

# HP Operations Manager

For the UNIX and Linux operating systems

Software Version: 9.20

## Deploying SiteScope Configuration with HPOM

Document Release Date: May 2014

Software Release Date: May 2014



## 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 1993–2014 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

Java is a registered trademark of Oracle and/or its affiliates.

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

Oracle is a registered trademark of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

## 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/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](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>

# Contents

Contents .....	3
Introduction .....	4
Concepts and Tasks .....	5
SiteScope Concepts .....	5
HPOM Concepts .....	5
Integration Concepts and Tasks .....	6
Installation and Configuration .....	8
Setting up a User Name and a Password for the SiteScope Administrator .....	9
Obtaining SiteScope Web Service Files .....	9
Installing and Registering the SiteScope Subagent .....	10
Configuring Integration .....	11
Configuring on HPOM .....	12
Exporting SiteScope Templates from SiteScope and Importing Them to HPOM .....	14
Creating or Modifying a SiteScope Template and Exporting It to HPOM (on the Same System) .....	14
Exporting All SiteScope Templates to HPOM (on Different Systems) .....	16
opc_sis_template2pol Tool Usage .....	17
Viewing the Log File .....	17
Managing Credentials .....	18
Assigning and Deploying SiteScope Policies .....	21
Example of Deploying SiteScope Templates to the SiteScope Server .....	22
Example of Deploying SiteScope Templates to Virtual Nodes .....	23
Parameter Resolution in SiteScope Policies and Deployment of SiteScope Monitors .....	24
Symbolic Values .....	25
Deleting SiteScope Templates and Monitors .....	26
Configuration Report .....	27

## Introduction

Both HP Operations Manager (HPOM) and HP SiteScope are monitoring solutions whose primary objective is to monitor, control, and maintain systems in distributed heterogeneous environments. The HPOM management concept is based on communication between a management server and managed nodes (that is, HP Operations agent processes running on managed nodes throughout the environment), whereas SiteScope monitors without the deployment of agent software on the servers to be monitored.

The combined functionality of SiteScope and HPOM provides an effective and in-depth monitoring solution that enables you to manage SiteScope templates with HPOM. To fully utilize and benefit from all the advantages of proactive monitoring, you can operate with unified policy concepts between HPOM and SiteScope, which means that SiteScope templates and monitors can be configured through the HPOM policy assignment and deployment.

Using HPOM as a framework for installing or updating SiteScope templates provides the following advantages:

- Automatic deployment of templates based on the group policy assignment (desired state handling)
- Parallel installation or update of the configuration data on a large number of remote SiteScope installations
- Scheduled roll-out of template deployment
- Version control for templates (including roll-back functionality)
- Configuration report

## Concepts and Tasks

Using HPOM as a framework for managing SiteScope templates enables you to improve all the aspects of monitoring, controlling, and maintaining systems in distributed heterogeneous environments. When managing SiteScope templates with HPOM, you should be familiar with the HPOM and SiteScope concepts described in this section.

### SiteScope Concepts

In SiteScope, you use templates to deploy sets of monitors that check systems with similar characteristics in the infrastructure.

- Templates

Templates provide an enterprise solution for standardizing the monitoring of different IT elements in your enterprise, including servers, applications, databases, network environments, and so on.

- Monitors

Monitors are tools for automatically connecting to and querying different kinds of systems and applications used in enterprise business systems. Different monitor types provide generic capabilities for performing actions specific to different systems. You create one or more instances of a monitor type by specifying parameters in the corresponding templates to instruct SiteScope how to monitor specific elements in your IT infrastructure.

For detailed information about SiteScope, see the *SiteScope documentation* that you can find at the following locations:

- <http://support.openview.hp.com/selfsolve/manuals>
- On the HP Operations management server file system after the processes of installation and initial configuration are completed:

`/opt/OV/nonOV/tomcat/b/www/webapps/topaz/amdocs/eng/pdfs/`

### HPOM Concepts

In HPOM, a policy is a configuration element that consists of at least two files—a policy header (containing attributes such as a name, a type, and a version) and one or more policy bodies (containing actual agent configuration). The policy is identified either by its name, its version, and its type, or by its UUID. Each policy has a policy type, which means that its body conforms to a specific set of rules. In addition to policy types predefined in HPOM, custom policy types can be created by the user.

