HP Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 9.0

Single-Host Installation Guide

Document Release Date: June 2010
Software Release Date: June 2010

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

Trademark Notices

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.

Document Changes

Chapter	Date	Version	Changes
	June 2010	9.0	Document Created

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

Contents

SA Single-Host Installation

This guide describes SA installation on a single host using the HP-supplied Oracle database.

Single-Host Installation Requirements

Supported SA Core Operating Systems

See the document *SA Supported Platforms*.

➤ Installation is supported on a physical host only, installation on virtual servers is not supported.

Supported Managed Server Operating Systems

For a complete listing of all platforms supported for SA, see the document *SA Supported Platforms* provided in the documentation directory of the distribution media or available for download at:

http://support.openview.hp.com/sc/support_matrices.jsp

SA 9.0 Installation Prerequisites

The SA Prerequisite Checker

The SA installation performs a prerequisite check to ensure that your server meets minimum baseline requirements for an SA installation. If your server fails to meet any of these requirements, the installation may fail. If this occurs, you may need to contact HP Technical Support to remedy the problem. The Prerequisite Checker also checks that the server meets certain recommended settings, however, these are recommendations and do not stop SA installation. For more information about SA prerequisites, see the *SA Simple/Advanced Installation Guide*.

MBSA 2.1 for SA 9.0

You must install Microsoft Windows MBSA 2.1 before beginning the SA installation. To obtain the required Windows patch management files, perform the following tasks:

1 Obtain the following files from Microsoft:

- **qchain.exe**

  The `qchain.exe` utility is a command-line program that chains hotfixes together.

When you chain updates, you install multiple updates without restarting the computer between each installation.

To download the package containing `qchain.exe`, search for “`qchain.exe`” at *http://www.microsoft.com* . Install the package on a Windows machine and note the location of the `qchain.exe` file.

- **WindowsUpdateAgent-x86.exe**

  The `WindowsUpdateAgent30-x86.exe` file is required to scan for patches on managed servers. To download the package containing `WindowsUpdateAgent30-x86.exe`, search for "Windows Update Agent" at *http://www.microsoft.com*. After downloading, you must rename the file "`WindowsUpdateAgent-x86.exe`".

- **WindowsUpdateAgent-x64.exe**

  The `WindowsUpdateAgent30-x64.exe` file is required to scan for patches on managed servers. To download the package containing `WindowsUpdateAgent30-x64.exe`, search for "Windows Update Agent" at *http://www.microsoft.com*. After downloading, you must rename the file "`WindowsUpdateAgent-x64.exe`".

- **WindowsUpdateAgent-ia64.exe**

  The `WindowsUpdateAgent30-ia64.exe` file is required to scan for patches on managed servers. To download the package containing `WindowsUpdateAgent30-ia64.exe`, search for "Windows Update Agent" at *http://www.microsoft.com*. After downloading, you must rename the file "`WindowsUpdateAgent-ia64.exe`".

2 Copy the files you obtained in the preceding steps to a directory that will be accessible by the SA Installer during installation. For example, you might copy the files to the following directory:

```
/opsw/win_util
```

3 Verify that the destination directory contains all these files:

```
WindowsUpdateAgent-x86.exe
WindowsUpdateAgent-x64.exe
WindowsUpdateAgent-ia64.exe
qchain.exe
```

4 Write down the name of the directory containing the Windows Update Agent files. You will need this location when you run the SA Installer and are prompted to provide the fully qualified directory path to the WUA files. You can also find the WUA file location by checking the SA parameter, `windows_util_loc`.

These patch management files will be copied to Windows servers when they are added to the server pool as SA managed servers. If you upload newer versions of the WUA files to SA later, they will be downloaded to all managed Windows servers during software registration. After the core is installed and running, you can upload new versions of these files with the Patch Settings window of the SA Client.

For more information about Windows Patch Management, see the *SA User’s Guide: Application Automation*.

Installation Basics

This section describes how to install SA on a *single-host server using the HP-supplied Oracle database*.

➤ If you plan to install a multiple-host SA Core, customize your SA Core Component layout, create a Multimaster Mesh, or use a database other than the HP-supplied Oracle database, you must use the advanced installation instructions in the *SA Simple/Advanced Installation Guide*.

