Quest™

Spotlight® on SQL Server Enterprise 11.7.1

Deployment Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.

Legend

> **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

> **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

> An information icon indicates supporting information.

Spotlight on SQL Server Enterprise Deployment Guide
Updated - December 2016
Version - 11.7.1

Contents

Welcome to Spotlight on SQL Server

Spotlight on SQL Server monitors the activity of SQL Server instances. Spotlight displays a visual representation of the status of the databases in your enterprise, enabling you to drill down to graphical flows that illustrate the rate at which data is moving between server components. Icons display the value of key statistics and measurements. A range of visual graphs and tabular grids provide you with detailed information about your SQL Server instance.

The components and dataflows change color to show you the source of any problem. When Spotlight on SQL Server detects a condition that it considers is a potential problem, it not only informs you about it, but advises you what you could look at to diagnose the problem further and suggests corrective actions.

Spotlight on SQL Server seamlessly combines data from several disparate sources into a single user interface. It collects and combines data from Windows performance counters, SQL Server system tables, SQL Server commands and the Windows registry, and presents them in logically related screens.

Note: There are two editions of Spotlight on SQL Server: Enterprise and Standard. This document is only appropriate for Spotlight on SQL Server Enterprise. Spotlight on SQL Server Enterprise is deploy-able with separate Spotlight Diagnostic Server and multiple Spotlight Clients.

2

The size and shape of your deployment

A minimal Spotlight on SQL Server deployment consists of

- a Spotlight Diagnostic Server (to collect Spotlight data),
- a Spotlight Client (to view Spotlight data) and
- a Playback Database (to store recent history).

These components are installed by the Spotlight on SQL Server installer. In a small deployment all these components can all be installed on the same host, however they don't have to be. Many Spotlight Clients can connect to one Spotlight Diagnostic Server. Where there are a large number of connections to be monitored or those connections are geographically widespread it may be appropriate to deploy multiple Spotlight Diagnostic Server where many Spotlight Clients monitor many connections through many Spotlight Diagnostic Server (a federation of Spotlight Diagnostic Server).

Where a Spotlight Diagnostic Server has access to the Internet, connections can additionally be monitored from a web browser or a mobile device.

Each Spotlight Diagnostic Server requires access to a Playback Database. One Playback Database is deployed per Spotlight Diagnostic Server. The Playback Database can be installed on the same host as the Spotlight Diagnostic Server, dependent on the number of SQL Server instances to be monitored. The Playback Database stores recent history.

Once Spotlight is installed you may choose to collect and store data for reporting and trending. This data is stored in a Spotlight Statistics Repository. Many Spotlight Diagnostic Server can write to the same Spotlight Statistics Repository.

Spotlight Clients, Spotlight Diagnostic Server, Playback Database, Spotlight Statistics Repository and monitored connections communicate over a Windows network. Appropriate permissions need to be in place to ensure communications flow. For more information, see Deployment over the Windows network on page 38.

Table 1: Factor in how many SQL Server instances you intend to monitor

SQL Server instances	Description
1 - 25	The Spotlight Diagnostic Server, Playback Database and Spotlight Statistics Repository can all be installed on the same host, as long as that host meets the minimum hardware requirements listed in the release notes.
More than 25	It is recommended that the Playback Database and Spotlight Statistics Repository be hosted on a different server than the Spotlight Diagnostic Server host. The host for the Playback Database and Spotlight Statistics Repository should be configured with an appropriate amount of I/O bandwidth to meet demand. If your environment uses a storage area network (SAN) it may be possible to install the Spotlight Statistics Repository and the Playback Database on the same host.
Lots	Consider a deployment of more than one Spotlight Diagnostic Server. A single Spotlight Diagnostic Server is designed to monitor a maximum of 100 SQL Servers, Analysis Services or Replication instances and 100 Windows servers. Exceeding this recommended limit on 32 bit environments may result in poor performance or product instability, due to the 1 Gb memory limit. On 64 bit environments theoretically more connections can be monitored as the 1 Gb limit no longer applies, however testing of this has been limited.

Install / Upgrade

Permissions required during installation

The Windows user installing Spotlight

When installing the Spotlight Diagnostic Server, Windows administrator privileges are required to register the Spotlight Diagnostic Server as a Windows service and to create the Windows user groups that are used to authenticate Spotlight clients.

When installing the Spotlight Diagnostic Server on a remote machine, the Windows account on the Spotlight client must have Windows administrator privileges on the Spotlight Diagnostic Server host. The local computer must be able to authenticate this user.

Elevated privileges

In many cases, the Spotlight installer will run at elevated privileges in order to perform the required actions. These privileges can specifically be allowed or disallowed by system administrators by means of standard Microsoft Installer (MSI) policy settings.

If the Spotlight Diagnostic Server user does not have privileges to start services, that privilege is granted by Spotlight during the installation process, if possible.

Multiple users of a system

If multiple users of a system install Spotlight for use, the additional users must be local administrators.

Install

Run the Spotlight on SQL Server installer. During installation you will be prompted to supply details for the Spotlight Client, Spotlight Diagnostic Server and Playback Database.

Table 2: Types of installation

Typical	Select to install the Spotlight Diagnostic Server on a computer networked to the current computer. Select to install the Spotlight Client on the current computer to connect to a pre-existing Spotlight Diagnostic Server.
Compact	Select to install the Spotlight Client and Spotlight Diagnostic Server on the current computer.

Table 3: About the Spotlight Client installation

Component	Description

Install location	Default installation folder (32 bit system)
	`C:\Program Files\Quest Software\Spotlight on SQL Server`
	Default installation folder (64 bit system)
	`C:\Program Files (x86)\Quest Software\Spotlight on SQL Server`
	i Note: Do not install the Spotlight Client in the same location as an existing (but different entity of) Spotlight.
	If you install a different Spotlight after you have installed Spotlight on SQL Server, do not install the new Spotlight in the Spotlight on SQL Server directory.

Table 4: About the Spotlight Diagnostic Server installation

Component	Description
Install location	Default installation folder for the Diagnostic Server (32bit and 64bit systems): `C:\Program Files\Quest Software\Diagnostic Server` During a Typical install the diagnostic server can be installed remotely. Consider installing the Spotlight Diagnostic Server on a computer that is always switched on. Some services require Internet access; see Spotlight services requiring Internet access.
Diagnostic Server Account	The Spotlight Diagnostic Server will run under this Windows account. Enter a domain user account or select the local system account. These credentials can later be used to authenticate Spotlight connections to monitor SQL Server instances and Windows Server.
Diagnostic Server Users	Spotlight uses the Spotlight diagnostic user groups to authenticate the Spotlight Client to the Spotlight Diagnostic Server, to authenticate a user's right to configure Spotlight and execute actions on monitored systems. The Windows user installing Spotlight (on the Spotlight Client) is automatically added to all Spotlight diagnostic user groups. For more information, see Spotlight diagnostic user groups on page 39. Add more users to the Spotlight diagnostic user groups if required. Members of these groups can be Windows users or Windows domain groups. Aliases are not supported.
Auto-update Diagnostic	Selected The Spotlight Diagnostic Server will receive minor updates (scripts and

Component	Description	
Server		configuration) automatically. Ensure the Spotlight Diagnostic Server can access the Internet. For more information, see Spotlight services requiring Internet access on page 16.
	Not Selected	All updates to the Spotlight Diagnostic Server will require a new version and installation of Spotlight on SQL Server.

Table 5: About the Playback Database installation

Component	Description
Instance	Select the SQL Server instance to install the Playback Database on. The Playback Database can be installed on the same Windows Server as the Spotlight Diagnostic Server or a different server dependent on the size of the deployment. For more information, see The size and shape of your deployment on page 7.
Authentication	Select Windows or SQL Server authentication.
Database	Optionally rename the database. The default name is *SpotlightPlaybackDatabase*. If the database has not already been created, click **Create** to create the database.

Upgrade

Use the Spotlight installer to upgrade from version 10.0 or later of Spotlight on SQL Server. To upgrade from an earlier version of Spotlight than 10.0, upgrade to at least version 10.0 before upgrading to 11.7. To upgrade from 10.5.0, first upgrade to 10.5.2 and then upgrade to 11.7.

Backup before upgrade

Backup all Spotlight configuration and saved collection data. For more information, see Backup Spotlight data on page 23.

Upgrade

On each Spotlight client, run the Spotlight on SQL Server executable.

Note:

- Following upgrade of the Spotlight Diagnostic Server, the Playback Database and Spotlight Statistics Repository are automatically upgraded the next time they are accessed by the Spotlight Diagnostic Server. If in your environment the Playback Database / Spotlight Statistics Repository are replicated as per a Microsoft Replication database the upgrade can fail if schema changes are required that can only be made when replication is turned off. To successfully upgrade, the steps are to: turn replication off, upgrade the Spotlight Diagnostic Server, then re-enable replication.
- If your enterprise has multiple Spotlight Clients then ensure all Spotlight Clients are included in the upgrade process. If the Spotlight Client and Spotlight Diagnostic Server are running different versions of Spotlight on SQL Server, the client will be unable to connect to the Spotlight Diagnostic Server.

Preservation of configuration information

The following information on the Spotlight Diagnostic Server is preserved when you upgrade:

- Connection properties for all monitored servers (including changes to scheduling and alarms)
- Enterprise views
- Collection properties
- Alarm Actions (These include running a program and sending an email.)
- Planned Outages
- Global options such as user-created Error Log rules
- Configuration information for the Spotlight Statistics Repository (this applies only if you installed the Spotlight Statistics Repository from an earlier version of Spotlight on SQL Server) and the Playback Database.

Alarms requiring acknowledgment

The Spotlight factory settings for alarms requiring acknowledgment changes on upgrade from Spotlight 11.2. Only Connection Failure alarms are now factory set to require acknowledgment.

The alarms that were factory set to require acknowledgment in Spotlight 11.2 and earlier are as follows. They are included here so you can choose to manually enable them to require acknowledgment again post upgrade if required.

- Availability Group - Failed Over
- Clusters - Failed over
- Diagnostic Server - Auto Update Success
- Error Log - Error Count
- LiteSpeed Backup Failed
- LiteSpeed Backup Warning
- Locks - Blocked Processes
- Locks - Deadlocks
- Mirroring Failedover
- SQL Agent - Jobs Failed

Monitoring your Spotlight on SQL Server connections on a mobile device

If you used Spotlight 11.1.x or earlier to monitor your Spotlight on SQL Server connections on a mobile device and intend to continue monitoring your connections on a mobile device then the following additional upgrade instructions are required.

1. Uninstall the **Spotlight Web Publisher** via **Windows | Control Panel | Programs and Features**. The Spotlight Web Publisher was required in the past to monitor SQL Server connections on a mobile device. It is now important that you uninstall it. By default the Spotlight Web Publisher was installed on the same computer as the Spotlight Diagnostic Server.
2. From the Spotlight Client, click **Configure | Spotlight Cloud**. Select **Upload data to Spotlight Cloud**. Ensure your Spotlight Cloud (Spotlight Essentials) account details are correct.

Uninstall

Multiple Spotlight clients and servers may be involved. Uninstall the Spotlight Diagnostic Server before you uninstall all Spotlight clients.

1. Optionally, backup before uninstall

Backup all Spotlight configuration and saved collection data. For more information, see Backup Spotlight data on page 23.

2. Uninstall the Spotlight Diagnostic Server

For the Windows server on which the Spotlight Diagnostic Server is installed:

1. Open **Windows Control Panel**.
2. Select **Programs and Features**
3. Select **Spotlight Diagnostic Server** and click **Remove**.

Note: A running Spotlight Diagnostic Server is automatically shut down before being uninstalled.

3. Uninstall Spotlight Clients

Repeat for each Windows server on which a client is installed:

1. Open **Windows Control Panel**.
2. Select **Programs and Features**
3. Select **Spotlight on SQL Server Enterprise** and click **Remove**.

