**Hewlett Packard
Enterprise**

HPE SiteScope

Software Version: 11.32

SiteScope Failover Guide

Document Release Date: March 2016
Software Release Date: March 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. HPE 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 HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2015 Hewlett Packard Enterprise Development LP

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.

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: https://softwaresupport.hp.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HPE Software Support web site at: **https://softwaresupport.hp.com**

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

HPE Software 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 HPE 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hp.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hp.com/web/softwaresupport/access-levels

HPE Software Integrations, Solutions and Best Practices

Visit the Integrations and Solutions Catalog at https://hpenterprise.sharepoint.com/teams/aztec/Portal/index.html to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at **https://hpln.hpe.com/group/best-practices-hpsw** to access a wide variety of best practice documents and materials.

Contents

Send Documentation Feedback

Welcome to SiteScope Failover

This guide provides detailed instructions on how to deploy and use the SiteScope Failover configuration to provide a backup SiteScope server to enable infrastructure monitoring availability after a SiteScope server failure.

This guide contains the following sections:

- **"Introduction to SiteScope Failover" on page 7**

  Describes the SiteScope Failover functionality and environment.

- **"Before Installing SiteScope Failover" on page 11**

  Describes the installation requirements and additional information to read before installing SiteScope Failover.

- **"Installing SiteScope Failover" on page 14**

  Describes how to install the SiteScope Failover server.

- **"Configuring SiteScope Failover" on page 25**

  Describes the SiteScope Failover configuration process.

- **"Troubleshooting SiteScope Failover" on page 33**

  Describes how to troubleshoot problems with SiteScope operations and mirroring.

Chapter 1: Introduction to SiteScope Failover

HPE SiteScope Failover is a special version of SiteScope that includes automated mirroring and failover functionality. It enables you to implement failover capability for infrastructure monitoring performed by a primary SiteScope by provisioning for backups, redundant, and failover mechanisms.

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. Ideally, a failover system automatically and transparently transfers the service provided by the failed system to the backup system. The backup system "mirrors" the services of the primary system. SiteScope Failover is a special SiteScope installation that performs the following:

- Automated, periodic mirroring of monitoring configurations from the primary SiteScope installation to the failover installation.
- Automated monitoring of the availability of the primary SiteScope installation.
- Automated transition to the failover from standby to active if the primary system fails or is temporarily taken out of service.

The SiteScope Failover Main Operations

This section gives an overview of the SiteScope Failover functionality and concepts. It contains the following:

- "Mirroring Configurations" below
- "Monitoring Primary Availability" on the next page
- "Failover Transition" on page 9

Mirroring Configurations

An important part of failover functionality is mirroring. Mirroring is an operation by which configuration data is replicated from the primary system to the failover system. SiteScope Failover mirrors monitor configurations so that the failover can provide the same infrastructure monitoring in the event that the primary SiteScope is unavailable.

As a system management tool, SiteScope can have a dynamic monitor configuration state. The SiteScope Failover installation periodically mirrors (copies) configuration data from the primary SiteScope to stay current with any changes to the monitoring configurations.

The following figure shows how new monitor instances added to the primary SiteScope are copied to the SiteScope Failover.
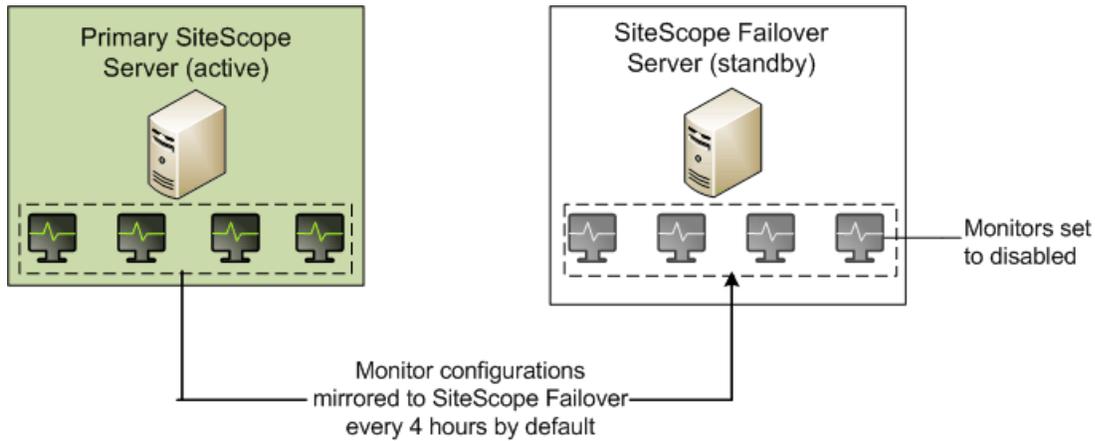
By default, SiteScope Failover is set to query the primary SiteScope every four hours and that is when any new or changed monitor configurations are copied.

Note: Do not make monitor configuration changes on the failover server. They are not copied back to the primary machine and will therefore be overwritten by the next mirroring operation. Perform all monitor configurations on the primary SiteScope and they will be mirrored to SiteScope Failover.

Monitoring Primary Availability

While the primary system is operational, failover systems are generally in standby mode. SiteScope Failover monitors the availability of the primary SiteScope by requesting its health status using Web services.
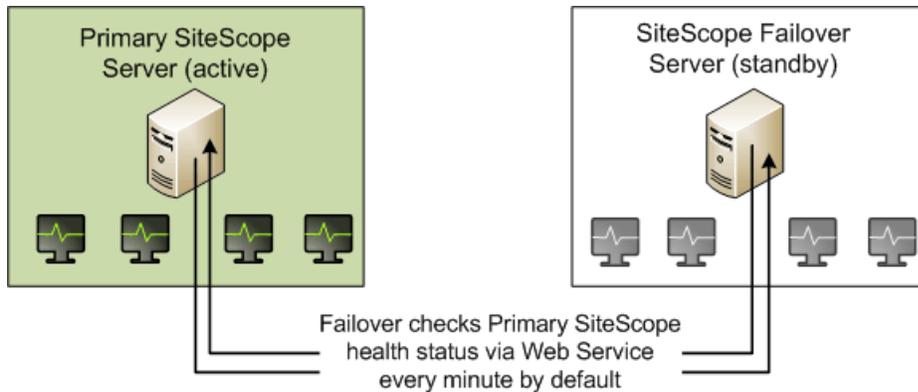
Failover Transition

