



Microsoft®

System Center Operations Manager

Guide to Microsoft System Center Management Pack for SQL Server 2017+ Reporting Services (Native Mode)

Microsoft Corporation

Published: January 2019

The Operations Manager team encourages you to provide any feedback on the management pack by sending it to sqlmpsfeedback@microsoft.com.

Copyright

This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes.

© 2018 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Windows, and Windows Server are trademarks of the Microsoft group of companies.

All other trademarks are the property of their respective owners.

Contents

Changes History.....	5
Get Started.....	5
Supported Configurations.....	6
Management Pack Scope	7
Files in this Management Pack.....	7
Mandatory Configuration	8
Management Pack Purpose	9
Monitoring Scenarios.....	9
Discovery of SQL Server 2017+ Reporting Services Instance.....	9
Discovery of SQL Server 2017+ Reporting Services Deployment	9
Availability of SQL Server 2017+ Reporting Services Components	10
Performance of SQL Server 2017+ Reporting Services Installation.....	11
Configure the Management Pack	12
Best Practice: Create a Management Pack for Customizations	12
How to Import a Management Pack	13
How to Enable Agent Proxy Option	13
How to Configure a Run As Profile	13
Security Configuration	14
Run As Profiles	14
Administration	15
Low-Privilege Environments	15
View Information in the Operations Manager Console.....	17
Version-Independent (Generic) Views and Dashboards	17
Reporting Services Views and Dashboards.....	19
Links	20
Appendix: Management pack Objects and Workflows	21
MSSQL Reporting Services: Deployment.....	21
MSSQL Reporting Services: Deployment Group	23
MSSQL Reporting Services: Deployment Seed.....	23
MSSQL Reporting Services: Deployment Watcher.....	24
MSSQL Reporting Services: Event Log Collection Target	33
MSSQL Reporting Services: Instance (Native Mode)	34
MSSQL Reporting Services: Instance Seed	48
MSSQL Reporting Services: Reporting Services Alerts Scope Group	49
MSSQL: Generic Server Roles Group	49
SQL Server Alerts Scope Group.....	49

Appendix: Run As Profiles.....	49
Appendix: Known Issues and Release Notes	52

Guide to Microsoft System Center Management Pack for SQL Server 2017+ Reporting Services (Native Mode)

This guide is based on version 7.0.12.0 of the Microsoft System Center Management Pack for SQL Server 2017+ Reporting Services (Native Mode).

Changes History

Release Date	Changes
January 2019 (version 7.0.12.0 RTM)	<ul style="list-style-type: none">• MP was prepared for GA release
November 2018 (version 7.0.11.0 CTP)	<ul style="list-style-type: none">• Added support for Power BI Report Server
October 2018 (version 7.0.10.0 RTM)	<ul style="list-style-type: none">• Replaced the Core Library in the delivery with the version 7.0.7.0, that version which is delivered with the most recent RTM version of the management pack for SQL Server 2017+.• Updated the monitoring of Memory Consumption and CPU Usage in order to collect performance data for all subprocesses in addition to the main SSRS service process.• Updated display strings.• Updated Summary dashboards.• Fixed minor issues found in the CTP version.
June 2018 (version 7.0.8.0 CTP)	The original release of this management pack.

Get Started

In this section:

- [Supported Configurations](#)
- [Management Pack Scope](#)

- [Mandatory Configuration](#)

Supported Configurations

This management pack is designed for the following versions of System Center Operations Manager:

- System Center Operations Manager 2012 R2;
- System Center Operations Manager 2016;
- System Center Operations Manager 1801;
- System Center Operations Manager 1807.

A dedicated Operations Manager management group is not required for this management pack.

The following table details the supported configurations for the management pack:

Configuration	Support
SQL Server Reporting Services instance (Native Mode)	<p>64-bit SQL Server 2017+ Reporting Services on 64-bit OS</p> <ul style="list-style-type: none"> • Windows Server 2012 • Windows Server 2016 <p>Verified with build 14.0.600.906.</p>
SQL Server Reporting Services Scale-out deployment	<p>Yes</p> <p>Only SQL Server 2017 and higher is supported. Installation of “Microsoft SQL Server 2017+ on Windows (Discovery)” is required. See Discovery of SQL Server 2017+ Reporting Services Deployment for more details.</p> <p>Verified with version 14.0.3045.24 of SQL Server.</p>
Power BI Report Server	<p>Yes</p> <p>Verified with build 15.0.2.557 (version 1.3.6816.37243).</p>

Clustered installation of SSRS	Not supported by SSRS
Use of Local System account or HealthService SSID as the action account	Supported with some restrictions It is highly recommended to use a domain account for the monitoring. See Run As Profiles for more details.
Agentless monitoring	No
Virtual environment	Yes

Management Pack Scope

The management pack enables the monitoring of the following features:

- SQL Server 2017+ Reporting Services Instance (Native Mode);
- Power BI Report Server Instance;
- Scale-out Deployment of SQL Server 2017+ Reporting Services and Power BI Report Server.

The management pack considers PBIRS as a special kind of SSRS and provides the same monitoring for PBIRS instances as it does for SSRS instances. In this guide, we will use “SSRS” or “Reporting Services” but all this is intended for both SQL Server 2017 Reporting Services and Power BI Report Server.