The Playback Database and Spotlight Statistics Repository

The Playback Database and Spotlight Statistics Repository are not removed when Spotlight is uninstalled. You may delete them independently. You may use the Playback Database again with another Spotlight installation.

4

Data collection and storage

Table 6: Components of Spotlight that collect and store data

Component	Description
Spotlight Diagnostic Server	The Spotlight Diagnostic Server is at the core of the Spotlight on SQL Server architecture. All Spotlight data passes through the Spotlight Diagnostic Server. The Spotlight Diagnostic Server is a Windows service. It runs under Windows credentials.
Playback Database	Recent history is stored in the Playback Database. The Playback Database is deployed on SQL Server. There is one Playback Database per Spotlight Diagnostic Server.
Spotlight Statistics Repository	Long term history for reporting and trending is stored in the Spotlight Statistics Repository. The Spotlight Statistics Repository is deployed on SQL Server. Deployment of the Spotlight Statistics Repository is optional per Spotlight Diagnostic Server.
Spotlight Cloud	Upload health performance data to the Spotlight Cloud. Deployment is optional per Spotlight Diagnostic Server.

Spotlight Diagnostic Server

The Spotlight Diagnostic Server is at the core of the Spotlight on SQL Server architecture. All Spotlight data passes through the Spotlight Diagnostic Server.

Installation

The Spotlight Diagnostic Server is a Windows service.

The Spotlight Diagnostic Server is installed by the Spotlight installer. For more information, see Install on page 9.

Most deployments of Spotlight have one Spotlight Diagnostic Server, however a deployment may consist of multiple Spotlight Diagnostic Server or a federation of Spotlight Diagnostic Server if the organization requires Spotlight to monitor more connections than a single Spotlight Diagnostic Server allows or the organization has setup geographic hubs.

Deployment

View data and configure Spotlight	Configure the Spotlight Diagnostic Server from Spotlight Clients.
Playback Database	Recent historical data is stored in the playback database. Each Spotlight Diagnostic Server requires its own Playback Database.
Spotlight Statistics Repository	Enabling of the Spotlight Statistics Repository is optional. Many Spotlight Diagnostic Server can connect to the same Spotlight Statistics Repository.
Monitored connections in the deployment	The Spotlight Diagnostic Server collects data from SQL Server, Windows and other supported connection types monitored by Spotlight. A single Spotlight Diagnostic Server is designed to monitor a maximum of 100 SQL Servers, Analysis Services or Replication instances and 100 Windows servers. Exceeding this recommended limit on 32 bit environments may result in poor performance or product instability, due to the 1 Gb memory limit. On 64 bit environments theoretically more connections can be monitored as the 1 Gb limit no longer applies, however testing of this has been limited.
Deployment over the Windows network	A Spotlight on SQL Server deployment consists of many components that may be spread over a wide network. Spotlight's ability to function, to collect and display data, may depend on account permissions granted over the network and specific open network ports.
Spotlight services requiring Internet access	The Spotlight Diagnostic Server requires access to the Internet when enabling Auto Update or Spotlight Cloud services.
Account permissions	The Windows account that the Spotlight Diagnostic Server runs under could be a domain user account or the local system account. These credentials can be used to authenticate Spotlight connections to monitor SQL Server instances and Windows Server, and to connect the Spotlight Diagnostic Server to the Playback Database and Spotlight Statistics Repository.

Maintenance

Backup Spotlight data	Spotlight configuration data is stored in the conf folder on the Spotlight Diagnostic Server. You can perform backups of the Spotlight configuration data by backing up this folder regularly.
Start and stop the Spotlight Diagnostic Server	The Spotlight Diagnostic Server is a Windows service and can be started and stopped via the Windows Control Panel.

Spotlight services requiring Internet access

The following Spotlight services require Internet access on the Spotlight Diagnostic Server. Use this page to ensure the Spotlight Diagnostic Server is appropriately configured.

Auto Update	Enable Auto Update so the Spotlight Diagnostic Server will receive minor updates (scripts and configuration) automatically.
Spotlight Cloud	Monitor Spotlight connections in a web browser or Spotlight Mobile. Upload performance data for health check analysis.

Windows Control Panel | Internet Options | Connections

On the computer hosting the Spotlight Diagnostic Server:

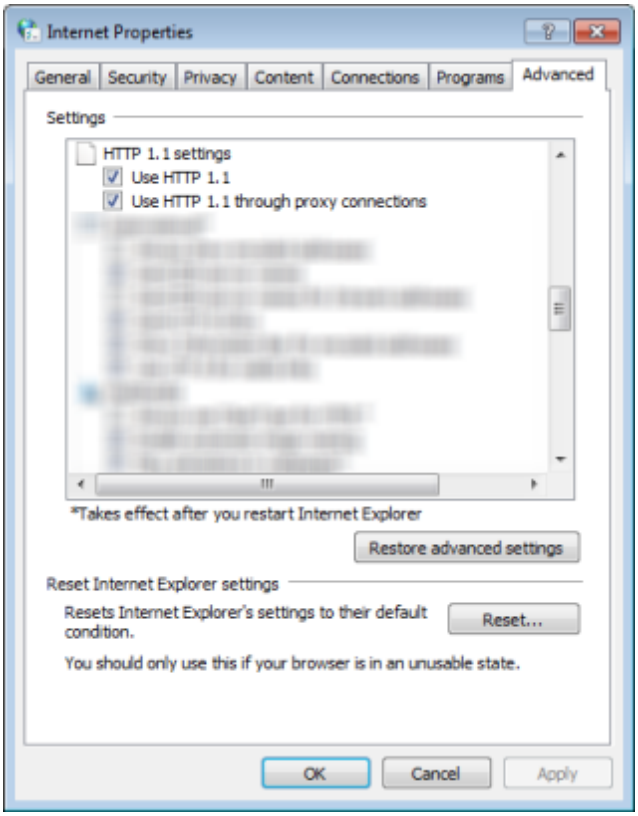
1. Open the **Control Panel | Internet Options**.
2. Select the **Connections** tab.
3. Click **LAN Settings**.
4. Ensure the settings on this screen are appropriate to the settings of your local environment.

Note: After the Spotlight Diagnostic Server is installed, restart the Spotlight Diagnostic Server after changes are made. For instructions see Start and stop the Spotlight Diagnostic Server.

Windows Control Panel | Internet Options | Advanced

On the computer hosting the Spotlight Diagnostic Server:

1. Open the **Control Panel | Internet Options**.
2. Select the **Advanced** tab.
3. Ensure **Use HTTP 1.1** and **Use HTTP 1.1 through proxy connections** are selected.



Note: After the Spotlight Diagnostic Server is installed, restart the Spotlight Diagnostic Server after changes are made. For instructions see Start and stop the Spotlight Diagnostic Server.

Internet URLs - Auto Update

An outgoing HTTPS connection to the following URL is used to retrieve updates.

`https://spotlight.blob.core.windows.net`

Enabling of Auto-update does not open a port that allows incoming connections.

Internet URLs - Spotlight Cloud

Spotlight Cloud requires incoming and outgoing HTTPS connections to the following URLs. To verify access to the Spotlight Cloud, open a web browser on the Spotlight Diagnostic Server host and look up these URLs.

URL	Web browser lookup
https://www.spotlightessentials.com	Successful display of the Spotlight web site confirms HTTPS port 443 is open.
https://api.spotlightessentials.com	Successful display of the text “Welcome to Spotlight Web API!” confirms access for uploading.

Start and stop the Spotlight Diagnostic Server

The Spotlight Diagnostic Server is a Windows service and can be started and stopped via the Windows Control Panel.

To start or stop the Spotlight Diagnostic Server

1. On the Spotlight Diagnostic Server, open **Windows Control Panel**.
2. Click **Administrative Tools | Services**.
3. From the list of available services, double click on the Spotlight Diagnostic Server name: **Spotlight Diagnostic Server**.
1. Click **Start** to start the Spotlight Diagnostic Server. Click **Stop** to stop the service.

> Note: If you attempt to stop the Spotlight Diagnostic Server whilst a program or command line action that runs in response to an alarm is still executing, the Spotlight Diagnostic Server will wait until that program or command line action has ended before stopping.

Java KeyStore

A Java KeyStore (JKS) is a repository of security certificates.

After successfully changing the password, you can use the Java keytool (Agent\bin\jre\bin\keytool.exe) to change or sign the Spotlight Diagnostic Server certificate, which is stored in the "sosse" key alias.

To set the KeyStore password:

1. Stop the Spotlight Diagnostic Server service. For more information, see Start and stop the Spotlight Diagnostic Server on page 18.
2. From the Spotlight Diagnostic Server install folder, navigate to folder **Agent\bin**
3. Open a cmd shell as the Administrator.
4. Execute command `DSKeyToolCLI -storepasswd`
5. Enter a new password of at least 6 characters.
6. Restart the Spotlight Diagnostic Server service. For more information, see Start and stop the Spotlight Diagnostic Server on page 18.

Verify that Alarm Actions and Planned Outages are working as expected.

Verify that a keystore password entry can be found in the Spotlight Diagnostic Server install folder **conf\Service\WebServic.xml**

For more information, see http://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html.

Deployment of federated Spotlight Diagnostic Server

The standard Spotlight configuration has one Spotlight Diagnostic Server. All connections are monitored through the Spotlight Diagnostic Server.

More than one Spotlight Diagnostic Server may be required when:

- The number of connections to monitor exceeds the design of one Spotlight Diagnostic Server. A single Spotlight Diagnostic Server is designed to monitor a maximum of 100 SQL Servers, Analysis Services or Replication instances and 100 Windows servers.
- Your organization is suited to the deployment of geographic hubs, where each geographic region deploys its own Spotlight Diagnostic Server.

Multiple Spotlight Diagnostic Server are deployed separately or as a federation.

Separate Spotlight deployments	Federation
A Spotlight Client monitors connections from one Spotlight Diagnostic Server at a time. The deployments do not share custom views, templates and alarm actions.	A Spotlight Client monitors connections from all Spotlight Diagnostic Server in the federation. Spotlight Clients in the federation share the same custom views, templates, alarm actions and list of planned outages.

For more information, refer to the *Spotlight on SQL Server Enterprise Federation Guide*.

Playback Database

Recent historical information (collected from monitored connections) is stored in the Playback Database.

Deployment

The Playback Database is deployed on SQL Server. For specifications, see the *Spotlight on SQL Server Enterprise Release Notes*.

The Playback Database is created by the Spotlight installer. For more information, see Install on page 9.

There is one Playback Database per Spotlight Diagnostic Server.

Configuration

Use a Spotlight Client to configure the Playback Database.

Maintenance

Backup Spotlight data	The Playback Database is deployed on SQL Server. The backup procedure is the same as for any other SQL Server database.
Maintenance plan for Spotlight Statistics Repository and Playback Database	It is highly recommended that regular maintenance is performed to maintain efficient data retrieval.

Spotlight Statistics Repository

Long term history for reporting and trending is stored in the Spotlight Statistics Repository.

Deployment

The Spotlight Statistics Repository is deployed on SQL Server. For specifications see the *Spotlight on SQL Server Enterprise Release Notes*.

The Spotlight Statistics Repository is not created during the installation of Spotlight on SQL Server. The Spotlight Statistics Repository is (optionally) enabled in the Spotlight Client for the Spotlight Diagnostic Server following installation of Spotlight.

Many Spotlight Diagnostic Server can connect to one Spotlight Statistics Repository.

Configuration

Use a Spotlight Client to enable, create and Configure the Spotlight Statistics Repository.

Maintenance

Backup Spotlight data	The Spotlight Statistics Repository is deployed on SQL Server. The backup procedure is the same as for any other SQL Server database.
Maintenance plan for Spotlight Statistics Repository and Playback Database	It is highly recommended that regular maintenance is performed to maintain efficient data retrieval.
Upgrade	Following upgrade of the Spotlight Diagnostic Server, the Spotlight Statistics Repository is automatically upgraded the next time it is accessed by the Spotlight Diagnostic Server. This may be some time following the upgrade of the Spotlight Diagnostic Server, depending on how often the Spotlight Statistics Repository is accessed. If in your environment the Spotlight Statistics Repository is replicated as per a Microsoft Replication database the upgrade can fail if schema changes are required that can only be made when replication is turned off. To successfully upgrade the Spotlight Statistics Repository, the steps are to: turn replication off, upgrade the Spotlight Diagnostic Server, then re-enable replication.