When the failover monitor detects that the primary SiteScope is unresponsive, the SiteScope Failover installation activates (enables) the mirrored monitors and begins running them, as indicated by the following figure.
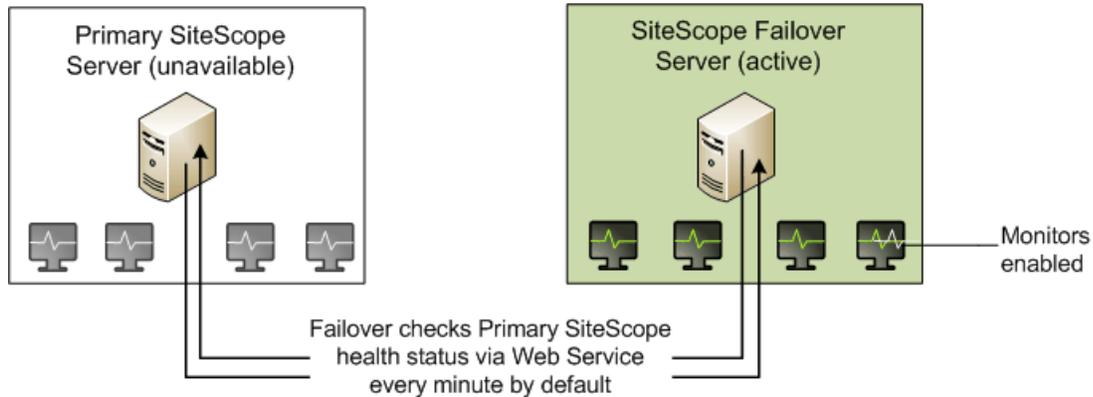
When SiteScope Failover first receives a health status indicating that the primary SiteScope is unavailable, it waits 3 minutes (by default) before starting the activation process.

When SiteScope Failover becomes active:

- Users should direct web browsers to the address of the failover SiteScope server to log in and view monitoring results.

- There may be a delay in viewing monitor results immediately after failover activation. On the SiteScope Failover machine, monitors that have recently been activated continue to be displayed with a disabled status until the monitors are updated for the first time. The time it takes to update the monitors is generally based on their update frequency.

 SiteScope Failover updates monitors in ascending order of update frequency. This means that monitors with the shortest frequency interval are run first after the failover is activated. For example, monitors that are configured to run every minute will be run before monitors scheduled for every ten minutes. Monitors with longer update intervals are initially displayed as disabled until their respective update intervals have past.

- The SiteScope Failover instance continues to watch for reactivation of the primary SiteScope. When it detects that the primary is again operational, SiteScope Failover returns to standby as follows:

  - If SiteScope Failover is configured for BSM integration, SiteScope Failover is restarted; all monitors are set to suspended.

  - If SiteScope Failover is not configured for BSM integration, SiteScope Failover remains started but changes all monitors to suspended.

SiteScope Failover Considerations and Limitations

This section describes considerations and limitations when using SiteScope Failover.

- Do not make monitor configuration changes on the failover server unless **Merge back configuration** is enabled on the primary SiteScope (**Preferences > Failover Preferences > Advanced Settings**). Otherwise, changes on the failover server are not copied back to the primary machine and will be overwritten by the next mirroring operation.

- To provide continuity of configuration and report data across a failover period, the SiteScope Failover can merge configuration data and daily log files from the SiteScope Failover to the primary SiteScope after it has recovered. Existing configuration data on the primary SiteScope is backed up and can be restored.

- If a primary SiteScope server is configured to report to BSM, when a SiteScope Failover instance becomes active, it automatically resumes reporting to BSM. Likewise, when the SiteScope Failover instance goes into standby mode, it stops reporting to BSM.

- The Reset operation in **Preferences > Integration Preferences > BSM Preferences Available Operations** is not supported on the SiteScope Failover server, even when SiteScope Failover is active.

- Monitors configured to target the primary SiteScope server do not mirror to the SiteScope Failover. If you configure a monitor on the primary SiteScope server to target the SiteScope server (either by accepting the default **SiteScope Server** in the **Server** field of the Monitor Settings area, or by typing the IP address of the SiteScope server machine), when the monitor settings are copied to the failover machine, the monitor targets the SiteScope Failover server instead of the primary SiteScope server.

- SiteScope Failover does not support copying of symbolic links when configuring a Script monitor.

Chapter 2: Before Installing SiteScope Failover

Installing SiteScope Failover is similar to a regular SiteScope installation. Most of the actions required for the initial SiteScope Failover setup are automated and are performed as part of the installation procedure or when you first access the server. Additional actions may be required depending on the configuration of the primary SiteScope. You can install SiteScope Failover on a Windows or UNIX platform.

This chapter includes:

- "Requirements for SiteScope Failover" below

- "Additional Information Related to the Installation" on the next page

- "Before You Begin" on the next page

- "Upgrading SiteScope Failover" on page 13

Requirements for SiteScope Failover

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

- Primary SiteScope and failover SiteScope both require the same version of SiteScope. If you upgrade the primary SiteScope, you must also upgrade the failover to the same version.

- Primary SiteScope and SiteScope Failover must be installed on separate machines but in the same relative drive and directory path. For example, if the primary SiteScope is installed in `C:\SiteScope` on the primary machine, you should install SiteScope Failover in `C:\SiteScope` on the failover machine. The reason is that your primary SiteScope may have monitors that refer to files within its SiteScope home directory. Installing SiteScope Failover with the same home directory ensures integrity in such file references.

- SiteScope Failover should be installed on a server with similar or identical server resources (processor speed and memory) as the primary SiteScope server. Since the failover is not intended to store monitor data for extended periods of time, the available disk space need not be as large as for the primary SiteScope.

- SiteScope Failover must be installed and run using the same basic permission levels as the primary SiteScope, to ensure that both can access needed file outside of SiteScope.

- The host names of the primary SiteScope and SiteScope Failover server should be resolved and be visible to each other using the common SiteScope port (by default, it is 8080 for a typical installation, and 8443 for SiteScope enabled for SSL). Note that the primary SiteScope and SiteScope Failover server can each use a different port.

- Key management for data encryption is not supported when using SiteScope Failover to provide backup infrastructure monitoring for the primary SiteScope.

Additional Information Related to the Installation

Review the following sections in the Installing SiteScope section of the HPE SiteScope Deployment Guide (available from the HPE Software Support site), as relevant to your target operating system:

- Installation Prerequisites - Linux

- Installing Dependencies on an Oracle Enterprise Linux 6.0, 6.1 Environment

- Installation Prerequisites - CentOS 6.2

- Installing SiteScope on an Cloud Services Instance Running on CentOS 6.2

- Troubleshooting and Limitations

- Installing SiteScope Using the Installation Wizard on a Machine Without X11 Server

If SiteSope is integrated with HPOM or BSM, you need to configure dependencies and install the Operations Agent (required for sending events and storing metrics data to HPOM or BSM). Review the following sections in the Integrating SiteScope with Operations Manager Products Guide (available from the HPE Software Integrations site):

- Installing the Operations Agent

- Installing Dependencies Required by the Operations Agent

Before You Begin

Obtain the following before you start the installation program:

- A SiteScope Failover license. This is provided with the Premium, Ultimate, and System Collector editions at no additional cost. For license purchase inquiries, contact your HPE sales representative or use the "Contact Us" link in the HPE SiteScope Product page.