Note

This management pack does not discover database objects for both SSRS Catalog Database and SSRS Temporary Database. It is recommended to import the management pack for SQL Server 2017+ to enable discovery, monitoring and health rollup for SSRS databases.

Windows Server management packs monitor aspects of the operating system that influence the performance of computers running SQL Server Reporting Services, such as disk capacity, disk performance, memory utilization, network adapter utilization, and processor performance.

Files in this Management Pack

This management pack includes the following files:

File	Description
Microsoft.SqlServer.ReportingServices.Discovery.mpb	Microsoft SQL Server 2017+ Reporting Services (Discovery). This Management Pack discovers Microsoft SQL Server 2017+ Reporting Services (Native Mode) and related objects. The

File	Description
	management pack contains the discovery logic only and requires a separate monitoring management pack to be imported to monitor the discovered objects.
Microsoft.SQLServer.ReportingServices.Monitoring.mpb	Microsoft SQL Server 2017+ Reporting Services (Monitoring). This management pack enables the monitoring of Microsoft SQL Server 2017+ Reporting Services (Monitoring, Native Mode).
Microsoft.SQLServer.ReportingServices.Core.Library.mpb	Microsoft SQL Server 2017+ Reporting Services Core Library. This library contains the basic components required for the monitoring of Microsoft SQL Server 2017+ Reporting Services (Monitoring, Native Mode).
Microsoft.SQLServer.ReportingServices.Core.Views.mpb	Microsoft SQL Server 2017+ Reporting Services Core Library (Views). This management pack defines views for Microsoft SQL Server 2017+ Reporting Services (Native Mode).
Microsoft.SQLServer.Visualization.Library.mpb	Microsoft SQL Server Visualization Library. This library contains basic visual components required for SQL Server dashboards.

Mandatory Configuration

To configure the management pack, complete the following steps:

- Review the section [“Configure the Management Pack.”](#)
- Grant required permissions as described in [“Security Configuration.”](#)
- Enable Agent Proxy option on all agents installed on the servers, which host either an Instance of SQL Server 2017+ Reporting Services or SQL Server instance with respective SSRS Catalog Database hosted. For more information about enabling Agent Proxy option, see [“How to Enable Agent Proxy Option.”](#)
- Import the Management Pack.
- Associate Microsoft SQL Server Run As profiles with accounts that have appropriate permissions. For more information about configuring Run As profiles, see [“How to Configure a Run As Profile.”](#)
- Make sure that TCP/IP protocol is enabled for SQL Server instance hosting the report server database.
- Note that the SQL Server Browser service is mandatory for Reporting Services discovery and monitoring. SQL Server Browser must be installed and turned on

as on the computers with Reporting Services installed, so as on the computers with SQL Server instances installed, which host the report server database.

Management Pack Purpose

In this section:

- [Monitoring Scenarios](#)
- [How Health Rolls Up](#)



Note

For details on the discoveries, rules, monitors, and views contained in this management pack, see the following sections of this guide:

- [Appendix: Management Pack Objects and Workflows](#)

Monitoring Scenarios

Discovery of SQL Server 2017+ Reporting Services Instance and Power BI Report Server.

The management pack automatically discovers instances of both SQL Server 2017+ Reporting Services and Power BI Report Server. To enable this, the management pack implements the following workflow:

1. Management pack reads the registry to detect if the installation of SSRS 2017+ or PBIRS exists on the server. If the installation has been detected, the management pack creates a “Seed” object.
2. If the “Seed” object has been discovered, the management pack reads various data sources (the registry, WMI, SSRS configuration file, etc.) to discover instance properties and a “Deployment Seed” object.



Note

The “Deployment Seed” object is an unhosted object and is managed by SCOM Management Server.



Note

Appropriate permissions are required to access all the necessary data sources. Please review the “[Security Configuration](#)” section of this guide for details.

Discovery of SQL Server 2017+ Reporting Services Deployment

SSRS Deployment includes the following components:

1. One or more instances of SQL Server 2017+ Reporting Services.

2. SSRS Database and SQL Server that hosts it. SSRS Database is a term which describes two databases used by SSRS: SSRS Catalog Database and SSRS Temporary Database.

Pre-installation of version 7.0.7.0 and later of “Microsoft SQL Server 2017+ on Windows (Discovery)” is a prerequisite for the discovery of SSRS Deployment. This MP file is part of the “Microsoft System Center Management Pack for SQL Server 2017+ on Windows” delivery. In the case of absence of “Microsoft SQL Server 2017+ on Windows (Discovery)”, the Management Pack will not discover and therefore monitor availability and performance of the SSRS Deployment. It does not affect the monitoring of SSRS Instance.

The management pack supports different kinds of installation of SQL Server. The SSRS Database may be deployed on:

- A stand-alone instance, either named or default one;
- A cluster instance;
- An availability group.

To find the SQL Server instance that hosts the SSRS Database, the management pack takes the connection string used by an SSRS Instance to connect to the database. The following formats of connection string are supported by the management pack:

- MachineName
- MachineName\InstanceName
- IPAddress
- IPAddress,PortNumber
- (local) and etc.

Deployment discovery runs on a SCOM Management Server and queries SCOM API to get the list of SSRS Instances, as well as the list of databases discovered on different SQL Servers.