Spotlight Cloud

Upload health performance data to the Spotlight Cloud.

To retrieve an analysis of this data, sign in with your Spotlight Cloud credentials to www.spotlightessentials.com

Configuration

The Spotlight Diagnostic Server must be configured to allow upload of data to the Spotlight Cloud.

1. Ensure the Spotlight Diagnostic Server can access the Internet. For more information, see Spotlight services requiring Internet access on page 16.
2. Create a Spotlight Cloud account if you do not already have one. Go to www.spotlightessentials.com. Note that the Spotlight Cloud was previously called Spotlight Essentials - you can sign in with a Spotlight Essentials account.
3. Use a Spotlight Client to Configure uploading to Spotlight Cloud. Data is uploaded from the Spotlight Diagnostic Server to the Spotlight Cloud.

TIP: In a corporate enterprise your Spotlight Cloud account may receive a request to join an organization. In an organization, performance analysis data is uploaded to the organization and is available to all members of the organization. Members of the organization see a combined heat map and alarms list.

Configure uploading to Spotlight Cloud

Enable functionality to monitor Spotlight connections from the Spotlight web site or Spotlight Mobile. Upload performance data for health check analysis.

Open this screen from the Spotlight Client

Click **Configure | Spotlight Cloud**.

Select the Diagnostic Server

For federated Spotlight Diagnostic Server you will be prompted to select the Spotlight Diagnostic Server to configure. Each Spotlight Diagnostic Server is independently configured for Spotlight Cloud.

Upload data to Spotlight Cloud

Select	Enable functionality to monitor Spotlight connections from the Spotlight web site or Spotlight Mobile. Upload performance data for health check analysis.
Clear	Spotlight Cloud services are disabled for this Spotlight Diagnostic Server. Spotlight connections cannot be monitored from the Spotlight web site or Spotlight Mobile. Performance data for health check analysis is not uploaded to the Spotlight Cloud.

Spotlight Cloud services account details

Email or Username Password	Enter Spotlight Cloud (Spotlight Essentials) account details. This section must be filled in when uploading of data to the Spotlight Cloud is enabled. Once filled in, the email (or username) signed in under is provided. Click Register Now to create a Spotlight Cloud account if you do not already have one. Registration is free.

Additional references

Web Site Reference	Description
Spotlight Cloud Services	The Spotlight web site.
Spotlight Mobile	Download, setup and install Spotlight Mobile.
Register now	Register for a Spotlight Cloud Services account
Spotlight terms of service	Spotlight Services Agreement

Important: If you monitored your Spotlight on SQL Server connections on a mobile device in the past (Spotlight 11.0 or earlier) then you must uninstall the **Spotlight Web Publisher** via **Windows | Control Panel | Programs and Features**. The Spotlight Web Publisher was required in the past to monitor SQL Server connections on a mobile device. It is now important that you uninstall it. By default the Spotlight Web Publisher was installed on the same computer as the Spotlight Diagnostic Server.

Maintenance plan for Spotlight Statistics Repository and Playback Database

It is recommended that a maintenance plan for both the Spotlight Statistics Repository and the Playback Database is implemented.

Both the Spotlight Statistics Repository and Playback Database support a large number of monitored servers and automatically maintain the age of data available. Due to the nature of the automatic purging of old data, the data may become fragmented and this may decrease the efficiency of data retrieval operations over time.

This topic provides guidance on how to configure and automate the maintenance of the Spotlight Statistics Repository and the Playback Database.

Database configuration

The Spotlight Statistics Repository and the Playback Database do not require the database to be run under the Full Recovery model. However, since Spotlight uses the model system database to create the repository, your Spotlight repository may inherit the Full Recovery setting. Unless you are required to use the Full Recovery model and are prepared to perform regularly scheduled log file backups, we recommend you change the repository recovery model to Simple. Doing so will help maintain a considerably smaller transaction log file.

To change the repository database to Simple recovery, run the following command:

```
ALTER DATABASE [SpotlightStatisticsRepository] SET RECOVERY SIMPLE;
```

Fragmentation and index performance

The Spotlight Statistics Repository implements a star schema because of the data warehousing-style simplicity it offers for data storage and retrieval. The star schema implements a primary fact table that references a number of dimension tables. The fact table holds collections and alarm data, and the dimension tables hold definition information on everything from instance information to collection names. Spotlight maintains the age of the data in the repository, but the continuous INSERT and DELETE operations performed for data insertion and purging can lead to fragmentation. Fragmentation will eventually lead to increased CPU and I/O resource consumption.

Although the Playback Database uses a simpler schema, its data will also become fragmented over time as new data is inserted and old data purged.

To best address performance concerns, fragmentation should be minimized and index statistics should be kept up-to-date. Spotlight's scheduled maintenance feature does this automatically. By default, the Spotlight Diagnostic Server runs maintenance procedures daily at 3am for the Playback Database and Spotlight Statistics Repository. The maintenance schedule can be changed in Spotlight Options. See the online help for more information.

Database backup

The Spotlight Statistics Repository and Playback Database should be included in the list of important databases which have a disaster recovery plan associated with them. The implementation of this task is dependent on the policies and infrastructure of your organization.

Backup Spotlight data

Backup all Spotlight configuration and saved collection data regularly and before upgrade or uninstall.

Spotlight Diagnostic Server	Back up the **Diagnostic Server\Agent** folder. C:\Program Files\Quest Software\Diagnostic Server\Agent TIP: To backup just the Spotlight configuration (configuration of connections, alarms and scheduling), backup the **Diagnostic Server\Agent\Conf** folder.
Playback Database	Backup the Playback Database. The Playback Database is deployed on SQL Server. The backup procedure is the same as for any other SQL Server database.
Spotlight Statistics Repository	If a Spotlight Statistics Repository is deployed in your environment then back it up. The Spotlight Statistics Repository is deployed on SQL Server. The backup procedure is the same as for any other SQL Server database.

Log of user actions

Spotlight maintains an audit log of user actions. This log is a historical record of who changed what configuration when.

The log is located in the Spotlight Diagnostic Server installation folder:

```
...\Agent\log\UserActionLog.csv
```

The data for the log is retrieved from the Playback Database.

For the following user actions the log records:

- The Spotlight user making the change.
- The time the change was made.
- The configuration that was changed (if applicable).
- The configuration value before and after the change (if applicable).

Table 7: Log of user actions - Changes to Configure | Spotlight

Configure Ribbon Tab	
 Connections	Manage the connections monitored by Spotlight. The log records all applied changes.
 Alarms	Set the thresholds and severities that determine when an alarm is raised. The log records all changes as applied to a monitored connection or template.
 Alarm Actions	Set actions for Spotlight to take when an alarm is raised. The log records all saved changes.
 Scheduling	Spotlight collects data according to set schedules. The log records all changes to these schedules as applied to a monitored connection or template.
 Planned Outage	Changes to Planned Outage are recorded in the log of user actions.
 SQL Analysis	The SQL Analysis dialog is used to determine what data is collected and displayed in the SQL Analysis - Workload View and the SQL Server | SQL Activity Drilldown | SQL Analysis page. The log records all changes to the SQL Analysis dialog as applied to a monitored connection or template.
 SQL Server Response Time	The log records changes to the SQL statement used to measure SQL Server response time as applied to a monitored connection or template.
 Custom Counters	The log records changes to the configuration of custom counters as applied to a monitored connection or template.
 Error Log Entries	The log records changes to the error log entries Spotlight is configured to scan the SQL Server error log for, as applied to a monitored connection or template.
 Monitored Files	The log records changes to the list of files tracked for size by Spotlight as applied to a monitored connection or template.
 Spotlight	Changes to the configuration of the Spotlight Client are not recorded in the log of user actions. The Spotlight Client is configured by changes to: • Configure | Spotlight | Change Display • Configure | Spotlight | Troubleshoot Spotlight

Configure Ribbon Tab	
Diagnostic Server	The log does not record changes to the Spotlight Client connected to the Spotlight Diagnostic Server. The log does not record changes made to the Select a Diagnostic Server dialog. The log does record changes to the configuration of the Diagnostic Server: • Configure the database maintenance schedule • Configure PagerDuty • Configure the auto-update facility • Configure the Diagnostic Server's mail server • Configure the Playback Database • Configure the SNMP Trap • Configure the Spotlight Statistics Repository • Configure the use of Extended Events • Federate Diagnostic Servers
Spotlight Cloud	The log records changes to the configuration - upload data to the Spotlight Cloud.
User Experience	Changes to User Experience are not recorded in the log of user actions.
Configuration Templates	Changes to Configuration Templates (Save, Delete, Rename) are recorded in the log of user actions.

Table 8: Log of user actions - Changes to the Spotlight License

Help | About | Product license	
Help | About | Product license	Changes to the product license are recorded in the log of user actions.

Table 9: Log of user actions - When an alarm is acknowledged, snoozed or ignored

Monitor | Alarms | Action	
Acknowledge	The log records when an alarm is acknowledged.
Snooze Alarm	The log records when an alarm is snoozed.
Ignore Alarm	The log records when an alarm is ignored.

Table 10: Log of user actions - on monitored SQL Server

Monitor | SQL Server Drilldowns	
SQL Activity	The log records when a user kills a session from the Spotlight Client. That is command Sessions | Kill Session.

Monitor | SQL Server Drilldowns	
Databases	The log records when a user runs the Update Statistics command on selected indexes from the Spotlight Client. This command is run from the Indexes page of the Databases drilldown.
Support Services	The log records when a user starts a SQL agent job from the Spotlight Client. That is command SQL Agent Jobs | Start Job.
	The log records when a user changes the running state (Start / Stop) of a service from the Spotlight Client. This change is actioned from the Service Status page of the Support services drilldown.
	The log records when a user takes the following actions on Cluster Services from the Spotlight Client: • Take Offline - Makes a cluster resource or cluster group unavailable. • Bring Online - Starts a cluster resource or group. • Move Group - Moves a cluster group to another node of the cluster.
Configuration	The log records when a user changes a configuration parameter from the Spotlight Client.
Error Log	The log records when a user archives the current error log file and opens a new log file from the Spotlight Client. That is command Cycle Error log.

Table 11: Log of user actions - on monitored Windows Server

Monitor | Windows Drilldowns	
Processes	The log records when a user: • Terminates a process from the Spotlight Client. • Changes the running state (start, stop, pause, resume) of a service or device from the Spotlight Client.

View data and configure Spotlight

Table 12: View data and configure Spotlight

Component	Description
Spotlight Client	The Spotlight Client is required to configure Spotlight and access Reporting and Trending data. The Spotlight Client is a comprehensive viewer to Spotlight data. The Spotlight Client is installed on a Windows server and connects to Spotlight Diagnostic Server on the Windows network.
Spotlight web site	Log in to the Spotlight web site with your Spotlight Cloud (Spotlight Essentials) credentials. Monitor your Spotlight connections, acknowledge and snooze alarms. View health performance analytics. Data is uploaded from Spotlight Diagnostic Server to the Spotlight Cloud over a secure Internet connection.
Spotlight Mobile	Monitor your Spotlight connections on your mobile device. Acknowledge and snooze Spotlight alarms on your mobile device. Data is uploaded from the Spotlight Diagnostic Server to Spotlight Cloud to Spotlight Mobile. A Spotlight Cloud (Spotlight Essentials) account is required to view data on a mobile device.

Spotlight Client

The Spotlight Client is a comprehensive viewer to Spotlight data. The Spotlight Client is required to configure Spotlight and access Reporting and Trending data.