Overview of the Installation Process

A single-host SA installation has the following phases:

1. *Pre-Installation*: Ensure that you have the information needed to complete the SA Installer interview, that you have all necessary permissions to complete the installation, and that you have the SA installation DVDs.
2. *Installing the HP-supplied Oracle Database*: The Oracle database is required for storage and tracking of information about your SA installation and its managed servers.
3. *Installation Interview*: Provide a password for the SA Administrator, choose a name for your SA facility, and specify the location of the required Windows patch management (MBSA) files.
4. Install SA.
5. *Upload SA content*: This is the minimum working set of data required for an SA functionality.
6. *Post-Installation*: Set up the SAS Web Client and the SA Client, create SA users.
7. *Search for Servers on your Network*: Scan for unmanaged servers on your network.
8. *Advanced post-installation tasks*: You may need to complete certain post-installation tasks based on the SA features you plan to implement.

Installation Procedure

This section contains instructions for running the Installer to install SA. The installer is a script called `install_opsware.sh` and is located on your SA distribution media.

Complete the following tasks to install SA:

Phase 1: Preparing to Install SA

1. You will need the *SA Product Software* DVD, *Agent and Utilities* DVD and the *Oracle_SA* installation DVD.
2. On the server where you will install the SA mount the *Product Software* DVD, *Agent and Utilities* DVD and the *Oracle_SA* DVD, or NFS-mount the directory that contains a copy of the DVD contents:

a Open a terminal window and log in as `root`.

b Change to the root directory:

```
cd /
```

The SA Installer must have *read/write root access* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Install the HP-supplied Oracle Database

Before SA begins the database installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements for the installation. The check insures that required packages are installed, required environment variables are set, sufficient diskspace is available, and so on. If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem or contact HP support services.

The SA distribution media includes an HP-supplied Oracle 11g Standard Edition database on the *Oracle_SA* DVD. Mount this DVD on the server you plan to use for your SA installation and enter the following command:

```
/<distro>/opsware_installer/install_opsware.sh
```

Once the database installation begins, you will be prompted to supply the values for two SA parameters:

- `opsware_admin user` (`truth.oaPwd`): the SA administrator password, the username is, by default, `admin`.

The password you specify here will the default password for all SA features that require a password unless you explicitly change the defaults.

- The name for your SA facility (`truth.dcNm`)

For more information about these parameters, see the “SA Installation Parameter Reference” in the *SA Simple/Advanced Installation Guide*.

You will see these prompts:

```
The Opsware Installer will now interview you to obtain the installation
parameters it needs. You can use the following keys to navigate forward
and backward through the list of parameters:

Control-P - go to the previous parameter
Control-N - go to the next parameter
Return - accept the default (if any) and go to the next parameter
Control-F - finish parameter entry
Control-I - show this menu, plus information about the current parameter

Press Control-F when you are finished. The Opsware Installer will perform
a final validation check and write out a response file that will be
used to install the Opsware components.

Parameter 1 of 2 (truth.oaPwd)Please enter the password for the opsware_admin
user. This is the password used to connect to the Oracle database.: opsware
```

```
Validating... OK.

Parameter 2 of 2 (truth.dcNm)Please enter the short name of the facility where
Opsware Installer is being run (no spaces): customer1
Validating... OK.

All parameters have values.  Do you wish to finish the interview? (y/n):
```

Press y to continue. You are then asked to supply the name of the response file in which to store your interview responses. The default is oiresponse.oracle.sas:

```
Name of response file to write [/usr/tmp/oiresponse.oracle_sas]:
Response file written to /usr/tmp/oiresponse.oracle_sas.

Would you like to continue the installation using this response file?
(y/n): y
```

Enter y to begin the database installation. When the installation is complete, a message to that effect is displayed. You can now continue with the SA installation.

Phase 3: Complete the SA Installer Interview and Install SA

Before SA begins the SA component installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements for the installation. The check insures that required packages are installed, required environment variables are set, sufficient diskspace is available, and so on. If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem or contact HP support services.

1. Mount the SA *Product Software* DVD. Invoke the installer script using the -r argument and specify the full path to the response file you created in Phase 2 (default: /usr/tmp/oiresponse.oracle_sas).

