# HP SiteScope

for the Windows, Solaris, and Linux operating systems

Software Version: 11.24

# Failover Manager Guide

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 Notices

© Copyright 2005 - 2014 Hewlett-Packard Development Company, L.P.

## Trademark Notices

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

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

iPod is a trademark of Apple Computer, Inc.

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

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

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

UNIX® is a registered trademark of The Open Group.

## Acknowledgements

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

This product includes software developed by the JDOM Project (**http://www.jdom.org**).

## 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 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**

# Table of Contents

# Welcome to This Guide

This guide provides detailed instructions on how to deploy, configure, and administer HP SiteScope Failover Manager to provide backup infrastructure monitoring availability after a SiteScope server failure.

---

**Note:** The classic SiteScope Failover (automated mirroring) solution was reinstated as a replacement for the SiteScope Failover Manager (shared drive architecture) solution which was introduced in SiteScope 11.00. While Failover Manager is supported for this release, we plan to stop support for it in the near future. If you are using the Failover Manager solution, we recommend that you start evaluating a move to the classic SiteScope Failover solution.

With the recent improvements, classic SiteScope Failover is a more robust solution. It is easy to install and configure, and it does not require additional hardware (you do not need a network drive to store SiteScope configuration data). For details on using the SiteScope Failover, see the *HP SiteScope Failover Guide* in **<SiteScope root directory>\sisdocs\pdfs\SiteScopeFailover.pdf**.

---

**This chapter includes:**

## How This Guide Is Organized

This guide contains the following chapters:

**Part I Introducing SiteScope Failover Manager**

Describes the SiteScope Failover Manager monitoring solution.

**Part II Deploying SiteScope Failover Manager**

Describes deployment planning and best practices, as well as how to install and configure the SiteScope Failover Manager environment. It also describes the SiteScope Failover Manager configuration files and settings.

**Part III Administering SiteScope Failover Manager**

Describes how to use the Failover Monitoring solution templates, and how to work with SiteScope Failover Manager after a failover event. It also describes how to use SiteScope Failover Manager with integrations, and how to troubleshoot problems.

**Part IV Appendix**

Describes how to configure Microsoft Cluster Service as an alternative solution for providing failover on SiteScope machines.

## Who Should Read This Guide

This guide is for the following users of SiteScope:

SiteScope administrators

Readers of this guide should be knowledgeable about enterprise system administration and SiteScope.

## How Do I Find the Information That I Need?

This guide is part of the HP SiteScope Help. The SiteScope Help provides a single-point of access for all SiteScope documentation.

You can access the SiteScope Help by selecting **Help** > **SiteScope Help** on the SiteScope server.

## Additional Online Resources

**Troubleshooting & Knowledge Base** accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help** > **Troubleshooting & Knowledge Base**. The URL for this Web site is http://h20230.www2.hp.com/troubleshooting.jsp.

**HP Software Support** accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help** > **HP Software Support**. The URL for this Web site is www.hp.com/go/hpsoftwaresupport.

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

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

To register for an HP Passport user ID, go to:

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

**HP Software Web site** accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help** > **HP Software Web site**. The URL for this Web site is www.hp.com/go/software.

## Documentation Updates

HP Software is continually updating its product documentation with new information.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to the HP Software Product Manuals Web site (http://h20230.www2.hp.com/selfsolve/manuals).

# Part I

## Introducing SiteScope Failover Manager

# 1

# Introduction to SiteScope Failover Manager

**This chapter includes:**



## About SiteScope Failover Manager

**Note:** The SiteScope Failover Manager solution (introduced in SiteScope 11.00) has been deprecated. While the shared-drive solution is supported for this release, HP might stop supporting it in the future. If you are using this solution, we recommend that you start evaluating a move to the classic SiteScope Failover solution. Based on customer feedback and preference, the classic SiteScope Failover solution was revived and enhanced. With the recent improvements, classic SiteScope Failover is a more robust solution, that is easier and cheaper to maintain. For details on the classic SiteScope Failover solution, see the *HP SiteScope Failover Guide* in **<SiteScope root directory>\sisdocs\pdfs\SiteScopeFailover.pdf**.

HP SiteScope Failover Manager is a special version of SiteScope that includes automated failover functionality. It enables you to implement failover capability for infrastructure monitoring by making sure that a failed SiteScope machine is automatically and quickly replaced by a different machine, with little service disruption.

A failover is a backup operation that automatically switches the functions of a primary system to a standby server if the primary system fails or is temporarily taken out of service. Provisioning for a failover is an important fault tolerance function for mission-critical systems that require high availability. In the event of a primary SiteScope failure, SiteScope Failover Manager performs automatic failover and transfers the service provided by the failed system to the backup system.

## Benefits of SiteScope Failover Manager

The SiteScope Failover Manager solution provides the following benefits:

- SiteScope Configuration sharing:
  - SiteScope is installed on a shared resource that is accessible to the failover machine.
  - When a primary SiteScope is down, the SiteScope Failover process activated by SiteScope Failover Manager continues monitoring from the exact point where the primary SiteScope left off.
  - No data loss in reports.
  - No configuration copying (configuration changes between primary and failover servers are transparent).
  - Configuration changes made on SiteScope Failover Manager are available on the primary SiteScope.

- SiteScope Failover Manager installation:
  - Standalone management application with no user interface, that is responsible for managing primary and failover instances. It is installed on a local disk—not on the shared resource.
  - SiteScope Failover Manager can monitor multiple primaries simultaneously from a single Failover Manager machine, and provide automatic backup for a single SiteScope instance during failover.
  - The data storage requirements for SiteScope Failover are significantly less than for a primary SiteScope. This is because the function of SiteScope Failover is to provide temporary monitoring continuity if a primary SiteScope fails.
- SiteScope Failover Manager is freely included with your regular SiteScope installation.

---

**Note:** Earlier versions of SiteScope Failover Manager were called **SiteScope High Availability**, which is sometimes referred to as **SiteScopeHA**. This name and reference may still appear during installation and use of the product.

---

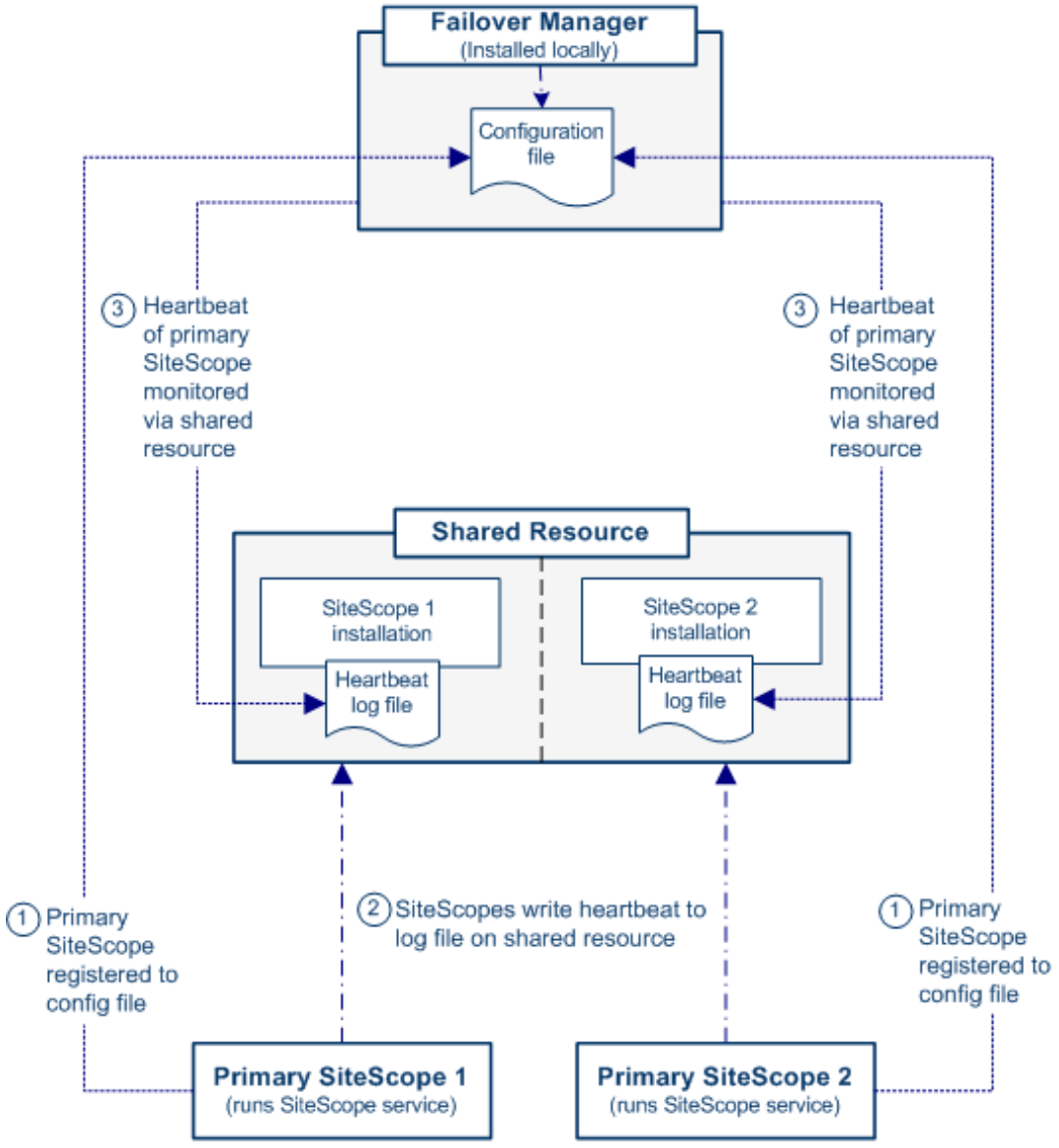
# SiteScope Failover Solution Architecture

SiteScope Failover Manager consists of the following components:

- **SiteScope Failover Manager Server.** This is used for managing and providing backup monitoring for multiple SiteScope instances when a primary SiteScope goes down. It is installed on a machine with access to the installation folder of the primary SiteScopes it is monitoring. The SiteScope Failover Manager creates a failover service (for Windows) or process (for UNIX) for each monitored SiteScope. When it detects that a primary SiteScope is down, it starts the Failover service or process while continuing to monitor the other primary SiteScopes.
- **Shared Resource.** This is a dedicated shared storage resource for the SiteScope installation folder. By placing the SiteScope installation folder on a shared resource, both the primary SiteScope and the SiteScope Failover Manager use the same SiteScope configuration, log, and data files. This enables the SiteScope Failover Manager to access and monitor the primary SiteScope. Multiple SiteScope installations can be stored on one or multiple shared resources.
- **Primary SiteScope Server.** This is a server with a typical SiteScope installation. The SiteScope installation has two run modes:
  - Primary. This is the mode used when SiteScope is running normally.
  - Failover. This is the mode used to support SiteScope Failover when the primary SiteScope goes down.

  Each mode writes data to a different heartbeat file on the SiteScope installation on the shared SiteScope installation.

The following diagram illustrates the SiteScope Failover architecture with multiple SiteScope installations stored on one shared resource.



# The SiteScope Failover Implementation Process

This section gives an overview of the SiteScope Failover process.

**1 Primary system is operational.**

SiteScope Failover Manager monitors the availability of SiteScopes registered in the configuration file. It does this by checking for activity in the **primary_heartbeat.log** file in the **<SiteScope installation>\heartbeat** folder on the shared resource for each SiteScope.

The primary SiteScope writes heartbeat events to the log according to a defined frequency (the default setting is every 15 seconds). This is the "heartbeat" indicator that the primary systems are running. The heartbeat frequency can be modified by changing the **heartbeatFrequencyInSec** value in the configuration files:

- On primary SiteScope:
  **<SiteScope installation>\conf\ha\primaryHAConfig.properties**.
- On Failover Manager:
  **<SiteScope installation>\ha\managerHAConfig.properties**.

---

**Note:** These two values should be synchronized with each other to ensure that the heartbeat monitoring frequency is not higher than the heartbeat writing value.

---

**2 Primary system goes down.**

SiteScope Failover Manager reads the heartbeat events in the **primary_heartbeat.log** file to determine if the primary SiteScope is up or down. If no changes are detected in the last 5 minutes (the default setting), it determines that the primary server is down.

**3 SiteScope Failover process is activated.**

After determining that a primary SiteScope is down, SiteScope Failover Manager activates the SiteScope Failover service/process to run from the installation folder of the monitored primary SiteScope on the shared resource. This enables SiteScope Failover Manager to act as a backup to the primary SiteScope, using the existing configurations from the primary SiteScope to monitor the environment.

When the failover system is active, heartbeat events are written to the **failover_heartbeat.log** file which is created in the **<shared resource><SiteScope installation directory>\heartbeat** directory. For heartbeat log file details, see "Heartbeat Files on the Shared Resource" on page 73.

---

**Note:** SiteScope Failover Manager can provide backup for only one primary SiteScope at a time. If other SiteScopes fail while the failover service is running, SiteScope Failover Manager is unable to provide backup for other primary SiteScopes until the first primary SiteScope that went down is operational.

---

**4 Primary system becomes operational again.**

When SiteScope Failover Manager detects that the primary SiteScope is ready to start, it disables the failover service/process and returns to standby mode. After the failover process has stopped, the primary SiteScope is started, and SiteScope Failover Manager reverts back to monitoring the availability of the primary SiteScope.

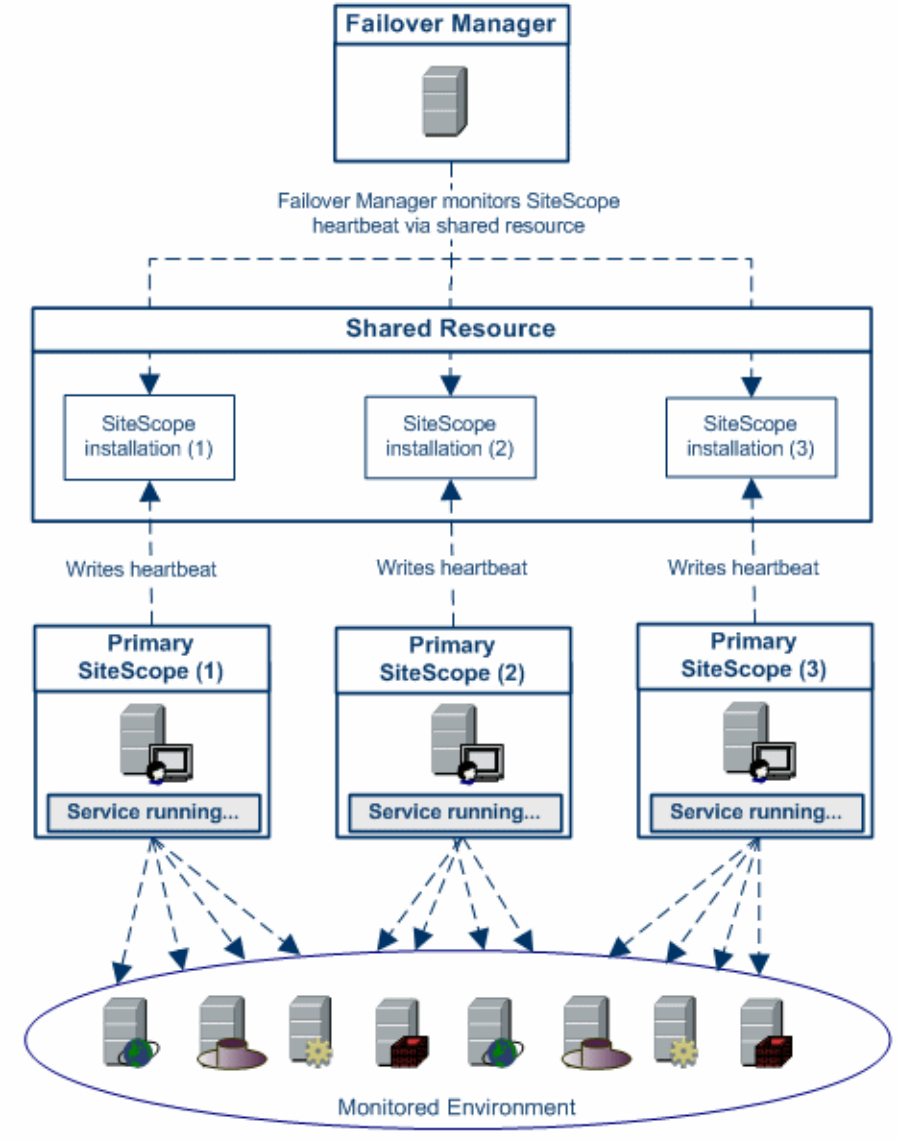
---

**Note:** The failover system is activated and deactivated using a locking mechanism. The purpose of this mechanism is to avoid configuration and data corruption as a result of the primary and failover servers simultaneously writing to the shared resource. For details on the locking mechanism, see "Understanding the Locking Mechanism" on page 65.