Deployment discovery not only creates “Deployment” object but also “Deployment Watcher” object. Both objects are unhosted.

SSRS Scale-out Deployment is a distributed application by its nature; therefore, the Deployment object is managed by Management Server, its purpose is to combine the health of various SSRS components and group respective SCOM objects.

Deployment Watcher is an auxiliary object, and is managed by either an agent installed on the server hosting SSRS Database or an agent hosting one of SSRS Instances from the given deployment. This object is used to collect information about SQL Server 2017+ Reporting Services deployment in its entirety.

Availability of SQL Server 2017+ Reporting Services Components

This management pack introduces a set of monitors, which enable the monitoring of both SSRS Deployments and SSRS Instances. The monitors verify the availability of these components from the following perspectives:

- SSRS Scale-out Deployment:
 - SSRS catalog database is accessible;
 - SSRS temporary database is accessible;
 - There are no broken references to shared data sources;
 - Number of failed report executions (expressed as a percentage of total report executions) is below the threshold;
 - All instances within deployment are discovered.
- SSRS Instance:
 - SSRS catalog database is accessible;
 - SSRS temporary database is accessible;
 - SSRS windows service is started;
 - SSRS web service is accessible;
 - SSRS report manager is accessible;
 - SSRS Instance is not using too much CPU resources;
 - SSRS Instance is not using too much memory resources;
 - There is no memory configuration conflict between SSRS Instance and SQL Server Database Engine (if both components are running on the same server);
 - Other processes allow enough memory resources for the SSRS Instance;
 - A number of failed report executions per minute is below the threshold for the given SSRS Instance.



Note

The management pack does not observe the health of SSRS Catalog Database and SSRS Temporary Database from the perspective of SQL Server Database health. You should install the management pack for SQL Server 2017+ to enable this functionality.



Note

Some monitors are disabled by default. Please review the “[Appendix: Management Pack Objects and Workflows](#)” section of this guide for more details about monitoring workflows implemented in this management pack.

Performance of SQL Server 2017+ Reporting Services Installation

This management pack collects the following performance metrics:

- SSRS Scale-out Deployment:
 - Failed report executions per minute
 - Report executions per minute
 - Number of reports
 - Number of shared data sources

- Number of subscriptions
- On-demand execution failures per minute
- On-demand executions per minute
- Scheduled execution failures per minute
- Scheduled executions per minute
- SSRS Instance:
 - CPU utilization (%)
 - WorkingSetMaximum (GB)
 - WorkingSetMinimum (GB)
 - Memory consumed by other processes (%)
 - Memory consumed by SSRS (GB)
 - Total memory on the Server (GB)
 - Total memory consumed on the server (GB)
 - Failed report executions per minute
 - Report executions per minute



Note

Please review the “[Appendix: Management Pack Objects and Workflows](#)” section of this guide for more details about monitoring workflows implemented in this management pack.

Configure the Management Pack

This section provides guidance on configuring and tuning this management pack.

In this section:

- [Best Practice: Create a Management Pack for Customizations](#)
- [How to Import a Management Pack](#)
- [How to Enable Agent Proxy Option](#)
- [How to Configure a Run As Profile](#)
- [Security Configuration](#)
 - [Run As Profiles](#)
 - [Required Permissions](#)

Best Practice: Create a Management Pack for Customizations

The management pack is sealed so that you cannot change any of the original settings in the management pack. However, you can create customizations, such as overrides or new monitoring objects, and save them to a different management pack. By default, the Operations Manager saves all customizations to the default management pack. As a

best practice, you should create a separate management pack instead for each sealed management pack you want to customize.

Creating a new management pack for storing overrides has the following advantages:

- When you create a management pack for the purpose of storing customized settings for a sealed management pack, it is helpful to base the name of the new management pack on the name of the management pack that it is customizing, such as “Microsoft SQL Server 2017+ Reporting Services Overrides”.
- Creating a new management pack for storing customizations of each sealed management pack makes it easier to export the customizations from a test environment to a production environment. It also makes it easier to delete a management pack, because you must delete any dependencies before you can delete a management pack. If customizations for all management packs are saved in the Default Management Pack and you need to delete a single management pack, you must delete the Default Management Pack first, which also deletes customizations to other management packs.

For more information about management pack customizations and the default management pack, see [Using Management Packs](#) article.

How to Create a New Management Pack for Customizations

1. Open the Operations console, and then click the **Administration** button.
2. Right-click **Management Packs**, and then click **Create New Management Pack**.
3. Enter a name (for example, SQLMP Customizations), and then click **Next**.
4. Click **Create**.

How to Import a Management Pack

For more information about importing a management pack, see [How to Import an Operations Manager Management Pack](#).

How to Enable Agent Proxy Option

To enable **Agent Proxy option**, complete the following steps:

1. Open the Operations Console and click the **Administration** button.
2. In Administrator pane, click **Agent Managed**.
3. Double-click an agent in the list.
4. On the Security tab, select **Allow this agent to act as a proxy and discover managed objects on other computers**.