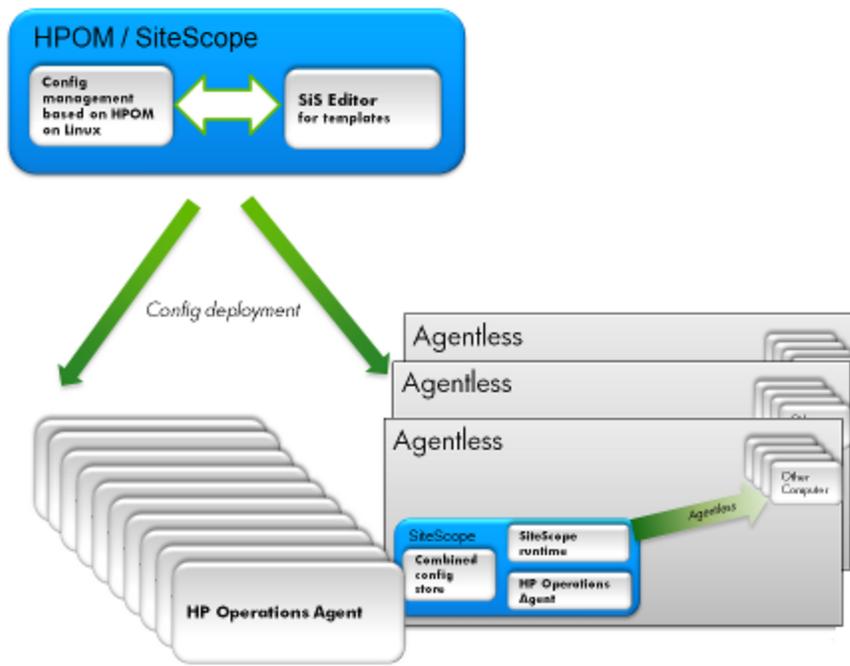
The policy group hierarchy is a tree-like arrangement in which each policy group is referenced through a unique path within the tree and has a world-wide unique UUID.

To add, modify, or delete policies and policy groups, use the `opcpolicy` command line tool . For detailed information about command options, see the `opcpolicy(1m)` manual page.

For detailed information about HPOM concepts and administration tasks, see the *HPOM Concepts Guide* and the *HPOM Administrator's Reference*.

## Integration Concepts and Tasks

The result of using HPOM as a framework for managing SiteScope templates is a SiteScope policy. The SiteScope policy is a SiteScope template that is converted into an HPOM policy and uploaded to the HPOM database. Its policy type is `sitescope`.



This integration allows you to easily upload SiteScope templates to HPOM by converting them into HPOM policies. This kind of policy can be enriched through a set of parameters (for example, a number of hosts that activate the deployment of the delivered template to monitors).

Managing SiteScope templates with HPOM involves the following:

- ["Exporting SiteScope Templates from SiteScope and Importing Them to HPOM"](#) on page 14
- ["Assigning and Deploying SiteScope Policies"](#) on page 21
- ["Deleting SiteScope Templates and Monitors"](#) on page 26
- ["Configuration Report"](#) on page 27

You can also deploy a SiteScope template with specified parameters (variables) as an HPOM policy to a SiteScope server. For details, see "[Parameter Resolution in SiteScope Policies and Deployment of SiteScope Monitors](#)" on page 24.

## Installation and Configuration

HPOM and SiteScope can be installed on the same system or on different systems. With some platforms (for example, Solaris and Linux) both products are supported, so it is possible to install HPOM and SiteScope on the same system. However, if you want to run an HP Operations management server on HP-UX, you must install SiteScope on a remote system because SiteScope cannot run on HP-UX.

To start using combined functionality of HPOM and SiteScope, your system must meet the following requirements:

- SiteScope version 11.12 or later is installed.

When installing SiteScope, make sure that SiteScope version 11.12 or later is installed on both of the following types of SiteScope servers:

- On the SiteScope system from which SiteScope templates will be exported and imported to the HP Operations management server.
- On all SiteScope systems that perform monitoring and are configured through the HP Operations management server by deploying policies.

After you install SiteScope, you can access it from the web browser. The default address is <http://localhost:8080/SiteScope>.

You can install the HP Operations agent during the SiteScope installation from the SiteScope installation media or after SiteScope is installed. For detailed information about installing the SiteScope subagent, see "[Installing and Registering the SiteScope Subagent](#)" on page 10.

- HPOM version 9.20 is installed.

**Note:** The HP Operations management server can run on Linux, Solaris, and HP-UX, whereas SiteScope can run on Linux, Solaris, and Windows.

After you have both SiteScope and HPOM installed, make sure to follow these tasks:

- Task 1: "[Setting up a User Name and a Password for the SiteScope Administrator](#)" on the next page
- Task 2: "[Obtaining SiteScope Web Service Files](#)" on the next page
- Task 3: "[Installing and Registering the SiteScope Subagent](#)" on page 10
- Task 4: "[Configuring Integration](#)" on page 11
- Task 5: "[Configuring on HPOM](#)" on page 12

## Setting up a User Name and a Password for the SiteScope Administrator

To set up a user name and a password for the SiteScope administrator in the SiteScope GUI, follow these steps:

1. Select **Preferences**→**User Management Preferences**.
2. In the User Management Preference window, double-click **SiteScope Administrator**.