---

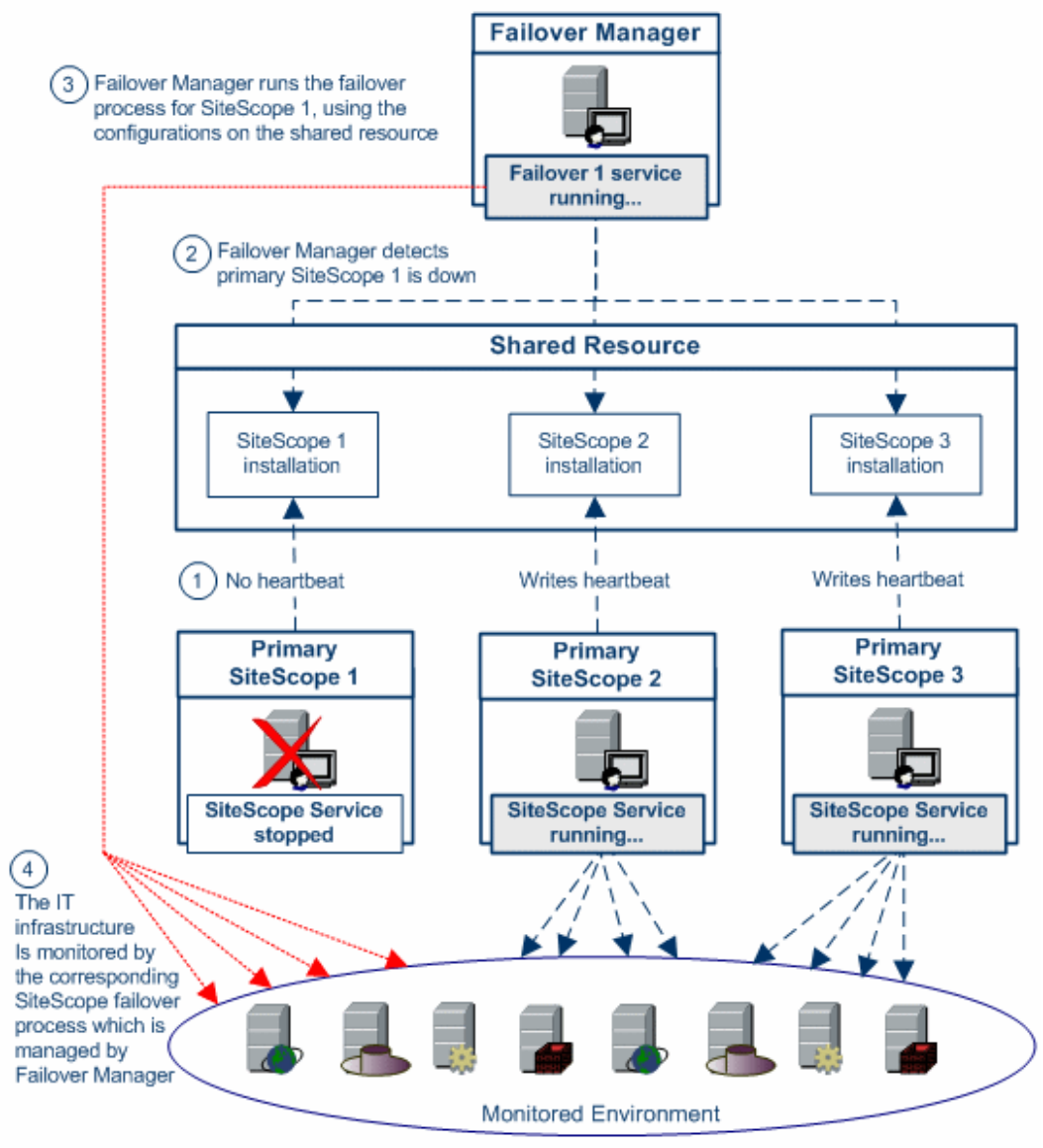
## Monitoring Primary Availability

The following figures illustrate the concept of the automated failover operation. The first figure represents normal operation with the primary SiteScope providing monitoring of the IT infrastructure and the failover in standby mode (monitoring the primary SiteScope heartbeat).



### Failover Transition

When SiteScope Failover Manager detects that a primary SiteScope is unresponsive, it activates the failover service. This enables backup monitoring using the existing configuration from the primary SiteScope.



To support monitoring multiple primary SiteScopes from a single Failover machine, each primary SiteScope installation must be configured to answer on a unique port number. You can use the SiteScope Configuration Tool to view the full list of ports used by SiteScope, and to update the port numbers where necessary. For details, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.

When failover is active, you can view the monitored environment using the SiteScope Failover Manager machine by entering the Failover Manager machine name/IP address and the corresponding port in the SiteScope URL.

---

**Note:** SiteScope Failover Manager can provide backup monitoring for only one primary SiteScope at a time—it is unable to provide backup for other primary SiteScopes that are down when the failover service is running.

---

# SiteScope Failover Manager Considerations and Limitations

This section describes other considerations and limitations when using SiteScope Failover Manager.

- SiteScope Failover Manager 11.20 supports working with SiteScope 11.00 or later. Upgrading from earlier versions of SiteScope Failover to version 11.00 is not supported.
- If a primary SiteScope server is configured to report to Business Service Management (BSM), when a SiteScope Failover instance takes control, it automatically reports to BSM since it is running from the same configuration. Since the primary and failover share the same data and configuration, there are no gaps in the SAM reports. When registering SiteScope to BSM, specify the failover machine in the **Failover Host** box in **Admin** > **System Availability Management** > **New SiteScope** > **Advanced Settings**.

---

**Note:** Make sure that the primary SiteScope is up when you register the failover environment to BSM (you cannot register SiteScope to BSM when the primary SiteScope is down and SiteScope Failover is running).

---

- Unable to monitor the primary SiteScope from the Failover Manager server for monitors configured to target the SiteScope Server. If you configure a monitor on the primary SiteScope server to target the SiteScope Server (by accepting the default **SiteScope Server** in the **Server** field of the Monitor Settings), when the monitor settings are copied to the failover machine, the monitor targets the Failover Manager server instead of the primary SiteScope server.

# Supported Network File Systems

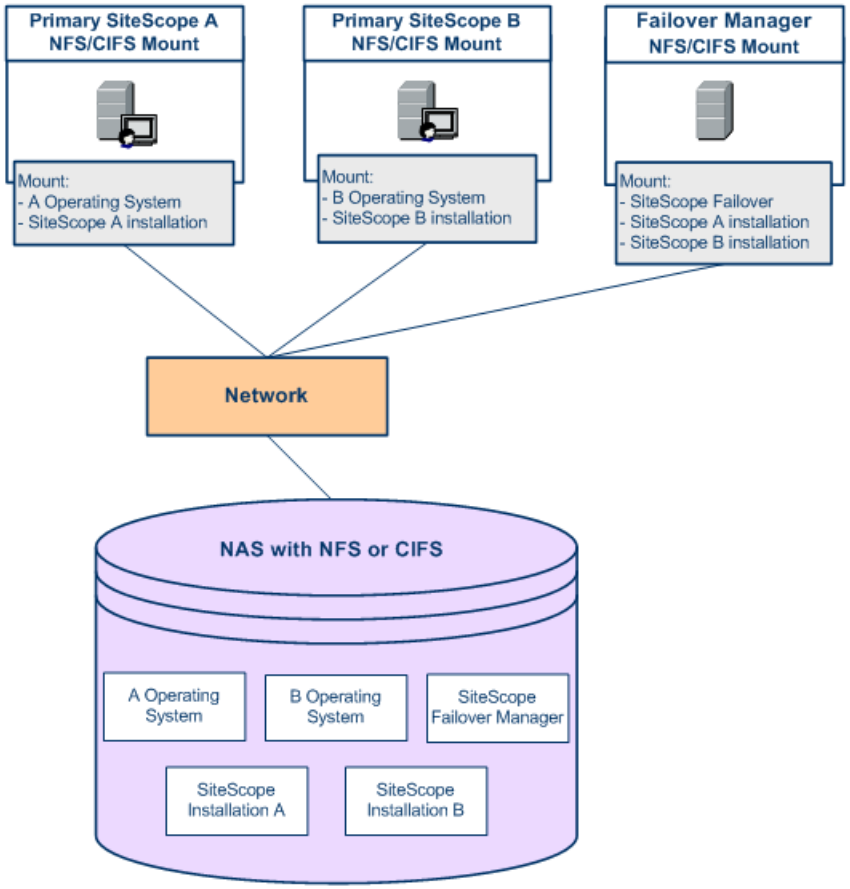
SiteScope Failover Manager supports the following network file system configurations for connecting to the drive:

➤ "Network Attached Storage (NAS) Failover Environment" on page 26

➤ "Cluster Failover Environment" on page 27

## Network Attached Storage (NAS) Failover Environment

SiteScope Failover Manager supports a connection to the storage area network using a Network File System (NFS) or Common Internet File System (CIFS) to connect to the drive.



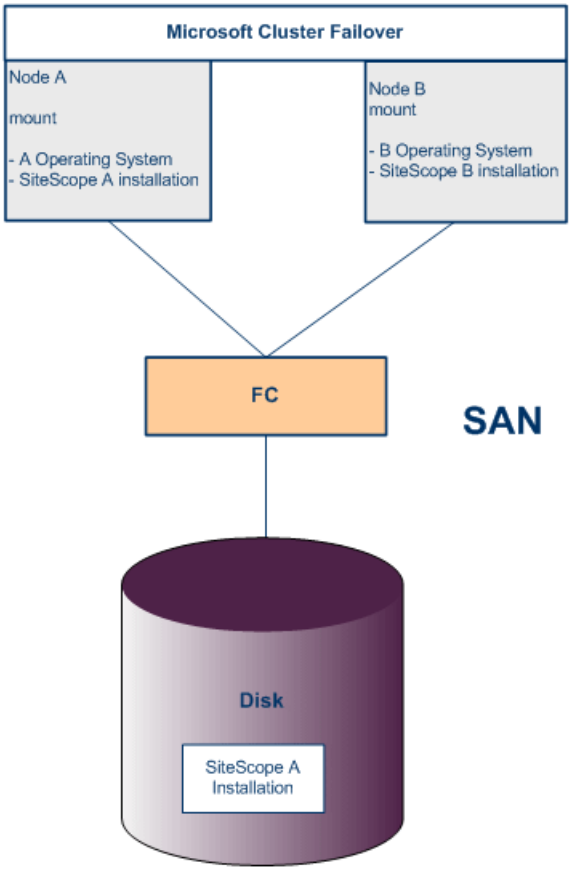

Primary SiteScope A and SiteScope Failover Manager mount the SiteScope A installation (logical volume) at the same moment.

For Windows, use: **\\hostname\share**

For UNIX, use: **/net/hostname/share**

## Cluster Failover Environment

SiteScope Failover Manager supports a direct connection to the storage area network using a standard cluster solution (such as Microsoft Cluster), where the Cluster manages the reads and writes to the drives.



# Part II

## Deploying SiteScope Failover Manager

# 2

# Installing SiteScope Failover Manager

**This chapter includes:**



## About Installing SiteScope Failover Manager

**Note:** SiteScope Failover Manager is deprecated as of this release and is available for backward compatibility only. While SiteScope Failover Manager is still supported, HP plans to stop supporting it in the future, and recommends that you evaluate the SiteScope Failover solution instead.

For information about SiteScope Failover, see the HP SiteScope Failover Guide in **<SiteScope root directory>\sisdocs\pdfs\SiteScopeFailover.pdf**.

Installing SiteScope Failover Manager is similar to a regular SiteScope installation. Most of the actions required for the initial SiteScope Failover Manager setup are automated and are performed as part of the installation procedure. You can install SiteScope Failover Manager on a Windows or UNIX platform.

- SiteScope Failover Manager for Windows platforms is provided as a self-extracting executable.
- SiteScope Failover Manager uses a multi-platform package for installing on UNIX platforms. Depending on the system configuration and requirements, you can use the user interface executable or the command line console mode.

## Requirements for SiteScope Failover Manager

The following outlines the basic requirements for installing and using SiteScope Failover Manager:

### General:

- Primary SiteScopes and SiteScope Failover Manager must be installed on the same platform.
- SiteScope Failover Manager can provide failover functionality for any regular SiteScope installation of the same version number (SiteScope 11.00 or later). Upgrading from earlier versions of SiteScope Failover to version 11.00 is not supported.

### Shared Resource:

- Primary SiteScopes must be installed on a shared resource that can be accessed by the SiteScope Failover Manager machine. You can install more than one primary SiteScope on the same shared resource. It is recommended to use a highly-reliable and stable system for the shared resource.

- (Windows platforms only) Both SiteScope Failover Manager and primary SiteScope machines must be in the same domain as the shared resource, and the SiteScope service must be set to run as a user that has read/write permissions on both machines. Perform the following to change the user account of the SiteScope and SiteScope Failover service on each primary SiteScope and on the SiteScope Failover Manager machine:
  - In **Administrative Tools**, open **Services**, and select **SiteScope/SiteScope Failover** from the list of services.
  - In the Properties dialog box, click the **Log On** tab, and in the **Log on as** area, select **This account**. Enter an account that has permissions to access the Failover machine and the shared resource, and click **OK** to save your settings.
  - In the Services dialog box, stop and then restart the **SiteScope/SiteScope Failover** service. The service now uses the new account.