- The installation path of the primary SiteScope. For example, `C:\SiteScope`

Upgrading SiteScope Failover

This section describes how to upgrade existing SiteScope Failover installations to SiteScope Failover 11.30 with minimum interruption to your system and operations.

1. **Prerequisites**

   SiteScope Failover 11.30 requires a Failover Edition license. This license is provided with the Premium, Ultimate, and System Collector editions at no additional cost. (The Failover license is dependent on the primary SiteScope license being active.) For licensing details, see the SiteScope Deployment Guide available on the HPE Software Support site.

2. **Disable the Merge back configuration on the SiteScope Failover**

   Disable the **Merge back configuration** option on the SiteScope Failover server if it is enabled in the Failover settings (**Preferences > Failover Preferences > Edit Failover Profile** dialog box).

3. **Upgrade the Primary SiteScope**

   For details, see the Upgrading SiteScope section of the SiteScope Deployment Guide.

   > **Note:** The primary SiteScope and SiteScope Failover both require the same version of SiteScope. If you upgrade the primary SiteScope, you must also upgrade the failover to the same version.

4. **Upgrade SiteScope Failover**

   Upgrade the SiteScope Failover server to the same version as the primary SiteScope. For details, see "Installing SiteScope Failover" on page 14.

   During the installation, import the Failover license. In the Settings screen of the SiteScope Configuration Wizard, enter the path to the SiteScope Failover license key file in the **License file** box, or click **Select** and select the SiteScope license key file.

5. **Configure SiteScope Failover**

   Perform all the steps in "How to Configure SiteScope Failover" on page 25 that are required for configuring the SiteScope Failover server.

   When adding a new Failover profile, make sure you enable synchronization on the SiteScope Failover server by selecting **Merge back configuration** in **Failover Profile Properties > Advanced Settings**.

Chapter 3: Installing SiteScope Failover

You can install SiteScope Failover on Windows or Linux environments using the Installation Wizard. Alternatively, you can install SiteScope on Linux platforms using a command line or console mode.

> **Note:** The installation instructions that follow are for SiteScope 11.30. SiteScope 11.3x service packs must be installed on top of SiteScope 11.30. For specific instructions for installing a SiteScope service pack, see the "Upgrading SiteScope" section of the SiteScope Deployment Guide supplied with the service pack.

This chapter includes:

- "Installing Using the Installation Wizard " below
- "Installing on Linux Using the Console Mode" on page 19
- "Additional Installation Actions" on page 23

Installing Using the Installation Wizard

Use the following steps to install SiteScope Failover on supported Windows or Linux environments using the installation wizard.

To install SiteScope Failover:

1. Obtain the SiteScope installation program file which can be accessed from the SiteScope release media.

   Both the standard and failover SiteScopes are installed from the same installation program.

2. Run the SiteScope installation according to your operating system.

   For Windows:

   a. Run **HPSiteScope_11.30_setup.exe**.

   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_11.30_setup.exe`

   For Linux:

   a. Log in to the server as user **root**.

   b. Run the installer by typing: `./HPSiteScope_11.30_setup.bin`.

   > **Note:** If your server has Microsoft Terminal Server service running, the service must be in **Install Mode** when you install SiteScope. If the service is not in the correct mode, the wizard

> displays an error message and then exits the installation. Change to install mode using the **change user** command. For details, refer to the Microsoft support site (http://support.microsoft.com/kb/320185).

3. The Choose Locale screen is displayed.

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

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

   If the installer detects an anti-virus program you can try installing SiteScope without disabling the anti-virus program.

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

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

6. 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**.

7. In the Product Customization screen, select **HP SiteScope Failover**.

   Click **Next** to continue.

8. The Select Features screen opens, displaying the HP SiteScope Failover folder.

   Click **Next** to continue.

9. If installing on Linux platforms, SiteScope is automatically installed in the **/opt/HP/SiteScope/** folder. Skip to step 11 on page 22.

   If installing on Windows, the Choose the folders screen opens.

   Accept the default directory location. C:\SiteScope, or click **Browse** to select another directory.

   > **Note:** Choose a directory in the same relative location as the primary SiteScope installation.

   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). To restore the default installation path, click **Reset**.

   Click **Next** to continue.

10. The Install Checks screen opens and runs verification checks.

    Click **Next** after the free disk space verification completes successfully.

    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 8 and 9.

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

12. The Installing screen opens and 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 components, the Introduction screen of the SiteScope Configuration Wizard opens.

    Click **Next**.

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

    Enter the required configuration information and click **Next**.

    - **Port.** The SiteScope port number. If the port number is already in use (an error message is displayed), enter a different port. If necessary, you can change the port later using the Configuration Tool. The default port is 8080.

    - **License file.** Enter the path to a valid SiteScope Failover license key file, or click **Select** and select the SiteScope license key file. A Failover license is provided with the Premium, Ultimate, and System Collector editions at no additional cost (the Failover license is dependent on the primary SiteScope license being active).

      > **Note:** License keys from earlier versions of SiteScope are not compatible with this version.

    - **Service name** (not applicable for Linux installations). The name of the SiteScope service. If the machine has a previous version of SiteScope installed, enter another name for the SiteScope service. The default service name is HP SiteScope Failover.

    - **Use local system account** (not applicable for Linux installations). By default, SiteScope 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 is running under a Local Systems account, it attempts to connect to remote servers using the name of the server.

    - **Use this account** (not applicable for Linux installations). Select to change the user account of the SiteScope service. You can set the SiteScope service to log on as a user with domain administration privileges. This gives SiteScope 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 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:
      >
      > i. In Windows Control Panel, double-click **Administrative Tools**.
      >
      > ii. Double-click Local Security Policy, and select **Local Policies > User Rights Assignment > Log On as a Service**.

       iii. Click **Add User or Group**, and select the user you want to grant logon service access to, and click **OK**.

       iv. Click **OK** to save the updated policy.

- Start SiteScope service after install (not applicable for Linux installations). Automatically starts the SiteScope service after the installation is complete.

15. The Import Configuration screen opens. Choose **Do not import configuration data** and click **Next**.

    You cannot import configuration data to SiteScope Failover.

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. The Done screen opens.