   ```
   /<distro>/opsware_installer/install_opsware.sh -r /usr/tmp/
   oiresponse.oracle_sas
   ```

2. The SA Installer displays the following or similar:

   ```
   <distro>/opsware_installer/install_opsware.sh -r /usr/tmp/
   oiresponse.oracle_sas

   Distribution version = opsware_<version>

   Script started, file is ...<log_information>

    Do you want to install all opsware components using default values of a
   single box core ?  (y/n): y
   ```

   The following is displayed simply because this is a first time installation.

   ```
   *******************************************
   The entry for "%oi.layout" in the response file does not exist or
   does not match the layout of the current system - legacy
   Forcing "--interview" mode
   *******************************************
   ```

During the following interview, the SA Installer uses the values you provided during database installation for the Administrator password and facility name. In addition you must provide the full path to the Windows Update Agent files you installed in MBSA 2.1 for SA 9.0 on page 7 (default:/opsw/win_util):

```
The Opsware Installer will now interview you to obtain the installation
parameters it needs. You can use the following keys to navigate forward
and backward through the list of parameters:

Control-P - go to the previous parameter
Control-N - go to the next parameter
Return - accept the default (if any) and go to the next parameter
Control-F - finish parameter entry
Control-I - show this menu, plus information about the current parameter

Press Control-F when you are finished. The Opsware Installer will perform
a final validation check and write out a response file that will be
used to install the Opsware components.

Parameter 1 of 3 (truth.oaPwd)Please enter the password for the
opsware_admin user. This is the password used to connect to the Oracle
database. [opsware]:
Validating... OK.

Parameter 2 of 3 (truth.dcNm)Please enter the short name of the facility
where Opsware Installer is being run (no spaces) [customer1]:
Validating... OK.

Parameter 3 of 3 (windows_util_loc)Please enter the directory that
contains the Microsoft's utilities (Press Control-I for list of required
files) [/tmp]: /opsw/win_util
Validating... OK.
```

3 When you have completed the interview, the Installer displays this message:

```
All parameters have values. Do you wish to finish the interview (y/n):
```

If you are satisfied with the parameter values you provided, press y.

If you want to review or change any values, press n. The Installer sequentially displays the parameters again, showing in brackets [ ] the values that you provided and provides a chance to change the values.

After modifying your responses, press y to finish the interview.

4 The installer prompts you to provide a file name to which your responses will be saved:

```
Name of response file to write
[/usr/tmp/oiresponse.slices_master_typical]
```

All of the parameter values you specified during the Interview will be written to a text response file and saved to the location you specify. You can enter the full path and name of the response file or accept the default location and name:

```
/usr/tmp/oiresponse.slices_master_typical
```

Record the fully qualified path to and name of the response file and store it where you can easily find it. You may need to use it again during future installations and upgrades.

5. After saving the response file, you can continue the installation using the response file you just created or end the installation and use the response file later.

   ```
   Would you like to continue the installation using this response file?
   (y/n):
   ```

   If you are satisfied with the responses you entered in the interview and you are ready to install SA now, enter y to continue.

➤ If you do not want to install SA after completing the interview, enter n. To use this response file later, invoke the Installer with the -r option and supply the fully qualified path to the file:

```
/opsware_system/opsware_installer/install_opsware.sh -r
<full_path_to_response_file>
```

6. After you press y to continue, SA is installed. A message is displayed when the installation is complete.

Phase 4: Upload the SA Content

1. In this phase, you must upload default content required for SA functionality. Mount the SA *Agent and Utilities* DVD or NFS-mount a directory that contains a copy of the DVD contents.

➤ The Installer must have *read/write root access* to the directories where it will install the SA data, including on NFS-mounted network appliances.

2. In a terminal window, log in as root and change to the root directory:

   ```
   cd /
   ```

3. Invoke the Installer with the -r (response file) argument. For example:

   ```
   <distro>/opsware_installer/install_opsware.sh -r
   /usr/tmp/oiresponse.slices_master_typical
   ```

   Specify the fully qualified path to the response file you saved in Phase 3, Step 4 above.