### Primary SiteScope:

- When installing primary SiteScopes, you must enter the UNC path to the folder where SiteScope will be installed. For example, \\remote-machine\shared\SiteScope.
- When monitoring multiple primary SiteScopes from a single Failover Manager machine, each primary SiteScope installation must be configured to answer on a unique port number. Use the SiteScope Configuration Tool to view the full list of ports used by SiteScope, and to update the port numbers where necessary. For details, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.
- All primary SiteScopes monitored by the SiteScope Failover Manager machine should have the same locale.

### SiteScope Failover Manager:

- SiteScope Failover Manager should be installed on a server with similar or identical server resources (processor speed and memory) as the primary SiteScope server.

- (Windows platforms only) When registering the primary SiteScopes for monitoring in the SiteScope Failover Manager configuration file, you must specify the UNC path of the primary SiteScopes and not a mapped drive. In addition, the path must also include the SiteScope service name and the user logon credentials.
- If the primary SiteScope is connected to an HP Operations Manager or BSM Gateway server and event or metrics integration with HP Operations Manager is enabled, the **HP Operations Agent** must be installed on the SiteScope Failover Manager machine. This enables SiteScope Failover Manager to send events and act as a data storage for metrics data that can be made available to HP Operations Manager and BSM applications if the primary SiteScope fails.

# Deployment Planning and Best Practices

Deploying SiteScope and SiteScope Failover Manager is a process that requires resource planning and a well-planned deployment strategy.

This section includes the following issues:


- "Do I need a SiteScope Failover Manager for each Primary SiteScope?" on page 34
- "How many SiteScope Failover Managers do I need?" on page 35
- "Will using a shared network device affect SiteScope performance?" on page 35
- "What precautions can be taken in case of site failure or for total disaster recovery?" on page 35


## Do I need a SiteScope Failover Manager for each Primary SiteScope?

While SiteScope Failover Manager can monitor multiple primaries simultaneously from a single Failover Manager machine, it can only provide backup for a single SiteScope instance during failover. However, you do not need to have a Failover Manager for each SiteScope instance to ensure continuous monitoring for all the SiteScopes.

### How many SiteScope Failover Managers do I need?

It is recommended to have one Failover Manager for every three primary SiteScopes. This is based on the probability that it is not likely that more than one out of every three primary SiteScopes are likely to fail at the same time. Using this ratio should ensure that sufficient backup resources are available at all times.

### Will using a shared network device affect SiteScope performance?

While the shared resource must be in the same domain as the primary SiteScope and Failover Manager, this should not affect performance when a large number of monitors are running per minute. The key to an effective solution is the quality of the network drive. It is important to use an industry-standard that is similar to what you would use for other enterprise clusters.

In addition, using a shared network device should not affect the time it takes to load the SiteScope user interface. The slowest issue here is the search time on the local disk. The network drive has a huge cache, and therefore the network search should be much faster than a search on the local disk.

### What precautions can be taken in case of site failure or for total disaster recovery?

It is recommended to periodically make a backup of your current SiteScope installation directory and all of the subdirectories within the directory to a remote system hub. You can back up the SiteScope installation as follows:

- Using the Configuration Tool. For details on using the Configuration Tool, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.
- Manually back up the required files. For the list of folders and files that should be copied to your backup destination, see "Backing up and recovering a SiteScope installation if unable to start SiteScope" in the *HP SiteScope Deployment Guide* PDF.

# Installing Primary SiteScope

Primary SiteScopes being monitored must be installed on a shared resource that can be accessed by the SiteScope Failover Manager machine. If you have an existing SiteScope 11.0x installation that is not installed on a shared resource, you must uninstall it, and then reinstall it on a shared resource. You should make a back up of your current SiteScope's configuration data before you uninstall it. For details, see "Backing Up SiteScope Configuration Data" and "Uninstalling SiteScope" in the *HP SiteScope Deployment Guide* PDF.

---

**Note:** SiteScope Failover Manager 11.20 can only be used to monitor the availability of primary SiteScopes running on versions of SiteScope 11.00 or later.

---

**1 Create a shared folder on a remote machine.**

You can install more than one primary SiteScope on the same shared resource.

**2 Install primary SiteScope (version 11.00 or later) on the shared folder.**

When installing SiteScope, check the following:

- The primary SiteScope is installed on a shared resource using the UNC path of the SiteScope installation folder. For example, \\remote-machine\shared\SiteScope (on Windows platforms) or /opt/HP/SiteScope (on UNIX platforms).
- If you are monitoring multiple primary SiteScopes from a single SiteScope Failover Manager machine, each primary SiteScope installation must be configured to answer on a unique port number. Use the SiteScope Configuration Tool to view the full list of ports used by SiteScope, and to update the port numbers where necessary. For details, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.

➤ To use data from an existing SiteScope installation (it must be SiteScope 11.00 or later), select **Use existing exported configuration file** in the Import Configuration screen when installing SiteScope, and specify the user data file that you want to import.

For details on installing SiteScope, see "Installing SiteScope" in the *HP SiteScope Deployment Guide* PDF.

**3 Change credentials for the SiteScope server (set SiteScope user having permissions to access the shared folder.**

The SiteScope service must be set to run as a user that has permissions on the remote machine. This user is common for the primary, failover (created by Failover Manager) and Failover Manager services, since they should not run as **Local System account**. Set the service log on account on the primary SiteScope as follows:

➤ In **Administrative Tools**, open **Services**, and select **SiteScope** from the list of services.

➤ In the Properties dialog box, click the **Log On** tab, and in the **Log on as** area, select **This account**. Enter an account that has permissions to access the shared resource, and click **OK** to save your settings.

➤ In the Services dialog box, stop and then restart the **SiteScope** service. The service now uses the new account.

# Installing SiteScope Failover Manager

Perform the following steps to install SiteScope Failover Manager on Windows platforms or on UNIX platforms using the user interface installer.

---

**Note:** To install SiteScope Failover Manager on UNIX platforms using the user interface installer, you must be able to access certain X Windows libraries that may not be available on all systems. If the installer indicates that it cannot run, use the console mode to install SiteScope Failover Manager as described in "Installing SiteScope Failover Manager on UNIX (Console Mode)" on page 55.

---

**To install SiteScope Failover Manager:**

1. Make a note of the installation path of the SiteScope installation that is the primary or production installation. For example, \\remote-machine\shared\SiteScope (on Windows platforms) or /opt/HP/SiteScope (on UNIX platforms).
2. Insert the installation media containing the SiteScope software into the drive on the machine where you want to install the Failover Manager. (Alternatively, you can download the SiteScope archive from the HP Downloads site.)

**3** Run the SiteScope Failover Manager installation executable program on the failover server according to your operating system.

**a** Determine which executable you need to use.

- **HPSiteScope_11.20_setup.exe**

  This installer automatically determine which SiteScope version to install. On a 32-bit operating system, SiteScope is installed as a 32-bit application. On a 64-bit operating system, SiteScope is installed as a 64-bit application.

- **HPSiteScope32on64_11.20_setup.exe**

  This installer is for 64-bit Windows operating systems only. SiteScope is installed as 32-bit application. This installation allows monitors that are not supported on the 64-bit Windows operating system to be supported. See "Monitors Not Supported by 64-Bit SiteScope" in the the *HP SiteScope Deployment Guide* PDF.

**b** Enter the location from which you are installing SiteScope according to your operating system and architecture, followed by the executable name.

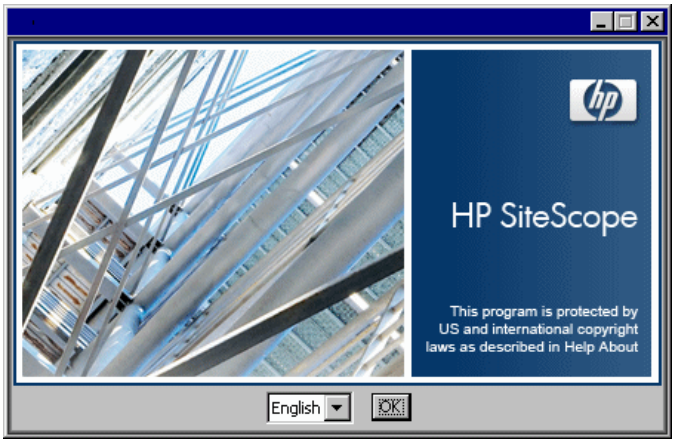
For example:

<DVD_ROOT>\Windows_Setup\SiteScope\
HPSiteScope_11.20_setup.exe

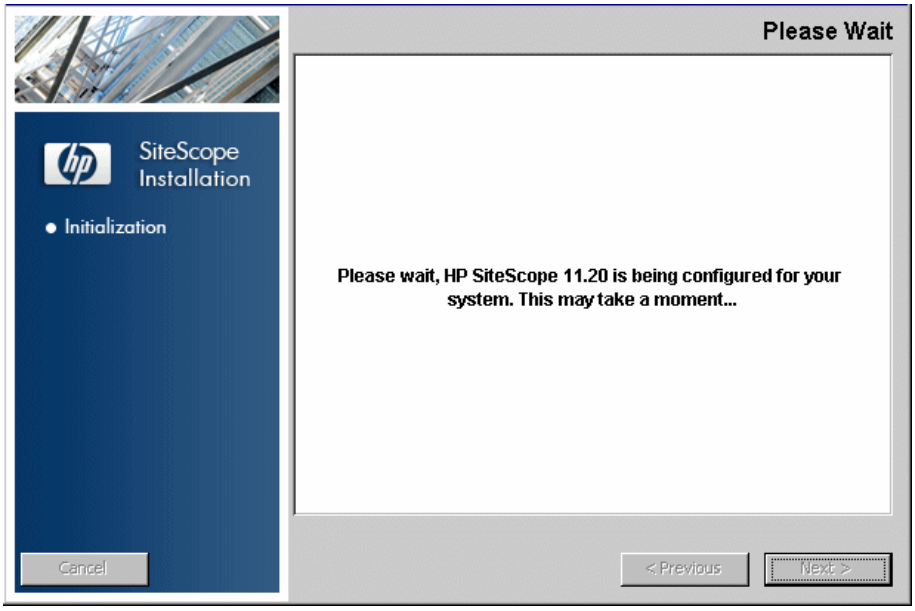
or

<DVD_ROOT>\Windows_Setup\SiteScope\
HPSiteScope32on64_11.20_setup.exe

**4** The Choose Locale screen is displayed.

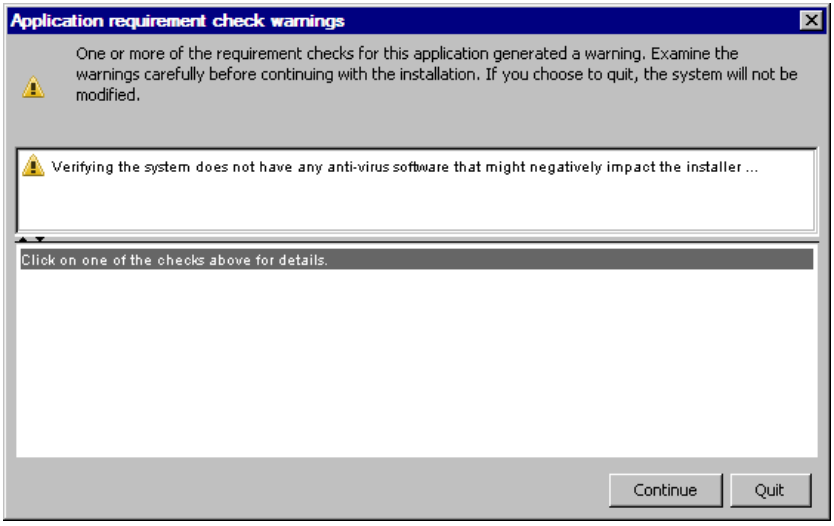



Click **OK** to continue with the installation. The Initialization screen is displayed.



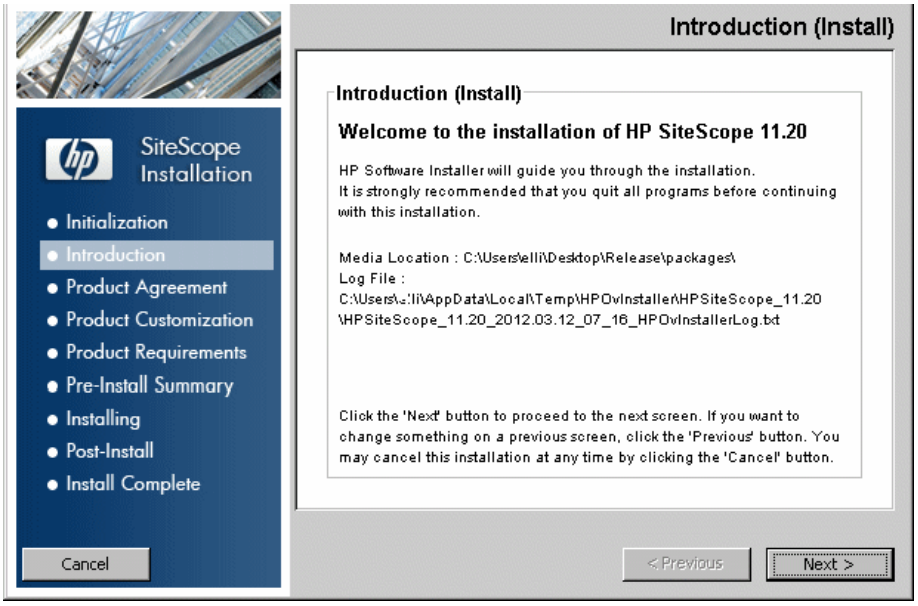
If the Installer detects any anti-virus program running on your system, it prompts you to examine the warnings before you continue with the installation.

**5** Read the warnings, if any, that appear in the **Application requirement** check warnings screen and follow the instructions as described in the screen.

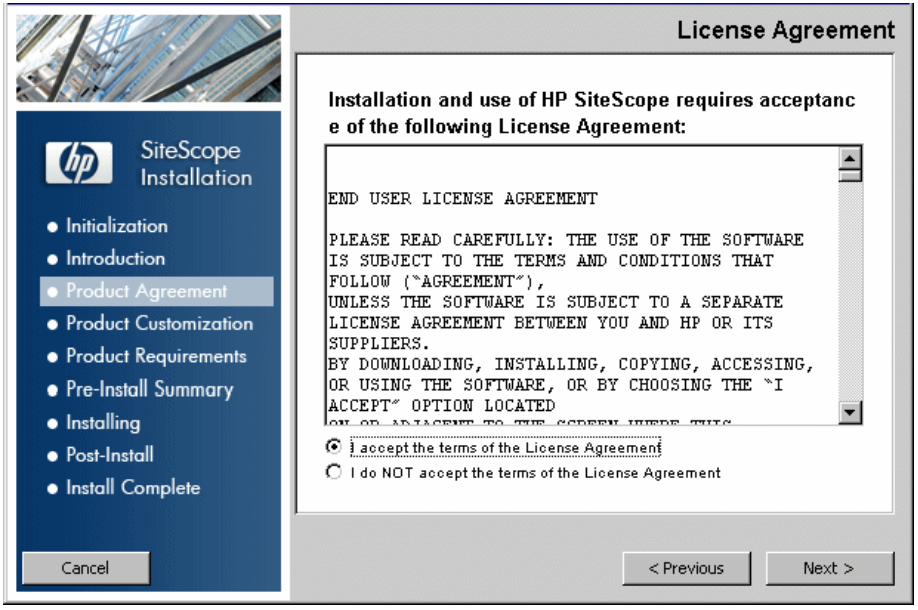



Click **Continue** to continue with the installation.