How to Configure a Run As Profile

To configure a **Run As profile**, complete the following steps:

1. Identify the names of the target computers, where the default action account has insufficient rights to monitor SQL Server 2017+ Reporting Services.
2. For each system, create or use an existing set of credentials that have at least the set of privileges described in the “[Security Configuration](#)” section of this management pack guide.
3. For each set of credentials identified in step 2, make sure a corresponding **Run As Account** exists in the management group. Create a **Run As Account** if necessary.
4. Setup the mappings between the targets and the **Run As Accounts** on the **Run As Accounts** tab of each of the **Run As Profiles**.



Note

Please refer to the “[Run As Profiles](#)” section for the detailed explanation of what Run As profiles are defined in the management pack.



Note

Please refer to the “[Appendix: Run As Profiles](#)” section for the full list of discoveries, rules, and monitors to identify the rules and monitors associated with each **Run As Profile**.

Security Configuration

This section provides guidance on configuring the security for this management pack.

Run As Profiles

When the management pack is imported for the first time, it creates three new Run As profiles:

- Microsoft SQL Server 2017+ Discovery Run As Profile
- Microsoft SQL Server 2017+ Monitoring Run As Profile
- Microsoft SQL Server 2017+ SCOM SDK Run As Profile

By default, all discoveries, monitors, and rules defined in SQL Server 2017+ Reporting Services management pack use accounts defined in “Default Action Account” Run As profile. If the default action account for the given system does not have the necessary permissions to discover or monitor the instance of SQL Server 2017+ Reporting Services, then those systems can be bound to more specific credentials in Microsoft SQL Server Run As profiles.



Note

It is not recommended to use Local System account or HealthService SSID as its special case to monitor SSRS, as some workflows run from the server hosting an SSRS instance and try to reach the SSRS Database usually installed on another server. You

will need to provide the computer accounts of all servers hosting SSRS instances with the required permissions to access the SSRS Database. A domain account is a more preferable option.

Administration

This section describes how to configure required permissions for the management pack. All workflows (discoveries, rules, and monitors) in this management pack are bound to Run As profiles described in the “[Run As Profiles](#)” section. To enable the monitoring, appropriate permissions should be granted to Run As accounts, and these accounts should be bound to respective Run As profiles. Subsections below describe how to grant permissions at Operating System, SQL Server and SQL Server Reporting Services level.



Note

For more information about configuring Run As profiles, see the “[How to Configure a Run As Profile](#)” section of this guide.



Note

Please refer to the “[Appendix: Run As Profiles](#)” section for the full list of discoveries, rules, and monitors to identify the rules and monitors associated with each **Run As Profile**.

Low-Privilege Environments

► Configure Permissions in Active Directory

1. In Active Directory, create three domain users that will be commonly used for low-privilege access to all target SSRS instances and SQL Server DBE instances hosting report database:
 - a. **SSRSMonitoring**
 - b. **SSRSDiscovery**
 - c. **SSRSDK**
2. Create a domain group named **SSRSMPLowPriv** and add the following domain users:
 - a. **SSRSMonitoring**
 - b. **SSRSDiscovery**

► Configure Permissions on the Agent Machine

1. Grant Local Administrator permissions to **SSRSMPLowPriv** group.

► Configure Permissions on the Instance of SQL Server 2017+ Reporting Services

1. Open Internet Explorer and connect to SSRS Report Manager.

2. Click “Site Settings” link in the upper right corner of the page to navigate to “Site Settings” page.
3. Click “Security” menu item on the left side of the “Site Settings” page.
4. Click “New Role Assignment” button.
5. On “New Role Assignment” enter the group name (<Your Domain>**SSRSMPLowPriv**) and check “System Administrator” checkbox.
6. Click the “OK” button to apply changes.

► **Configure Permissions on SQL Server 2017+ Reporting Services Catalog Database**

1. In SQL Server Management Studio, for the instance of SQL Server Database Engine, which hosts SSRS Catalog Database, create a login for “**SSRSMPLowPriv**”.
2. Create an **SSRSMPLowPriv** user in both SSRS Catalog and Temporary databases.
3. Assign db_datareader role for **SSRSMPLowPriv** on both SSRS Catalog and Temporary databases.

► **Configure Permissions on the System Center Operations Manager Management Server**

1. Grant Local Administrator permissions to **SSRSSDK** account.

► **Configure Permissions on the System Center Operations Manager**

1. Open SCOM Console and navigate to “Administration” pane.
2. Select “User Roles” view (located under the “Security” folder).
3. Right-click “Operations Manager Operators” role and click “Properties” in the context menu.
4. In the “General Properties” tab, click “Add” button.
5. Find **SSRSSDK** user and click “OK”.
6. Click the “OK” button to apply changes and close “User Role Properties” dialog.

► **Configure System Center Operations Manager**

1. Import SQL Server Management Pack, if it has not been imported.
2. Create **SSRSMonitoring**, **SSRSDiscovery** and **SSRSSDK** Run As accounts with “Windows” account type. For more information about how to create a Run As account, see [How to Create Run As Account in Operations Manager 2012](#). For more information about various Run As Account types, see [Managing Run As Accounts and Profiles in Operations Manager 2012](#).
3. On System Center Operations Manager console, configure the Run As profiles as follows:
 - a. Set “Microsoft SQL Server 2017+ Discovery Run As Profile” Run As profile to use **SSRSDiscovery** Run As account.

- b. Set “Microsoft SQL Server 2017+ Monitoring Run As Profile” Run As profile to use **SSRSMonitoring** Run As account.
- c. Set “Microsoft SQL Server 2017+ SCOM SDK Run As Profile” Run As profile to use **SSRSSDK** Run As account.



