values stored in your templates.

See Quick Start to Application Configuration of the *SA User Guide: Application Configuration*.

Global Shell

The SA Global Shell enables you to manage servers by using a command-line interface. You can remotely perform the following tasks:

- Complete routine maintenance tasks on managed servers.
- Troubleshoot, identify, and remediate problems on managed servers.

The Global Shell consists of a file system and a command-line interface to that file system for managing servers in SA. The file system is known as the SA Global File System (OGFS). All object types in the OGFS (such as servers, customers, and facilities) are represented as directory structures in this file system.

The SA Global Shell also manages user permissions for accessing the file system, Windows Registry, and Windows Services objects on managed servers.