Installation

The Spotlight Client is installed on a Windows server. For specifications see the *Spotlight on SQL Server Enterprise Release Notes*.

The Spotlight Client is installed by the Spotlight installer. For more information, see Install on page 9. The Spotlight Client can be installed on the same Windows server as the Spotlight Diagnostic Server but does not have to be.

Deployment

The Spotlight Client connects to a single Spotlight Diagnostic Server or a federation of Spotlight Diagnostic Server.

Spotlight Diagnostic Server	Address the Spotlight Client to a Spotlight Diagnostic Server. In a federation of Spotlight Diagnostic Server, select any Spotlight Diagnostic Server in the federation.
Spotlight Cloud	Use the Spotlight Client to Configure uploading to Spotlight Cloud. In a federation of Spotlight Diagnostic Server each Spotlight Diagnostic Server is independently configured for Spotlight Cloud.
Playback Database	Use the Spotlight Client to configure the Playback Database. In a federation of Spotlight Diagnostic Server each Spotlight Diagnostic Server connects to its own Playback Database.
Spotlight Statistics Repository	Use the Spotlight Client to enable and configure the Spotlight Statistics Repository and generate reports. In a federation of Spotlight Diagnostic Server each Spotlight Statistics Repository is independently configured in relation to the Spotlight Diagnostic Server.
Monitored connections in the deployment	Use the Spotlight Client to manage the connections monitored by Spotlight.

Troubleshooting

All data to / from the Spotlight Client passes through the Spotlight Diagnostic Server. Verify the Spotlight Client can connect to the Spotlight Diagnostic Server.

Permissions for the Spotlight Client	The Windows credentials used to run the Spotlight Client grant required permissions for the Spotlight Client to access the Spotlight Diagnostic Server, to configure the Spotlight Diagnostic Server, to acknowledge and snooze alarms, and execute actions on monitored systems like kill and pause. If the Spotlight Client is in a different Windows domain to the domain that the Spotlight Diagnostic Server is in, the domain that the Spotlight Diagnostic Server is in must trust the domain that the Spotlight Client users are in.

Network ports	Spotlight's ability to function, to collect and display data, may depend on account permissions granted over the network and specific open network ports.
Verify Internet Options on the Spotlight Client	The Spotlight Client connects to the Spotlight Diagnostic Server via Internet port 40403. If you have customized Internet Options on the Spotlight Client, verify that your customized configurations do not conflict with Spotlight. See the online help for more information.
Spotlight Version	Ensure the Spotlight Client and Spotlight Diagnostic Server come from the same version of Spotlight. When upgrading Spotlight on SQL Server you must upgrade both the Spotlight client and Spotlight Diagnostic Server.

Permissions for the Spotlight Client

The Windows credentials used to run the Spotlight Client grant required permissions for the Spotlight Client to access the Spotlight Diagnostic Server, to configure the Spotlight Diagnostic Server, to acknowledge and snooze alarms, and execute actions on monitored systems like kill and pause.

The Windows credentials used to run the Spotlight Client must be a member of at least one of the following groups to access the Spotlight Diagnostic Server. The Spotlight Diagnostics User groups are created on install of the Spotlight Diagnostic Server. The Spotlight diagnostic user groups are as follows.

- Administrator - Spotlight Diagnostic Administrators
- User - Spotlight Diagnostic Users
- Read-only - Spotlight Diagnostic Read-Only

The following tables document the permissions granted to each level of membership. For membership information and to increase your level of membership, see Spotlight diagnostic user groups.

Table 13: Permission to configure Spotlight

Configure Ribbon Tab		Administrator	User	Read-only
Connections	Add/Delete connection profiles	Yes	Yes	No
	Add/Replace/Delete tags	Yes	Yes	No
	Enable/Disable monitoring connections	Yes	Yes	No
Alarms		Yes	Yes	No
Alarm Actions	Alarm Action Editor	Yes	Yes	No
	Run a program when a threshold is reached	Yes	No	No
Scheduling		Yes	Yes	No
Planned Outage	Add, edit and remove planned outagaes	Yes	No	No
SQL Analysis		Yes	Yes	No
SQL Server		Yes	No	No

Configure Ribbon Tab		Administrator	User	Read-only
Response Time				
Custom Counters		Yes	Yes	No
Error Log Entries		Yes	Yes	No
Monitored Files		Yes	Yes	No
Spotlight	Change Display	Yes	Yes	Yes
	Troubleshoot Spotlight	Yes	Yes	Yes
Diagnostic Server	Select a Diagnostic Server	Yes	Yes	Yes
	Configure the database maintenance schedule	Yes	Yes	No
	Configure PagerDuty	Yes	Yes	No
	Configure the auto-update facility	Yes	Yes	No
	Configure the Diagnostic Server's mail server	Yes	Yes	No
	Configure the Playback Database	Yes	Yes	No
	Configure the SNMP Trap	Yes	Yes	No
	Configure the Spotlight Statistics Repository	Yes	Yes	No
	Configure the use of Extended Events	Yes	Yes	No
	Federate Diagnostic Servers	Yes	Yes	No
Spotlight Cloud	Configure uploading to Spotlight Cloud	Yes	Yes	No
User Experience		Yes	Yes	No
Configuration Templates	Apply Configuration To…	Yes	Yes	No
	Save as Template	Yes	Yes	No
	Delete Template	Yes	Yes	No
	Rename Template	Yes	Yes	No

Table 14: Permission to acknowledge, snooze and ignore alarms from the Spotlight Client

Monitor | Alarms | Action	Administrator	User	Read-only
Acknowledge	Yes	Yes	No
Snooze Alarm	Yes	Yes	No
Ignore Alarm	Yes	Yes	No

Table 15: Permission to execute tasks on a monitored SQL Server from the Spotlight Client

Monitor | SQL Server Drilldowns		Administrator	User	Read-only
SQL Activity	Sessions | Kill Session	Yes	No	No
Databases	Indexes | Update Statistics	Yes	No	No
Support Services	SQL Agent Jobs | Start Job	Yes	No	No
	Service Status | Start / Stop Service	Yes	No	No
	Cluster Services | Take Offline Cluster Services | Bring Online Cluster Services | Move Group	Yes	No	No
Configuration	Change parameter	Yes	No	No
Error Log	Cycle Error log	Yes	No	No

Table 16: Permission to execute tasks on a monitored Windows Server from the Spotlight Client

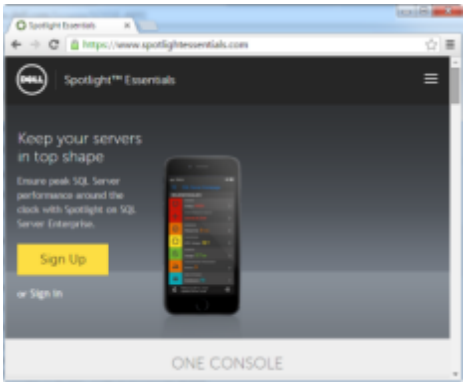
Monitor | Windows Drilldowns		Administrator	User	Read-only
Processes	Processes | Terminate	Yes	No	No
	Services | Start	Yes	No	No
	Services | Stop	Yes	No	No
	Services | Pause	Yes	No	No
	Services | Resume	Yes	No	No

Spotlight web site

Monitor Spotlight connections from the Spotlight web site.

Monitoring features include a heat map, an alarms list, alarm details and the ability to snooze and acknowledge alarms.

Sign in with Spotlight Cloud credentials to www.spotlightessentials.com



Configuration

The Spotlight Diagnostic Server must be configured to allow you to monitor Spotlight connections from the Spotlight web site.

1. Create a Spotlight Cloud (Spotlight Essentials) account if you do not already have one. Do this at www.spotlightessentials.com.
2. Use a Spotlight Client to Configure uploading to Spotlight Cloud.

TIP: In a corporate enterprise your Spotlight Cloud (Spotlight Essentials) account may receive a request to join an organization. In an organization, performance analysis data is uploaded to the organization and is available to all members of the organization.

Deployment

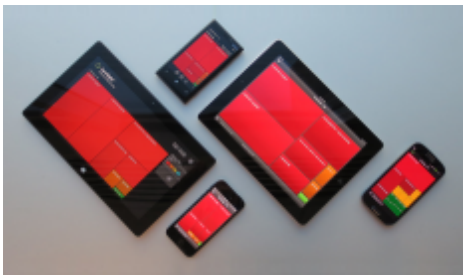
Spotlight Diagnostic Server	Data is uploaded from the Spotlight Diagnostic Server to the Spotlight Cloud. Ensure the Spotlight Diagnostic Server has access to the Internet. For more information, see Spotlight services requiring Internet access on page 16.
Playback Database	Use a Spotlight Client to configure the Playback Database for the Spotlight Diagnostic Server. The Spotlight web site does not have the facility to configure the Playback Database.
Spotlight Statistics Repository	Use a Spotlight Client to access the Spotlight Statistics Repository. The Spotlight web site does not have access to the Spotlight Statistics Repository.
Monitored connections in the deployment	Use a Spotlight Client to manage the connections monitored by the Spotlight Diagnostic Server. The Spotlight web site does not have the facility to manage Spotlight connections.

Spotlight Mobile

Monitor Spotlight connections on a mobile device.

Monitoring features include a heat map, alarms list and alarm details and the ability to snooze and acknowledge alarms.

The Spotlight Mobile app is available for native Windows 8, Windows 8 Phone, iPad, iPhone and android app. For more information see www.spotlightessentials.com.



Configuration

1. Create a Spotlight Cloud (Spotlight Essentials) account if you do not already have one. Do this at www.spotlightessentials.com.
2. Use a Spotlight Client to Configure uploading to Spotlight Cloud.
3. Download and Install Spotlight Mobile from www.spotlightessentials.com.
4. Sign in to Spotlight Mobile with your Spotlight Cloud account. If you have many Spotlight Cloud accounts then each can be added to Spotlight Mobile.
5. You may be given the opportunity to decline to receive push notifications from Spotlight on this mobile device. For information on push notifications, see the online help. For information on the receipt of these push notifications, refer to the *Spotlight Mobile User Guide*.

Deployment

Spotlight Diagnostic Server	Data is uploaded from the Spotlight Diagnostic Server to Spotlight Cloud to Spotlight Mobile. Ensure the Spotlight Diagnostic Server has access to the Internet. For more information, see Spotlight services requiring Internet access on page 16.
Playback Database	Use a Spotlight Client to configure the Playback Database for the Spotlight Diagnostic Server. Spotlight Mobile cannot be used to configure the Playback Database.
Spotlight Statistics Repository	Use a Spotlight Client to access the Spotlight Statistics Repository. Spotlight Mobile has no access to the Spotlight Statistics Repository.
Monitored connections in the deployment	Use a Spotlight Client to manage the connections monitored by the Spotlight Diagnostic Server. Spotlight Mobile cannot be used to manage Spotlight connections.

