

Guide to Microsoft System Center Management Pack for Azure SQL Managed Instance



Microsoft® System Center Operations Manager

Published in July 2020 by Microsoft Corporation.

This guide is based on version 7.0.22.0 of the Management Pack for Azure SQL Managed Instance.

The Operations Manager team encourages you to provide 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.

© 2020 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.

Table of Contents

- [Guide to Microsoft System Center Management Pack for Azure SQL Managed Instance](#)
 - [Copyright](#)
 - [Table of Contents](#)

- Changes History
- Management Pack Scope and Supported Configurations
 - Managed Instance Supported Configurations and Features
 - Supported Tiers
 - Managed Instance Features
 - SCOM Configurations
 - Prerequisites
 - Management Pack Delivery
- Monitoring Configuration
 - Configuring Monitoring with Managed Instance Automatic Discovery monitoring template
 - Configuring Monitoring with Managed Instance monitoring template (specifying connections strings manually)
 - Configuring Azure SQL Managed Instance Monitoring Pool
 - Security Configuration
 - Least-Privilege Configuration
 - Monitor "Securables Configuration Status"
- Appendix: Known Issues and Troubleshooting

Changes History

July 2020 - version 7.0.22.0 RTM

Notes to Release

This release can't be installed on top of any previous version of the management pack. If you have a previous version already installed, remove it before installing this one.

Changelog

- **What's New**

- Updated monitor "Securables Configuration Status"
- Updated monitor "Job Duration" to add current job run's duration to its alert description
- Updated UI of wizard "Automatic Discovery"
- Updated alerting rules to avoid gathering SQL Log events that happened during maintenance mode
- Updated dashboards
- Updated display strings

- **Bug Fixes**

- Fixed: Self-diagnostic alerting rules fire alerts for SQL Server MP log events

April 2020 - version 7.0.21.0 CTP

- **What's New**

- Management pack was completely redone being based on up-to-date SQL Server MP codebase

September 2019 - version 1.0.1.0 CTP

- **What's New**

- Disabled "XTP Configuration Monitor"
- Disabled "Database Backup Status Monitor"
- Rebuild management pack and verify against the current version of Managed Instance Provided a few minor UI improvements to the Add Monitoring Wizard

February 2018 - 1.0.0.0 CTP

- The original release of this management pack

Management Pack Scope and Supported Configurations

This management pack is designed to monitor Azure SQL Managed Instance and the corresponding entities by means of T-SQL queries. Azure SQL Managed Instance is an automatically managed cloud instance running within Azure SQL Database cloud service.

Managed Instance Supported Configurations and Features

Supported Tiers

- General Purpose
- Business Critical (monitoring of Read-Scale Replicas is not supported yet)

Managed Instance Features

- Database Engine
- Database
- Agent and Jobs
- Memory-Optimized Data (In-Memory OLTP)
- Failover Groups, including secondary read-only replicas
- Authentication Mode — both SQL Server Authentication and Azure AD Authentication are supported.

SCOM Configurations

This management pack offers only agentless monitoring of Managed Instance. All the management pack workflows run by management servers included to a dedicated management server pool. The management pack does not require a dedicated management group and can work in virtual environments. List of supported versions of SCOM is as following:

- System Center Operations Manager 2012 R2
- System Center Operations Manager 2016
- System Center Operations Manager 1801
- System Center Operations Manager 1807
- System Center Operations Manager 2019

Prerequisites

- **.NET Framework 4.6.1+**

Installation of .NET Framework 4.6.1+ on all management servers participating in the Managed Instance monitoring is required.

- **Permanent and continuous ability to connect with managed instances from management servers**

Managed instance is usually being deployed on an isolated private network which means that there should be a permanent VPN connection on servers from which the managed instances must be accessible. Management servers participating in the Managed Instance monitoring have to be constantly able to access managed instances to be monitored.