Important

If you have imported the management pack for SQL Server 2017+ (e.g. Microsoft SQL Server 2017+ on Windows (Discovery)), please note that they use the same Run As Profiles. Therefore, you should adjust the Low Privilege configuration for the SQL Server management packs as well.

View Information in the Operations Manager Console

Version-Independent (Generic) Views and Dashboards

This management pack introduces a common folder structure, which will be used by future releases of management packs for different components of SQL Server. The following views and dashboards are version-independent and show information about all versions of SQL Server:



Microsoft SQL Server 2017+



Active Alerts



Computers



SQL Server Roles



Summary



Task Status



Integration Services



SQL Server Database Engines



Active Alerts



All Performance Data



Summary


















Task Status



Always On High Availability



Database Engines

-  Database Engines
-  Databases
-  Filegroups
-  Database Engines on Linux
 -  Database Engines
 -  Databases
 -  Filegroups
 -  Summary
-  Database Engines on Windows
 -  Database Engines
 -  Databases
 -  Filegroups
 -  Summary
-  Memory-Optimized Data
-  SQL Agent




Note

The “Computers” view displays the computers on which the agents are installed and the management pack discovery is running. Note that this view does not display computers configured for agentless monitoring.

“SQL Server Roles” dashboard provides an information about all instances of SQL Server Database Engine, SQL Server Reporting Services, SQL Server Analysis Services and SQL Server Integration Services:

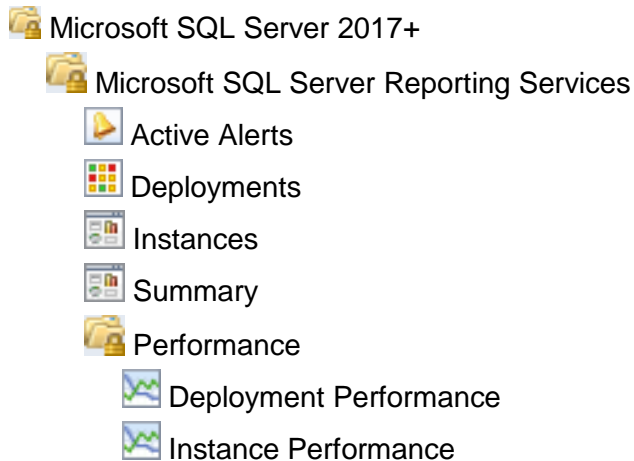
For more information, see the guide to Microsoft SQL Server dashboards.

The management pack for SQL Server 2017+ Reporting Services introduces a comprehensive set of state, performance and alert view, which can be found in the dedicated folder:

-  **Note**

Some views may contain a very long list of objects or metrics. To find a specific object or group of objects, you can use **Scope**, **Search**, and **Find** buttons on the Operations Manager toolbar. For more information, see the [“Finding Data and Objects in the Operations Manager Consoles”](#) article in the Operations Manager Help.

This management pack includes a set of rich dashboards, which provide detailed information about SQL Server 2017+ Reporting Services Instances and Deployments. The structure of the management pack views and folders is as follows:



Links

The following links connect you to information about common tasks that are associated with System Center Management packs:

1. [Management Pack Life Cycle](#)
2. [How to Import an Operations Manager Management Pack](#)
3. [Creating a Management Pack for Overrides](#)
4. [Managing Run As Accounts and Profiles](#)
5. [How to Export an Operations Manager Management Pack](#)
6. [How to Remove an Operations Manager Management Pack](#)

With questions about the Operations Manager and management packs, refer to [System Center Operations Manager community forum](#) (<http://go.microsoft.com/fwlink/?LinkID=179635>).

Important

All information and content on non-Microsoft sites is provided by the owner or the users of the website. Microsoft makes no warranties, express, implied, or statutory, as to the information at this website.

Appendix: Management pack Objects and Workflows

MSSQL Reporting Services: Deployment

Reporting Services (native mode) support a scale-out deployment model that allows running multiple report server instances that share a single report server database. Scale-out deployments are used to increase the scalability of report servers to handle more concurrent users and larger report execution loads. It can also be used to dedicate specific servers to process interactive or scheduled reports.

MSSQL Reporting Services: Deployment - Discoveries

MSSQL Reporting Services: Native Mode Deployment Discovery

This rule discovers all instances of MSSQL Reporting Services Native Mode Deployments.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	14400
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Deployment - Unit monitors

All deployment instances are discovered

The monitor raises an alert if not all SSRS Instances are discovered for the given SSRS Deployment.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True

Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	604800
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold for count of unmatched instances	The monitor will create an alert if the count of unmatched instances is more or equal to the specified value.	1
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Deployment - Dependency (rollup) monitors

Database Security

Rolls up all Database security monitors to the Reporting Services Deployment.

Instances Configuration

Rolls up all Reporting Services Instances configuration monitors to the Reporting Services Deployment.

Instances Security

Rolls up all Reporting Services Instances security monitors to the Reporting Services Deployment.

Deployment Watcher Security

Rolls up all Reporting Services Deployment Watcher security monitors to the Reporting Services Deployment.

Instances Performance

Rolls up all Reporting Services Instances performance monitors to the Reporting Services Deployment.