The Edit Administrator window opens.

3. In the Edit Administrator window, enter the user name and the password.

## Obtaining SiteScope Web Service Files

**Note:** Obtaining SiteScope web service files is required if you plan to run the HP Operations management server on HP-UX. However, you can use *Method 2* to obtain web service files in other environments as well (for example, in an environment in which SiteScope resides on a Windows system).

To obtain the SiteScope web service files, choose one the following methods:

- **Method 1:**

Copy the following files from the SiteScope 11.12 or later installation to the same location (that is, /opt/HP/SiteScope/) on the HP Operations management server:

```
/opt/HP/SiteScope/integrations/om/lib/*.jar  
/opt/HP/SiteScope/WEB-INF/lib/ss_integration_om.jar  
/opt/HP/SiteScope/WEB-INF/lib/javacore.jar  
/opt/HP/SiteScope/integrations/om/bin/export_template_om.sh  
/opt/HP/SiteScope/integrations/om/bin/run_api_call.sh
```

- **Method 2:**

Use the OM\_SiS\_WebServicesClient.tar file that you can find at the following location on the HP Operations management server:

```
/opt/OV/contrib/OpC/SiteScope
```

The OM\_SiS\_WebServicesClient.tar file contains the following files:

```
/opt/HP/SiteScope/integrations/om/lib/*.jar  
/opt/HP/SiteScope/WEB-INF/lib/ss_integration_om.jar  
/opt/HP/SiteScope/WEB-INF/lib/javacore.jar
```

```
/opt/HP/SiteScope/integrations/om/bin/export_template_om.sh  
/opt/HP/SiteScope/integrations/om/bin/run_api_call.sh
```

To untar the `OM_SiS_WebServicesClient.tar` file, run the following commands:

```
cd /  
  
tar xvf /opt/OV/contrib/OpC/SiteScope/OM_SiS_WebServicesClient.tar
```

## Installing and Registering the SiteScope Subagent

The process of installing the SiteScope subagent differs depending on whether you have HPOM and SiteScope installed on the same system or on different systems. Choose one of the following ways:

- ***HPOM and SiteScope are installed on the same system:***

Depending on the platform, use either  
`/opt/HP/SiteScope/installation/components/oa_template_management/all/install.sh`  
or  
`<SITESCOPE_HOME>\installation\components\oa_template_management\all\install.bat` as follows:

- ***Solaris:***

```
install.sh -install solaris32  
  
install.sh -install solaris64
```

- ***Linux:***

```
install.sh -install linux32  
  
install.sh -install linux64
```

- ***Windows:***

```
install.bat -install windows32  
  
install.bat -install windows64
```

- ***HPOM and SiteScope are installed on different systems:***

Use the Configuration Tool. For example:

```
cd /opt/HP/SiteScope/bin
```

```
./config_tool.sh -i console
```

For detailed information about using the Configuration Tool, see the *SiteScope documentation*.

After you install the SiteScope subagent, make sure that the subagent process is registered by running the following command:

```
ovc -status AGENT
```

An output similar to the following one appears:

```
opcmsgi    OVO Message Interceptor    AGENT,EA    (23297) Running
agtrep     OV Discovery Agent          AGENT,AgtRep (28218) Running
opcacta    OVO Action Agent            AGENT,EA    (23302) Running
opcmona    OVO Monitor Agent           AGENT,EA    (21820) Running
opcple     OVO Logfile Encapsulator    AGENT,EA    (28164) Running
opcmsga    OVO Message Agent           AGENT,EA    (23340) Running
sisconfig  SiS Configuration          AGENT       (3667)  Running
```

All SiteScope subagent logs are added to `$OvDataDir/log/system.0.en_US`. In addition, an internal cache file can be found at the same location. For example, on Unix:

```
/var/opt/OV/log/system.0.en_US
Jul 27, 2011 3:29:56
PM;16;10;com.hp.ov.xpl.log.OvLogger;logMessage;com.hp.ov.opr.sisconfig;INFO;
Importing template to path: Deployed from Operations Manager/OVO:computer.compan
y.com/gena ping2 (:Gena),
templateName: gena ping2 succeeded
Jul 27, 2011 3:29:56
PM;17;10;com.hp.ov.xpl.log.OvLogger;logMessage;com.hp.ov.opr.sisconfig;INFO;
Enabling monitor group: Deployed from Operations Manager/OVO:computer.compan.y.co
m/gena ping2 (:Gena) done.
```

For troubleshooting purposes, you can remove the cache file after stopping the subagent with the `ovc -stop sisconfig` command. The location of the cache file where `sisconfig` stores information about which policies are deployed to SiteScope as well as about policy mapping to the SiteScope templates and monitor instances is as follows:

```
$OvDataDir/datafiles/sisconfig/polcache.temp
```

When you remove the cache file, make sure that you start `sisconfig` again. After that, you can redeploy the configuration from the HP Operations management server to start with the new configuration.