Management Pack Delivery

Management Pack delivers as a download on microsoft.com and is also available on the SCOM Online Catalog. The download provides the next files:

- Microsoft.Azure.ManagedInstance.ManagementPack.msi — management pack installer
- AzureSQLMIMPGuide.pdf — this operations guide


Management Pack includes the following files:

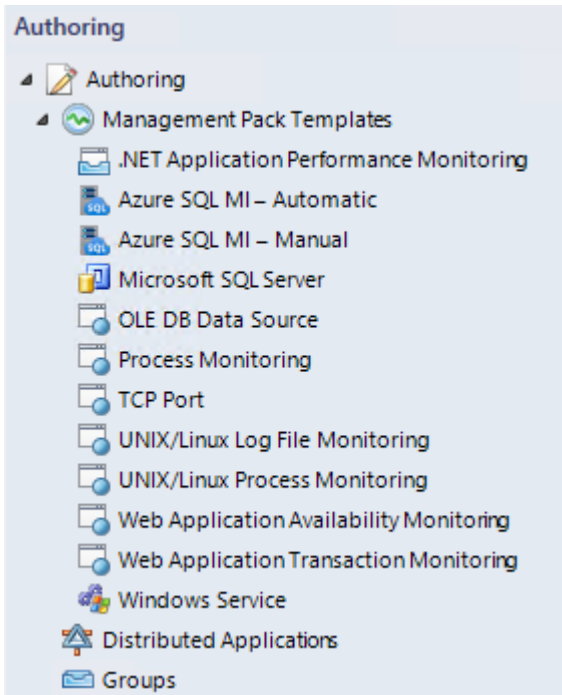
- Microsoft.Azure.ManagedInstance.Discovery.mpb
- Microsoft.Azure.ManagedInstance.Monitoring.mpb
- Microsoft.Azure.ManagedInstance.Views.mp
- Microsoft.SQLServer.Core.Library.mpb
- Microsoft.SQLServer.Visualization.Library.mpb

Monitoring Configuration

This management pack has two monitoring templates to configure the Managed Instance monitoring.

- "Azure SQL MI – Automatic" template. This template enables to configure the monitoring so that any Managed Instance within a specified subscription is being discovered automatically. This is the preferable option.
- "Azure SQL MI – Manual" template. This template is to add to monitoring only chosen managed instances by specifying their connection strings.


 Using both templates at the same time may cause the manually-added instances to be monitored by two sets of monitoring workflows which leads to redundant use of resources and also may lead to performance issues.



Configuring Monitoring with Managed Instance Automatic Discovery monitoring template

In SCOM Console, navigate to **Authoring | Management Pack Templates**, right-click **Azure SQL MI - Automatic** and select **Add Monitoring Wizard....**

In **Monitoring Type** window, select **Azure SQL MI - Automatic** and click the **Next** button. In **General Properties** window, provide your template **Name** and **Description**, as well as **Select destination management pack** where the template will be stored.

 Azure Endpoints

Monitoring Type

General Properties

Azure Endpoints

SPN Configuration


Auto-Create SPN Status

Subscription Permissions

SQL Connection Settings

Configure Instances Filtering

Summary

 Help

Configure Azure Endpoints

Enable checkbox if you want to change default Azure Endpoints


Authority URI:

Management Service URI:

Database Resource URI:

Graph API resource URI:

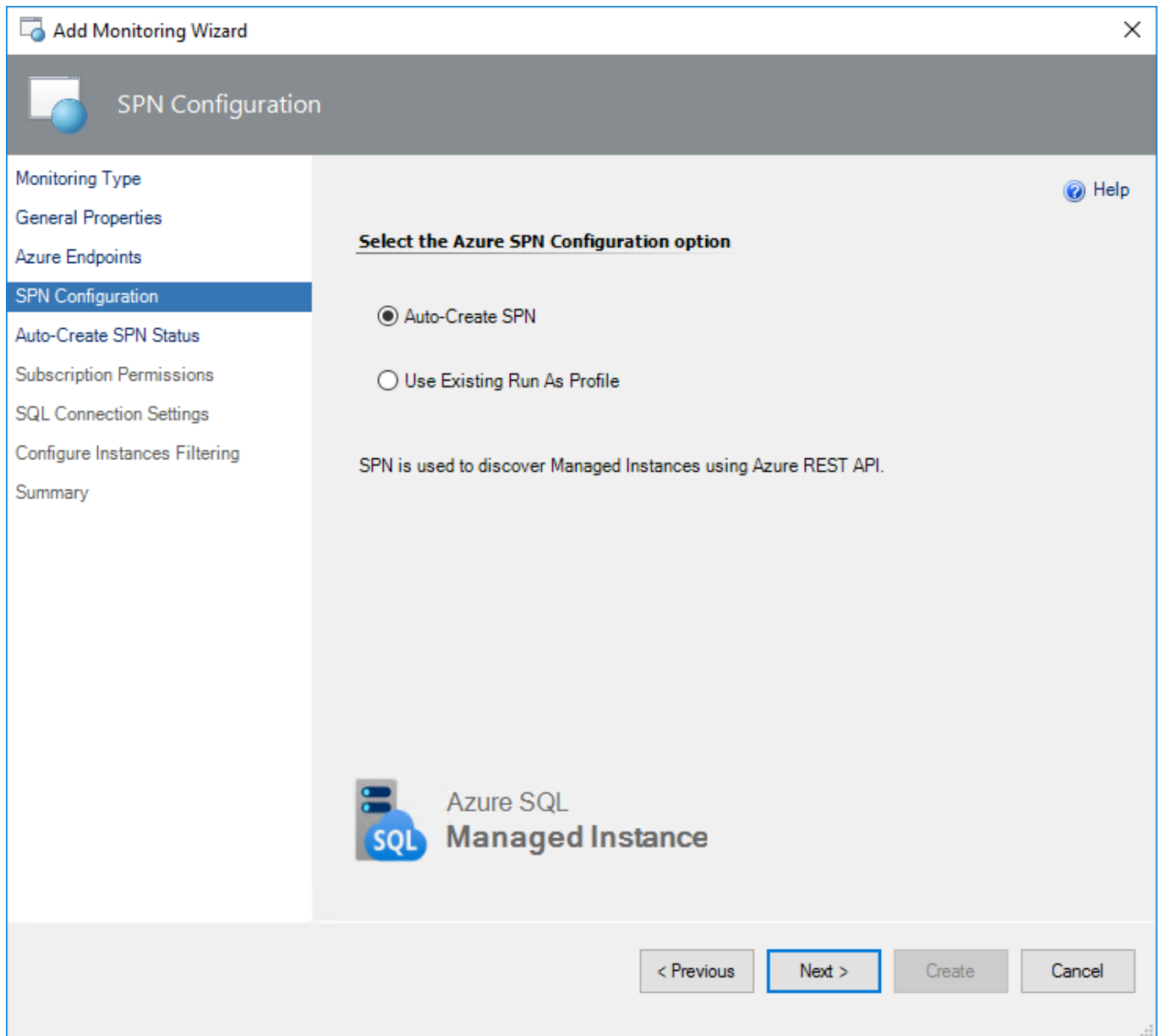
Graph Client ID:

 Azure SQL
Managed Instance

< Previous **Next >** Create Cancel

If you need to change the default Azure Endpoints, check the corresponding box. The endpoints used for creating Azure Service Principal are as follows:

- Authority URI: <https://login.windows.net>
- Management Service URI: <https://management.azure.com>
- Database Resource URI: <https://database.windows.net>
- Graph API Resource URI: <https://graph.windows.net>



To create Azure AD Application, Active Directory Administrator (Service Administrator or Co-Administrator) rights are needed. Non-admin users can create Azure AD Applications if the administrator grants a corresponding permission. It is necessary to have Owner (or higher) role for the target subscriptions for further assigning of the roles to the application (for the detailed information, see [Use portal to create Active Directory application and service principal that can access resources](#) article).