**6** In the Introduction (Install) screen that opens, click **Next**.



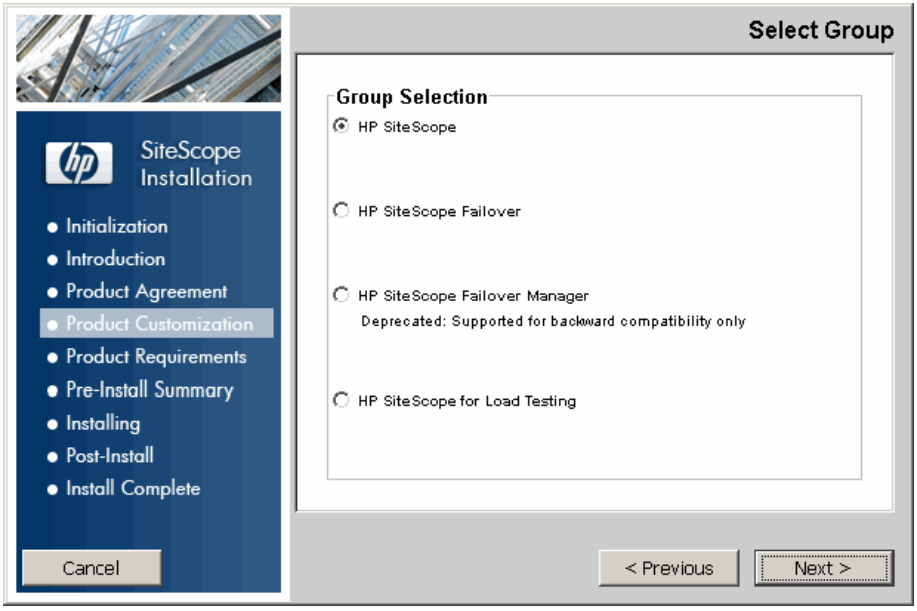

**7** The license agreement screen opens.



Read the SiteScope License Agreement.

To install SiteScope, select **I accept the terms of the License Agreement**, and then click **Next**.

**8** In the Product Customization screen, select the **HP SiteScope Failover Manager** setup type, and click **Next**.

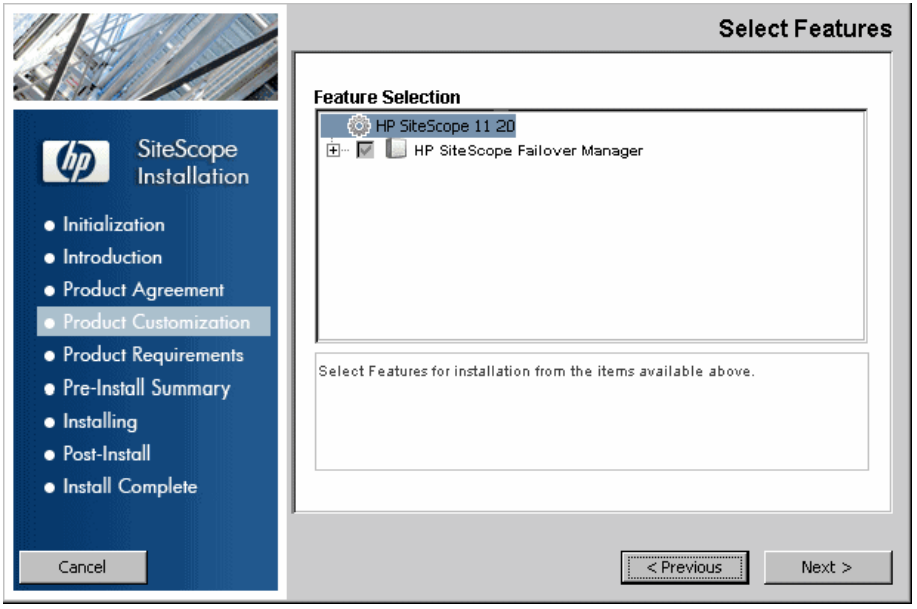



---

**Note:** The **HP SiteScope for Load Testing** and **HP System Health** options are not available when installing on Solaris or Linux platforms.

---

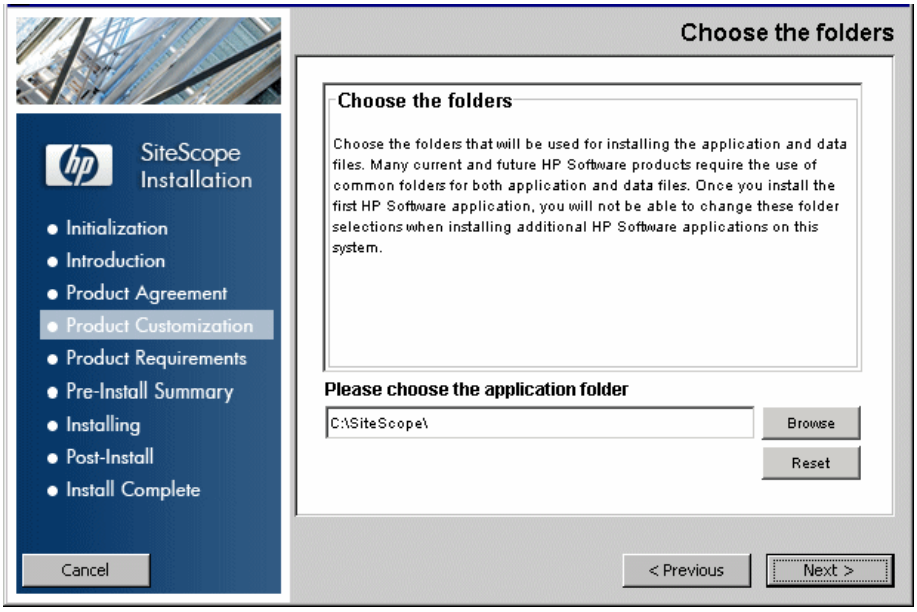
**9** The Select Features screen opens, displaying the SiteScope Failover Manager folder.




Click **Next** to continue.

**10** If installing on Solaris or Linux platforms, SiteScope Failover Manager is automatically installed in the **/opt/HP/SiteScope/** folder. Skip to step 11 on page 46.

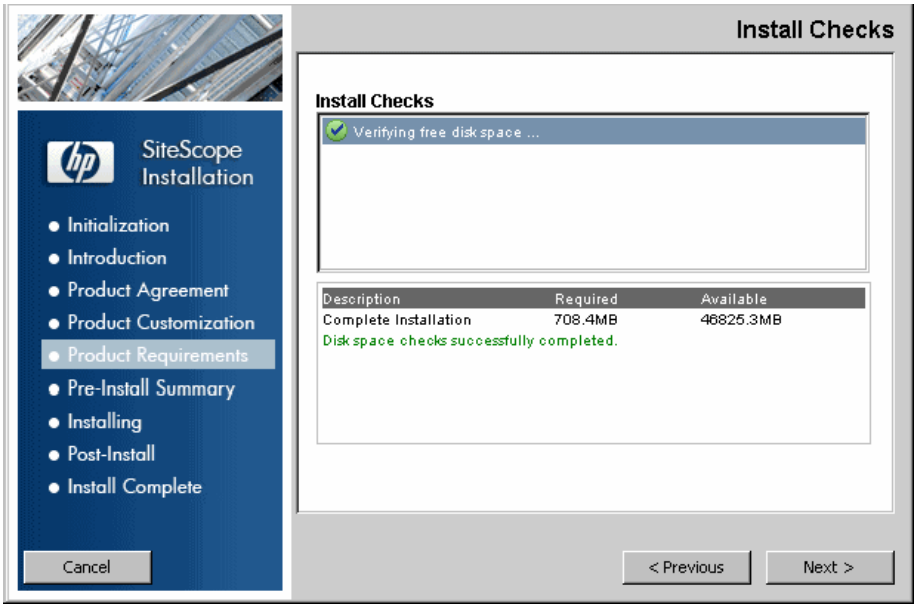
The Choose the folders screen opens.




Enter the full path of the Failover Manager server.

The installation path must not contain spaces or non-Latin characters in its name, and must end with a folder named **SiteScope** (the folder name is case sensitive). After entering the new directory name, click **Next**.

**11** The Install Checks screen opens and runs verification checks.



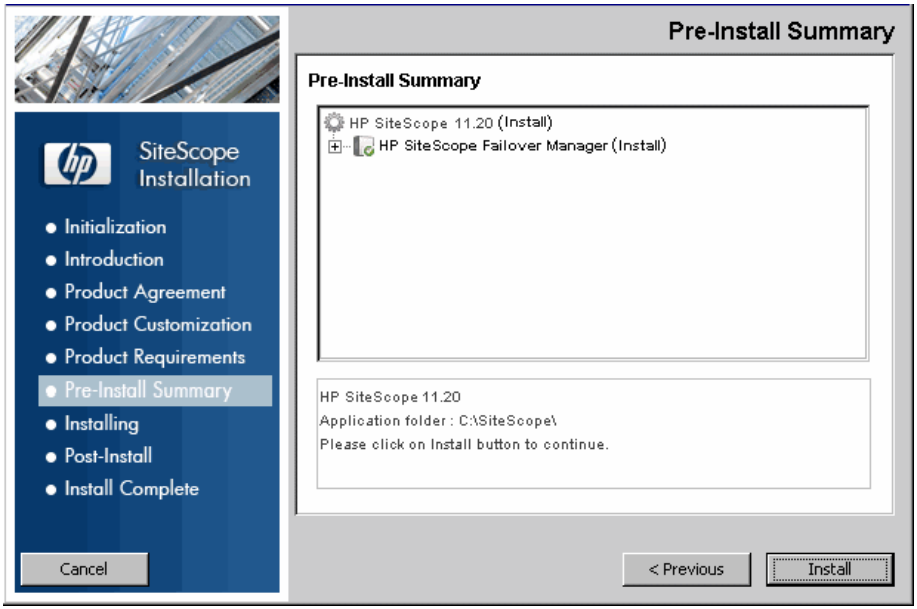

Click **Next** after the free disk space verification is completes successful.

If the free disk space verification is not successful, do the following:

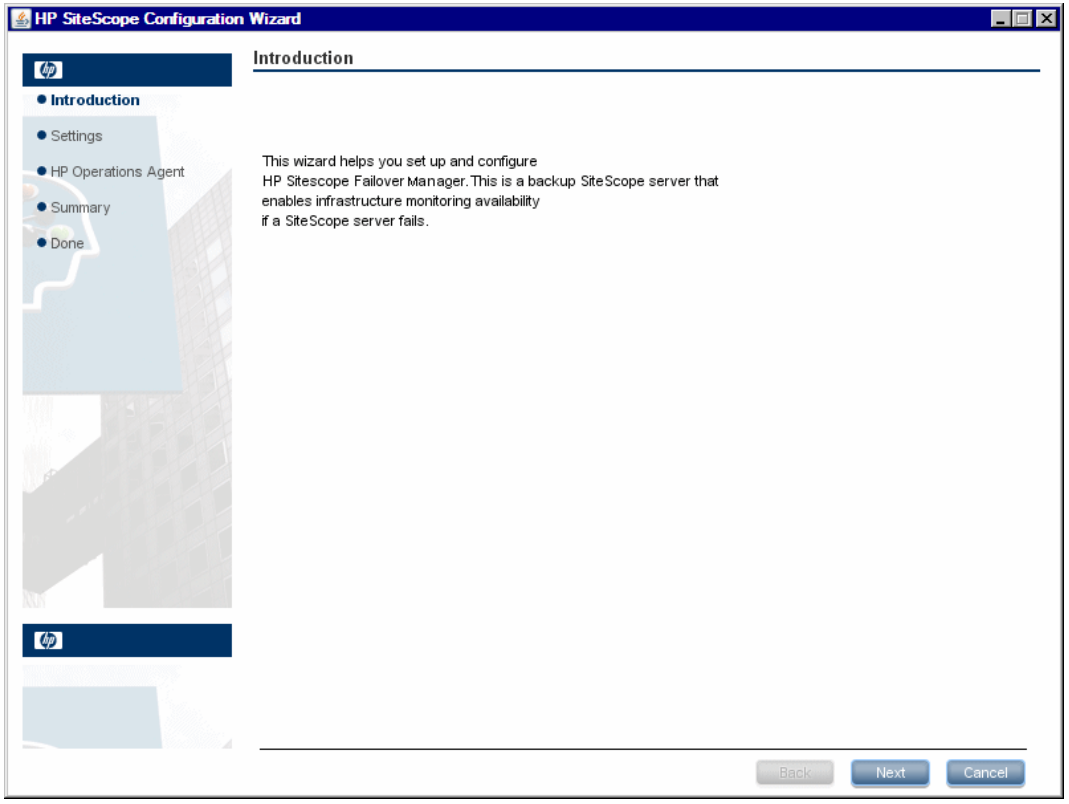
- Free disk space, for example by using the Windows Disk Cleanup utility.
- Repeat steps 9 and 10.

**12** In the Pre-Install Summary screen, click **Install**.

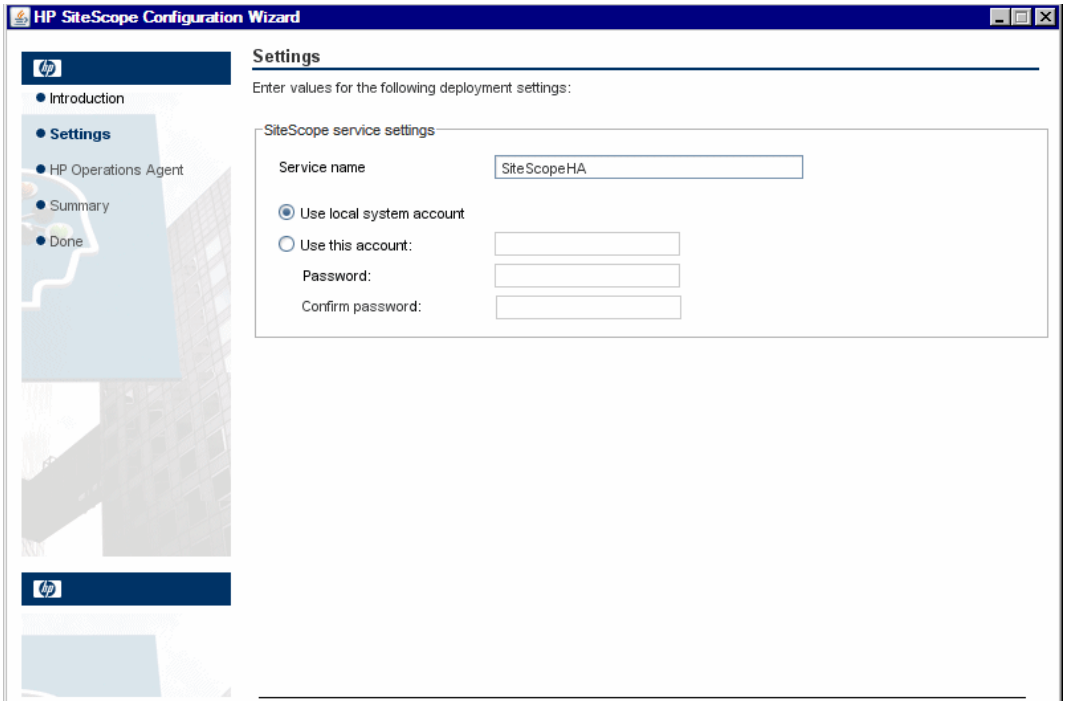
The Installer selects and installs the required SiteScope software components. Each software component and its installation progress is displayed on your screen during installation.