Monitored connections in the deployment

Table 17: Spotlight on SQL Server is able to monitor the following connections

Connection type	Requirements
SQL Server	Spotlight can monitor SQL Server instances of the following versions: • SQL Server 2016 (32-bit and 64-bit) • SQL Server 2014 (32-bit and 64-bit) • SQL Server 2012 (32-bit and 64-bit) • SQL Server 2008 R2 (32-bit and 64-bit) • SQL Server 2008 (32-bit and 64-bit) • SQL Server 2005 (32-bit and 64-bit) Spotlight on SQL Server also supports MSDE (2000), SQL Express (2005) and SQL Server 2008 Express Edition. Note that use of these versions to host playback or Spotlight Statistics Repository databases is not supported. Spotlight continues to monitor SQL Server 2000 instances Service Pack 3 or later, however no further support (fixes) will be provided. Spotlight cannot monitor earlier versions of SQL Server (version 7.x and earlier). Spotlight supports all SQL Server sort orders, including case-sensitive and binary sort orders. Spotlight cannot monitor SQL Server instances where the instance name contains non-US ASCII characters. On each monitored instance Spotlight requires the network setting "File and Print Sharing" to be enabled. UDP port 1434 should be open. If UDP port 1434 is closed then the port number must be included in the address used to connect Spotlight to the SQL Server instance.
Database Cloud Service	Spotlight can be used to monitor SQL Azure.
Windows Server	Spotlight can monitor the following operating systems: • Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 8 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows Vista (32-bit and 64-bit) • Microsoft Windows Server 2012 R2 (64-bit)

Connection type	Requirements
	• Microsoft Windows Server 2012 (64-bit) • Microsoft Windows Server 2008 R2 (64-bit) • Microsoft Windows Server 2008 (32-bit and 64-bit) • Microsoft Windows Server 2003 (32-bit and 64-bit), however as this operating system is deprecated, WMI issues will no longer be investigated by support. Spotlight requires the network setting "File and Print Sharing" to be enabled and any firewall configured to open TCP port 135.
Virtualization	Spotlight can monitor virtual environments and virtual guest machines in a virtual environment. The following is supported: • VMware ESX infrastructure. VMware vCenter 2.5 (or later). VMware ESX Server 4.0 (or later) • Hyper-V 6.2 and above. The username used to connect to the virtual guest machine must have at least a read-only role. Ensure any firewall is configured to open TCP port 135.

Configure Spotlight

Configure Spotlight from the Spotlight Client **Configure** ribbon.

Icon	Ribbon Select	Description
	Connections	Manage the connections monitored by Spotlight.
	Alarms	Set the thresholds and severities that determine when an alarm is raised. Disable an alarm. Set an alarm to require acknowledgment. Configure keyed alarms. Collect additional diagnostic information on an alarm.
	Alarm Actions	Set actions for Spotlight to take when an alarm is raised. The actions Spotlight can take include running a program and sending an email. Conditions on taking the action can be defined, such as the day of the week, the time of day, the severity of the alarm, the alarm type and the connection type.
	Scheduling	Spotlight collects data according to these set schedules.
	Planned Outage	Enter the scheduled maintenance times for the connections Spotlight monitors so Spotlight does not raise alarms and attempt to collect data during the outage period.
	SQL Analysis	Enable SQL Analysis. Configure the filters used to gather SQL Analysis data.
	SQL Server Response	Set the SQL statement that is used to measure SQL Server response time.

Icon	Ribbon Select	Description
	Time	
	Custom Counters	Create and configure Custom Counters for monitoring connections to SQL Servers and Windows servers.
	Error Log Entries	Request Spotlight raise an alarm when a specified entry is logged in the SQL Server error log.
	Monitored Files	Track the growth of specified files (usually log files) on monitored Windows Servers.
	Spotlight	Customize the Spotlight Client look and feel. Configure operations for the Spotlight Diagnostic Server.
	Diagnostic Server	Configure operations for the Spotlight Diagnostic Server.
	Spotlight Cloud	Enable functionality to monitor Spotlight connections from the Spotlight web site or Spotlight Mobile. Upload performance data for health check analysis.
	User Experience	Influence the design of future versions of Spotlight and help us improve its quality, reliability and performance.

Configure | Connections

Spotlight connects to the SQL Server, Windows Server and other supported connection types in your enterprise. Spotlight monitors the activity and performance of these connections. Use this screen to add and remove connections and configure connection properties.

Open this screen from the Spotlight Client

Click **Configure | Connections**.

Click Add a new connection

Connection type	Description
Analysis Services	SQL Server Analysis Services servers.
Availability Groups	Always On Availability Groups. An availability group is a set of user databases that fail over together.
Hyper-V	Virtual machines on a Hyper-V server.
Replication	SQL Server Replication environments.
SQL Azure	SQL Azure databases.

Connection type	Description
SQL Server	SQL Server instances. (SQL Server | Connection Details)
VMware	Virtual machines on a monitored VMware server.
Windows	Windows Servers including hosts of database connections. (Windows Server | Connection Details)

TIP: Spotlight can add SQL Server instances and Windows Server via discovery or by importing details from a file.

6

Deployment over the Windows network

A Spotlight on SQL Server deployment consists of many components that may be spread over a wide network.

Section	Description
Network ports	Spotlight's ability to function, to collect and display data, may depend on account permissions granted over the network and specific open network ports.
Spotlight diagnostic user groups	Spotlight diagnostic user groups are Windows groups created on install of Spotlight. Spotlight uses these groups to authenticate Spotlight Client access to the Spotlight Diagnostic Server. Membership of these groups affects the Spotlight Client's ability to configure Spotlight and execute actions on monitored Windows Server and SQL Server instances.
Troubleshooting WMI	The Spotlight Diagnostic Server uses WMI queries to retrieve performance counter information from Windows server hosts. Verify WMI is working and returns data properly.
How to limit the number of ports used by WMI	In order to effectively use WMI between fire walled hosts, you can limit the number of ports used by the DCOM subsystem and only open those ports.

Network ports

A Spotlight on SQL Server deployment consists of many components that may be spread over a wide network. Spotlight's ability to function, to collect and display data, may depend on account permissions granted over the network and specific open network ports.

Table 18: Network ports on the Spotlight Diagnostic Server

Network port	Description
TCP	This port is used by the Spotlight client to communicate with the Spotlight Diagnostic Server. This

Network port	Description
3843	port must be open for incoming connections on the Spotlight Diagnostic Server host.
TCP 3166	This port is used by the Spotlight Diagnostic Server to communicate with the Spotlight OOP Collector process on the same host. No external connections are required on this port.
TCP 443	This port is used by the Spotlight Diagnostic Server to communicate with Spotlight Cloud. This port must be open for outgoing connections on the Spotlight Diagnostic Server host when Configure uploading to Spotlight Cloud is enabled.
TCP 40403	This port is used by the Spotlight client to communicate with the Spotlight Diagnostic Server. This port must be open for incoming connections on the Spotlight Diagnostic Server host.

TIP: The Spotlight Diagnostic Server uses WMI queries to retrieve performance counter information from monitored Windows Server and hosts of database connections. Verify TCP port 135 is open on monitored Windows server and hosts of database connections.

SQL Server uses UDP 1434 to locate the SQL Server instance port number. If UDP 1434 is closed then the SQL Server instance port number must be included in the connection string used to connect Spotlight to the SQL Server instance.

Checks to verify ports are open

- Verify a firewall is not blocking port traffic.
- Verify no other service is using the port.
- Verify the port is not configured as an ephemeral port. This issue may arise if you have configured your Windows ports beyond Windows Factory settings or your Windows host is Windows 2008 with Exchange Server 2007. For more information on ephemeral (dynamic) ports, see https://support.microsoft.com/en-us/kb/929851

Spotlight diagnostic user groups

The Spotlight diagnostic user groups are Windows groups created on install of Spotlight. Spotlight uses membership of these groups to authenticate Spotlight Client access to the Spotlight Diagnostic Server. There are three groups. The level of membership affects the user's right to configure Spotlight and execute actions on monitored Windows Server and SQL Server instances.

Group	Description
Spotlight Diagnostic Users	Members of this group are granted user privileges to Spotlight. They can do the usual diagnostic tasks. For example, they can view the home pages, the drilldown pages, browse the playback data and change alarm thresholds.
Spotlight Diagnostic	Members of this group are granted administrator privileges in addition to user privileges. They can kill database sessions and change sensitive configuration items.

Group	Description
Administrators	Note: Administrative changes are logged. The logged entry includes the date, time, connection name, user and client IP address, a brief description of the action, and whether it succeeded or not. The log file is: ..\Agent\log\admin-audit.log in the Spotlight Diagnostic Server installation folder.
Spotlight Diagnostic Read-Only	Members of this group can view the home pages, the drilldown pages, the playback data and alarm cases. They cannot make changes to Spotlight's operation. For example, they cannot alter the state of Spotlight on SQL Server and Monitored Servers.

Add members, increase / decrease your level of membership

Your Network Administrator can add members, increase and decrease your membership as required.

Members can be Windows users or Windows domain groups. Aliases are not supported.

The privileges available to a user correspond to the highest Spotlight diagnostic user group that user is a member of. Spotlight diagnostic read-only users have the fewest privileges, but if a user is also a member of the Spotlight diagnostic administrators group then that user will have administrator privileges.

Any change to a user's role by modifying these Windows groups will not take effect until that user restarts their Spotlight Client and it reconnects to the Spotlight Diagnostic Server. For this reason, it is recommended that the Spotlight Diagnostic Server be restarted if the role changes need to take immediate effect.

Using Spotlight

Your membership of the Spotlight diagnostic user groups impacts your ability to use Spotlight:

Component	Description
Spotlight Client	To connect the Spotlight Client to the Spotlight Diagnostic Server, the Windows user on the Spotlight Client must be a member of at least one Spotlight diagnostic user group. To use the Spotlight Client to configure Spotlight or execute a user action such as kill a session, the Windows user on the Spotlight Client must be a member of a Spotlight diagnostic user group that is allowed to perform that action. For details see Permissions for the Spotlight Client.
SCOM	The Spotlight Management Pack for SCOM is appropriate for organizations that use SCOM (System Center Operations Manager) as their centralized monitoring system and wish to use Spotlight as their tool of choice for SQL Server monitoring. The Windows user(s) running the SCOM Console and SCOM Management Server must be member(s) of the Spotlight Diagnostic Administrators Group for each Spotlight Diagnostic Server. This ensures that a secure connection to the Spotlight Diagnostic Server can be made through Port 40403 and that Spotlight information can be retrieved. For details, see the *Spotlight Management Pack for SCOM User Guide*.

Troubleshooting WMI

Spotlight uses WMI queries to retrieve performance counter information from Windows Server (and SQL Server host). Spotlight needs access to this information before it can connect to Windows Servers (and SQL Server hosts).

WMI Test 1

This test checks that requests are reaching WMI.

Run this test from the Windows server being monitored.

1. Click **Control Panel | Administrative Tools | Event Viewer** to open the Event Viewer.
2. Click **View | Show Analytic and Debug Logs** to select this menu option.
3. Click **Applications and Service Logs**
4. Click to expand **Microsoft | Windows | WMI-Activity**
5. Right click **Trace | Enable Log**.

   Tip: To save log entries, right click **Trace | Save All Events As**.
6. If nothing is displayed then the request never reached WMI. The issue is a security or networking issue.

   If events with error messages are displayed then those events can be investigated. If you encounter WMI errors: For more information, see WMI errors on page 42.

WMI Test 2

This test checks that Microsoft tools can connect to WMI.

Run this test from the Spotlight Diagnostic Server.

1. Login to the Spotlight Diagnostic Server under the account used to run the Spotlight Diagnostic Server.
2. Click **Control Panel | Administrative Tools | Computer Management**.
3. Right click **Computer Management (Local) | Connect to another computer**.
4. Specify the *HOSTNAME* where *HOSTNAME* is the name of machine you want to monitor with Spotlight.
5. Click **Services and Applications**.
6. Right click **WMI Control | Properties** to open the WMI Control Properties dialog.
7. Ensure the **General** tab is open.

If successful, try to monitor *HOSTNAME* with Spotlight again.

WMI Test 3

This test checks that WMI is working and returns data properly.

If you encounter WMI errors: For more information, see WMI errors on page 42.

1. Run this command on the machine you want to monitor. Run this command locally from the command prompt.

   wmic path Win32_PerfRawData_PerfDisk_LogicalDisk get FreeMegabytes

2. Run either of the following commands on the Spotlight Diagnostic Server.

   wmic /node: *HOSTNAME* /user: *DOMAIN\USER* path Win32_OperatingSystem get BuildNumber, Caption, CSDVersion, Version

   or

   wmic /node: *HOSTNAME* /user: *DOMAIN\USER* path Win32_PerfRawData_PerfDisk_LogicalDisk get FreeMegabytes

HOSTNAME	Identify the host computer you want to monitor with Spotlight. Use the fully qualified domain name, machine name or IP-address.
DOMAIN\USER	Valid Windows login credentials.