   The Installer displays following options:

   ```
   Welcome to the Opsware Installer.
   Please select the components to upgrade.
   1 ( ) Software Repository - Content (Install once per mesh)
   Enter a component number to toggle ('a' for all, 'n' for none.
   ```

4. At the install prompt, select `Software Repository - Content`:

   Press c to continue. The Installer uploads the SA content.

When the upload of the SA content completes, SA installation is done.

Phase 5: Post-Installation Tasks

Launch the SAS Web Client

To launch the SAS Web Client:

1 In a supported web browser, enter the following URL:

```
http://<SA_hostname>
```

where `<SA_hostname>` is the host name or IP address of the server on which you installed SA.

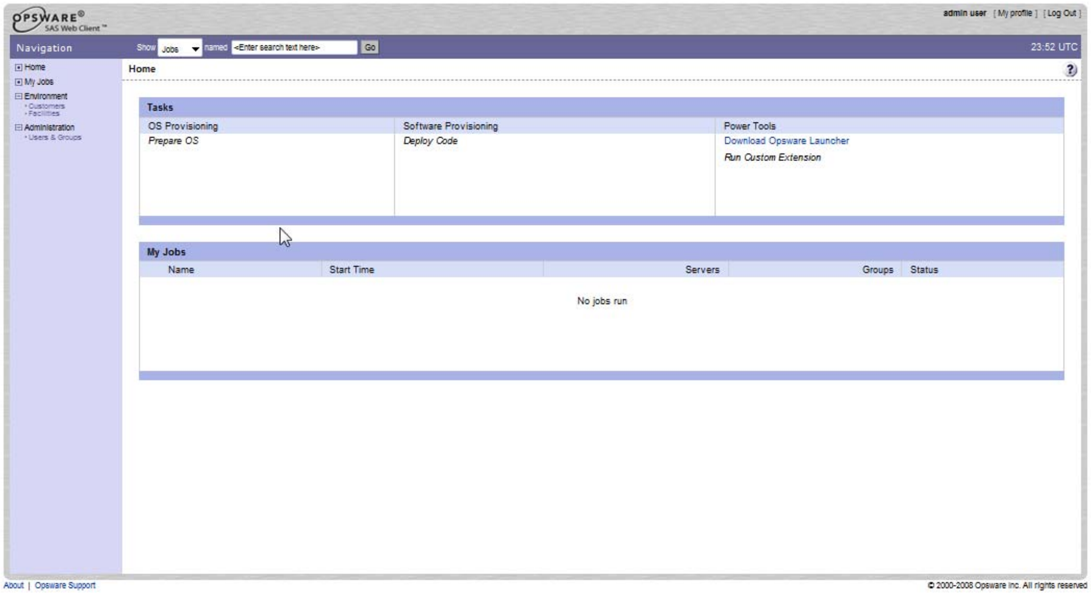
2 The browser displays instructions for installing the required SA security certificate.

3 The SAS Web Client Logon screen displays and prompts you for a user name and password.

Enter the SA Administrator username and password. The default is `admin` and the password you specified in Phase 1.

4 After you are logged in, you see the SAS Web Client home page.

Figure 1 The SAS Web Client Home Page]



Tasks

OS Provisioning	Software Provisioning	Power Tools
Prepare OS	*Deploy Code*	Download Opsware Launcher
		Run Custom Extension