**13** After installing the SiteScope Failover Manager components, the Introduction screen of the SiteScope Configuration Wizard opens. Click **Next**.



**14** The Settings screen of the SiteScope Configuration Wizard opens.



Enter the required configuration information, and then click **Next**:

- **Service name** (not applicable for Solaris or Linux installations). Enter the name of the SiteScope Failover service or use the default service name, SiteScopeHA.
- **Use local system account** (not applicable for Solaris or Linux installations). By default, SiteScope Failover Manager is installed to run as a Local System account. This account has extensive privileges on the local computer, and has access to most system objects. When SiteScope Failover Manager is running under a Local Systems account, it attempts to connect to remote servers using the name of the server.
- **Use this account.** Select to change the user account of the SiteScope Failover service. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope Failover Manager access privileges to monitor server data within the domain. Enter an account and password (and confirm the password) that can access the remote servers.

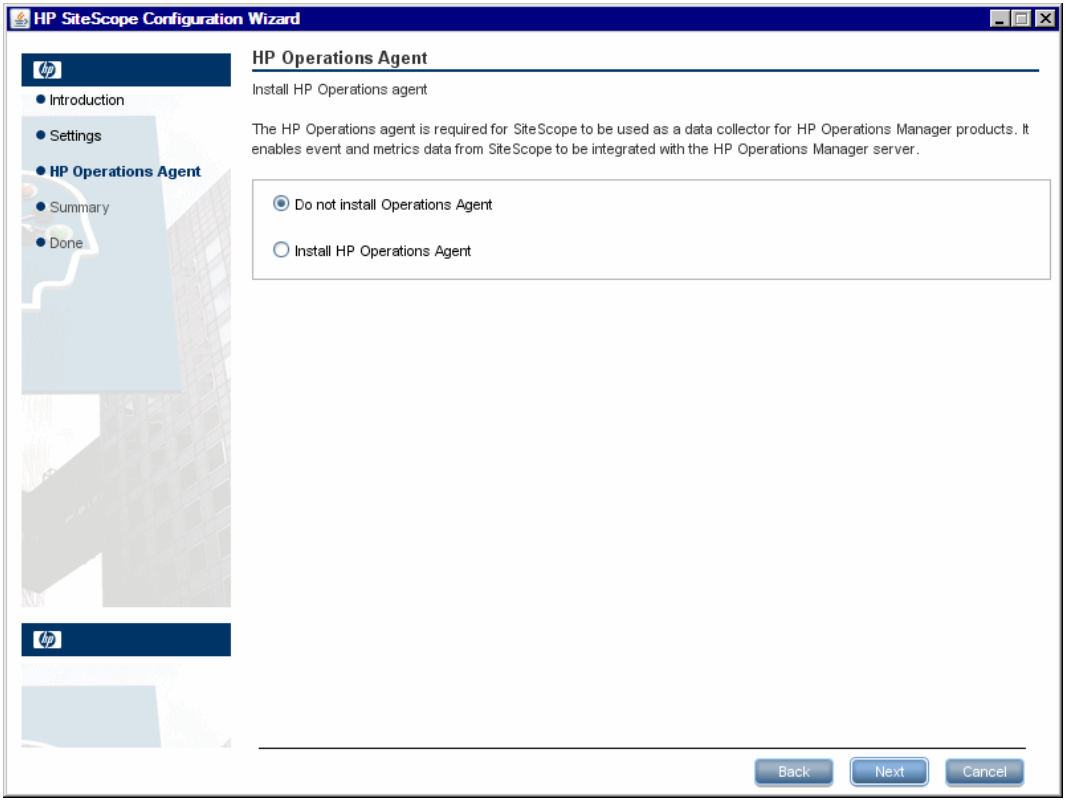
---

**Note:** When SiteScope Failover Manager is installed to run as a custom user account, the account used must have **Log on as a service** rights. To grant a user logon service access:

1. In Windows Control Panel, double-click **Administrative Tools**.
2. Double-click **Local Security Policy**, and select **Local Policies** > **User Rights Assignment** > **Log On as a Service**.
3. Click **Add**, and select the user you want to grant logon service access to and click **OK**.
4. Click **OK** to save the updated policy.

---

**15** The Install HP Operations Agent screen opens. The HP Operations agent is required if the primary SiteScope is integrated to send events and metrics to HP Operations Manager, or to Operations Management in BSM.



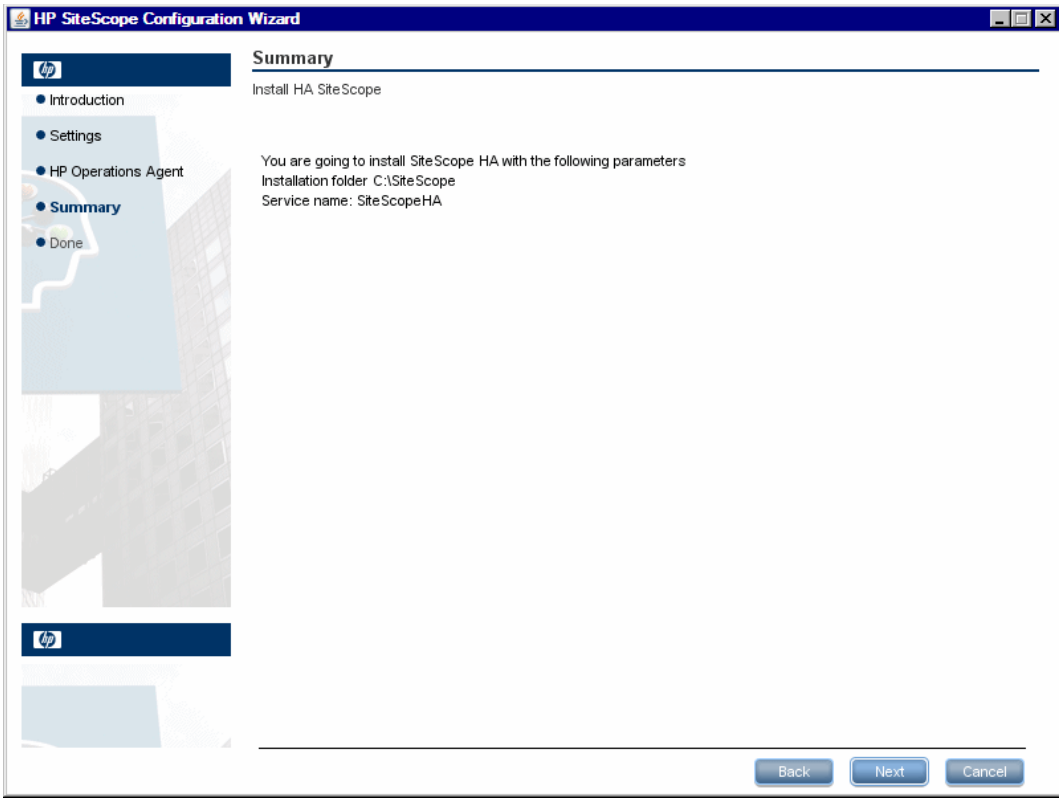

Select one of the following options and click **Next**:

- **Do not install HP Operations Agent.** The HP Operations agent is not installed. If necessary, you can install the agent later using the Configuration Tool. For details, see "Using the SiteScope Configuration Tool" in the *HP SiteScope Deployment Guide* PDF.
- **Install HP Operations Agent.** Select to install the HP Operations agent on the Failover Manager server. The agent enables Failover Manager to send events and act as a data storage for metrics data if the primary SiteScope fails.

**Note:**

- If you install SiteScope and the HP Operations agent on a machine that already has the agent installed, SiteScope overrides it and upgrades the current agent.
- The HP Operations agent is supported on SiteScopes running on the environments listed in the HP SiteScope Support Matrices section in the release notes (in SiteScope, select **Help** > **What's New?**). Consequently, the SiteScope integration with HPOM and BSM is only supported on these environments.

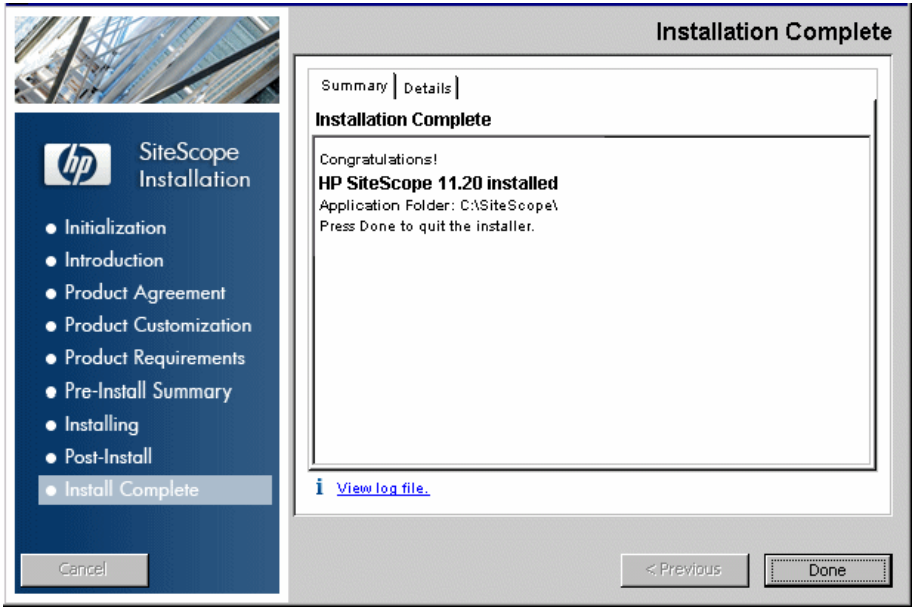
**16** The Summary screen opens.




Check that the information is correct and click **Next** to continue, or **Back** to return to previous screens to change your selections.

**17** In the Done screen, click **Finish** to close the SiteScope Configuration Wizard.

**18** When the installation finishes, the Installation Complete window opens displaying a summary of the installation paths used and the installation status.




If the installation was not successful, review the installation log file for any errors by clicking the **View log file** link in the **Installation Complete** window to view the log file in a web browser.

For more information about the installed packages, click the **Details** tab.

Click **Done** to close the installation program.

If the installation program determines that the server must be restarted, it prompts you to restart the server.

**19** After successfully installing SiteScope Failover Manager, you need to register the primary SiteScopes to be monitored, and configure the primary SiteScope and Failover Manager settings. For details, see "Configure SiteScope Failover Manager" on page 61.

# Installing SiteScope Failover Manager on UNIX (Console Mode)

SiteScope Failover Manager uses a multi-platform package for installing on UNIX platforms. Depending on the system configuration and requirements, you can use the user interface executable or the command line console mode. For details on installing using the user interface mode, see "Installing SiteScope Failover Manager" on page 38.

Perform the following steps to install SiteScope Failover Manager on UNIX platforms using the command line console mode.

**To install SiteScope Failover Manager using the console mode installer:**

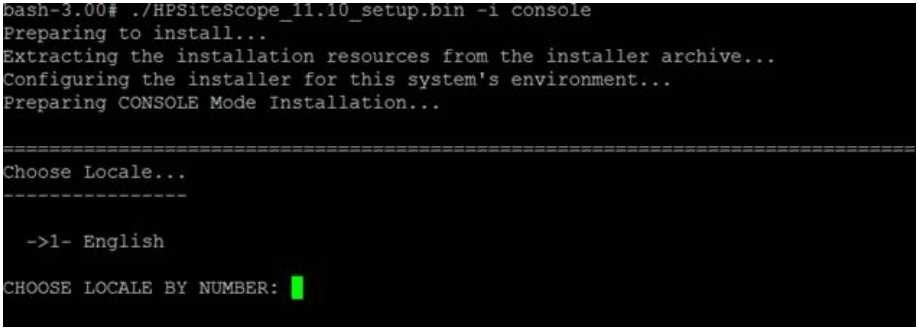
1. Download the SiteScope Failover Manager setup file to the machine where you want to install SiteScope Failover.

2. Run the following command:

```
HPSiteScope_11.20_setup.bin -i console
```

   The installation script initializes the Java Virtual Machine to begin the installation.

3. The Choose Locale screen is displayed.

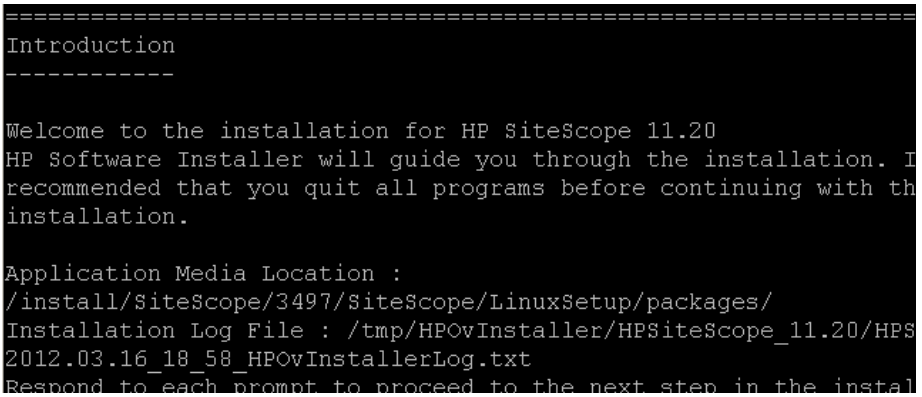



   Enter the number 1 to select English, and press ENTER to continue.

4. A confirmation screen is displayed.

   Press ENTER to continue.

**5** The Introduction screen is displayed.




Press ENTER to continue with the installation.

**6** The text of the license agreement is displayed. The SiteScope License Agreement requires several pages to display. Read each page as it is presented. Press ENTER to continue to the next page. When you have viewed all the pages of the license agreement, you have the option to accept or not accept the license agreement.

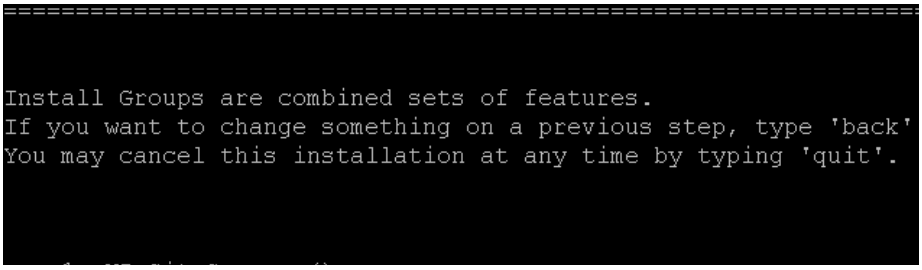

To install SiteScope, you must accept the terms of the license agreement. The default selection is to not accept the agreement. To accept the license agreement and continue the installation, enter Y.