Additional testing

You may want to consider a WMI Diagnostic Utility provided by Microsoft. It is a utility to help system administrators diagnose and repair problems with the WMI service. See: http://www.microsoft.com/en-us/download/details.aspx?id=7684.

WMI errors

The following is a guide to troubleshooting WMI errors.

Error	Solution
The RPC server is unavailable.	Spotlight on SQL Server is not able to establish a connection with the Windows server to be monitored.
Exception from HRESULT: 0x800706BA	Verify the following: • **The address of the server is entered correctly.** Verify correct host name or IP address. For more information, see Windows Server | Connection Details on page 56. Verify the host is available (not currently shut down). • **The Remote Procedure Call (RPC) service is running on the Windows server to be monitored.** Verity that "Remote Procedure Call (RPC)" is running and set to auto start after restart.

Error	Solution
	• **TCP Port 135 is open to internal traffic on the Spotlight Diagnostic Server and the Windows server to be monitored.** WMI opens an undetermined port in addition to port 135. This can be troublesome in a firewalled environment. Specifying a port range for WMI is recommended for this type of environment. For more information, see How to limit the number of ports used by WMI on page 47. • **The Windows server to be monitored is not blocked by the firewall.** Either configure WMI to use a fixed ports range (For more information, see How to limit the number of ports used by WMI on page 47.) or enable remote administration exception. Follow these steps to enable remote administration exception. On the Windows server to be monitored: 1) Open the Group Policy Object Editor (gpedit.msc), open Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall 2) Open either Domain Profile or Standard Profile, depending on which profile you want to configure. 3) Enable the following exceptions: "Allow Remote Administration Exception" and "Allow File and Printer Sharing Exception". https://msdn.microsoft.com/en-us/library/windows/desktop/aa394603(v=vs.85).aspx • **The "TCP/IP NetBIOS Helper" service is running.** Verity that "TCP/IP NetBIOS Helper" is running and set to auto start after restart. • **The "Windows Management Instrumentation" service is running on the Windows server to be monitored.** Verity that "Windows Management Instrumentation" is running and set to auto start after restart.
Access is denied. Exception from HRESULT: 0x80070005 (E_ACCESSDENIED)	The Windows user specified is unknown to the Windows server or does not have administrator rights. For more information, see How to configure WMI with minimum required user permissions on page 59.
WMI connection time outs	The timeout value defaults to the value DCOM specifies (usually 60 seconds). You can adjust this value via dcomcnfg.exe
WMI query failed: Invalid class. [0x80041010]	The WMI class does not exist on the Windows server being monitored. Solution: Recreate the WMI classes. **Windows Connections** Either of the following will recreate the WMI classes:

Error	Solution
	• Open a command prompt window and run the following command: **wmiadap /f** • Windows Server 2003: Use the Microsoft Extensible Counter List (Exctrlst) utility to enable the following counters: Win32_PerfDisk, Win32_PerfNet, Win32_PerfOS and Win32_PerfProc. http://download.microsoft.com/download/win2000platform/exctrlst/1.00.0.1/nt5/en-us/exctrlst_setup.exe A reboot of the Windows server is required. **SQL Server Analysis Services Connections** Either of the following will recreate the WMI classes: • Open a command prompt window on the server hosting the SQL Server Analysis Services instance. Run the following command: **wmiadap /f** • Unregister and re-register the WMI classes. To do so:

Error	Solution
	1. On the problematic machine with SQL Server Analysis Services installed, find out the SQL installation path. See below for the default installation path. Your installation path may be different. **SQL Server Analysis Services 2014** C:\Program Files\Microsoft SQL Server\MSAS12.MSSQLSERVER\OLAP\bin\Counters **SQL Server Analysis Services 2012** C:\Program Files\Microsoft SQL Server\MSAS11.MSSQLSERVER\OLAP\bin\Counters **SQL Server Analysis Services 2008** C:\Program Files\Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\bin\Counters **SQL Server Analysis Services 2005** C:\Program Files\Microsoft SQL Server\MSSQL.2\OLAP\bin **Note:** You are looking for the folder that contains the following files: **For unamed instances:** MSSQLServerOLAPService perf-MSSQLServerOLAPServicemsmdctr.ini **For named instances:** MSOLAP$*Your_SSAS_NamedInstanceName* perf-*Your_SSAS_NamedInstanceName*msmdctr.ini If you need to check the named instance name, use services.msc. 2. At the command prompt, change folder to the installation path. For example, cd C:\Program Files\Microsoft SQL Server\MSAS10.MSSQLSERVER\OLAP\bin\Counters

Error	Solution
	3. Run the following commands to unload and load counters: unamed instances: **unlodctr MSSQLServerOLAPService** **lodctr perf-MSSQLServerOLAPServicemsmdctr.ini** named instances: **unlodctr MSOLAP$*Your_SSAS_NamedInstanceName*** **lodctr perf-*Your_SSAS_NamedInstanceName*msmdctr.ini** **Tip:** Replace *Your_SSAS_NamedInstanceName* with the SQL Server Analysis Services named instance name. If you need to check the named instance name, use services.msc. 4. Run the following command to parse all the performance libraries on the Windows server and refresh the performance counter classes on the Windows server: **wmiadap /f** 5. Use wbemtest.exe to verify the WMI Classes exist.
WMI query failed: Invalid query. [0x80041017]	The columns returned by the WMI class are incomplete or unexpected. Solution: On the Windows server to be monitored, update the WMI classes by running the following command at the command prompt. **wmiadap.exe /f** See https://msdn.microsoft.com/en-us/library/windows/desktop/aa394603(v=vs.85).aspx for more information.
0x80014064 User credentials cannot be used for local connections	This error occurs when wmic command is executed locally on the target machine and credentials specified
[0x800705af]	The paging file is too small for this operation to complete. For Windows Server 2008 R2 you may find the following link useful: https://blogs.technet.microsoft.com/kevinholman/2010/06/09/wmi-leaks-memory-on-server-2008-r2-monitored-agents/
WMI query failed: Out of memory. [0x80041006]	1. At the command prompt run "wbemtest" 2. Connect to the "root" namespace (not "root\default", just "root") 3. Click **Open Instance**. Specify "__ProviderHostQuotaConfiguration=@" 4. Select **Local Only** for easier readability. You will see the threshold values.

Error	Solution
	5. Increase the MemoryPerHost value to something greater. For example, double it (256 MB) 6. Save Property 7. Save Object 8. Click **Exit**. 9. Restart WMI services.
Invalid verb	The wmic command has attempted to access a WMI class that does not exist. Solution: Check the spelling of parameters on the wmic command.
Invalid Global Switch	The specified host, user or domain name contains special characters like '-' or '/'. Solution: Modify the command by adding quotation marks. wmic /node: 'MonHostFQDN' /user: 'DOMAIN\USER' path Win32_PerfRawData_PerfDisk_LogicalDisk get FreeMegabytes

How to limit the number of ports used by WMI

Windows WMI uses the RPC and DCOM subsystems in Windows. The ports that are used in WMI are auto-negotiated between hosts. In order to effectively use WMI between fire walled hosts, you can limit the number of ports used by the DCOM subsystem and only open those ports.

The following outlines instructions to limit the number of ports that DCOM will use.

Follow these instructions on each monitored host.

1. Open regedt32.exe
2. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc
3. If there is no subkey titled "Internet", create one.
4. Inside the Internet key, create a REG_MULTI_SZ value named "Ports". Each line of the Ports value should specify a range of ports available to DCOM. For this example, add a single line that reads "3000-3100".
5. Add a new REG_SZ value named "PortsInternetAvailable", set it to "Y"
6. Add a new REG_SZ value named "UseInternetPorts", set it to "Y"
7. Open up TCP port 135 to internal traffic. (It may also be necessary to open up UDP 135)
8. Open up the DCOM port range (e.g. 3000-3100) to internal traffic.

See the following link for more information:

http://support.microsoft.com/default.aspx?scid=kb;en-us;154596

To resolve any problems using WMI, see Troubleshooting WMI

Monitoring SQL Servers

The Spotlight Diagnostic Server collects data from the SQL Server instances it connects to and uses WMI queries to retrieve performance counter information from the Windows Server hosts (Monitoring Windows Servers and hosts of database connections). This data is then displayed in real time on a Spotlight Client or other Spotlight viewer (View data and configure Spotlight).

SQL Server | Connection Details

Open this screen from the Spotlight Client

1. Click **Configure | Connections**.

2. Select the **SQL Server** connection type.
3. Click **Add a new connection** or to edit, right click the connection and select **Properties**.

   TIP: Spotlight can add multiple SQL Server instances via discovery or by importing details from a file.

Specify the connection details for this SQL Server instance

Field	Description
Address	The connect string used to link to the SQL Server (that is, the Server Name, Server Instance Name, or IP address). For a Microsoft Cluster Server (MSCS) enter the virtual name of the cluster.
Authentication	The authentication for Spotlight to use to connect to the SQL Server instance. Select **Windows Authentication (using Diagnostic Server credentials)** to use the Windows user configured to run the Spotlight Diagnostic Server. Ensure this account is trusted by the SQL Server. Alternatively, fill in the **Database User** and **Password** fields. Ensure the database user has

Field	Description	
	sufficient account permissions to retrieve performance data from the SQL Server instance and host by WMI. Typically the account will be a member of the sysadmin server role. It could be a SQL Server login (such as 'sa'). If this is not feasible in your environment, see How to grant SQL Server account permissions to a trusted user. The connection will fail if the account permissions are insufficient to allow Spotlight to collect the data it needs.	
Read Only Intent	Select this option if the SQL Server instance hosts a secondary replica of an Availability Group and for this secondary replica ApplicationIntent=ReadOnly. Failure to select this option when required will result in some data not being collected for the secondary replica; this will be most noticeable on the SQL Server | Databases drilldown.	
Use Extended Events	Selected	The Spotlight Diagnostic Server will use Extended Events to collect data from the SQL Server instance. The data is used by: • SQL Server | Workload Analysis Drilldown • SQL Server | Wait Events Drilldown • Deadlock checks: SQL Server | SQL Activity Drilldown, Locks - Deadlocks Alarm. If you select to use Extended Events (following a period of time when the use of Extended Events was deselected) the SQL Server | Workload Analysis Drilldown and SQL Server | Wait Events Drilldown may take a few minutes to repopulate with data.
	Not Selected	The Spotlight Diagnostic Server will use SQL Server Trace to collect data for deadlock checks. The Spotlight Diagnostic Server will NOT collect data for the SQL Server | Workload Analysis Drilldown and SQL Server | Wait Events Drilldown. If you set this value after the connection to the SQL Server is established then the change will not show up immediately on the user interface as the Workload Analysis Drilldown and Wait Events Drilldown will continue to show historical data till no data is available.
	Note that the setting for Use Extended Events can be set collectively for all SQL Server on the Spotlight Diagnostic Server from Configure the use of Extended Events.	
Connection	Select the Windows server hosting the SQL Server.	
	Do not monitor	Select **Do not monitor** if you do not want to monitor the Windows server.
	Cluster (monitor active node)	Select **Cluster (monitor active node)** for a Microsoft Cluster Server (MSCS). Spotlight uses the current host node name to select the operating system connection. Therefore each Windows node in the cluster must be monitored by Spotlight. Verify each Windows node is in the list of Windows server connections.
	Click **Create** to add a Windows server to the list. This opens Windows Server | Connection Details.	

TIP: When done, click **Test** to verify Spotlight can successfully establish a connection with the details provided. If there are connection problems see Monitoring SQL Servers.