My Jobs

Name	Start Time	Servers	Groups	Status

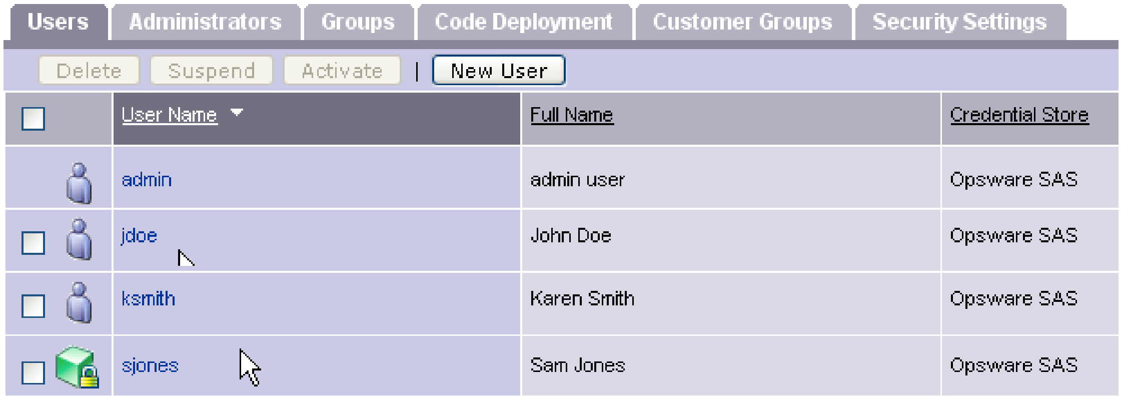
No jobs run

Create a User Account with Administrator Privileges

You must create a new Administrator user and assign the appropriate SA privileges.

1 From the Navigation panel on the left, select **Administration ➤ Users & Groups**. The Users & Groups: View Users screen displays.

Figure 2 Users & Groups: View Users Screen



□	User Name	Full Name	Credential Store
	admin	admin user	Opsware SAS
□	jdoe	John Doe	Opsware SAS
□	ksmith	Karen Smith	Opsware SAS
□	sjones	Sam Jones	Opsware SAS

2 Select the Users tab.

3 Click the New User button. The New User Profile Editor page displays.

4 Complete the required fields (labeled in bold font).

The Login User Name can be different than the first, last, and full names. The Login User Name is not case sensitive and cannot be changed after the user is created.

5 Under User Privileges: Group Membership, select the SA Administrators user group.

6 Click **Save** to create the new administrator user.

Create an SA User as a Member of the Software Policy Setters and Software Deployers User Groups

This user has the privileges to scan your facility's network for servers not yet managed by SA.

1 From the Navigation panel on the left, select **Administration ➤ Users & Groups**. The Users & Groups: View Users screen displays.

2 Select the Users tab.

3 Click the New User button. The New User Profile Editor displays'

4 Complete the required fields, which are labeled in bold font.

The Login User Name may be different than the first, last, and full names. The Login User Name is not case sensitive and cannot be changed after the user is created.

5 Under User's Privileges: Group Membership, click the checkbox for the Software Policy Setters and the Software Deployers user groups.

6 Click Save to create the new user.

Grant the Software Policy Setters and Software Deployers User Groups the Required Facility Privileges

1 From the Navigation panel on the left, select **Administration ➤ Users & Groups**. The Users & Groups: View Users screen displays.

2 Select the Groups tab.

3 Select the Software Policy Setters group.

4 Select the Facilities tab.

5 Enable read/write privileges for your facility for this user group.

6 Save your changes.

7 Do the same for the Software Deployers users group.

Download and Install the SA Client Launcher

➤ The SA Client requires a Microsoft Windows-based system that is connected to the network on which SA is installed.

The SA Client, which is required for some SA features, must be downloaded and installed.

1 Logon to the SAS Web Client as the SA Administrator user you created above.

1 From the SAS Web Client home page, click on *Download the SA Client* launcher link in the Power Tools panel on the upper right side of the screen.

2 Save the file to a directory on your local hard drive.

3 Double click the file to begin the installation and follow the on screen instructions.

Phase 6: Scan for Unmanaged Servers on your Network

In this phase, SA scans your network to discover any servers not managed by SA. After SA discovers your unmanaged servers, you are given the choice to bring each server into the SA Managed Server Pool.

You can scan for unmanaged servers in several ways:

- By specified IP addresses
- By IP address ranges
- Using pre-prepared lists of IP addresses

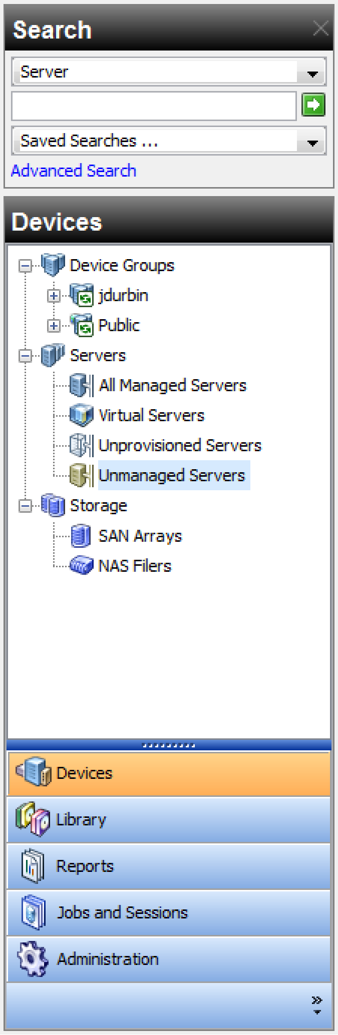
This section does not attempt to describe all methods, rather it uses a single method for simplicity. For more information about scanning for unmanaged servers (using the Discovery and Deployment utility (ODAD), see the *SA User Guide: Server Automation*.