---

**Note:** To cancel the installation after viewing the SiteScope License Agreement, enter N.

---

**7** The SiteScope setup type screen opens.




Enter the number 2, and then press ENTER to continue.

**8** The Select Features screen opens.


Enter the number 1 and then press ENTER to continue. Press ENTER again to confirm your choice.

**9** The Install Requirements screen is displayed. Press ENTER to continue.

**10** The Pre-Installation Summary screen opens. Press ENTER to continue.

**11** The Install Features screen opens and the installation process starts. When the installation process is complete, the post-installation configuration screen opens.

**12** The Install HP Operations Agent screen opens. The HP Operations agent is required if the primary SiteScope is integrated to send events and metrics to an HP Operations Manager or BSM server.


Enter the number 1 if you do not want to install the HP Operations agent.

Enter the number 2 to install the HP Operations agent on the SiteScope Failover Manager server. The agent enables Failover Manager to send events and act as a data storage for metrics data if the primary SiteScope fails.

Press ENTER to continue with the installation.

**13** The console displays the installation parameters for confirmation. Enter 1 to proceed with the installation using the parameters indicated or enter 2 to return to make changes, and then press ENTER. The installation process starts.

**14** When the installation process is completed, an installation status message is displayed. Press ENTER to continue and exit the installer.

## Additional Installation Actions

The following are additional actions you may need to perform depending on the configuration of the primary SiteScope. In some cases, you may need to restart the SiteScope Failover Manager installation for the changes to take effect. See the corresponding sections of the SiteScope Help documentation for more information.

- If any changes are made to the SiteScope service in the Windows registry on the primary SiteScope server, match these changes in the **go.bat** file in **<shared resources>:\<SiteScope installation>\bin** directory.
- Secure Shell (SSH) servers must be copied, installed, and set up on the failover machine to match any SSH logins and monitoring performed on the primary SiteScope.

- Client libraries, custom scripts, and other API "helper" programs for any Application monitors on the primary SiteScope (for example, BroadVision, WebLogic, WebSphere, and so forth) must be installed and set up in the same location on the failover machine. It is also recommended to install and configure them on the shared resource.
- DHCP library files must be copied from the primary to the failover machine to enable the DHCP monitor type.

# Troubleshooting and Limitations

This section describes the following troubleshooting and limitations for installing SiteScope Failover Manager.

### HP Operations agent fails to install

The HP Operations agent fails to install when SiteScope Failover Manager is installed on a Windows platform.

**Proposed Solution:**

1. After installing SiteScope Failover Manager, copy the **<SiteScope root directory>\install\components\oa\win32** or **\win64** folder locally.
2. Install the HP Operations agent manually by running the command: cscript opc_inst.vbs from the **win32** or **\win64** folder.

# 3

# Configuring SiteScope Failover Manager

**This chapter includes:**



## Configure SiteScope Failover Manager

This describes how to configure SiteScope Failover Manager to monitor the IT infrastructure when the primary SiteScope fails, using the existing configuration data from the primary SiteScope.

This task includes the following steps:

### 1 Prerequisites

Make sure that you followed the requirements for installing primary SiteScopes and SiteScope Failover Manager. For details, see "Requirements for SiteScope Failover Manager" on page 32.

### 2 Register the primary SiteScopes to be monitored

Navigate to <**SiteScope Failover installation**>**\ha** on the Failover Manager machine, and edit the **monitoredSiteScopes.properties** file as follows:

- For SiteScopes running on UNIX platforms, enter the path of the SiteScope installation directory which is mounted on the Failover machine. For example: /opt/HP/SiteScope or /mnt/HP/SiteScope (depending on where the SiteScope directory on the shared resource was mounted to the UNIX file system). For assistance on mounting a directory on a UNIX environment, contact your system administrator.
- For SiteScopes running on Windows platforms, enter the path (use a separate line for each SiteScope being registered) in the format:

  <SiteScope installation on shared directory>;<Service Name>;<Username>;<Encrypted Password>;<JMX port # (optional)>

  where:

  - <SiteScope installation on shared directory> is the UNC path of each SiteScope to be monitored. For example, \\computer1.yourdomain.com\PrimarySiS1\SiteScope\
  - <Service Name> is the name of the SiteScope Failover service for backing up SiteScope. For example, SiteScope_failover.
  - <Username> is the name of the domain user with access to the shared directory.
  - <Encrypted Password> is the user password. Encrypt the password using the SiteScope Encryption Tool by running the command: <**SiteScope root**>**\tools\AutoDeployment\encrypt_password.bat** <**password**>. Enter space and the password value (for example myPassword), and click Enter. Use the returned string as the encrypted password.
  - <JMX port> is the SiteScope JMX port; the standard port is 28006.

For example:

```
\\share\SiteScope;SiteScope_failover;DOMUSER1;
(sisp)a4VNEsnGdso/s8Ri/miKeQ==;28006
```

---

**Note:** Failover Manager must be restarted before any changes to the **monitoredSiteScopes.properties** file can take effect. For details on the file, see "monitoredSiteScopes.properties" on page 70.

---

### 3 Configure the primary SiteScope settings - optional

If you plan to modify the configuration settings on a primary SiteScope, stop the SiteScope services/processes on the primary SiteScope machine. For details, see "Starting and Stopping the SiteScope Service/Process" on page 64.

On the shared resource, navigate to **<SiteScope root directory>\conf\ha**, and open the **primaryHAConfig.properties** file. Modify the settings as necessary. For setting details, see "primaryHAConfig.properties" on page 68.

### 4 Configure the Failover Manager settings - optional

If you plan to modify the configuration settings on the Failover Manager machine, stop the SiteScope Failover service/process. For details, see "Starting and Stopping the SiteScope Service/Process" on page 64.

On the Failover Manager machine, navigate to **<SiteScope root directory>\conf\ha** and open the **managerHAConfig.properties** file. Modify the settings as necessary. For setting details, see "managerHAConfig.properties" on page 71.

### 5 Start the SiteScope and SiteScope Failover service/process

Restart the SiteScope services or processes on any machines on which you modified failover configuration settings.

For details on starting SiteScope processes or services, see "Starting and Stopping the SiteScope Service/Process" on page 64.

## Starting and Stopping the SiteScope Service/Process

You can start and stop the SiteScope service manually on Windows platforms by using the Services control panel. On UNIX platforms, you can start and stop SiteScope manually by using the shell scripts supplied with the product.

**To start or stop the SiteScope service on Windows platforms:**

1. Open the Services control panel by selecting **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
2. Select **SiteScope** in the list of services and right-click to display the action menu.
3. Select **Start** or **Stop** as applicable from the action menu.

**To start or stop the SiteScope process on Solaris and Linux:**

1. Open a terminal window on the server where SiteScope is installed.
2. Run the start or stop command shell script using the following syntax:
   - For start command: <SiteScope installation path>/SiteScope/start
   - For stop command: <SiteScope installation path>/SiteScope/stop

   For example:

   /opt/HP/SiteScope/stop

# Testing SiteScope Failover Manager

To verify that SiteScope Failover Manager is operational and is functioning, stop the service or process on the primary SiteScope. For details on stopping a service, see "Starting and Stopping the SiteScope Service/Process" on page 64.

After the SiteScope service or process has stopped, SiteScope Failover Manager should start up after the requirements in the **managerHAConfig.properties** file have been met (based on the default settings, this should take about 5 minutes).

# Understanding the Locking Mechanism

A locking mechanism is used to activate and deactivate the failover system on the monitored SiteScope servers. This is to avoid data and configuration corruption as a result of both primary and failover machines writing simultaneously on the shared resource.

The lock is passed between SiteScope primary and failover machines to determine which one is controlling SiteScope. This ensures that only a single SiteScope process is running at one time. The lock keeper is the controller that can perform read/write operations.

The lock files are located in the **<SiteScope installation>\heartbeat** directory on the shared resource.

| File | Description |
|---|---|
| **sitescope.lock** | When a SiteScope primary or failover is in the process of starting up, it requests the **sitescope.lock** file from Failover Manager. It waits until the lock is acquired before it can complete the start up. |
| **request.lock** | This file is created by the primary SiteScope when it is ready to start up after a recovery. This is a signal to Failover Manager that the failover system is no longer required. When Failover Manager detects the **request.lock**, it shuts down the failover service and releases the lock, enabling the primary to start. |

## Lock Mechanism Process

**1 Primary SiteScope waiting to start.**

Each time a SiteScope primary is in the process of starting up, it tries to create the **sitescope.lock** file, or to acquire the existing one on the shared resource in the **<SiteScope root directory>\heartbeat** directory. This is required for the primary SiteScope to take control over the **sitescope.lock** file and to complete the start up.

**2 Primary SiteScope starts up.**

Provided the lock is available, the primary SiteScope gets the lock, and the SiteScope process is started.

---

**Note:** If the primary SiteScope does not get the lock (for example, if the lock file is occupied by the failover process), it makes repeated requests for the lock according to the **numberOfPrimaryLockRequestRetries** value in the **<SiteScope root directory>\conf\ha\primaryHAConfig.properties** file.

---

**3 Primary SiteScope shuts down.**

When the primary SiteScope goes down, the SiteScope process stops running and the **sitescope.lock** is released.

---

**Note:** If the primary SiteScope is disconnected from the network, it is automatically shutdown to avoid corruption.

---

**4 Failover Manager is activated.**

Once Failover Manager detects that the primary SiteScope has gone down (by monitoring the **primary_heartbeat.log** file), it takes control over SiteScope (acquires the **sitescope.lock**) and activates the failover system.

Failover Manager goes into detection mode (waiting for the **request.lock**).

**5 Primary system becomes operational again.**

When the primary SiteScope is ready to restart, it creates the **request.lock** file. This is the sign that the primary system is ready to restart and that the failover system is no longer required.

When Failover Manager detects the request, it stops the failover system, and releases the lock.

The primary SiteScope acquires the **sitescope.lock** and the SiteScope process is restarted. The **request.lock** file is removed from the directory.

Failover Manager returns to standby mode (monitoring the primary SiteScope heartbeat).

# Primary SiteScope Configuration Files

SiteScope Failover Manager uses configuration files and settings not used by regular SiteScope. This section describes the files and the key configuration settings on the primary SiteScope and Failover Manager that are used for SiteScope Failover.

This section includes:



## primaryHAConfig.properties

This file contains configuration properties for the primary SiteScope. It is located in the **<SiteScope root directory>\conf\ha** directory on the shared resource.

| Property | Description |
|---|---|
| **heartbeatFrequencyInSec** | The frequency, in seconds, that SiteScope writes heartbeat data for the primary and failover SiteScopes, to the **primary_heartbeat.log** and **failover_heartbeat.log** on the shared resource.<br>**Default value:** 15 seconds<br>**Minimum value:** 10 seconds<br>**Note:** This value, which is used by both primary and failover services, should be synchronized with the heartbeat monitoring frequency in the **managerHAConfig.properties** file on the Failover Manager to ensure that the heartbeat monitoring frequency is not higher than the heartbeat writing value. |

| Property | Description |
|---|---|
| **numberOfPrimaryLock RequestRetries** | The number of times that the primary SiteScope makes a request for the lock. SiteScope needs to acquire the lock to start the SiteScope service.<br>**Default value:** 3<br>**Minimum value:** 1 |
| **primaryLockRequest TimeoutInSec** | Amount of time, in seconds, that the primary SiteScope waits between sending requests for the lock. SiteScope needs to acquire the lock to start the SiteScope service.<br>**Default value:** 30 seconds<br>**Minimum value:** 10 seconds |

## ha.log

This file provides a record of actions performed by the primary SiteScope. It contains information regarding the time that the primary SiteScope tries to acquire the lock, acquires the lock, and releases the lock.

The name of the current primary SiteScope log is **ha.log** and it is located in the **<SiteScope root directory>\logs directory** on the shared resource. When the current log reaches its size limit, it is closed and a new log is created. Older logs are named ha.log.1, ha.log.2, and so forth. The higher the number concatenated to the name, the older the log.

# Failover Manager Configuration Files

This section describes the files and the key configuration settings on the Failover Manager machine.

This section includes:



## monitoredSiteScopes.properties

This file contains a list of all SiteScopes monitored by the Failover Manager. It is located in the **<SiteScope root directory>\ha** directory on the SiteScope Failover Manager server.

- For SiteScopes running on UNIX platforms, enter the directory which is mounted on the Failover machine. For example:

  /opt/HP/SiteScope (mounted directory on filer)

  For details on mounting a directory on a UNIX environment, contact your system administrator.

- For SiteScopes running on Windows platforms, enter the path of the SiteScopes to be monitored in the format:

  <SiteScope installation on shared directory>;<Service Name>;<Username>;<Encrypted Password>;<JMX port # (optional)>

  Use a separate line for each SiteScope being monitored.

  For a detailed explanation of the path format, see "Register the primary SiteScopes to be monitored" on page 62.

---

**Note:** Failover Manager must be restarted before any changes to this file can take effect.

---

## managerHAConfig.properties

This file contains configuration properties for the Failover Manager. It is located in the **<SiteScope installation>\ha** directory on the SiteScope Failover Manager server.

| Property | Description |
|---|---|
| **heartbeatFrequencyInSec** | The frequency, in seconds, that SiteScope Failover Manager writes heartbeat data to the **heartbeat.log** file on the shared SiteScope installation folder.<br>**Default value:** 15 seconds<br>**Minimum value:** 10 seconds |
| **progressTouchFrequencyInSec=30** | The frequency, in seconds, that SiteScope Failover Manager touches the **Progress.html** page and changes its last modification time.<br>**Default value:** 30 seconds<br>**Minimum value:** 10 seconds |
| **lockRequestDetectorFrequencyInSec=30** | When failover is active, this is the frequency that Failover Manager checks for the **release.lock** file. The **release.lock** file is a signal that the primary system is ready to restart and that the failover system is no longer required.<br>**Default value:** 30 seconds<br>**Minimum value:** 10 seconds |
| **numberOfAnalysisRetries** | The number of times that Failover Manager attempts to collect heartbeat analysis data before it determines that SiteScope is down.<br>**Default value:** 5<br>**Minimum value:** 1 |
| **failoverMonitoringFrequencyInMin=1** | The frequency, in minutes, that Failover Manager monitors the heartbeat.<br>**Default value:** 1 minute<br>**Minimum value:** 1 minute |

## ha.log

This file provides a record of actions performed by the Failover Manager, and the time they were performed. It contains information regarding the heartbeat analysis process, the Failover Manager state (standby, active), and the failover state for each monitored SiteScope.

The name of the current SiteScope Failover Manager log is **ha.log** and it is located in the **<SiteScope root directory>\logs directory** on the SiteScope Failover Manager server. When the current log reaches its size limit, it is closed and a new log is created. Older logs are named ha.log.1, ha.log.2, and so forth. The higher the number concatenated to the name, the older the log.

# Heartbeat Files on the Shared Resource

The **primary_heartbeat.log**, **failover_heartbeat.log**, and **heartbeat.log** are log files that contain records of heartbeat events written to the **<SiteScope root directory>\heartbeat** directory on the shared resource.