Instances Availability

Rolls up all Reporting Services Instances availability monitors to the Reporting Services Deployment.

Deployment Watcher Configuration

Rolls up all Reporting Services Deployment Watcher configuration monitors to the Reporting Services Deployment.

Database Configuration

Rolls up all Database configuration monitors to the Reporting Services Deployment.

Deployment Watcher Availability

Rolls up all Reporting Services Deployment Watcher availability monitors to the Reporting Services Deployment.

Database Availability

Rolls up all Database availability monitors to the Reporting Services Deployment.

Deployment Watcher Performance

Rolls up all Reporting Services Deployment Watcher performance monitors to the Reporting Services Deployment.

Database Performance

Rolls up all Database performance monitors to the Reporting Services Deployment.

MSSQL Reporting Services: Deployment Group

This object discovery populates the Local Deployment group to contain all Deployment objects.

MSSQL Reporting Services: Deployment Group - Discoveries

MSSQL Reporting Services: Deployment Group Discovery

This object discovery populates Deployment Group to contain all Deployment objects.

MSSQL Reporting Services: Deployment Seed

It is a seed for Microsoft SQL Server 2017+ Reporting Services (Native Mode) Deployment installation. This object indicates that Deployment exists within the managed environment. This object is unhosted and managed by SCOM Management Servers.

MSSQL Reporting Services: Deployment Seed - Discoveries

MSSQL Reporting Services: Deployment Seed Discovery

This rule discovers Deployment Seed of Microsoft SQL Server 2017+ Reporting Services (Native Mode).

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	14400
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Deployment Watcher

Deployment Watcher is a hidden object, which is used as a target to run monitoring workflows for Deployment object. Deployment Watcher is an unhosted object. The server hosting SSRS Catalog Database is used to manage this object. If the server hosting the database has no agent installed, then one of SSRS servers will take responsibility of running the respective workflows.

MSSQL Reporting Services: Deployment Watcher - Discoveries

MSSQL Reporting Services: Native Mode Deployment Discovery

This rule discovers all instances of MSSQL Reporting Services Native Mode Deployments.

Name	Description	Default value
------	-------------	---------------

Enabled	Enables or disables the workflow.	Yes
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	14400
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Deployment Watcher - Unit monitors

Database accessible

The monitor changes its state and raises an alert if the deployment watcher fails to connect to Reporting Services Database.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

Misconfigured data sources

The monitor alerts if misconfigured data sources are detected.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	604800
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold	The monitor will change state and register an alert if the number of misconfigured data sources is higher than the threshold.	0
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

Number of failed report executions

The monitor alerts if the number of failed report executions expressed as a percentage of total number of report executions is higher than the threshold. The monitor will raise an alert and change its state only when several consecutive checks have failed.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True

Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	300
Number of samples	Indicates, how many times a measured value should breach a threshold before the state is changed.	6
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold	The monitor alerts if the number of failed report executions expressed as a percentage of total number of report executions is higher than the threshold.	50
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

Temporary database accessible

The monitor raises an alert if the deployment watcher fails to connect to Reporting Services Temporary Database.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	

Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Deployment Watcher - Rules (non-alerting)

MSSQL Reporting Services: Report executions per minute (Deployment)

The rule collects the total number of report executions per minute for entire Deployment of SQL Server Reporting Services. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Number of reports

The rule collects the number of reports deployed to SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Number of subscriptions

The rule collects the number of subscriptions configured for SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15
---	--	----

MSSQL Reporting Services: Number of shared data sources

The rule collects the number of shared data sources deployed to SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Scheduled execution failures per minute

The rule collects the number of scheduled execution failures per minute for entire SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No

Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Scheduled executions per minute

The rule collects the number of scheduled executions per minute for entire SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Failed report executions per minute (Deployment)

The rule collects the number of failed report executions per minute for entire Deployment of SQL Server Reporting Services.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: On-demand executions per minute

The rule collects the number of on-demand executions per minute for entire SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	

Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: On-demand execution failures per minute

The rule collects the number of on-demand execution failures per minute for entire SSRS Deployment. The rule queries SSRS Catalog database to get the information.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Event Log Collection Target

This object is used to collect module errors from event logs of computers that have Reporting Services components.

MSSQL Reporting Services: Event Log Collection Target - Discoveries

MSSQL Reporting Services: Event Log Collection Target Management Server Discovery

This discovery rule discovers an event log collection target for a Microsoft SQL Server Reporting Services. This object is used to collect module errors from event logs of management server computers.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	14400
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	

MSSQL Reporting Services: Event Log Collection Target - Rules (alerting)

An error occurred during execution of a SSRS MP managed module

The rule oversees the Event Log and watches for error and warning events submitted by SQL Server Reporting Services management pack. If one of the workflows (discovery, rule or monitor) fails, an event is logged, and a critical alert is reported.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	Yes
Priority	Defines Alert Priority.	2
Severity	Defines Alert Severity.	2

MSSQL Reporting Services: Instance (Native Mode)

This object describes the generic instance of a native mode installation of Microsoft SQL Server 2017+ Reporting Services.

MSSQL Reporting Services: Instance (Native Mode) - Discoveries

MSSQL Reporting Services: Instance Discovery (Native Mode)

This rule discovers all instances of Microsoft SQL Server 2017+ Reporting Services (Native Mode).