    To access the SiteScope user interface, click the URL on the screen.

    > **Note:** If you did not select **Start SiteScope service after install** in the Configuration Settings screen, you need to start the SiteScope service before you can connect to SiteScope. For details, see Getting Started with SiteScope in the HPE SiteScope Deployment Guide (available from the HPE Software Product Manuals site).

    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 installing SiteScope on a Linux environment, set the permissions for the SiteScope installation directory to have read, write, and execute permissions for the user account that is used to run the SiteScope application. The permissions must also be set for all subdirectories within the SiteScope installation directory.

20. Download and install any SiteScope minor-minor releases and/or service packs that have been applied to the primary SiteScope. Service packs are available from the location from which you downloaded SiteScope. For details, on installing a minor-minor releases, see the Upgrading SiteScope section of the HPE SiteScope Deployment Guide (available from the HPE Software Product Manuals site).

21. Other changes may be required on the SiteScope Failover system. See "Additional Installation Actions"

> **Note:** SiteScope Failover requires configuration before it can be made active. For details, see "How to Configure SiteScope Failover" on page 25.

Installing on Linux Using the Console Mode

You can install SiteScope on Linux environments using a command line or console mode. Use this option if you are installing SiteScope on a remote server, or for any other reason that prevents you from using the user interface.

To install SiteScope using the console mode:

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

   Alternatively, copy the SiteScope setup file to a disk or network location where it is accessible to the user account that is to be used to install SiteScope.

2. Run the following command:

   `HPSiteScope_11.30_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 to select the desired locale, 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.

```
Install Groups are combined sets of features.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope: ()
    2- HP SiteScope Failover: ()

Please select one of the above groups ...: 1
```

Type 2 and then press ENTER to continue.

8. The Select Features screen opens.

```
================================================================================
Select Features
---------------

Install Features represent a group of functionality
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope(Required)

Please Select Features(Use a comma to separate your choices)
    : 1
```

Enter the number 1 (required) to install SiteScope.

Press ENTER to continue with the installation.

9. The Install Requirements screen opens.

```
================================================================================
Install Requirements Checks
---------------------------


================================================================================
 Verifying : Verifying free disk space ...  [Completed]
 Verifying : Checking for previous installations...  [Completed]
================================================================================
Performing checks ...
Details :  performing checks ... please wait
Executing initialize action :
Install check requirements successfully completed
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.

Please hit Enter to continue:
```

Press ENTER to continue with the installation.

10. The Pre-Installation Summary screen opens.

```
================================================================================
Pre-Installation Summary
------------------------

Review the following before continuing:

Application Name
    HP SiteScope

Application Shortname
    HPSiteScope

Application Revision
    11.30

Application Directory
    /opt/HP/SiteScope/

Data Directory
    /var/opt/HP/SiteScope/

If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.




PRESS <ENTER> TO CONTINUE: 
```

Press ENTER to continue with the installation.

11. The Install Features screen opens and the installation process starts.

```
================================================================================
Install Features
----------------

Checking the status of packages


Checking the installation status of selected packages


Processing of 10 packages (Using Native rpm) scheduled.
Completed checking the installation status of all packages.
This process might take a while. Please do not interrupt...
```

When the installation process is complete, the post-installation configuration screen opens.

12. The port prompt is displayed.

```
================================================================================
Installing...
------------


 [================|================|================|================]
 [----------------|----------------|----------------|----------------]
 : ==============================================================================
 ----------------------------------------------------------------
Enter the HP SiteScope port number
Port [8080]
PRESS <1> to accept the value [8080], or <2> to change the value

```

Enter the number 1 to accept the default port 8080, or enter number 2 to change the port, and then enter a different number in the change port prompt.

Press ENTER to continue with the installation.

13. The license file path prompt is displayed.

```
Enter the path to license file
File name []
PRESS <1> to accept the value [], or <2> to change the value

```

Enter the number 1 to leave the license file path empty (it is not necessary to enter license information at this point to use SiteScope during the free evaluation period), or enter the number 2, and then enter the license file path in the next text box.

> **Note:** License keys from previous versions of SiteScope are not compatible with this version.
> License key delivery can be fulfilled automatically through http://webware.hp.com.

Press ENTER to continue with the installation.

14. The Import Configuration Data screen opens.

```
Import configuration data from an existing configuration file or SiteScope
installation
->1 - Do not import: ()
  2 - Import from file: ()
  3 - Import from folder: ()

```

Enter the number 1.

You cannot import configuration data to SiteScope Failover.

Press ENTER to continue with the installation.

15. The console displays the installation parameters for confirmation.

```
------------------------------------------------------------------
HP SiteScope will be configured with the following settings
SiteScope user interface port: 8080
License file: None
Press <1> to continue, or <2> to change values:
1
  : Please wait ...
```

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 completes. An installation status message is displayed.

```
==================================================================
Installation Complete
--------------------


Congratulations!
HP SiteScope 11.30
The installation has been successfully completed.
Application Directory: /opt/HP/SiteScope/

View log file./tmp/HPOvInstaller/HPSiteScope_11.30/HPSiteScope_11.30_2014.09.10
_15_02_HPOvInstallerLog.txt
[root@myd-vm04854 Release]#
```

16. After installing SiteScope on a Linux environment, set the permissions for the SiteScope installation directory to have read, write, and execute permissions for the user account that is used to run the SiteScope application. The permissions must also be set for all subdirectories within the SiteScope installation directory.

17. Download and install any SiteScope service packs that have been applied to the primary SiteScope. Service packs are available from the location from which you downloaded SiteScope.

18. Other changes may be required on the SiteScope Failover system. See "Additional Installation Actions" below.

> **Note:** SiteScope Failover requires configuration before it can be made active. See "How to Configure SiteScope Failover" on page 25.

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 instance for the changes to take effect. See the corresponding sections of the SiteScope Help for more information.

- Make changes to the Windows registry on the failover system to match any changes made on the primary SiteScope server. For example, if you make changes to JVM heap space on the primary SiteScope, you

should make the same changes on the failover system.

- ODBC database connections must be set up on the failover machine to match those on the primary SiteScope.

- JDBC drivers must be copied, installed, and set up on the failover machine to match any database monitoring being performed on the primary SiteScope.

- 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 on the failover machine.

- DHCP library files must be copied from the primary to failover machine in order to enable the DHCP monitor type.

- When the primary SiteScope server requires a secure connection, SiteScope Failover must also be configured for a secure connection. For details, see the section on Configuring SiteScope to Use a Secure Connection in the HPE SiteScope Deployment Guide (available from the HPE Software Support site).