When the primary SiteScope is up, it writes events to the **primary_heartbeat.log** file. Failover Manager reads the events to conclude the status of the primary SiteScope, and to determine the appropriate action to take. When SiteScope Failover Manager is up, it writes events to the **failover_heartbeat.log** file. Failover Manager also writes heartbeat events to the **heartbeat.log** file.

The events are common to all heartbeat files, except the RELEASED_LOCK_ACK event, which is relevant only to primary SiteScopes.

| Event | Description |
|---|---|
| START | Primary SiteScope/SiteScope Failover started up. |
| HEARTBEAT | Heartbeat events indicate that the SiteScope is up and running. By default, heartbeat events are written to the log every 15 seconds.<br>Heartbeat events are written to the log according to the **heartbeatFrequencyInSec** frequency defined in:<br>➤ **<SiteScope root directory>\conf\ha\ primaryHAConfig.properties** for primary SiteScopes<br>➤ **<SiteScope root directory>\ha\ managerHAConfig.properties** for Failover Manager |
| SHUTDOWN | Primary SiteScope/SiteScope Failover is down due to one of the following: |
| RELEASED_LOCK_ ACK | This event is logged by Failover Manager when it detects that the primary SiteScope has recovered and is ready to restart. Failover Manager shuts down the failover service (and releases the lock), and writes this event to the log to indicate that the primary is starting up. |

# Part III

## Administering SiteScope Failover Manager

# 4

# Monitoring Using SiteScope Failover Manager

**This chapter includes:**



## Using Failover Monitoring Templates

Failover Monitoring solution templates are preconfigured monitor set templates designed to monitor the failover environment. Using the Failover Monitoring solution templates, you can rapidly deploy solution-specific SiteScope monitors with settings that are optimized for monitoring the availability of primary and failover SiteScope machines.

When a primary SiteScope is registered to the Failover Manager configuration file, it is recommended to deploy the Failover Monitoring solution template (for Windows or UNIX) to the primary SiteScope, according to the platform on which SiteScope is running. A Failover Monitoring solution template should be deployed to each primary SiteScope server being monitored by the Failover Manager.

The solution template creates a monitor group container on the primary SiteScope in which the specially configured failover monitors are added. The Failover monitors are SiteScope log monitors with settings that are optimized for monitoring the availability of the target primary SiteScope and the failover service.

After the solution template is deployed, you can configure alerts on the deployed monitors to notify you of changes in status on the primary SiteScope and when a failover occurs. For example, you can configure a Failover alert to receive email notification when the primary SiteScope goes down.

Since the Failover Monitoring solution template is deployed on SiteScope, this means that when the primary SiteScope is up, you can view the deployment using the primary SiteScope URL, and when SiteScope Failover Manager is up, you can view it using the SiteScope Failover URL (since they share the same configuration). For details, see "Monitoring When the Primary SiteScope Goes Down" on page 81.

This section also includes:



## Failover Template Monitors

The Failover Monitoring solution templates are located in the **Solution Templates** folder in the SiteScope template tree. All the monitors are Log File monitors which are configured to search for a particular text match in the Failover Manager **ha.log** file. The information from this file is used as a trigger for activating alert actions.

The monitoring frequency is defined by the **Frequency** setting in the Monitor Run Settings pane on the Failover monitor. By default, each monitor is set to run every 60 seconds.

The following table provides an overview of the monitors in the Failover Monitoring solution template.

| Failover Monitors | Description | Threshold Settings |
|---|---|---|
| Failed to Start SiteScope Failover | This is a log monitor that is used to detect if the failover service has failed to start after the primary SiteScope has gone down.<br>When the monitor is in error, the Failover Manager logs a message to the **ha.log** file, and the monitor checks for a match. Configure an alert to notify you if the monitor is in error. | Error if matches =="n/a'" or > 0<br>Good if ==0 |
| Failed to Stop SiteScope Failover | This is a log monitor that is used to detect if the failover service has failed to stop after the Failover Manager has requested it to shutdown.<br>When the monitor is in error, the Failover Manager logs a message to the **ha.log** file, and the monitor checks for a match. Configure an alert to notify you if the monitor is in error. | Error if matches =="n/a'" or > 0<br>Good if ==0 |
| Primary SiteScope has Recovered | This is a log monitor that is used to detect if the primary SiteScope has recovered after a failure.<br>The monitor is configured to be in error when there is match. | Error if matches =="n/a'" or > 0<br>Good if ==0 |

| Failover Monitors | Description | Threshold Settings |
|---|---|---|
| Primary SiteScope is Down | This is a log monitor that is used to detect if a primary SiteScope has gone down.<br>The monitor is in error status when the primary SiteScope is down. | Error if matches =="n/a'" or > 0<br>Good if ==0 |
| Primary SiteScope Status Unknown | This is a log monitor that is used to detect if the primary SiteScope status is unknown. The Failover should not be up and running as a backup when the primary SiteScope status is unknown.<br>The monitor is configured to be in error when there is match. | Error if matches =="n/a'" or > 0<br>Good if ==0 |

## Variables Used in Failover Monitoring Solution Templates

The following table provides a description of variables used in Windows and UNIX Failover Monitoring solution templates.

| Variable | Description | Default Value |
|---|---|---|
| %%Failover_Manager_HA_Log%% | The full UNC path to the Failover Manager **ha.log** file. | **On Windows:** \<Failover Manager server>\SiteScope\logs\ha.log<br>**Example:** \\host1.example.com\c$\SiteScope11FailoverManager\SiteScope\logs\ha.log<br>**On UNIX:** /opt/HP/SiteScope/logs/ha.log |
| %%Failover_Manager_Host%% | The host name of the Failover Manager host. | **Example:** host1.example.com |
| %%Failover_Manager_Log_Encoding%% | The encoding of the monitored log file (such as UTF-8, CP1252, Shift-JIS, windows-1252, or EUC-JP). | UTF-8 |

| Variable | Description | Default Value |
|---|---|---|
| %%Failover_Manager_Password%% | Password to the Failover Manager host. | |
| %%Failover_Manager_User% | The user name with admin credentials to the Failover Manager host. | |
| %%Primary_Installation_Path%% | The full installation path of SiteScope Primary. If meta characters are used in the installation path, they should be escaped if you want the characters to have their normal meaning. | **On Windows:** \\\\<Shared folder>\\<Primary server>\\SiteScope<br>**Example:** \\\\filer.example.com\\Shared\\SiteScope11_on_host1\\SiteScope<br>**On UNIX:** /<HA mount point>/SiteScope<br>The Primary installation path on UNIX should use "/" as delimeter between directories instead of "//" or "\/".<br>**Example:** \/opt\/HA\/SiteScope11_on_host2\/SiteScope<br>or<br>/opt/HA/ SiteScope11_on_host2/SiteScope |

# Monitoring When the Primary SiteScope Goes Down

This task describes the steps involved in configuring the environment to ensure failover monitoring when the primary SiteScope goes down.

This task includes the following steps:

- "Deploy the Failover Monitoring solution template to the primary SiteScope" on page 82
- "Modify Failover monitor configuration properties - optional" on page 82
- "Configure alerts and reports" on page 83

➤ "View monitor results during failover" on page 83

➤ "View monitor results when the primary SiteScope is back up" on page 84

### 1 Deploy the Failover Monitoring solution template to the primary SiteScope

The solution template can be deployed from template tree in the SiteScope user interface, using a CSV file, or using an XML file external to the SiteScope user interface. For a detailed overview of the steps involved in deploying a solution template, see the Templates section in *Using SiteScope* in the SiteScope Help.

Once deployed, the Failover Monitoring solution template creates a new monitor group container in which the individual Failover monitors are added. The monitor group container is assigned a name in the format Failover Monitors on <primary SiteScope installation path>. For details on the Failover Monitoring solution template properties, see the Solution Templates section in *Using SiteScope* in the SiteScope Help.

### 2 Modify Failover monitor configuration properties - optional

You can modify monitor configuration properties for Failover monitors in the same way as any other monitors in SiteScope.

For example, you can modify conditions that determine the reported status of each monitor instance in the Threshold Settings. For details on modifying monitor thresholds, see the Threshold Settings section in *Using SiteScope* in the SiteScope Help.

### 3 Configure alerts and reports

Configure alerts on the deployed Failover monitors to notify you of changes in status on the primary SiteScope and when a failover occurs. For details on configuring alerts, see the SiteScope Alerts section in *Using SiteScope* in the SiteScope Help.

You can also configure reports for the newly created Failover monitors. For details on configuring reports, see the SiteScope Resports section in *Using SiteScope* in the SiteScope Help.

### 4 View monitor results during failover

If a primary SiteScope goes down, an alert is triggered notifying you of the change in status of the primary SiteScope. To view monitoring results during a failover, redirect your Web browsers to the address of the failover SiteScope server.

To access SiteScope from the Failover Manager machine, use the format:

http://<Failover Manager machine name/IP address>:
<corresponding failover port>/SiteScope

For example, http://localhost:8080/SiteScope.

---

**Note:**

- When SiteScope Failover Manager supports multiple SiteScopes, each primary SiteScope must be configured to use a different port to avoid port collisions. Use the SiteScope Configuration Tool to change the SiteScope user interface and other ports that are already in use. The Failover Manager port is used to access SiteScope from the Failover Manager machine.
- If there are SiteScope user names and passwords defined on the primary SiteScope, enter the same user names and passwords to access the failover.

---

### 5 View monitor results when the primary SiteScope is back up

When the primary SiteScope recovers, an alert is triggered if an alert was configured on the **Primary SiteScope has Recovered** monitor. To view monitoring results, redirect your Web browser to the address of the primary SiteScope instance using the format:

http://<Primary SiteScope name>:<Primary SiteScope port>/SiteScope

# 5

# SiteScope Failover Manager Reference

**This chapter includes:**



## SiteScope Failover Manager and BSM Integration

If a primary SiteScope is configured with a failover and is reporting to Business Service Management (BSM) and the failover SiteScope is activated, SiteScope Failover Manager configures itself to report to BSM under the same profile as the primary. Secondary profiles do not have to be created for the BSM database.

# SiteScope Failover Manager and Event Integrations

If the primary SiteScope is configured to send events to HP Operations Manager (HPOM), or to Operations Management in BSM, the HP Operations agent must also be installed on the Failover Manager to enable it to send events when the primary SiteScope is down. In addition, the agent on both the failover and primary SiteScope servers must be connected to HPOM or Operations Management, and the SiteScope policies must be uploaded and installed on the agent nodes in HPOM or Operations Management to enable the integration.

---

**Note:** While event integration with HPOM or BSM can be configured on primary SiteScopes, it is not supported for high availability (failover) when Microsoft Cluster Service is used to provide backup monitoring.

---

This section also includes:


- "Connecting the Failover Agent to HPOM" on page 86
- "Connecting the Failover Agent to Operations Management" on page 88


## Connecting the Failover Agent to HPOM

1. Open **Environment Variables** from the Windows Control Panel, and make sure the failover server has the same SITESCOPE_HOME environment variable value as the one on the primary SiteScope. Typically, the failover server has the variable value of the local installation.
2. Stop the HP Operations agent on both the failover and primary SiteScope servers, and then restart the agents with administrator privileges to access the log file on the shared resource.

   To start the agent with chosen user permissions, run the command:

   ```
   cscript "%OvInstallDir%\bin\ovswitchuser.vbs"-existinguser
   <DOMAIN\USER> -existinggroup <GROUP> -passwd <PASSWORD>
   ```

   Thereafter, you can stop the agent by using the ovc -kill command, and start it by using the ovc -start command.

**3** On the Failover server, manually connect the HP Operations agent to the HPOM server by entering the command:

"%OvInstallDir%\bin\OpC\install\opcactivate.vbs" -srv <server>

---

**Note:** The HP Operations agent on the primary SiteScope should be connected through the Connection Settings section in **Preferences** > **Integration Preferences** > **HP Operations Manager Integration** > **HP Operations Manager Integration Main Settings**. For details, see the Working with Operations Manager and BSM Using the HP Operations Agent section in *Using SiteScope* in the SiteScope Help.

---

**4** When both agents are connected to HPOM and their connection request has been approved on the HPOM management server, upload the SiteScope policies to HPOM and install the policies on the agents:

**a** Copy the policy files from <**SiteScope root directory**>**tools****OMIntegration****Raw** to the HPOM management server.

**b** Upload the policies by running the command:

ovpmutil cfg pol upl "<policies folder>/config.mm"

The uploaded policies are displayed in **Policy Management** > **Policy Groups** > **HP SiteScope Integration**.

**c** Install the policies by selecting them and dragging them to the nodes of the connected agents as follows:

| Policy Name | Install on... |
|---|---|
| SiteScope_Hosts_Discovery | Primary and Failover agent |
| HP_SiteScope_to_Operations_Manager _Integration | Primary and Failover agent |
| HP_SiteScope_to_Operations_Manager _Integration_by_Log_File | Primary agent only |
| HP_SiteScope_HA_to_Operations _Manager_Integration_by_Log_File | Failover agent only |

## Connecting the Failover Agent to Operations Management

To connect the failover agent to Operations Management, perform the connection steps common to Windows and UNIX platforms, and then perform the platform-specific steps for signing and installing the policies files.

---

**Note:** The HP Operations agent on the primary SiteScope should be connected to Operations Management through the Connection Settings section in **Preferences** > **Integration Preferences** > **HP Operations Manager Integration** > **HP Operations Manager Integration Main Settings**. For details, see the Working with Operations Manager and BSM Using the HP Operations Agent section in *Using SiteScope* in the SiteScope Help.

---

**To manually connect the failover agent to Operations Management (for both Windows and UNIX):**

1. Stop the HP Operations agent on both the failover and primary SiteScope servers, and then restart the agents with administrator privileges to access the log file on the shared resource.

   To start the agent with chosen user permissions, run the command:

   ```
   cscript "%OvInstallDir%\bin\ovswitchuser.vbs"-existinguser
   <DOMAIN\USER> -existinggroup <GROUP> -passwd <PASSWORD>
   ```

   Thereafter, you can stop the agent by using the ovc -kill command, and start it by using the ovc -start command.

2. On the Failover server, manually connect the HP Operations agent to Operations Management by running the command:

   ```
   <agent installation folder>/bin/OpC/install/opcactivate -srv <server>
   ```

3. On Operations Management server run the command:

   ```
   ovcm -listpending -l
   ```

   Find the request ID of your failover machine and run the command:

   ```
   ovcm -grant <request id>
   ```

4 In the <**Sitescope root directory**>**tools****OMIntegration****Policies** folder, open the **F516CEC3-3AD4-4627-9CFD-BB155B894349_data** file and change the log file name from **HPSiteScopeOperationsManagerIntegration.log** to **HPSiteScopeOperationsManagerIntegration.HA.log**.

**To sign and install the policies files on UNIX platforms:**

1 In the <**Sitescope root directory**>**tools****OMIntegration****Policies** folder, edit the **F6EB1B5F-2A65-419D-BC00-D71E9D90FAC3_data** and **F516CEC3-3AD4-4627-9CFD-BB155B894349_data** policies files by replacing **/opt/HP/SiteScope** with the path in the **/opt/HP/SiteScope/ha/monitoredSiteScopes.properties file** on the Failover server.