## Configuring Integration

On SiteScope, make sure that the OM integration is enabled. HPOM integration settings are available only if the OM integration is configured and SiteScope is connected to HPOM. By enabling the OM integration, additional functionalities of templates and monitors are available.

In SiteScope, configure the HP Operations agent connection settings to the HP Operations management server by following these steps:

1. Select **Preferences**→**Integration Preferences**.

In the Integration Preferences page, do one of the following:

- Click the **New Integration** button, and then select **HP Operations Manager Integration**.
- Select an existing integration, and then click the **Edit Integration** button.

2. In the HP Operations Manager Integration window, expand the HP Operations Manager Integration Main Settings panel, and then enter the installation path of the HP Operations agent on the SiteScope machine and the name or the IP address of the HP Operations management server.

3. Click **Connect** to connect the agent to the HP Operations management server.

A connection request is sent from the agent to the specified server.

**Caution:** Make sure that you enable SiteScope to send events to HPOM by selecting the Enable sending events check box in the Configuration Settings area. Additionally, if SiteScope and HPOM are installed on the same system, you must enable exporting all templates from SiteScope and importing them to HPOM as policies by selecting the Enable export template to OM check box.

4. *Optional:* Click the **Analyze** button to verify the success of each phase of the process. For example, you can verify connectivity between the agent and the server by checking the `bbcutil` connection protocol.

## Configuring on HPOM

On HPOM, check that a new policy type is registered by running the following command:

```
/opt/OV/bin/OpC/Utils/opcpoltype -list SiteScope
```

If the new policy is not registered, make sure to register it by running the following command:

```
/opt/OV/bin/OpC/Utils/opcpoltype -reg -xml  
/opt/OV/contrib/OpC/SiteScope/sitescope.xml
```

The following is an example of the new policy type that is registered on the HP Operations management server:

```
sitescope.xml  
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>  
<policyTypeList>  
  <policyType>  
    <policyTypeName>SiteScope</policyTypeName>  
    <policyTypeAgentType>sitescope</policyTypeAgentType>  
    <policyTypeUUID>f35c5cdb-63ed-448f-8fff-d192bdeac144</policyTypeUUID>  
    <policyTypeEditor>midas:text</policyTypeEditor>  
    <policyTypeTarget>agent</policyTypeTarget>
```

```
</policyType>  
</policyTypeList>
```

## Exporting SiteScope Templates from SiteScope and Importing Them to HPOM

Depending on whether HPOM and SiteScope are installed on the same system or on different systems, choose one of the following methods to export templates from SiteScope and import them to HPOM:

- If HPOM and SiteScope are installed on the same system:

["Creating or Modifying a SiteScope Template and Exporting It to HPOM \(on the Same System\)" below](#)

- If HPOM and SiteScope are installed on different systems:

["Exporting All SiteScope Templates to HPOM \(on Different Systems\)" on page 16](#)

### Creating or Modifying a SiteScope Template and Exporting It to HPOM (on the Same System)

If HPOM and SiteScope are installed on the same system, you can create or modify a template in SiteScope and then move this template to HPOM. This means that you can either create a new template or modify an existing template to contain the text or the variables that you choose, and then import this template to HPOM.

To create or modify a template and then import it to HPOM, follow these steps:

1. In the SiteScope user interface, select the **Templates** context.

The template tree is displayed in the left pane.

2. Depending on whether you want to create a new template or modify an existing template, do one of the following:

- Create a SiteScope template within a template container.

You create a template by adding and configuring groups, remote server definitions, monitors, alerts, and variables to the template. You use template variables as substitution markers for configuration settings that you want to change dynamically or interactively each time you deploy the template. For details, see ["Managing Credentials" on page 18](#).

SiteScope also provides template examples for monitoring in Windows and UNIX environments (Unix HP basic template and Windows basic template). These templates are available from the Template Examples folder in the template tree. The following example shows Windows basic template. This template contains a template