Perform the following tasks to scan for an unmanaged server on your network:

1 Log on to the SA Client as the SA Superuser you created above by double clicking on the SA Client program file or shortcut.

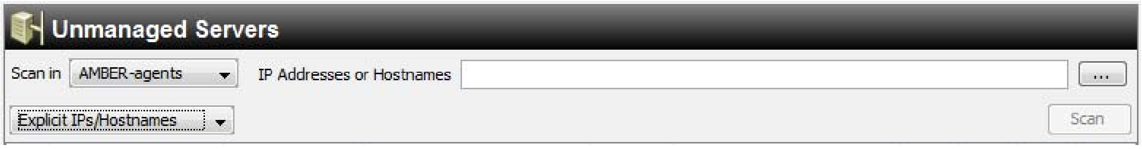
2 On the SA Client main screen, select the Devices tab and then select Unmanaged Servers in the navigation pane.

Figure 3 Select Unmanaged Servers



3 Select *Explicit IPs/Hostnames* from the drop down list to specify a list of specific IP addresses to scan, separated by spaces (commas not supported). For convenience, you can click the ellipsis (...) button to display a simple text editor that allows you to more easily enter multiple IP addresses. You can also save the file for future use. Clicking `OK` will cause the IP addresses you entered to populate the *IP Address or Hostnames* field.

Figure 4 Specifying Specific IP Addresses or Hostnames



Scan in AMBER-agents

IP Addresses or Hostnames

Explicit IPs/Hostnames

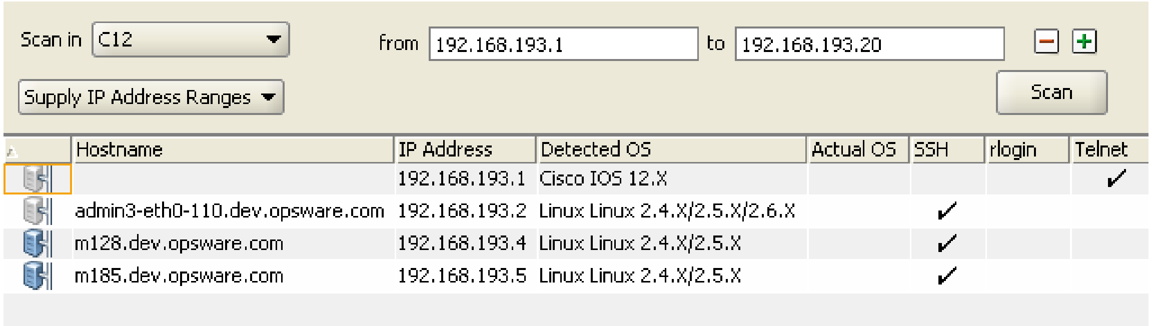
4 Click **Scan** to begin the scan for unmanaged servers.

When the scan is complete, a list of discovered unmanaged servers is shown. SA displays each server's:

- status
- IP address
- host name

- detected operating system
- any open ports that can be used to connect to the server.