- When the primary SiteScope server requires SSL with client certificate authentication, SiteScope Failover must be configured for SSL with client certificate authentication. Client certificate authentication must be enabled and configured on the primary SiteScope and SiteScope Failover servers. For details, see "How to Configure SiteScope Failover for SSL With Client Certificate Authentication" on page 28.

- SiteScope and SiteScope Failover support user authentication using smart cards. Smart cards store certificates verifying users' identity and allow access to secure environments. For details on enabling smart card authentication, see the section on configuring smart card authentication enforcement in the SiteScope Deployment Guide (available from the HPE Software Support site).

Chapter 4: Configuring SiteScope Failover

This chapter includes:

- "How to Configure SiteScope Failover" below
- "How to Configure SiteScope Failover for SSL With Client Certificate Authentication" on page 28
- "Test SiteScope Failover Configuration" on page 30
- "SiteScope Failover and BSM Integration" on page 31
- "SiteScope Failover and Operations Manager Integration" on page 32

How to Configure SiteScope Failover

This section includes information about configuring SiteScope Failover for its initial use.

1. **Access the user interface**

   After you have installed SiteScope Failover, access the user interface to configure SiteScope Failover.

   Open a supported web browser and enter the SiteScope Failover server name with the port number selected during the installation.

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

   The user interface to SiteScope Failover is very similar to the primary user interface. However, title bar indicates SiteScope Failover.

2. **Verify the License**

   You activate SiteScope Failover by installing SiteScope Failover and entering the SiteScope Failover license file (supplied at no additional cost when purchasing a Premium, Ultimate, or System Collector edition license). The Failover license is dependent on the primary SiteScope license being active. SiteScope Failover can mirror and provide failover functionality for any regular SiteScope installation of the same version number.

   a. In the SiteScope Failover user interface, choose **Preferences > General Preferences**.

   b. Expand the **Licenses** group.

   c. Enter a new license file if needed, and click **Save**.

3. **Configure Lightweight Single Sign-On (LW-SSO) for the Authentication Strategy**

   This is the default single sign-on authentication strategy for SiteScope. LW-SSO is embedded in SiteScope and does not require an external machine for authentication.

SiteScope Failover and primary SiteScope must be configured with the same LW-SSO passphrase.

  a. Access the primary SiteScope user interface.

  b. Select **Preferences > General Preferences > LW SSO Settings**.

  c. Write down or copy the text from the **Communication security passphrase** field.

  d. Access the SiteScope Failover user interface.

  e. Navigate to **Preferences > General Preferences > LW SSO Settings**.

  f. Paste or enter the communication security passphrase, and then click **Save**.

  g. Restart SiteScope Failover.

4. **Add Certificates to SSL-Enabled SiteScope Failover**

SiteScope Failover must be enabled for SSL if the primary SiteScope is enabled for SSL. Also, if the primary SiteScope is not enabled for SSL then SiteScope Failover cannot be enabled for SSL.

The procedure to enable SiteScope Failover to use SSL is the same as the procedure for standard SiteScope. See Configuring SiteScope to Use SSL in the HP SiteScope Deployment Guide.

> **Note:** The `serverKeystore` string used when generating the certificates must be typed in the same case as specified in the documentation, otherwise it will fail when using SiteScope Failover with SSL.

If self-signed certificates are used, both primary and SiteScope Failover must have the same certificates imported. For example, assume the following SiteScope server URLs:

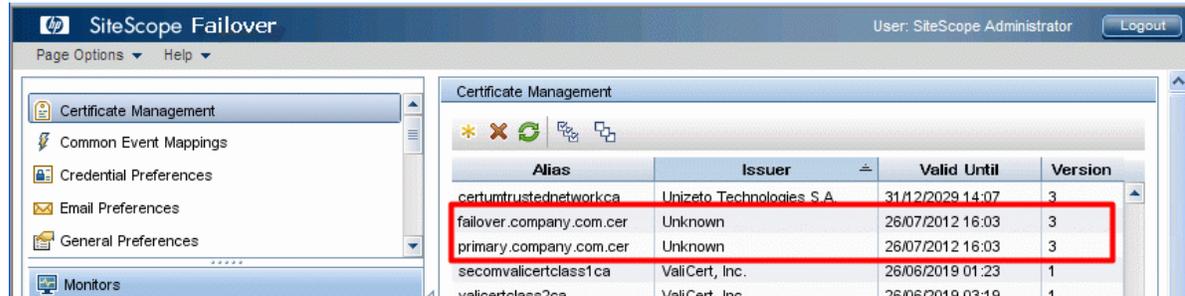- Primary: `https:\\primary.company.com:8443\`

- Failover: `https:\\failover.company.com:8443\`

On the **primary.company.com** server, the certificates for **primary.company.com** and **failover.company.com** should be added. Similarly, on the **failover.company.com** server, the certificates for **primary.company.com** and **failover.company.com** should also be added:

On primary SiteScope:
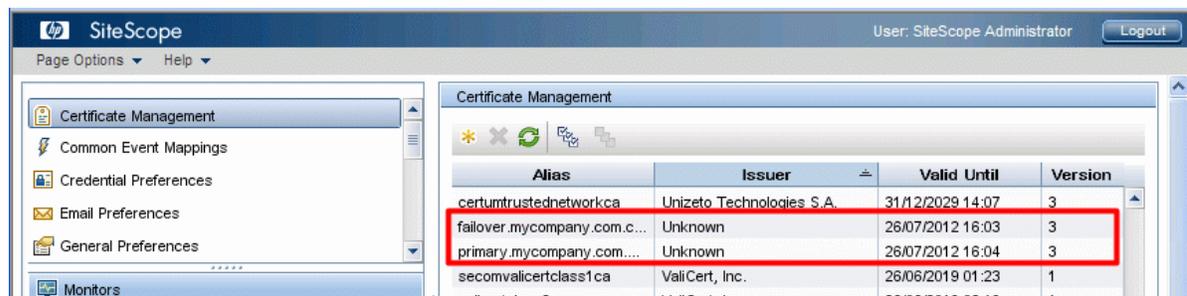
On SiteScope Failover:

For information about viewing and importing certificates by using the Certificate Management page, see the SiteScope Help.

5. **Specify Schedule Settings**

The schedule settings can determine how often the mirroring operation occurs and how often the SiteScope Failover checks the primary SiteScope availability.

  a. In the SiteScope Failover user interface, select **Preferences > Schedule Preferences**.

  b. In the Failover Schedule Preferences group, create a new absolute or range schedule.

     For information about creating absolute or range schedules, see the SiteScope Help.

> **Note:** You do not need to define schedule settings if you want to use the default schedule for these operations.