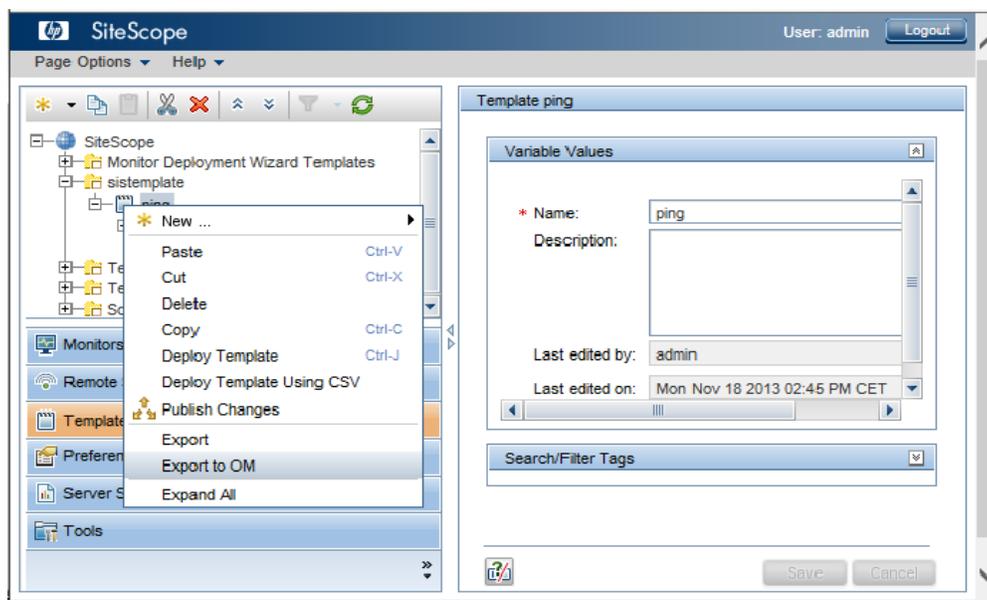
group, Windows monitors for %%host%, two template monitors (CPU and Memory), four user-defined variables (host, user, password, and frequency), and a template remote server.

For detailed information about creating templates, see the *SiteScope documentation*.

- Choose the template that you want to modify from the Monitor Deployment Wizard Templates template container, and then modify its properties to meet your needs.

**Note:** When modifying a template belonging to the Deployed from Operations Manager template container, it is recommended that you create your own template container that you will use for the development, copy the template to this new template container, and then modify the template.

3. From the template tree, right-click the template or template container that you want to import to HPOM, and then select **Export to OM**, as shown in the following figure:



After a short time, an output similar to the following one should be displayed:

Template was successfully exported to Operations Manager.

**Note:** If you modify the same template or template container in SiteScope and then again select **Export to OM**, a new version is created because the binary file changed. This means that the policy version is always increased when a new HPOM policy related to this template is uploaded to the HPOM database.

4. In the OMU context of the Administration UI, from the Administrative menu, click **Browse**→**Policy Bank**, and then check that the template is imported.

After you successfully import the SiteScope template to HPOM (the template is also converted to the HPOM policy), you can continue with the policy assignment and deployment. For details, see ["Assigning and Deploying SiteScope Policies" on page 21](#).

## Exporting All SiteScope Templates to HPOM (on Different Systems)

If HPOM and SiteScope are installed on different systems, you can export all SiteScope templates from a SiteScope server and import them to the HP Operations management server by using the `opc_sis_template2pol` command line tool. By downloading all templates from a specific container on a remote or local SiteScope server and uploading them to the HP Operations management server, templates are converted into policies of the SiteScope policy type, allowing you to assign and deploy them.

To export all templates from SiteScope and import them to HPOM as policies, on the HP Operations management server, run the following command:

```
/opt/OV/bin/OpC/opc_sis_template2pol -sis_group_container <sis_group_container> -sis_user <sis_user> -sis_passwd <sis_passwd> -sis_hostname <sis_hostname>
```

In this instance, `<sis_group_container>` is a group container for all SiteScope templates, `<sis_user>` is a SiteScope user (usually `admin`), `<sis_passwd>` is the password of the SiteScope user, and `<sis_hostname>` is the hostname of the system where SiteScope runs (the default is the local host).

For example:

```
/opt/OV/bin/OpC/opc_sis_template2pol -sis_group_container sistemplate -sis_user admin -sis_passwd admin
```

The following is an example output:

```
Target Policy Group set to default: SitescopePolicies
```

```
Convert to OM Policy:
```

```
Source SiS Template: VMware Host
```

```
Source SiS Template: ping
```

```
Source SiS Template: Unix HP basic template
```

```
opcpolicy upload policies
```

```
dupl_ignored: "ping (:sistemplate)" 0001.0000 SiteScope
```

```
uploaded: "Unix HP basic template (:sistemplate)" 0001.0012 SiteScope
```

```
uploaded: "VMware Host (:sistemplate)" 0001.0016 SiteScope
```

```
1 policies out of 3 from directory /var/opt/OV/share/tmp/OpC/mgmt_sv/tmp_sis/templates/27173/pol were uploaded, check logfile
```

```
opcpolicy upload groups
```

```
Operation successfully completed.
```

After you run the `opc_sis_template2pol` command, check in the Administration UI that a root element named `SitescopePolicies` is created in the HPOM Policy Bank. You can view the elements contained within `SitescopePolicies` by clicking **SitescopePolicies**. To further view the elements, simply click the desired item.