Monitoring SQL Servers

Table 19: Connection to the SQL Server

Section	Description
SQL Server | Connection Details	Use a Spotlight Client to create a connection from the Spotlight Diagnostic Server to the SQL Server instance. Ensure the address used for this connection is a valid server name, server instance name or IP address. For a Microsoft Cluster Server (MSCS) use the virtual name of the cluster. Verify UDP port 1434 is open. If UDP port 1434 is closed then the port number must be included in the address used to connect Spotlight to the SQL Server instance.
SQL Server account permissions	Spotlight requires necessary account permissions to connect to the SQL Server instance. The user account must have sufficient account permissions to retrieve performance data from the SQL Server instance and host by WMI. Typically a database account will be a member of the sysadmin server role. It could be a SQL Server login (such as 'sa'). If this is not feasible in your environment, a SQL Server account can be configured with the necessary privileges. See How to grant SQL Server account permissions to a trusted user. The Windows account that runs the Spotlight Diagnostic Server can be used provided that account is trusted by the SQL Server. When using Windows authentication to connect to a SQL Server, and that SQL server is in a different domain to the Spotlight Diagnostic Server, the domain the SQL Server is in must trust the domain the Spotlight Diagnostic Server is in. Note: The Spotlight connection to the SQL Server instance will fail if the user account permissions are insufficient to allow Spotlight to collect the data it needs.
Connection to the Windows host	Verify the SQL Server host is in a domain. Spotlight cannot monitor a SQL Server database when the Windows host is in a workgroup. If the SQL Server is hosted within Microsoft Cluster Server (MSCS) then at SQL Server | Connection Details ensure the Windows Server host is selected as Cluster (monitor active node). Spotlight uses the current host node name to select the operating system connection. Therefore each Windows node in the cluster must be monitored by Spotlight. Verify each Windows node is in the list of Windows server connections. See also Monitoring Windows Servers and hosts of database connections.
Troubleshooting WMI	The Spotlight Diagnostic Server uses WMI queries to retrieve performance counter information from the Windows server host. Verify WMI is working and returns data properly. Verify TCP port 135 is open on the Windows server host.
Network ports	Ensure ports are open as outlined in the Microsoft KBase article that describes SQL Server firewall connectivity issues: http://msdn.microsoft.com/en-us/library/cc646023.aspx.
Microsoft Data Access	If Spotlight cannot connect to the SQL Server instance you may need to upgrade Microsoft Data Access Components (MDAC) on the Spotlight Client host AND the Spotlight

Section	Description
Components (MDAC)	Diagnostic Server host. More information is available from the Microsoft Download Center (search for MDAC).
Troubleshooting	If Spotlight cannot connect to the SQL Server instance then use another tool such as Microsoft's SQL Server Management Studio or **sqlcmd** to connect to the SQL Server instance. Is the issue with Spotlight's ability to connect to the SQL Server instance or with any any/every tool's ability to connect to the SQL Server instance? Check the System Requirements and Known Issues sections of the *Spotlight on SQL Server Release Notes* for further assistance.

Table 20: Collect and display data and user actions

Problem area	Description
Execute user actions on the SQL Server instance from the Spotlight Client	In order to execute actions on the SQL Server instance (like kill a session) from the Spotlight Client, the Windows user running the Spotlight Client must be a member of at least one of the Spotlight diagnostic user groups.
Data display and collection problems - SQL Server connection	Known issues where errors, unknown values or missing values or too many "0" values are reported on the SQL Server home page or its drilldowns.
General troubleshooting	Check the Known Issues section of the *Spotlight on SQL Server Release Notes*.

How to grant SQL Server account permissions to a trusted user

Spotlight connects to the SQL Server instance using the authentication defined by SQL Server | Connection Details. Spotlight requires necessary account permissions to connect to the SQL Server instance. Typically the account will be a member of the sysadmin server role. It could be a SQL Server login (such as 'sa'). It could be the Windows account that runs the Spotlight Diagnostic Server provided that account is trusted by the SQL Server.

In some environments the above may not be feasible. The following instructions are provided for these environments. Run the following SQL script (as sysadmin) to grant the required permissions to user *TrustedUser*. Note the comment lines at the end of the script and un-comment as appropriate for your environment.

Known issues with this script	Description
No data on the SQL Server | Support Services Drilldown | Service Status page	This script does not grant sufficient privileges to view the data on this page.
Error: The SQL Server Agent service status cannot be determined because a registry key cannot be read due to lack of permission.	The script QS_Services.sql only can be executed successfully under login with SQL Server sysadmin rights. If the script QS_Services.sql is executed without a sysadmin account the error (documented to the left) will be raised.

Script to grant permissions to TrustedUser

```
use master
grant ALTER TRACE to TrustedUser
grant VIEW SERVER STATE to TrustedUser
grant VIEW ANY DEFINITION to TrustedUser
USE [master]
GO
CREATE USER [TrustedUser] FOR LOGIN [TrustedUser]
GO
USE [msdb]
GO
CREATE USER [TrustedUser] FOR LOGIN [TrustedUser]
GO
grant VIEW DATABASE STATE to TrustedUser
use msdb
EXECUTE sp_addrolemember
@rolename = 'SQLAgentReaderRole',
@membername = 'TrustedUser'
use msdb
EXECUTE sp_addrolemember
@rolename = 'TargetServersRole',
@membername = 'TrustedUser'

grant select on dbo.log_shipping_monitor_history_detail to TrustedUser
grant select on dbo.log_shipping_monitor_primary to TrustedUser
grant select on dbo.log_shipping_monitor_secondary to TrustedUser
grant select on dbo.log_shipping_primary_databases to TrustedUser
grant select on dbo.log_shipping_secondary_databases to TrustedUser
grant select on dbo.log_shipping_primary_secondaries to TrustedUser
grant select on dbo.log_shipping_primaries to TrustedUser
grant select on dbo.log_shipping_secondary to TrustedUser
grant select on dbo.log_shipping_secondaries to TrustedUser
grant select on dbo.sysjobs to TrustedUser
grant select on dbo.sysalerts to TrustedUser
grant select on dbo.sysjobhistory to TrustedUser
grant execute on dbo.sp_help_jobhistory to TrustedUser
```

```
grant select on msdb.dbo.syssessions to TrustedUser
grant select on msdb.dbo.sysjobactivity to TrustedUser
use master
grant EXECUTE on xp_servicecontrol to TrustedUser
grant EXECUTE on xp_enumerrorlogs to TrustedUser
grant EXECUTE on xp_readerrorlog to TrustedUser
grant EXECUTE on xp_sqlagent_enum_jobs to TrustedUser
grant execute on xp_regread to TrustedUser

declare @dbnumber int
declare @dbname sysname
declare @use nvarchar(4000)
declare @Quest_dblist table (
      row int identity,
      name sysname
)
insert into @Quest_dblist (name)
      select name from master.dbo.sysdatabases;
set @dbnumber = @@rowcount
while @dbnumber > 0
begin
      select @dbname =name from @Quest_dblist where row = @dbnumber
      set @use = N'USE ' + quotename(@dbname)
            + N'CREATE USER [TrustedUser] FOR LOGIN [TrustedUser]';
      exec (@use)
      set @dbnumber = @dbnumber - 1
end
-----un-comment the following line for SQL Server 2008 and above.
--Grant CONTROL SERVER to TrustedUser
-----un-comment the following line for SQL Server 2012 and above.
--Grant ALTER ANY EVENT SESSION to TrustedUser
```

Data display and collection problems - SQL Server connection

Known issues where unknown values or missing values or too many "0" values are shown on the SQL Server home page or its drilldowns.

Data Display	Description
SQL Server | Wait Events Drilldown	<Unknown> entries in the **All Workload | Database** tree and **SQL not available** entries in the **All Workload | Statement** tree may mean: • SQL Server did not add the metric to the event. Perhaps the metric was too difficult to get or the metric was no longer available. • The event was created by a process that does not have that metric. Typically these are internal SQL Server processes.
SQL Server performance counters	When SQL Server performance counters are missing, Spotlight will not be able to collect the data it requires, and will display "0" for many of its components. Most obvious will be the Memory icons on the SQL Server Home Page, which will show 0 MB of memory used by SQL Server. Also, many of the flows on the home page will show no activity, and many drilldowns will show incomplete information.
Errors on the SQL Server | SQL Activity Drilldown | Sessions page	If errors are displayed on the SQL Activity drilldown | Sessions page then install **SQL Server Management Tools** on the Spotlight Diagnostic Server host. The version of SQL Server Management Tools required is dependent on the most current version of SQL Server monitored. When monitoring SQL Server 2012, SQL Server 2012 Management Tools are required.
No data on the SQL Server | Support Services Drilldown | Service Status page	The Spotlight log in to the SQL Server instance (as defined in Configure | Connections | SQL Server) must be a member of the sysadmin server role to view the data on this page.

SQL Server performance counters

Spotlight on SQL Server uses **sys.dm_os_performance_counters** (sysperfinfo for SQL Server 2000) to retrieve data for many of its displays. In some rare cases, this table may not contain information.

When SQL Server performance counters are missing, Spotlight will not be able to collect the data it requires, and will display "0" for many of its components. Most obvious will be the Memory icons on the SQL Server | Home Page, which will show 0 MB of memory used by SQL Server. Also, many of the flows on the home page will show no activity, and many drilldowns will show incomplete information.

Spotlight on SQL Server raises the Missing SQL Performance Counters Alarm shortly after connecting if it detects that the sysperfinfo or sys.dm_os_performance_counters table contains no data.

Verify the sys.dm_os_performance_counters table contains no data

Run the following SQL in the appropriate version of SQL Server Management Studio for SQL Server. If this query returns no records, then your SQL Server performance counters are missing. Spotlight on SQL Server will not be able to operate correctly.

```
select * from sys.dm_os_performance_counters
```

For SQL Server 2000 run the following SQL in Query Analyzer (select * from master..sysperfinfo)

Enable performance counters

Sometimes, for a variety of reasons, the SQL Server Performance Monitor counters will not show up as they should. Often, but not always, this problem can be fixed by following these steps.

1. At the command prompt, type the following:

   ```
   unlodctr.exe MSSQLServer
   ```

2. Then type:

   ```
   lodctr.exe <SQL Server path>\binn\sqlctr.ini
   ```

3. Reboot the server.

More information

Open the SQL Server Knowledge Base at http://msdn.microsoft.com.

Monitoring Windows Servers and hosts of database connections

The Spotlight Diagnostic Server uses WMI queries to retrieve performance counter information from monitored Windows Servers and Windows hosts of database connections. This data is then displayed in real time on a Spotlight Client or other Spotlight viewer (View data and configure Spotlight).

Windows Server | Connection Details

Open this screen from the Spotlight Client

1. Click **Configure | Connections**.

2. Select the **Windows** connection type.
3. Click **Add a new connection** or to edit, right click the connection and select **Properties**.

   TIP: Spotlight can add Windows Server via discovery or by importing details from a file.

Specify the operating system connection details

Field	Description
Address	The IP address, hostname, or URL of the Windows Server. If the Windows Server is in a different domain to the Spotlight Diagnostic Server host then specify the address as a fully qualified address (for example, machine1.domain.company.corp). The connection may work intermittently if the address is not fully qualified. Spotlight can only connect to Windows servers in a domain. Spotlight cannot connect to Windows servers in a workgroup. Spotlight cannot connect to databases hosted on Windows servers in a workgroup.

Field	Description
Authentication	The authentication for Spotlight to use to connect to the Windows server. Select **Use Diagnostic Server credentials** to use the Windows user configured to run the Spotlight Diagnostic Server. You are required to select this option for the Windows Server that hosts the Spotlight Diagnostic Server. If you select this option and the Windows Server is remote from the Spotlight Diagnostic Server then ensure the Windows user running the Spotlight Diagnostic Server can access the Windows Server. (By default the Spotlight Diagnostic Server runs under the "Local System" account, which will not have privileges on a remote Windows Server). If you select this option and the Windows Server is in a different domain from the Spotlight Diagnostic Server then ensure the domain the Windows Server is in trusts the domain of the user running the Spotlight Diagnostic Server. Alternatively, fill in the **User** and **Password** fields. Include the Windows domain in the user name. For example, “domain\johnsmith”, instead of “johnsmith”. The account must have the privileges required to retrieve server information, query the registry, and access WMI and performance monitor objects. An account with administrative rights to the Windows server allows this. Alternatively an account can be configured with the necessary privileges as per How to configure WMI with minimum required user permissions.