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	14400
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Instance (Native Mode) - Unit monitors

Report manager accessible

The monitor raises an alert if monitoring workflow cannot connect to SSRS web service.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True
Ignored status codes checkup	This parameter allows checking if responses from the web services with admittedly invalid status codes should be passed as valid ones. You can set a list of valid codes divided by semicolons.	
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	300
Number of samples	Indicates, how many times a measured value should	6

	breach a threshold before the state is changed.	
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

Memory consumed by SSRS Instance

The monitor alerts if the memory usage by the SSRS process is close to the limit defined by WorkingSetMaximum setting.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True
Critical threshold	The monitor will change its state to critical if the observed value exceeds the critical threshold.	90
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Warning threshold	The monitor will change its state to warning if the observed value is between warning and critical thresholds.	80

Failed Report Executions

The monitor checks if the number of failed report executions per minute does not exceed the threshold expressed as an absolute value. The monitor will raise an alert and change its state only when several consecutive checks have failed. Note: This monitor is disabled by default. Please use overrides to enable it when necessary.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	300
Number of samples	Indicates, how many times a measured value should breach a threshold before the state is changed.	6
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold	The monitor checks if the number of failed report executions per minute doesn't exceed the threshold expressed as an absolute value.	100
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

Windows service state

The monitor alerts if SSRS Windows service is not in running state for a longer period than the threshold.

Name	Description	Default value
------	-------------	---------------

Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True
Alert, only if service startup type is automatic	This may be set to 'true' or 'false' only. The workflow will not consider the current startup type setting of the service if this parameter is set to 'false'. The default is 'true'.	true
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	60
Number of samples	Indicates, how many times a measured value should breach a threshold before the state is changed.	15
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

Database accessible

The monitor raises an alert if the monitoring workflow cannot access the Reporting Services Database. Note: This monitor is disabled by default. Please use overrides to enable it when necessary.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900

Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	200

Configuration conflict with SQL Server

The monitor alerts if there is a SQL Server process running on the server, and WorkingSetMaximum setting for the SSRS Instance does not allow enough memory for the SQL server process. Note: This monitor is disabled by default. Please use overrides to enable it when necessary.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	604800
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold	The monitor will change state and register an alert if SSRS and SQL Server are running on the same box, and WorkingSetMaximum exceeds the threshold.	40
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

Memory consumed by others

The monitor alerts if the memory consumed by processes other than SSRS does not allow SSRS to allocate the amount of memory prescribed by WorkingSetMinimum setting. The monitor uses the following formula to determine the state:

$$(\{\text{WorkingSetMinimum}\} + \{\text{Memory Consumed By Others}\}) * 100 / \{\text{Total Memory}\} < \{\text{Threshold (\%)}\}$$

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Number of samples	Health State changes if the number of threshold breaches is greater than or equal to the Minimum Number of Breaches.	4
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold	The monitor alerts if the sum of memory consumed by processes other than SSRS and value of WorkingSetMinimum expressed as a percentage of total server memory exceeds the threshold.	100
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

CPU utilization (%)

The monitor alerts if the CPU usage by the SSRS process is close to 100%.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes

Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	300
Number of samples	Indicates, how many times a measured value should breach a threshold before the state is changed.	6
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Threshold	The monitor alerts if the CPU utilization caused by the SSRS process is higher than the threshold.	95
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

Temporary database accessible

The monitor raises an alert if the instance failed to connect to Reporting Services Temporary Database. Note: This monitor is disabled by default. Please use overrides to enable it when necessary.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run	300

	before being closed and marked as failed.	
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	200

Instance configuration state

The monitor raises an alert if SSRS instance has certain configuration problems.

Name	Description	Default value
Enabled	Enables or disables the workflow.	No
Generate Alerts	Defines whether the workflow generates an Alert.	True
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

Web service accessible

The monitor raises an alert if monitoring workflow cannot connect to SSRS web service.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	True

Ignored status codes checkup	This parameter allows checking if responses from the web services with admittedly invalid status codes should be passed as valid ones. You can set a list of valid codes divided by semicolons.	
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	300
Number of samples	Indicates, how many times a measured value should breach a threshold before the state is changed.	6
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Instance (Native Mode) - Rules (non-alerting)

MSSQL Reporting Services: CPU utilization (%)

The rule collects CPU usage by SSRS Instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	300
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	

Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
-------------------	---	-----

MSSQL Reporting Services: Total memory on the Server (GB)

The rule collects the total size of memory in gigabytes on the computer, where the instance is located.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Memory consumed by other processes (%)

The rule collects memory usage by other processes on the instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	

Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
-------------------	---	-----

MSSQL Reporting Services: WorkingSetMinimum (GB)

The rule collects the value of WorkingSetMinimum setting in gigabytes for the given SSRS Instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Total memory consumed on the server (GB)

The rule collects the total size of memory used in gigabytes on the computer, where the instance is located.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900

Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Failed report executions per minute

The rule collects the number of report execution failures per minute for the given SSRS Instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Report executions per minute

The rule collects the number of report executions per minute for the given SSRS Instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes

Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300
Timeout for database connection (seconds)	The workflow will fail and register an event if it cannot access the database during the specified period.	15

MSSQL Reporting Services: Memory consumed by SSRS (GB)

The rule collects the amount of memory consumed by the given SSRS Instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: WorkingSetMaximum (GB)

The rule collects configuration for WorkingSetMaximum setting in gigabytes for instance.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Generate Alerts	Defines whether the workflow generates an Alert.	No
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	900
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run before being closed and marked as failed.	300

MSSQL Reporting Services: Instance Seed

It is a seed for Microsoft SQL Server 2017+ Reporting Services (Native Mode) installation. This object indicates that the particular server computer contains Microsoft SQL Server 2017+ Reporting Services (Native Mode) installation.