After you successfully download the information from the SiteScope system and upload it to the HP Operations management server (that is, after you convert templates to policies), you can continue with the policy assignment and deployment. For detailed information about assigning and deploying policies, see ["Assigning and Deploying SiteScope Policies" on page 21](#).

## opc\_sis\_template2pol Tool Usage

The usage of the `opc_sis_template2pol` command line tool is as follows:

```
opc_sis_template2pol -help |
    { -sis_group_container <directory> |
      -sis_template_file <XML_template_file> }
    [ -sis_hostname <hostname> ]
    [ -sis_user <user> ]
    [ -sis_passwd <passwd> ]
    [ -sis_port <port> ]
    [ -target_group <policy_group> ]
```

The following table shows which options are available with this command line tool and their descriptions:

<b>opc_sis_template2pol Command Line Tool Options</b>	<b>Description</b>
<code>-sis_group_container &lt;directory&gt;</code>	Group container for all SiteScope templates to be downloaded from SiteScope and uploaded to HPOM
<code>-sis_template_file &lt;XML_template_file&gt;</code>	Single template to be downloaded from SiteScope and uploaded to HPOM
<code>-sis_hostname &lt;hostname&gt;</code>	Hostname of a remote system where SiteScope runs (the default is local host)
<code>-sis_user &lt;user&gt;</code>	SiteScope user (usually <code>admin</code> )
<code>-sis_passwd &lt;passwd&gt;</code>	Password for a SiteScope user
<code>-sis_port &lt;port&gt;</code>	SiteScope port number (if it is not specified, use <code>8080</code> )
<code>-target_group &lt;policy_group&gt;</code>	Target group on HPOM to which templates are uploaded (the default is <code>SitescopePolicies</code> )

## Viewing the Log File

While exporting templates from SiteScope and importing them to HPOM, the following log file is created:

```
/var/opt/OV/log/OpC/mgmt_sv/opc_sis_template2pol.log
```

In this log file, you can find the information about the processes that take place after you run the `opc_sis_template2pol` command.

## Managing Credentials

When managing credentials for SiteScope resources that require user authentication, you are allowed to add, update, and delete credentials that are used in configuring SiteScope monitors and templates. HPOM administrator uses `CRYPT:<VALUE>` in a variable to crypt the value of SiteScope policy variables. For example, if one of the policy variables is a password, this password must be encrypted:

```
variables:      host=%%NODEGROUP:SiteScopeNodes%%,user=root,
                password=CRYPT:<password>,frequency=700
```

After encryption is done (during the process of storing the data into the database), the next time you modify the policy, it looks as follows:

```
variables:      host=%%NODEGROUP:SiteScopeNodes%%,user=root,
                password=1ABG1S2688L4KdVnJ2/SpA==,frequency=700
```

SiteScope credentials must be available on the agent to access SiteScope. The following three methods that are available for managing the SiteScope password are listed in the order of the priority (1-3, with number 1 being of greatest priority):

1. Use a local command line tool to set the credentials that are called on the SiteScope system:

- *On Windows:*

```
%OvInstallDir%\sbin\siskonfig\sisSetCredentials.bat
```

- *On UNIX:*

```
/opt/OV/sbin/siskonfig/sisSetCredentials.sh
```

An output similar to the following one should be displayed:

```
Set SiteScope login credentials for agent siskonfig connector.
SiteScope login: admin
SiteScope password:
Repeat SiteScope password:
SiteScope port: 8080
Updating config namespace with sitescope login data.
```

The credentials can be verified by using `ovconfget opr.siskonfig`.

2. Deploy the `xpl conf` credentials with the `nodeinfo` policy:

For example:

```
;XPL config
[opr.sisconfig]
sis_login=admin
sis_password=CRYPT:<password>
sis_port=8080
```

This results in the following:

```
;XPL config
[opr.sisconfig]
sis_login=admin
sis_password=1ABG1S2688L4KdVnJ2/SpA==
sis_port=8080
```

To encrypt `sis_passwd=CRYPT:<value>`, you must enable the CRYPT functionality by running the following command:

```
/opt/OV/bin/ovconfchg -ovrg server -ns opc -set OPC_NODEINFO_CRYPT
TRUE
```

**Caution:** Make sure that you always first deploy credentials, and then SiteScope policies.

3. Use the Sam Admin to add the SiteScope note with `user/passwd/port`:

```
https://<HPOM_server>:8444/topaz/samadmin/GetSiteScopesList.do
```

The user and the password are as follows:

```
user: opc_adm
passwd: <passwd_of_opc_adm>
```

In the Sam Admin, add SiteScope. The credentials are then included in the SiteScope policy header.