In **SPN Configuration** window, you can select between two options: **Auto-Create SPN**, **Use Existing Run As Profile**.

Auto-Create SPN: Azure SQL MI MP Library creates a new Azure Service Principal Name automatically (using Azure REST API - see Azure REST API Reference article). Then, a new Run As Account will be created with this SPN.

Use Existing Run As Profile: You have already configured a Run As Profile with appropriate SPN credentials.

If you select **Auto-Create** SPN option, a Microsoft Azure sign-in window will be displayed after clicking the **Next** button. In this window, fill in your work, school or personal Microsoft account credentials and click the **Sign in** button.

Add Monitoring Wizard ✕

Auto-Create SPN Status

Monitoring Type Help

General Properties

Azure Endpoints

SPN Configuration

Auto-Create SPN Status

Subscription Permissions

SQL Connection Settings

Configure Instances Filtering

Summary

Auto-create SPN Status

The following Application was created successfully, keep the below data.

Run As Account Name:
Azure_SQL_ManagedInstance_RunAsAccount_2020-07-03

Tenant ID:
[Redacted]

Application ID:
[Redacted]

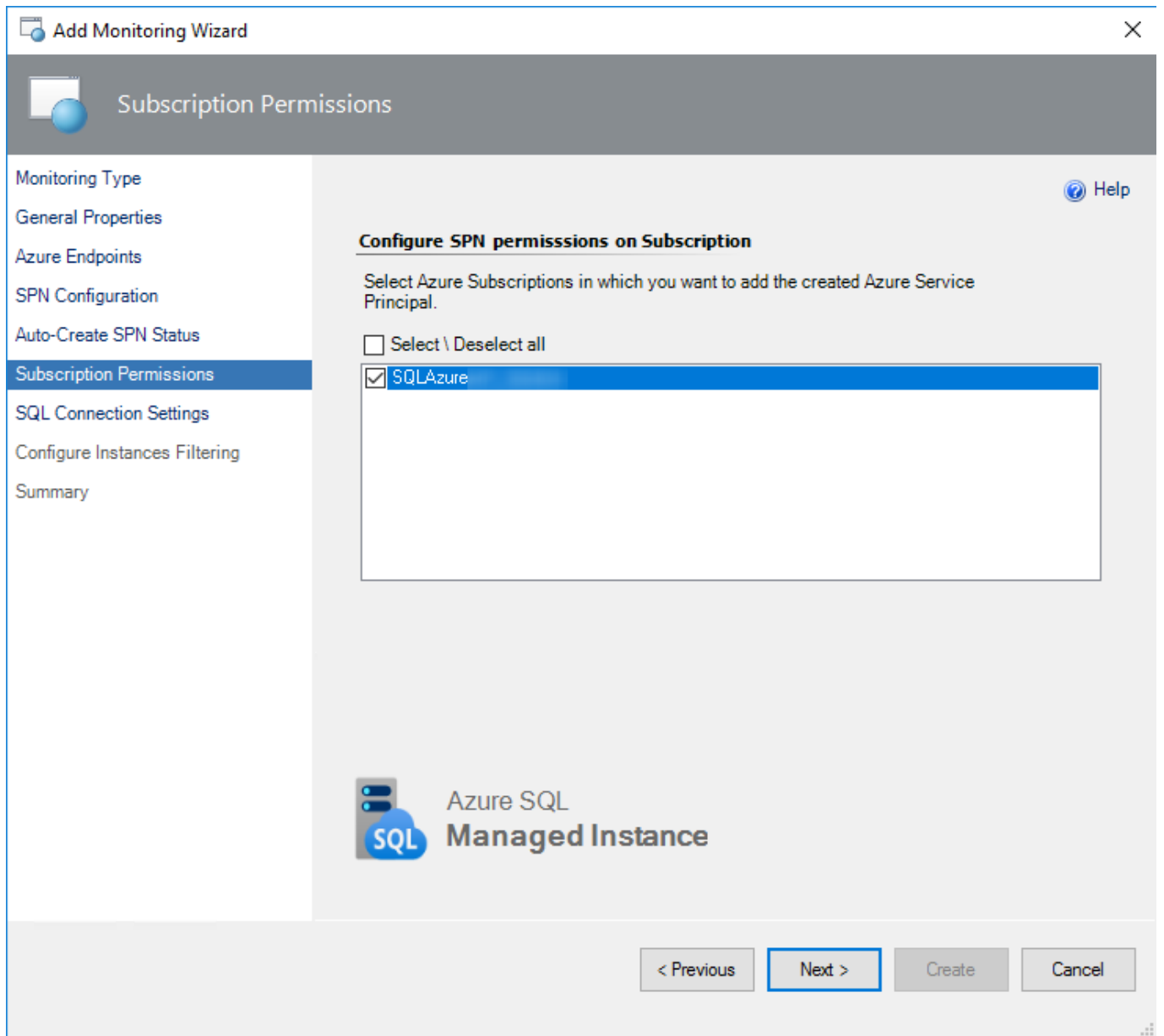
Client Secret:
[Redacted]