2 Sign the edited policies by running the following command:

```
/opt/HP/SiteScope/integrations/om/bin/signPolicy.sh
/opt/HP/SiteScope/tools/OMIntegration/Policies/8760A73D-F7F9-4BF0-93FE-
CABED896EF28_header.xml
/opt/HP/SiteScope/integrations/om/bin/signPolicy.sh
/opt/HP/SiteScope/tools/OMIntegration/Policies/F516CEC3-3AD4-4627-9CFD-
BB155B894349_header.xml
/opt/HP/SiteScope/integrations/om/bin/signPolicy.sh
/opt/HP/SiteScope/tools/OMIntegration/Policies/F6EB1B5F-2A65-419D-BC00-
D71E9D90FAC3_header.xml
```

3 Install the policies by running the following command:

```
 /opt/OV/bin/ovpolicy -install -file
/opt/HP/SiteScope/tools/OMIntegration/Policies/F6EB1B5F-2A65-419D-BC00-
D71E9D90FAC3_header.xml
/opt/OV/bin/ovpolicy -install -file
/opt/HP/SiteScope/tools/OMIntegration/Policies/F516CEC3-3AD4-4627-9CFD-
BB155B894349_header.xml
/opt/OV/bin/ovpolicy -install -file
/opt/HP/SiteScope/tools/OMIntegration/Policies/8760A73D-F7F9-4BF0-93FE-
CABED896EF28_header.xml
```

**To sign and install the policies files on Windows platforms:**

1. Open **Environment Variables** from the Windows Control Panel, and make sure the failover server has the same SITESCOPE_HOME environment variable value as the one on the primary SiteScope. Typically, the failover server has the variable value of the local installation.
2. Sign the edited policies by running the following command:

```
"<SiteScope path>\integrations\om\bin\signPolicy.bat" -windows
"<SiteScopePath>\tools\OMIntegration\Policies\8760A73D-F7F9-4BF0-93FE-
CABED896EF28_header.xml"
"<SiteScope path>\integrations\om\bin\signPolicy.bat" -windows
"<SiteScopePath>\tools\OMIntegration\Policies\F516CEC3-3AD4-4627-9CFD-
BB155B894349_header.xml"
"<SiteScope path>\integrations\om\bin\signPolicy.bat" -windows
"<SiteScopePath>\tools\OMIntegration\Policies\F6EB1B5F-2A65-419D-BC00-
D71E9D90FAC3_header.xml"
```

3. Install the policies by running the following command:

```
"<agent path> \bin\ovpolicy" -install -file
"<SiteScopePath>\tools\OMIntegration\Policies\F6EB1B5F-2A65-419D-BC00-
D71E9D90FAC3_header.xml"
"<agent path> \bin\ovpolicy" -install -file
"<SiteScopePath>\tools\OMIntegration\Policies\F516CEC3-3AD4-4627-9CFD-
BB155B894349_header.xml"
"<agent path> \bin\ovpolicy" -install -file
"<SiteScopePath>\tools\OMIntegration\Policies\8760A73D-F7F9-4BF0-93FE-
CABED896EF28_header.xml"
```

## SiteScope Failover Manager and Metrics Integrations

If the primary SiteScope is connected to an HP Operations Manager or BSM Gateway server and metrics integration with HP Operations Manager is enabled, the HP Operations agent must be installed on the Failover Manager to enable it to report metrics data when the primary SiteScope is down. The agent can be installed during SiteScope Failover Manager installation.

If the primary SiteScope goes down, continuous data graphing can be achieved using the HP Performance Manager or BSM reporting tools (Graphing component in Operations Management) by selecting both the primary SiteScope and SiteScope Failover Manager for graphing.

---

**Note:** While metrics integration with HP Operations Manager can be configured on primary SiteScopes, it is not supported for high availability when Microsoft Cluster Service is used to provide failover monitoring.

---

## Troubleshooting and Limitations

This section describes troubleshooting and limitations for working with SiteScope Failover Manager.


- "Not all SiteScope Failover Manager events are displayed in the log file" on page 92
- "SiteScope Failover Manager cannot write heartbeats and create a lock request if no disk space is available on the shared resource" on page 92
- "SiteScope installed on a shared drive cannot be uninstalled from the Programs menu or from Add or Remove Programs in the Control Panel" on page 93
- "The Failover service stops with a NullPointerException after starting primary SiteScope, stopping Failover Manager, and starting SiteScope Failover" on page 93
- "SiteScope active service process runs on the SiteScope Failover Manager machine even after the primary SiteScope is up" on page 93

### Not all SiteScope Failover Manager events are displayed in the log file

To display all SiteScope Failover Manager events in the **<SiteScope root directory>\logs\ha.log** file, change the file to DEBUG mode.

1 Open **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava\log4j.properties** file in a text editor.

2 Replace the following:

```
#
# HA categories
#
log4j.category.com.mercury.sitescope.ha=INFO, ha.appender
log4j.additivity.com.mercury.sitescope.ha=false
```

with:

```
#
# HA categories
#
log4j.category.com.mercury.sitescope.ha=DEBUG, ha.appender
log4j.additivity.com.mercury.sitescope.ha=false
```

### SiteScope Failover Manager cannot write heartbeats and create a lock request if no disk space is available on the shared resource

When there is no more space in the file system, primary SiteScopes and the Failover Manager stop working.

**Suggested Solution:**

This can be prevented by monitoring the available disk space on the shared resource machine and taking action before it runs out of space.

### SiteScope installed on a shared drive cannot be uninstalled from the Programs menu or from Add or Remove Programs in the Control Panel

Unable to uninstall SiteScope installed on a remote path (shared drive) in Windows by selecting **Start** > **Programs** > **HP SiteScope** > **Uninstall HP SiteScope** or from **Add or Remove Programs** in the Control Panel.

**Suggested Solution:**

Uninstall SiteScope by running the installer file (**HPSiteScope_11.20_setup.exe** or **HPSiteScope_11.20_setup.bin**) and selecting the **Uninstall** option.

### The Failover service stops with a NullPointerException after starting primary SiteScope, stopping Failover Manager, and starting SiteScope Failover

This error is caused when SiteScope Failover is started from the **go.bat**. While SiteScope can be run on Windows environments using the **go.bat** file when it is not run as a service, the **go.bat** file cannot be used to run SiteScope Failover.

**Suggested Solution:**

If you need to start SiteScope Failover manually, you should do so by starting the service and not the **go.bat**.

### SiteScope active service process runs on the SiteScope Failover Manager machine even after the primary SiteScope is up

If SiteScope Failover Manager installed on Solaris is configured with a very small **numberOfAnalysisRetries** (less than 3) in the **managerHAConfig.properties** file, there could be conflicts in detecting the process ID (PID) between the primary SiteScope and its failover.

**Suggested Solution:**

Make sure that the **numberOfAnalysisRetries** in the **<SiteScope installation>\ha\managerHAConfig.properties** file is not less than 3.

# Part IV

## Appendix

# A

# Failover Solution Using Microsoft Cluster Service

**This chapter includes:**



## Introduction to Using Microsoft Cluster Service

Microsoft Cluster Service can be used as an alternative to SiteScope Failover Manager for providing failover on SiteScope machines. The Microsoft Cluster Service solution is suitable for medium and larger-sized enterprises.

Microsoft Cluster Server is clustering software that supports clusters nodes which are specially linked servers running the cluster service. The primary purpose of clustering is to provide failover and reinstantiation of services and resources, thereby providing increased availability for the services.

With Microsoft Cluster Server, when one server in a cluster fails or is taken offline, the other server in the cluster takes over the failed server's operations. Clients using server resources experience little or no interruption of their work because the resource functions move from one server to the other.

Microsoft Cluster Server is comprised of clustering software and the Cluster Administrator. The clustering software enables the servers of a cluster to exchange specific types of messages that trigger the transfer of resources at the appropriate times. The Cluster Service runs on each cluster server. The Cluster Administrator is a graphical application that is used to manage a cluster. You can access the Cluster Administrator from each SiteScope client machine and manage your cluster from it.

---

**Note:** While the event integration with HP Operations Manager and BSM and metrics integration with HP Operations Manager can be configured on primary SiteScopes, these integrations are not supported for high availability when Microsoft Cluster Service is used to provide failover monitoring.

---

## Install and Configure SiteScope on Cluster Servers

In our example, SiteScope_1 and SiteScope_2 represent two SiteScope machines on which the Microsoft cluster service (agent) is installed. Both machines share a disk resource, Disk E.

This task includes the following steps:

- "Create and configure the Microsoft Cluster Service on the assigned SiteScope machines" on page 99
- "Configure cluster resources" on page 99
- "Set the owner machine and verify the disk resource is online" on page 100
- "Install SiteScope on SiteScope_1 and set SiteScope service startup type to Manual" on page 101
- "Create a corresponding SiteScope service on SiteScope_2" on page 101
- "Create a generic service resource on the cluster" on page 102
- "Test failover" on page 103

### 1 Create and configure the Microsoft Cluster Service on the assigned SiteScope machines

For help creating a Microsoft cluster service, consult your system administrator or refer to the Microsoft Guide to Creating and Configuring a Server Cluster Under Windows Server 2003. This guide is available from http://www.microsoft.com/downloads/details.aspx?familyid=96F76ED7-9634-4300-9159-89638F4B4EF7&displaylang=en.

For information on creating and configuring a server cluster on a VM Workstation, see: http://communities.vmware.com/message/853923;jsessionid=FBFFE873899512916627A53BFE7D6632.

### 2 Configure cluster resources

Click **Start** > **Programs** > **Administrative Tools** > **Cluster Administrator** to access the Cluster Administrator.

Configure the following cluster resources and their dependencies under your Cluster Group, and verify that their possible owners are the SiteScope machines.

| **Cluster Resources** | |
|---|---|
| Cluster IP Address | ➤ Resource type: IP Address<br>➤ Dependencies: none<br>➤ Parameters: Cluster IP as the Address value |
| Cluster Name resource | ➤ Resource type: Network Name<br>➤ Resource name: For example, Lab_resource06<br>➤ Dependencies: Cluster IP Address<br>➤ Parameters: Cluster Name |
| Physical Disk (shared disk) | ➤ Resource type: Physical Disk<br>➤ Dependencies: Cluster IP Address<br>➤ Parameters: the disk (in our example, E) |

| **Cluster Resources** | |
|---|---|
| Physical Disk - Quorum Disk Q (internal) | ➤ Resource type: Physical Disk<br>➤ Dependencies: none<br>➤ Parameters: the disk (Q Quorum) |
| SiteScope service (created after installing SiteScope) | ➤ Resource type: Generic Service<br>➤ Dependencies: Disk E<br>➤ Parameters: SiteScope service name |

---

**Note:**

- ➤ The **Possible owners** for each resource are the cluster servers assigned for SiteScope monitoring (SiteScope_1 and SiteScope_2).
- ➤ Cluster name or IP address should be used in SiteScope URL as the gateway server.
- ➤ Static IP addresses should be used for SiteScope machines and the cluster address.

---

### 3 Set the owner machine and verify the disk resource is online

**a** Select one of the machines on which to install SiteScope (in our example, SiteScope_1), and set it to be the owner. To switch ownership between the agents, go to **<MY-CLUSTER> > Groups > Cluster Group**, and right-click **Move Group**. The owner machine is displayed in the **Owner** column in the right pane.

**b** Verify the Physical Disk resource is online. Go to **<MY-CLUSTER> > Groups > Cluster Group**, right-click the Disk E resource in the right pane, and select **Bring Online**. The shared driver is now available on the selected machine, SiteScope_1, and not on the other machine.

### 4 Install SiteScope on SiteScope_1 and set SiteScope service startup type to Manual

**a** Install SiteScope on the shared driver (Disk E) using the SiteScope installation wizard. For installation details, refer to the *HP SiteScope Deployment Guide* PDF.

**b** Set the SiteScope service startup type to Manual. In **Administrative Tools** > **Services**, right-click the SiteScope service, and then click **Properties.** On the General tab, in the **Startup type** box, click **Manual** and then click **OK**.

**c** Verify SiteScope is up. Open a Web browser and try to access the SiteScope user interface using the cluster name or IP address. In our example: http://Lab_resource06:8080/SiteScope.

### 5 Create a corresponding SiteScope service on SiteScope_2

**a** Switch ownership to SiteScope_2. Go to <**MY-CLUSTER**> > **Groups** > **Cluster Group**, and right-click **Move Group**. SiteScope_2 is now the owner machine.

**b** Verify that Disk E on SiteScope_2 is online (right-click the Disk E resource, and select **Bring Online**).

**c** Create a service on SiteScope_2 by performing the following:

- Make a copy of the command from the **MS_Cluster_Service_Creation_Cmd.txt** file located in the <**SiteScope root directory**>**conf****ha** directory.
- Replace <SiteScope root on shared disk> and <SiteScope service name> with the relevant values.
- Run the command in a command window.
- Verify the service was created by checking for the following success message: Creating Service. Service install success.

---

**Note:** Service names must be the same on both SiteScope machines.

---

**d** Create a heartbeat parameter by performing the following:

- Make a copy of the command from the **MS_Cluster_Heartbeat_Param_Cmd.txt** file located in the <**SiteScope root directory**>**conf****ha** directory.
- Replace <SiteScope root on shared disk> and <SiteScope service name> with the relevant values.
- Run the command in a command window.
- Verify the heartbeat parameter was updated successfully (if there was no error message) by checking the registry key. You can also check for the following success message: Value Changed Successfully At SYSTEM\CurrentControlSet\Services\<SiteScope_service_name>\serviceHeartbeatPath\.
  end perfex

---

**Note:** You can manually create and set the heartbeat parameter directly from the registry.

---

**e** Set the SiteScope service startup type to Manual. In **Administrative Tools** > **Services**, right-click the SiteScope service, and then click **Properties.** On the General tab, in the **Startup type** box, click **Manual** and then click **OK**.

**f** Verify SiteScope is up. Open a Web browser and try to access the SiteScope user interface using the cluster name or IP address. In our example: http://Lab_resource06:8080/SiteScope.

### *6* Create a generic service resource on the cluster

**a** Right-click the Cluster Group, and select **New** > **Resource**.

**b** In the **New Resource** page, perform the following, and then click **Next**:

- Type a resource name and description
- In the **Resource type** box select **Generic Service**
- In the **Group** box select **Cluster Group**

**c** In the **Possible Owners** page, select the SiteScope machines as the resource owners, and click **Next**. In our example, select SiteScope_1 and SiteScope_ 2.

**d** In the **Dependencies** page, select the SiteScope installation disk as the resource dependency, and click **Next**. In our example, select Disk E.

**e** In the **Generic Service Parameters** page, type the SiteScope service name, and click **Next**.

**f** In the **Registry Replication** page, click **Finish**.

## 7 Test failover

You can test failover by shutting down the SiteScope owner machine and verifying that you can still access SiteScope through the Cluster IP address or cluster name. The Cluster Administrator should also be updated to show the new owner.

---

**Note:** For information on verifying that resources will failover, refer to the "Test Installation" section of the Guide to Creating and Configuring a Server Cluster Under Windows Server 2003.

---

# Index

## K



## L



## M



## O



## P



## S



## T



## U