To check the policy, run the following command:

```
/opt/OV/bin/ovpolicy -list -level 4
```

An output similar to the following one should be displayed:

```
sitescope          "Unix HP basic template (:rose)"  enabled  0001.0002
  policy id       : "78492476-b467-71e0-1326-103946370000"
  owner          : "OV0:computer.company.com"
  category       : <no categories defined>
  attribute (1)  : "product_id" ""
  attribute (2)  : "checksum_header" "42c5d0e5b5ee00bcb82353e7b8c1567ae9052
313"
  attribute (3)  : "version_info" ""
  attribute (4)  : "version_id" "d32e86d2-b468-71e0-1326-103946370000"
  attribute (5)  : "SitescopeUser" "admin"
```

```
attribute (6) : "SitescopePassword" "gFQ3HLKJe+Env0hvE0yhA=="  
attribute (7) : "SitescopePort" "8080"
```

## Assigning and Deploying SiteScope Policies

After SiteScope templates are uploaded to HPOM as policies, you can continue with the assignment and deployment of such policies to managed nodes.

**Caution:** Make sure that you always first deploy credentials, and then SiteScope policies.

To assign and deploy a SiteScope policy, follow these steps:

1. In the OMU context of the Administration UI, from the Administrative menu, click **Browse**→**Policy Bank**.
2. From the list of all policies and policy groups, select the policy that you imported to HPOM and you want to deploy.

The attributes and values of the selected policy are displayed.

**Caution:** Do not change the name of the policy or the policy group. If you do so, the deployment may fail.

3. Check the attributes and values of the selected policy or policy group, determine to which node or node group you need to assign the selected policy or policy group, and then do the assignment by following these steps:
  - a. Click **Assign to Node / Node Group...**, and then choose the node or the node group to which you want to assign the selected policy or policy group.
  - b. Click the **OK** button.
4. After you assign the policy or the policy group to the node or the node group, you must distribute it to the node or the node group by selecting **Deploy Configuration...** from the Actions Menu.

The window containing the elements to be deployed appears.

5. Make sure that the following check boxes are selected:
  - Distribute Policies
  - Distribute Actions
  - Distribute Monitors
  - Distribute Commands
  - Distribute Instrumentation

6. After you select the needed check boxes, click the **OK** button.

A note similar to the following one should appear:

```
Distribution was successful.
```

```
Additional information:
```

```
Node computer2.company.com:
```

```
Create distribution data and inform agent...Done.
```

```
Create distribution data and inform agent...Done.
```

After assigning and deploying a policy, you see an output similar to the following one after you run the `/opt/OV/bin/ovpolicy -list` command:

```
* List installed policies for host 'localhost'.
```

Type	Name	Status	Version
sitescope	"ping_var_host (:rose)"	enabled	0001.0002

In SiteScope, a new template container appears, Deployed from Operations Manager. This template container is created during the deployment and the deployed SiteScope template is listed there.

## Example of Deploying SiteScope Templates to the SiteScope Server

Usually a SiteScope template is assigned to the SiteScope server and not to the system that should be monitored by this SiteScope server.

In this example, SiteScope server S1 monitors nodes n1, n2, and n3 with the SiteScope ping template. The data file of the SiteScope ping policy is similar to the following one:

```
variables:  
host=%%NODEGROUP:ping_node_group%%,interval=600
```

If you add nodes n1, n2, and n3 to the HPOM node group `ping_node_group`, during the deployment to S1, the policy is resolved as follows:

```
variables:  
host=n1,interval=600  
host=n2,interval=600  
host=n3,interval=600
```

Thus, the parameters are specified for SiteScope server S1.

If you do not want to add nodes n1, n2, and n3 into the HPOM node bank, you can also use the `%%FILE:<nodename_file>%%` resolution type instead of `%%NODEGROUP:<nodegroup>%%`. In

this case, `<nodename_file>` points to the file that contains node names (one node name per line). This file can be managed by another application, for example, an asset management tool.

## Example of Deploying SiteScope Templates to Virtual Nodes

You can also assign SiteScope policies to the node that should be monitored. To do this, add this system as a virtual node to the HPOM node bank (for details, see the *HPOM documentation*). The physical node of this virtual node must be the SiteScope server that performs the monitoring. When deploying configuration to this virtual node, the policies are deployed to the SiteScope server.

## Parameter Resolution in SiteScope Policies and Deployment of SiteScope Monitors

Deploying a SiteScope monitor with HPOM means that a SiteScope template with specified parameters (variables) is deployed as an HPOM policy to a SiteScope server<sup>1</sup>.

A SiteScope policy consists of four files that correspond to the SiteScope template from which the policy is derived. These files are similar to the following ones:

```
Header file:          e3e30af4-b2d1-71e0-1cb3-103925be0000_header.xml
Data:                e3e30af4-b2d1-71e0-1cb3-103925be0000_data
Parameter definition: e3e30af4-b2d1-71e0-1cb3-103925be0000_params.xml
Binary SiteScope template: e3e30af4-b2d1-71e0-1cb3-103925be0000_sis
```

The above files represent a pure and uninstantiated template. However, when monitors (that is, instances of templates that are created by replacing the variables in the templates with their actual values) are created from the SiteScope policy, the SiteScope policy becomes instantiated. Instantiation takes place on the HP Operations management server before the configuration is deployed to the SiteScope servers. You can also use the Administration UI policy editor to edit the policy data part and add or remove monitors.