Application Name:
Azure_SQL_ManagedInstance_App_c718e6a0-a559-4f92-b5c1-90616042986d

Azure SQL
Managed Instance

< Previous **Next >** Create Cancel

Upon successful creation of the application, the corresponding authentication data will be displayed in **Auto-Create SPN Status** window.



On **Subscription Permissions** pick the Azure Subscriptions where Management Pack should managed instances to be monitored.

Add Monitoring Wizard

SQL Connection Settings

Monitoring Type

General Properties

Azure Endpoints

SPN Configuration

Auto-Create SPN Status

Subscription Permissions

SQL Connection Settings

Configure Instances Filtering

Summary

Help

SQL Connection Settings

Configure settings for SQL connections to discovered Managed Instances.

Authentication

Select authentication method for SQL connections

Azure Active Directory (AAD)

SQL Credentials (SQL)

Existing SQL Run As Account:

New...

Use Private endpoint for SQL connections

This option allows to select which endpoint will be used for discovery and monitoring Managed Instances: Public or Private. Public is the default choice.

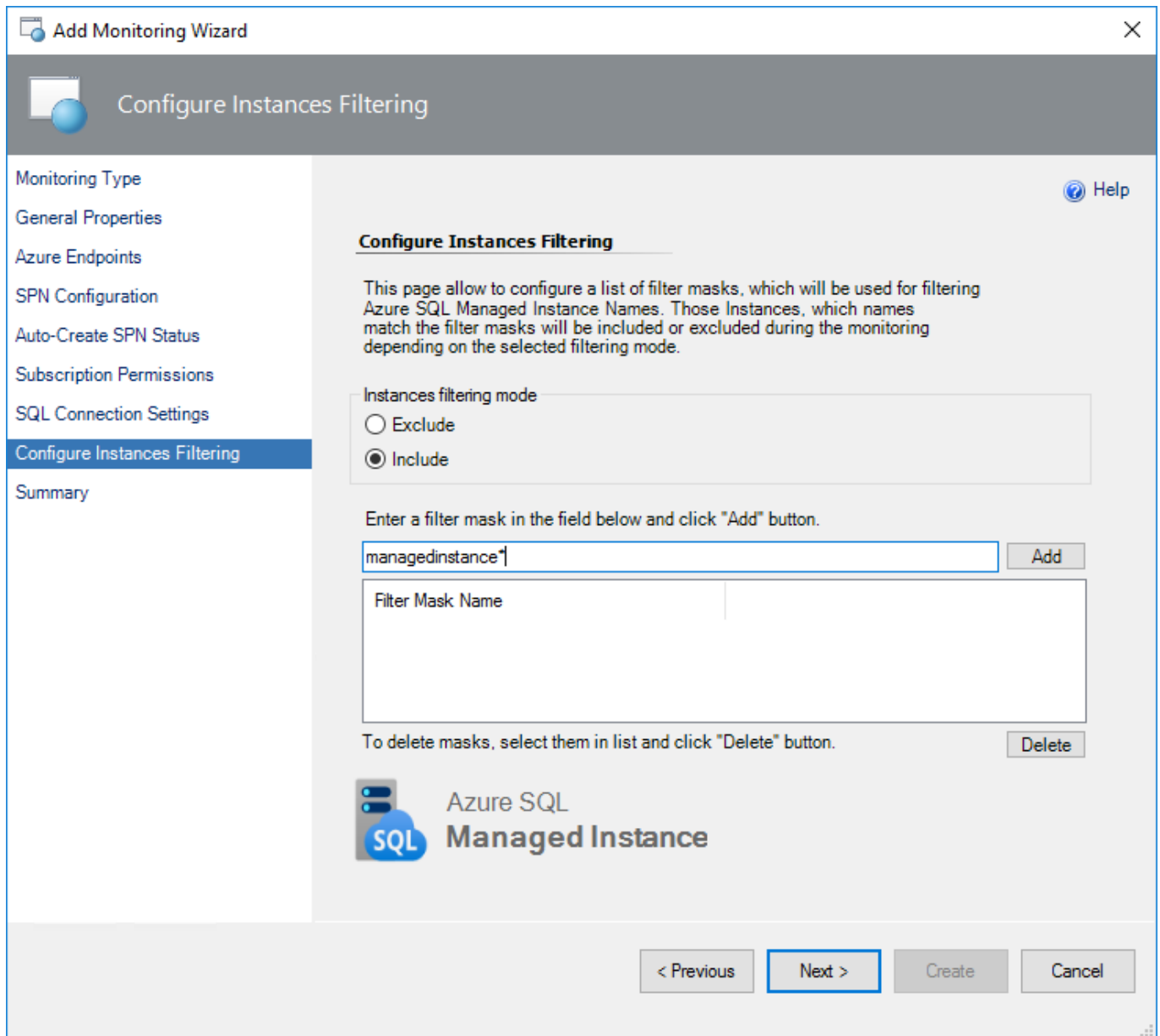
Azure SQL
Managed Instance

< Previous Next > Create Cancel

Management Pack supports two methods of authentication for connections to Managed Instance:

- Azure Active Directory
- SQL Authentication

No matter what option you choose, make sure to grant the chosen monitoring account with the required permissions on all managed instances to be monitored. See [Security Configuration](#) for details.