6. **Specify Notification Settings**

The notification settings determine the email server configuration, the notifications template, and other related settings.

  a. In the SiteScope Failover user interface, select **Preferences > Failover Preferences**.

  b. Select **Default Settings > Edit**.

     The Default Failover Settings dialog appears.

     For information about notification settings, see the SiteScope Help.

  c. Specify the settings as required, and then click **OK**.

7. **Create a New Failover Profile**

You define a profile to store the configuration settings that control how SiteScope Failover operates. These behaviors include frequency of checking primary SiteScope availability and mirroring.

  a. In the SiteScope Failover user interface, select **Preferences > Failover Preferences**.

  b. In the right panel, click **New Profile** to open the New Failover Profile dialog.

     For information about defining a profile by using this dialog, see the SiteScope Help.

> **Note:** For an SSL environment, make sure that the primary SiteScope host name is identical to that used in the server certificate (the name is case sensitive), otherwise the connection will fail

> due to an SSL error.

c. Specify the settings as required, and then click **OK**.

> **Note:** When using the **Merge back configuration** option in the Advanced Settings panel, you can enable this setting on the SiteScope Failover server even when the primary SiteScope is already down; this setting does not need to be set in advance in order to send configuration data created when SiteScope Failover was active back to the primary SiteScope when it becomes active.

The profile is created and displayed by name in the Failover Preferences page.

The new profile is also listed on the primary SiteScope Failover Preferences page.

8. **Test the SiteScope Failover Configuration**

For details, see "Test SiteScope Failover Configuration" on page 30.

How to Configure SiteScope Failover for SSL With Client Certificate Authentication

This section includes information about configuring SiteScope Failover for SSL with client certificate authentication when the primary SiteScope server requires SSL. SiteScope Failover must be enabled for SSL if the primary SiteScope is enabled for SSL. Also, if the primary SiteScope is not enabled for SSL then SiteScope Failover cannot be enabled for SSL.

1. **Prerequisites**

   Client certificate authentication must be enabled and configured on the primary SiteScope and SiteScope Failover servers. This can be done either:

   - Using the SiteScope Hardening Tool (recommended). For details, see the section on Using the SiteScope Hardening Tool in the HPE SiteScope Deployment Guide (available from the HPE Software Support site).

   - Manually. For details, see the section on Manually Configuring SiteScope to Use a Secure Connection in the HPE SiteScope Deployment Guide (available from the HPE Software Support site).

2. **Create a Failover Profile for SSL SiteScope Before Enabling Client Certificate Authentication**

   For task details, see "How to Configure SiteScope Failover" on page 25.

3. **Create the Keystore with the Client Certificate Signed by the Trusted CA**
   This client certificate will be sent for SSL authentication between the primary and SiteScope Failover server.

- To create the keystore using the SiteScope Hardening Tool (recommended), see the section on How to Use the Hardening Tool to Configure SiteScope to Connect to a BSM Server That Requires a Client Certificate in the HPE SiteScope Deployment Guide (available from the HPE Software Support site).

- To manually create the keystore:

  ○ On Windows platforms, run the command:

    ```
    C:\SiteScope\java\bin\keytool -import -alias sitescope_client_cert -file
    C:\SiteScope\templates.certificates\client_cert.cer -keystore
    C:\SiteScope\templates.certificates\clientKeystore.jks -storepass <your_
    keystore_password>
    ```

  ○ On Linux platforms, run the command:

    ```
    /opt/HP/SiteScope/java/bin/keytool -import -alias sitescope_client_cert -
    file
    /opt/HP/SiteScope/templates.certificates/client_cert.cer -keystore
    /opt/HP/SiteScope/templates.certificates/clientKeystore.jks –storepass
    <your_keystore_password>
    ```

4. **Add Service Parameters to the Primary SiteScope and SiteScope Failover**

   On the primary SiteScope and SiteScope Failover server, perform the following:

   - On Windows platforms, open the Windows registry (**HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\SiteScope (or HP SiteScope Failover) \serviceParam**), and add the following string to the beginning of the (Default) entry:

     ```
     -Djavax.net.ssl.keyStore="C:\SiteScope\templates.certificates\clientKeystore.jks
     -Djavax.net.ssl.keyStorePassword=<your_ keystore_password>
     -Djavax.net.ssl.keyStoreType=JKS
     ```

     Note: If you created the keystore using the SiteScope Hardening Tool, the file name will be **BSMClientKeystore** (without an extension). This file can be used as it is, or it can be copied and renamed.

   Alternatively, you can use the **go.bat** option from the **<SiteScope root directory>\bin** directory to add service parameters.

   - On Linux platforms, in the **/opt/HP/SiteScope/bin/start-monitor** file, modify the java parameters using Linux file path as follows:

     ```
     -Djavax.net.ssl.keyStore="/opt/HP/SiteScope/templates.certificates/clientKeystore.jks
     -Djavax.net.ssl.keyStorePassword=<your_ keystore_password>
     -Djavax.net.ssl.keyStoreType=JKS
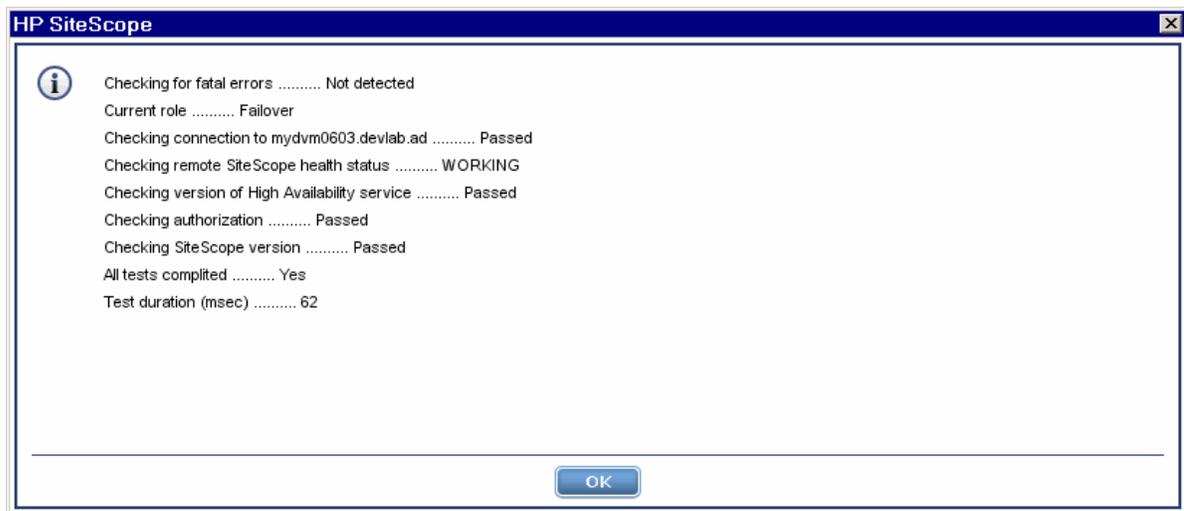     ```

# Test SiteScope Failover Configuration

SiteScope Failover configuration is tested from both the SiteScope Failover user interface and the primary SiteScope interface.