Virtualization details

Field	Description
Connection	If this Windows server is hosted by a virtual server then select the name of the virtual server. TIP: Click **Create** to add a virtual server to the list.
VM Name	Select the name of the virtual machine from those hosted by the virtual server.

TIP: When done, click **Test** to verify Spotlight can successfully establish a connection with the details provided. If there are connection problems see Monitoring Windows Servers and hosts of database connections.

Monitoring Windows Servers and hosts of database connections

Table 21: Connection to the Windows Server (SQL Server host)

Section	Description
Windows Server | Connection Details	Use a Spotlight Client to create a connection from the Spotlight Diagnostic Server to the Windows Server (host of the database connection). If the Windows Server is in a different domain to the Spotlight Diagnostic Server host then ensure the address provided is fully qualified (for example, machine1.domain.company.corp). The connection may work intermittently if the address is

Section	Description
	not fully qualified.
Windows Domains	Spotlight can only connect to Windows servers in a domain. Spotlight cannot connect to Windows servers in a workgroup. Spotlight cannot connect to databases hosted on Windows servers in a workgroup.
Windows Account Permissions	Spotlight requires authentication to connect to the Windows server and retrieve performance data. There are two ways to do this at Windows Server | Connection Details: use Diagnostic Server credentials or fill in the user and password fields. When **Use Diagnostic Server credentials** is selected, Spotlight uses the Windows user configured to run the Spotlight Diagnostic Server. Selecting this option is required to connect to the Windows Server that hosts the Spotlight Diagnostic Server. If you select this option and the Windows Server is remote from the Spotlight Diagnostic Server then ensure the Windows user running the Spotlight Diagnostic Server can access the Windows Server. (By default the Spotlight Diagnostic Server runs under the "Local System" account, which will not have privileges on a remote Windows Server). If you select this option and the Windows Server is in a different domain from the Spotlight Diagnostic Server then ensure the domain the Windows Server is in trusts the domain of the user running the Spotlight Diagnostic Server. Alternatively, fill in the User and Password fields. Include the Windows domain in the user name. For example, “domain\johnsmith”, instead of “johnsmith”. The account must have the privileges required to retrieve server information, query the registry, and access WMI and performance monitor objects. An account with administrative rights to the Windows server allows this. Alternatively an account can be configured with the necessary privileges as per How to configure WMI with minimum required user permissions.
Troubleshooting WMI	The Spotlight Diagnostic Server uses WMI queries to retrieve performance counter information from the Windows Server. If there are problems, you may want to verify WMI is working and returns data properly. Verify TCP port 135 is open on the Windows server.

Table 22: Collect and display data and user actions

Section	Description
Execute user actions on the Windows Server from the Spotlight Client	In order to execute actions on the Windows Server (like kill a session) from the Spotlight Client, the Windows user running the Spotlight Client must be a member of at least one of the Spotlight diagnostic user groups.
Data display and collection problems - Windows Server connection	Ensure necessary components are enabled on the Windows Server (SQL Server host) to ensure correct data display and collection.
Troubleshooting	Check the Known Issues section of the *Spotlight on SQL Server Release Notes*.

How to configure WMI with minimum required user permissions

Spotlight requires authentication to connect to the Windows server and retrieve performance data. There are two ways to do this at Windows Server | Connection Details: use Diagnostic Server credentials or fill in the user and password fields. If you choose to fill in the user and password fields, the account must have the privileges required to retrieve server information, query the registry, and access WMI and performance monitor objects. An account with administrative rights to the Windows server allows this.

In some environments it may not be feasible to connect to the Windows server with an account that is a member of the Administrators group. The following instructions are provided for these environments. Note that there are known issues with this procedure as documented below.

1. Setup permission to read data
2. Grant permissions to get information about services
3. Provide access to the Registry keys used by Spotlight
4. Run Windows Component Services
5. Configure WMI permissions

Following are known issues with configuring WMI with minimum required permissions

Known Issue	Description
The OpenSessions collection	The OpenSessions collection sends a list of the open Windows network sessions to your server. The list includes who is connected and from where, how long they have been connected and how many files they have open. The OpenSessions collection is used in: • The Windows Server | Home Page | Network panel | Open Sessions count. • The Network Drilldown | Sessions page. Spotlight does not alarm on this data.
The Physical Disk Drive collection	The Physical Disk Drive collection populates the Disks Drilldown | Disk Summary page. This drilldown contains a list of the physical disks installed on the server. Its data is relatively static as it only changes when disks are added, removed or repartitioned. Inside of this known issue a Generic Failure error will be returned.

1. Setup permission to read data

Note: This is step 1 of the procedure for how to Configure WMI with minimum required user permissions.

Spotlight User is the windows user that will be used in the connection to the Windows server and/or Windows host of the database connection. For more information, see Configure | Connections on page 36.

1. Click **Control Panel | Administrative Tools | Computer Management** to open the Computer Management dialog.

2. Double click **Local Users and Groups | Groups**.
3. Double click **Performance Log Users**. Add the *Spotlight User* to this group. OK.
4. Double click **Performance Monitor Users**. Add the *Spotlight User* to this group. OK.

2. Grant permissions to get information about services

> Note: This is step 2 of the procedure for how to Configure WMI with minimum required user permissions.
>
> *Spotlight User* is the windows user that will be used in the connection to the Windows server and/or Windows host of the database connection. For more information, see Configure | Connections on page 36.

Retrieve the user SID

From the Windows command prompt, type **powershell** and click Enter to open the Powershell.

Run the following command to retrieve the user SID of the *Spotlight User*. Replace *domainName* and *userName* with the domain name and user name for the *Spotlight User* account.

```
[wmi]"win32_useraccount.domain='domainName',name='userName'"
```

Retrieve the current SDDL for the Services Control Manager

From the Windows command prompt, run the following command to retrieve the current SDDL for the Services Control Manager. The SDDL is saved in the file called *file.txt*.

```
sc sdshow scmanager > file.txt
```

The SDDL looks something like this. For more information see Microsoft KB914392.

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:
(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

Modify the SDDL

Copy the section of the SDDL that ends in IU (Interactive Users). This section is one complete bracketed clause ie (A;;CCLCRPRC;;;IU). Paste this clause directly after the clause you copied from.

In the new text, replace *IU* with the user SID of the *Spotlight User*.

The new SDDL looks something like the following:

```
D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU) (A;;CCLCRPRC;;;S-1-5-21-214A909598-1293495619-
13Z157935-75714)(A;;CCLCRPRC;;;SU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA) S:(AU;FA;KA;;;WD)
(AU;OIIOFA;GA;;;WD)
```

Set the security credentials for accessing the Service Control Manager

The sdset command on sc sets the security credentials for accessing the Service Control Manager (scmanager). Note the permissions on scmanager are being replaced. Setting security credentials is not additive. That's why we needed to copy the existing permissions.

```
sc sdset scmanager "D:(A;;CC;;;AU)(A;;CCLCRPRC;;;IU)(A;;CCLCRPRC;;;SU)
(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)(A;;CCLCRPRC;;;S-1-5-21-214A909598-1293495619-
13Z157935-75714)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)"
```

3. Provide access to the Registry keys used by Spotlight

Note: This is step 3 of the procedure for how to Configure WMI with minimum required user permissions.

Spotlight User is the windows user that will be used in the connection to the Windows server and/or Windows host of the database connection. For more information, see Configure | Connections on page 36.

On the Windows server and/or Windows host of the database connection in RegEdit open the following nodes.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
```

On each node

1. Right click and select **Permissions**.
2. Add the *Spotlight User*. OK.
3. Select the *Spotlight User*. Select **Read access**.

4. Run Windows Component Services

Note: This is step 4 of the procedure for how to Configure WMI with minimum required user permissions.

Spotlight User is the windows user that will be used in the connection to the Windows server and/or Windows host of the database connection. For more information, see Configure | Connections on page 36.

From the Windows command prompt, type **dcomcnfg** and click Enter to open the Component Services dialog.

Configure COM security

1. From the Component Services dialog click **Computers | My Computer**.
2. Right click **My Computer** and select **Properties**.
3. From the Properties dialog, click **COM Security**.
4. From Access Permissions, click **Edit Limits**.
    a. Add the *Spotlight User*.
    b. Allow **Remote Access**.
    c. Click OK to close the Access Permission dialog and save changes.

5. From Launch and Activation Permissions, click **Edit Limits**.
    a. Add the *Spotlight User*.
    b. Allow **Remote Launch** and **Remote Activation**.
    c. Click OK to close the Launch and Activation Permission dialog.
6. Click Ok to close the Properties dialog and save changes.

Configure DCOM security

1. From the Component Services dialog double click **Computers | My Computer | DCOM Config | Windows Management and Instrumentation**.
2. Right click **Windows Management and Instrumentation | Properties**.
3. Click **Security | Launch and Activation Permissions | Edit**.
    a. Add the *Spotlight User*.
    b. Allow **Remote Launch** and **Remote Activation**.
    c. Click OK to close the Launch and Activation Permission dialog and save changes.
4. Click OK to close the Windows Management and Instrumentation Properties dialog and save changes.

5. Configure WMI permissions

Note: This is step 5 of the procedure for how to Configure WMI with minimum required user permissions.

Spotlight User is the windows user that will be used in the connection to the Windows server and/or Windows host of the database connection. For more information, see Configure | Connections on page 36.

From the Windows command prompt, type **wmimgmt.msc** and click Enter to open the WmiMgmt dialog.

1. Right click **WMI Control (Local) | Properties**.
2. Click **Security**.
3. Expand the **Root** node. Select **cimv2**.
4. Click the **Security** button to open security settings for WMI on this computer.
5. Click **Advanced** to open the advanced security settings for this WMI namespace.

    Add the *Spotlight User*. Click **Edit**. Allow:

    - Execute Methods
    - Enable Account
    - Remote Enable
    - Read Security

    Ensure these permissions apply to this namespace and all the namespaces under it by selecting **This namespace and subnamespaces** in the **Apply to** drop down box.

    Click OK to save the new permissions.
6. Click OK to close the Advanced Security Settings dialog. Click OK to close the Security for ROOT dialog.

7. Returning to the **Root** node, select **DEFAULT**.
8. Click the **Security** button to open security settings for DEFAULT.
9. Click **Advanced** to open the advanced security settings.

   Add the *Spotlight User*. Click **Edit**. Allow:

   - Execute Methods
   - Enable Account
   - Remote Enable
   - Read Security

   Ensure these permissions apply to this namespace and all the namespaces under it by selecting **This namespace and subnamespaces** in the **Apply to** drop down box.

   Click OK to save the new permissions.
10. Click OK to close all dialogs.

Data display and collection problems - Windows Server connection

Data Display	Description
Windows Server | Home Page | Disks Panel Windows Server Disks Drilldown	If disk counters are disabled on the monitored Windows Server you may notice the following: • The Spotlight home page Disks Panel and Disks Drilldown show no data. • Various I/O charts on the SQL I/O Activity tab and Windows Activities drilldowns, and disk graphs on the Databases drilldown show no data. • Errors executing "LogicalDisk" or "PagingFile" queries. ***To enable disk counters*** 1. Open a command line window on the monitored Windows Server. 2. Type the following at the command prompt: **diskperf -y** 3. Restart the Windows Server.
Windows Server | Network Drilldown	If the Network Drilldown | NBT page is displaying no data, the likely cause is that the appropriate performance counters are not enabled on the monitored Windows server. ***To enable the collection of network data*** • Windows Server 2003: Use the **Exctrlst** utility to ensure the **PerfNet** counters are active on the Windows Server. Download **Exctrlst** from the Microsoft Web site (download). • Verify at least one network device is using NBT (NetBIOS over TCP/IP). To do this, check the properties of all network connections (in particular, **Advanced TCP/IP Settings | WINS**) to ensure that the NetBIOS setting is not disabled.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/company/contact-us.aspx or call +1 949 754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product