Figure 5 Sample Unmanaged Server Scan Results



Scan in C12

from 192.168.193.1 to 192.168.193.20

Supply IP Address Ranges

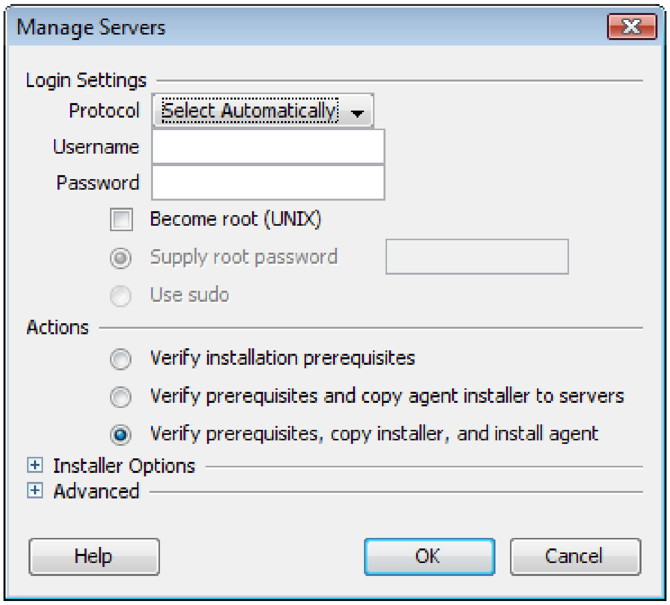
Hostname	IP Address	Detected OS	Actual OS	SSH	rlogin	Telnet
	192.168.193.1	Cisco IOS 12.X				✓
admin3-eth0-110.dev.opsware.com	192.168.193.2	Linux Linux 2.4.X/2.5.X/2.6.X		✓		
m128.dev.opsware.com	192.168.193.4	Linux Linux 2.4.X/2.5.X		✓		
m185.dev.opsware.com	192.168.193.5	Linux Linux 2.4.X/2.5.X		✓		

Bringing a server Under SA Management

1 Select server(s) you want to manage with SA. The SA Client supports hot keys to make multiple selections.

2 From the **Actions** menu, select **Manage Server**. The Manage Servers dialog box appears as shown

Figure 6 Manage Servers Dialog



Manage Servers

Login Settings

Protocol: Select Automatically

Username:

Password:

□ Become root (UNIX)

● Supply root password

○ Use sudo

Actions

○ Verify installation prerequisites

○ Verify prerequisites and copy agent installer to servers

● Verify prerequisites, copy installer, and install agent

⊞ Installer Options

⊞ Advanced

3 Select a network protocol to use for connecting to the server from the drop-down list.

In most cases, choosing *Select Automatically* to allow SA to select an appropriate protocol for each server is recommended.

For VMware ESXi servers where the Linux-based service console (COS) has been removed, you must choose VMware ESX Web Services. For more information on managing virtual servers, see the *SA User Guide: Server Automation*.

4 Enter a username and password to use for logging into the managed server.

Windows-based systems: log in using the Windows administrator username/password.

Unix-based systems: log in as `root`. If logging in as `root` is not permitted, select the *Become root (UNIX)* checkbox. Select *Supply root password* and enter the password or select *Use sudo* if `sudo` access is enabled for that account.

If you log in using `sudo`, the sudo user's configuration file (typically `/etc/sudoers`) must allow the account to run any command with root privileges. This is typically accomplished by using the "ALL" alias in the `sudoers` file.

➤ If you are unable to bring the server under SA management by logging in as root, see the *SA User Guide: Server Automation* for more details about logging in as a non-root user for agent deployment.

5 Select V*erify prerequisites, copy installer, and install agent*.

See "Agent Installation Using ODAD" in the *SA User Guide: Server Automation* for more information.

6 Accept the default Installer options.

7 Click **OK**. SA performs the required actions on the selected unmanaged servers to bring them into the Managed Server Pool.

8 The SA Client displays the results and updates the status icons for the new managed servers.

You can now use SA to manage these servers.

➤ At this point it would be a good idea to perform the tutorials in the *SA Getting Started* guide and become familiar with the SA interfaces and features. The *SA Getting Started* guide also provides interactive tutorials.

Phase 7: Optional Advanced Tasks

Depending on the SA features you plan to implement, there are additional advanced post-installation task you may need to perform. For more information about these tasks, see the *SA Simple/Advanced Installation Guide*.

Some of these tasks include:

- Unattended installation of the SA Client
- Configuring contact information in SA Help
- Installing Application Configuration (AppConfig) content
- Storage Visibility and Automation requirements
- Server Automation Reporting (SAR) requirements
- DHCP configuration for OS Provisioning
- Network configuration requirements for OS Provisioning
- Windows Patch Management preparation tasks