**To test the SiteScope Failover configuration from the SiteScope Failover machine:**

1. In the SiteScope Failover user interface, select **Preferences > Failover Preferences**.

2. In the right panel, select **Default Settings > Test**.

   The Test Failover dialog box appears.

3. (Optional) To test the email notifications, enter an email address and click **Send Test Notifications**.

4. To test the SiteScope Failover configuration, click **Test**. The test results appear:
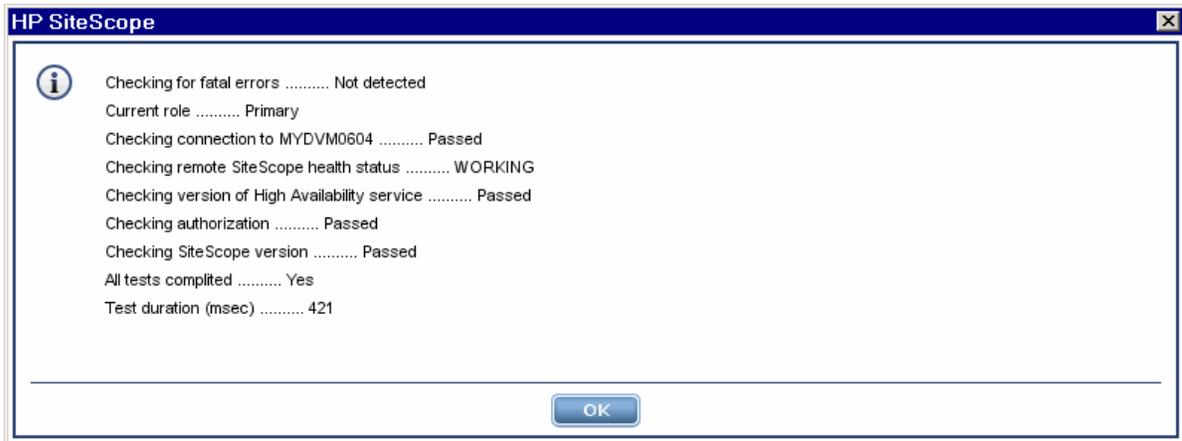
   **HP SiteScope**

   (i) Checking for fatal errors .......... Not detected
   Current role .......... Failover
   Checking connection to mydvm0603.devlab.ad .......... Passed
   Checking remote SiteScope health status .......... WORKING
   Checking version of High Availability service .......... Passed
   Checking authorization .......... Passed
   Checking SiteScope version .......... Passed
   All tests complited .......... Yes
   Test duration (msec) .......... 62

   OK

   > **Note:** If the connection fails for an SSL environment, see "Connection to SiteScope Failover Configuration Failed for an SSL Environment" on page 37.

5. Review the results for failure information, then click **OK**.

To test the SiteScope Failover configuration from the primary SiteScope machine:

1. In the SiteScope user interface, select **Preferences > Failover Preferences**.

2. In the right panel, select **Default Settings > Test**. The Test Failover dialog box appears. The test results appear:



> **Note:** If the connection fails for an SSL environment, see "Connection to SiteScope Failover Configuration Failed for an SSL Environment" on page 37.

3. Review the results for failure information, then click **OK**.

# SiteScope Failover and BSM Integration

The process for integrating SiteScope Failover with BSM is the same as for the primary SiteScope. For details on the integration process, see the section on "How to Configure SiteScope to Communicate with BSM" in the Using SiteScope Guide or in the BSM Application Administration Guide in the BSM Help.

Make sure in step 3: "Connect the installed SiteScope with BSM", when adding the SiteScope to SAM Administration in BSM, that you enter the Failover host name in the New/Edit SiteScope Page in the **Advanced Settings > Failover Host** field.

If the SiteScope Primary goes down, and SiteScope Failover is activated, the SiteScope Failover re-registers on the BSM-side and sends topology and metrics under the Primary Display Name. When the primary is operational again, it re-registers on the same profile and starts sending data.

# Disabling Reporting to BSM From SiteScope Failover

If a primary SiteScope is configured for reporting to BSM and the failover SiteScope is activated, SiteScope Failover automatically configures itself to report topology and metrics to BSM. In some cases, you may want to disable reporting topology and metrics to BSM from SiteScope Failover.

**To disable reporting to BSM from SiteScope Failover:**

1. In the SiteScope Failover user interface, select **Preferences > Failover Preferences**.

2. Select the profile for which you want to disable reporting to BSM and click **Edit**.

3. Expand the **Advanced Settings** panel.

4. Click **Disable BSM Integration**, and then click **OK**.

**Note:** SiteScope Failover reports to BSM only after the first mirroring occurred since the primary SiteScope was registered to BSM.

# SiteScope Failover and Operations Manager Integration

The process for integrating SiteScope Failover with HP Operations Manager (HPOM) is the same as for the primary SiteScope. For details on the integration process, see Integrating SiteScope with HP Operations Manager Products (check the HP Software Integrations site for the latest version of this guide).

Note that the same version of the HP Operations agent must be installed on the SiteScope Failover machine as is installed on the primary SiteScope.

When the primary SiteScope goes down and SiteScope Failover is activated, the Operations Agent from the Failover machine starts sending events and metrics to HPOM. When the primary SiteScope is operational again, the Operations Agent from the primary machine start sending events and metrics again.

# Chapter 5: Troubleshooting SiteScope Failover

This chapter describes procedures for diagnosing and troubleshooting problems that may occur when working with SiteScope Failover.

This chapter includes:

- "Error Log File" below
- "Failover Activation Issues" on the next page
- "Authorization Errors Related to LW-SSO" on the next page
- "Incorrect Report Data" on page 35
- "Notifications Not Received" on page 35
- "Rebuild SiteScope from the SiteScope Failover" on page 35
- "SiteScope Failover Failed to Create a New Profile with the Primary SiteScope that Already Uses SSL with Client Certificate Authentication" on page 36
- "Failover Profile Not Being Created on the SiteScope Server" on page 36
- "Connection to SiteScope Failover Configuration Failed for an SSL Environment" on page 37
- "SiteScope Failover Configuration Fails with WSDL Timeout Error" on page 37
- "Events sent from SiteScope Failover Fail to Show in BSM" on page 38

# Error Log File

Errors encountered during SiteScope Failover mirroring operations are written to the **high_availability.log**. This log is located in the **<SiteScope root directory>\logs** directory on the failover server.