MSSQL Reporting Services: Instance Seed - Discoveries

MSSQL Reporting Services: Instance Seed Discovery (Native Mode)

This rule discovers a seed for Reporting Services installation. This object indicates that the particular server computer contains a Microsoft SQL Server 2017+ Reporting Services (Native Mode) installation.

Name	Description	Default value
Enabled	Enables or disables the workflow.	Yes
Interval (seconds)	The recurring interval of time in seconds in which to run the workflow.	14400
Synchronization Time	The synchronization time specified by using a 24-hour format. May be omitted.	
Timeout (seconds)	Specifies the time the workflow is allowed to run	300

	before being closed and marked as failed.	
--	---	--

MSSQL Reporting Services: Reporting Services Alerts Scope Group

SQL Server Reporting Services Alerts Scope Group contains SQL Server Reporting Services objects, which can throw alerts.

MSSQL Reporting Services: Reporting Services Alerts Scope Group - Discoveries

[MSSQL Reporting Services: Reporting Services Alerts Scope Group Discovery](#)

This object discovery populates the Reporting Services Alerts Scope Group to contain all SQL Server Reporting Services Roles.

MSSQL: Generic Server Roles Group

Generic Server Roles Group contains all SQL Server root objects such as Database Engine instance.

MSSQL: Generic Server Roles Group - Discoveries

[MSSQL Reporting Services: Server Roles Group Discovery](#)

This object discovery populates the Server Roles group to contain all SQL Server Roles.

SQL Server Alerts Scope Group

SQL Server Alerts Scope Group contains SQL Server objects, which can throw alerts.

SQL Server Alerts Scope Group - Discoveries

[MSSQL Reporting Services: SQL Alerts Scope Group Discovery](#)

This object discovery populates the SQL Alerts Scope Group to contain all SQL Server Reporting Services Roles.

Appendix: Run As Profiles

Run As Profile	Workflow Type	Workflow
Microsoft SQL Server 2017+ Discovery Run As Profile	Discovery	MSSQL Reporting Services: Deployment Seed Discovery
	Discovery	Microsoft SQL Server 2017+ Reporting Services (Discovery)
Microsoft SQL Server 2017+ SCOM SDK Run As Profile	Discovery	MSSQL Reporting Services: Native Mode Deployment Discovery
	Monitor	All deployment instances are discovered
Microsoft SQL Server 2017+ Monitoring Run As Profile	Monitor	Configuration conflict with SQL Server
	Monitor	CPU utilization (%)
	Monitor	Database accessible
	Monitor	Database accessible
	Monitor	Instance configuration state
	Monitor	Memory consumed by others
	Monitor	Memory consumed by SSRS Instance
	Monitor	Misconfigured data sources
	Monitor	Number of failed report executions
	Monitor	Number of failed report executions
	Monitor	Report manager accessible
	Monitor	Temporary database accessible
	Monitor	Temporary database accessible
	Monitor	Web service accessible
	Monitor	Windows service state
	Rule	MSSQL Reporting Services: CPU utilization (%)
	Rule	MSSQL Reporting Services: Failed report executions per minute
	Rule	MSSQL Reporting Services: Failed report executions per minute (Deployment)
	Rule	MSSQL Reporting Services: Memory consumed by other processes (%)

Run As Profile	Workflow Type	Workflow
	Rule	MSSQL Reporting Services: Memory consumed by SSRS (GB)
	Rule	MSSQL Reporting Services: Number of reports
	Rule	MSSQL Reporting Services: Number of shared data sources
	Rule	MSSQL Reporting Services: Number of subscriptions
	Rule	MSSQL Reporting Services: On-demand execution failures per minute
	Rule	MSSQL Reporting Services: On-demand executions per minute
	Rule	MSSQL Reporting Services: Report executions per minute
	Rule	MSSQL Reporting Services: Report executions per minute (Deployment)
	Rule	MSSQL Reporting Services: Scheduled execution failures per minute
	Rule	MSSQL Reporting Services: Scheduled executions per minute
	Rule	MSSQL Reporting Services: Total memory consumed on the server (GB)
	Rule	MSSQL Reporting Services: Total memory on the Server (GB)
	Rule	MSSQL Reporting Services: WorkingSetMaximum (GB)
	Rule	MSSQL Reporting Services: WorkingSetMinimum (GB)

Appendix: Known Issues and Release Notes

The DeploymentSeedDiscovery module fails if the instance is stopped or paused

Issue: When the instance is stopped or paused,

Microsoft.SqlServer.ReportingServices.Windows.Module.Discovery.DeploymentSeedDiscovery module fails with the following error: "An error occurred during discovery."

Resolution: No resolution required, as this is a by-design behavior. Start or resume the instance to eliminate the issue.