The structure of the template data file is as follows:

```
Source_template: <template_name_in_sitescopes>
variables       : <var_name_1>=<value_1>[,<var_name_2>=<value_2>[,...]]
```

For example:

```
Source_template: ping_var_host
host=%HOST%,user=me,port=8080
```

The symbolic values (`%%value%%`) are replaced when you create a monitor from this template by filling in the required values. For more information on symbolic values, see ["Symbolic Values" on the next page](#).

**Caution:** You may not change the value of `Source_template` because it represents the link to the SiteScope template name that is defined in the binary file.

It is possible to duplicate the variables line. In this case, each line specifies one monitor instance.

For example:

```
variables:      myhost1.company.com,user=me,port=8081
                myhost2.company.com,user=you,port=8082
```

<sup>1</sup>Deploying SiteScope monitors through HPOM policies allows you to deploy more than one monitor through a policy.

## Symbolic Values

For convenience, you can use a series of symbolic values in the template variables. These symbolic values are resolved to their actual values during deployment.

For example:

```
variables:    host=%%HOST%%
             %%NODEGROUP:<nodegroup_name>%%
             %%FILE:<file>%%
             %%FILE:<file>.$SISHOST%%
```

%%HOST%% is resolved through the node name of a node to which the policy is distributed.

%%NODEGROUP:<nodegroup\_name>%% uses all nodes that are assigned to a specified node group.

%%FILE:<file>%% is a file on the HP Operations management server that includes a list of nodes.

%%FILE:<file>.\$SISHOST%% is a file on the HP Operations management server that includes a list of nodes with the extension of the node name on which SiteScope runs.

## Deleting SiteScope Templates and Monitors

To delete all HPOM deployed templates and monitors, simply deassign all HPOM policies. By doing this, the `sisconfig` subagent deletes all Deployed from Operations Manager folders from the SiteScope Monitors and Templates.

## Configuration Report

The following are the examples of the commands that you can use to generate reports:

- Desired state of the SiteScope template distribution:

```
/opt/OV/bin/OpC/opcragt -distrib -force -simulate computer1
```

**Note:** When the `-simulate` option is used together with the `-distrib` option, `opcragt` displays the files that will be deployed to the managed node.

```
Node computer1.company.com:
Deployment information for node computer1.company.com
-----
Policies:
  UnixBasicSisTemplate (SiteScope), version 0001.0001
  DiscoverOM (Service_Auto_Discovery), version 0001.0000
  SiteScope Discovery (Service_Auto_Discovery), version 0003.0001
  computer2_Parameters (SiteScope_DeployTemplates), version 0001.0002
Done.
```

If the policy is assigned to virtual nodes and not directly to the SiteScope server, you can check the list of nodes. For example, if the ping template is assigned to virtual nodes `myhost.company.com` and `yourhost.company.com`, and both virtual nodes are served through SiteScope server `mySiSsrv.company.com`, run the following command to check the list of nodes:

```
/opt/OV/bin/OpC/opcragt -dist -simulate mySiSsrv.company.com
```

The output is as follows:

```
...
  PingTemplate (:PingGroup) (SiteScope), version 0002.0000
    applied for nodes: myhost.company.com,yourhost.company.com
```

- All SiteScope templates imported to the HPOM database (lists names, types, and versions of all policies in the HPOM database):

```
/opt/OV/bin/OpC/utills/opcpolicy -list_pols pol_type=sitescope
```

List of all Policies in the HPOM database:

```
=====
Name          = JoSeTMPL (JoSeGRP)
Version       = 0001.0021
Type (GUI)    = SiteScope
Type (agent)  = sitescope
```

```
=====
Name          = Unix template (:Import)
Version       = 0001.0000
Type (GUI)    = SiteScope
Type (agent)  = sitescope
=====
Name          = Unix template (:Import rose)
Version       = 0001.0000
Type (GUI)    = SiteScope
Type (agent)  = sitescope
=====
Name          = Unix template (:Import rose)
Version       = 0001.0001
Type (GUI)    = SiteScope
Type (agent)  = sitescope
=====
```

- All configuration items or nodes that have the specific SiteScope template through the policy assignment:

```
/opt/OV/bin/OpC/utils/opcpolicy -list_resolved_assigns pol_
name=UnixBasicSisTemplate pol_type=SiteScope
```

```
computer2.company.com
computer5.company.com
computer3.company.com
computer3.company.com
computer21.example.ad
computer1.company.com
computer1.company.com
```