Entries are made to this file if the SiteScope Failover is scheduled to mirror configurations from the primary SiteScope but is unable to connect to the primary. Entries are also made to this file if individual mirroring operations fail or encounter errors.

# Failover Activation Issues

This section includes the troubleshooting suggestions for issues relating to SiteScope Failover activation and general operations.

- **Detecting if a SiteScope Failover was Activated**

  To determine if a SiteScope Failover has been activated:

  - Ask the recipients in the notifications list if they received an email about SiteScope Failover has been activated.

  - Review the **high_availability.log**.

- **SiteScope Failover License Issues**

  A Failover license is provided with the Premium, Ultimate, and System Collector editions, and is dependent on the primary SiteScope license being active. If the primary SiteScope edition license has expired or exceeded its capacity, the Failover license will not be active.

  a. Check the validity of the license edition used by the primary SiteScope. For license inquiries, contact your HPE sales representative or use the "Contact Us" link in the HPE SiteScope Product page.

  b. If you renew the license on the primary SiteScope, import the Failover license file to the SiteScope Failover server. Select **Preferences > General Preferences > Licenses**, and enter the path to your SiteScope license file in the **License file** box, or click the **Select** button, and select the license file.).

  c. Restart the SiteScope Failover service. On Windows platforms, the default service name is **Failover**.

     After entering a valid Failover license and restarting the service or process, SiteScope Failover disables the mirrored monitors as long as it can detect the primary SiteScope.

# Authorization Errors Related to LW-SSO

Lightweight Single Sign-On (LW-SSO) is the default single sign-on authentication strategy for SiteScope. If the LW-SSO init string differs for the primary SiteScope and SiteScope Failover, authorization errors occur.

To resolve authorization errors, see "Configure Lightweight Single Sign-On (LW-SSO) for the Authentication Strategy " on page 25.

# Incorrect Report Data

If reports seem to contain incorrect data, check that both the primary SiteScope and SiteScope Failover machines have synchronized time.

You can use the OS embedded time synchronization services (see http://en.wikipedia.org/wiki/Network_Time_Protocol).

# Notifications Not Received

If notifications are not being received as expected, check the following areas:

1. In the SiteScope Failover user interface, select **Preferences > Failover Preferences**.

2. Select **Default Settings > Test**.

   In the Default Failover Settings dialog box, enter an email address and click **Send Test Message**. This also allows you to test the format of the notification.

3. If the email message was not received:

   a. Select **Preferences > Failover Preferences**.

   b. In the Failover Preferences page, click **Default Settings > Edit**.

   c. Review the settings on the dialog box for correctness.

# Rebuild SiteScope from the SiteScope Failover

If the primary SiteScope cannot be accessed due to an operating system or hardware issue, you can rebuild the primary SiteScope as follows:

**Option 1:** Use the SiteScope Configuration Tool to create an archive on the SiteScope Failover server, and then restore it on the primary SiteScope. No additional changes are required. This will restore the current state of failover.

**Option 2:** SiteScope Failover stores the previous states of the primary configuration (mirroring results). By default, only two snapshots are stored, but you can customize this setting in the **Failover Profile >Advanced Settings >Number of backups**.

Each backup is saved as a zip file, and is located on the SiteScope Failover server in the **<SiteScope Failover root directory>\high_availability\failover\<PRIMARY_HOST_NAME>\history\** folder.

You can use one of these old snapshots to restore the primary server.

To restore the zip file, delete the **\groups** and **\persistency** folders from the file system of the primary SiteScope server, and then unpack the zip file to the SiteScope root folder to overwrite existent files.

> **Note:** After performing one of these options, you should perform any additional SiteScope configuration changes that were previously configured, such as adding libraries or configuring SSL. The failover profile must be recreated from the beginning.

# SiteScope Failover Failed to Create a New Profile with the Primary SiteScope that Already Uses SSL with Client Certificate Authentication

If SiteScope Failover fails to create a new profile with the primary SiteScope that already uses SSL with client certificate authentication, client certificate authentication should be temporarily disabled and be enabled after creating the Failover profile.

To disable authentication you should perform the following:

- Edit the **<SiteScope root directory>\Tomcat\conf\server.xml** file on both the primary SiteScope and SiteScope Failover servers.

- In the HTTPS connector settings, set **clientAuth="false"** , and then restart SiteScope.

  ```
  <Connector port="8443" ………….    clientAuth="false" />
  ```

To enable client certificate authentication after creating the Failover profile, set this key to "=true".

Failover Profile Not Being Created on the SiteScope Server

Problem: Unable to create a failover profile when using the classic SiteScope Failover solution.

Possible Solutions:

- If you get "ERROR - LW SSO token is wrong. "General Preferences > LW SSO Settings > LW SSO Init String", make sure the string is the same on both the primary SiteScope and the SiteScope Failover server.

- Make sure that the same system time is set on both the primary SiteScope and the SiteScope Failover server (the current system time is used in the authorization process).

Connection to SiteScope Failover Configuration Failed for an SSL Environment

If the connection to the SiteScope Failover configuration fails for an SSL environment, make sure that the automatically resolved Failover host name is identical to the name used in the server certificate (the name is case sensitive). The Failover host name is available in the user interface, but the field is not editable.

If the name is different, perform the following:

1. Stop the SiteScope service.

2. Correct the name in the **<SiteScope root directory>\high_availability\ha.config.xml** file.

3. Start the SiteScope service.

This operation should be performed after stopping of SiteScope service.

SiteScope Failover Configuration Fails with WSDL Timeout Error

Problem: Getting a "Failed to access the WSDL… Connection timed out." error when setting up SiteScope Failover. If you change the primary host name to any non-existent host, the error message remains unchanged.

Possible causes:

1. The firewall, anti-virus, or other third party software is blocking the TCP port when using non-standard ports.

2. The host name cannot be resolved.

Possible solutions:

- Temporarily suspend such software to see if this is causing the problem.

- Try to open the user interface of the primary and failover servers from each other.

Events sent from SiteScope Failover Fail to Show in BSM

Problem: Events sent from SiteScope Failover (when the primary SiteScope server is down) do not show up in BSM, even though the Operations Agent was installed and the failover server is configured to send events.

Possible solution: Remove the SiteScope Failover certificate in BSM and in the OM integration on the SiteScope Failover server, and integrate the Operations Agent again.

Send Documentation Feedback

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

Feedback on SiteScope Failover Guide (SiteScope 11.32)

Just add your feedback to the email and click send.

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

We appreciate your feedback!