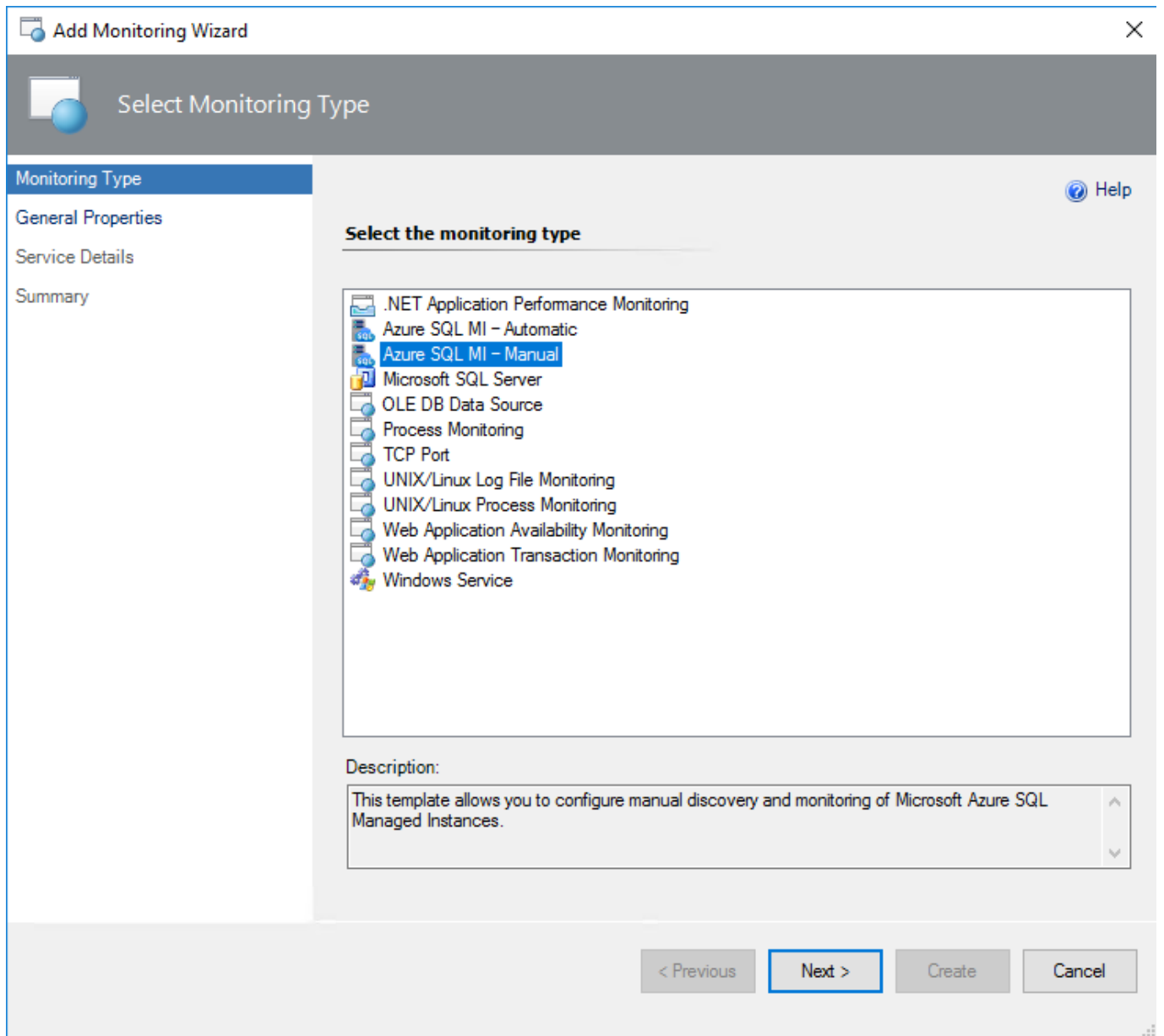
If you do not need all Managed Instances to be discovered and monitored, set up filters on **Configure Instances Filtering**. Use **Exclude** to list down names (an asterisk replaces any symbol/symbols) of instances that should not be discovered. Or use the **Include** method to define only those instances that should be discovered.

Configuring Monitoring with Managed Instance monitoring template (specifying connections strings manually)

In SCOM Console, navigate to **Authoring | Management Pack Templates**, right-click **Azure SQL MI - Manual** and select **Add Monitoring Wizard...**

In **Monitoring Type** window, select **Azure SQL MI - Manual** and click the **Next** button. In **General Properties** window, provide your template **Name** and **Description**, as well as **Select destination management pack** where the template will be stored.

In **Monitoring Type** window, select **Microsoft Azure Managed Instance** and click the **Next** button.



In the **General Properties** window, provide a **Name** and **Description** for your template, as well as **Select destination management pack** where the template will be stored.

Add Monitoring Wizard [Close]

General Properties

Monitoring Type
General Properties
Service Details
Summary

Enter a friendly name and description

Name:

Description:

Management pack

Select destination management pack:

<Select Management Pack> [v] [New...]

[< Previous] [Next >] [Create] [Cancel]

[Help]


You can also create a new destination management pack by clicking the corresponding button.



General Properties

General Properties

Knowledge

 Help

Management Pack General Properties

ID :

Name :

Version :

For example, 1.0.0.0

Description :

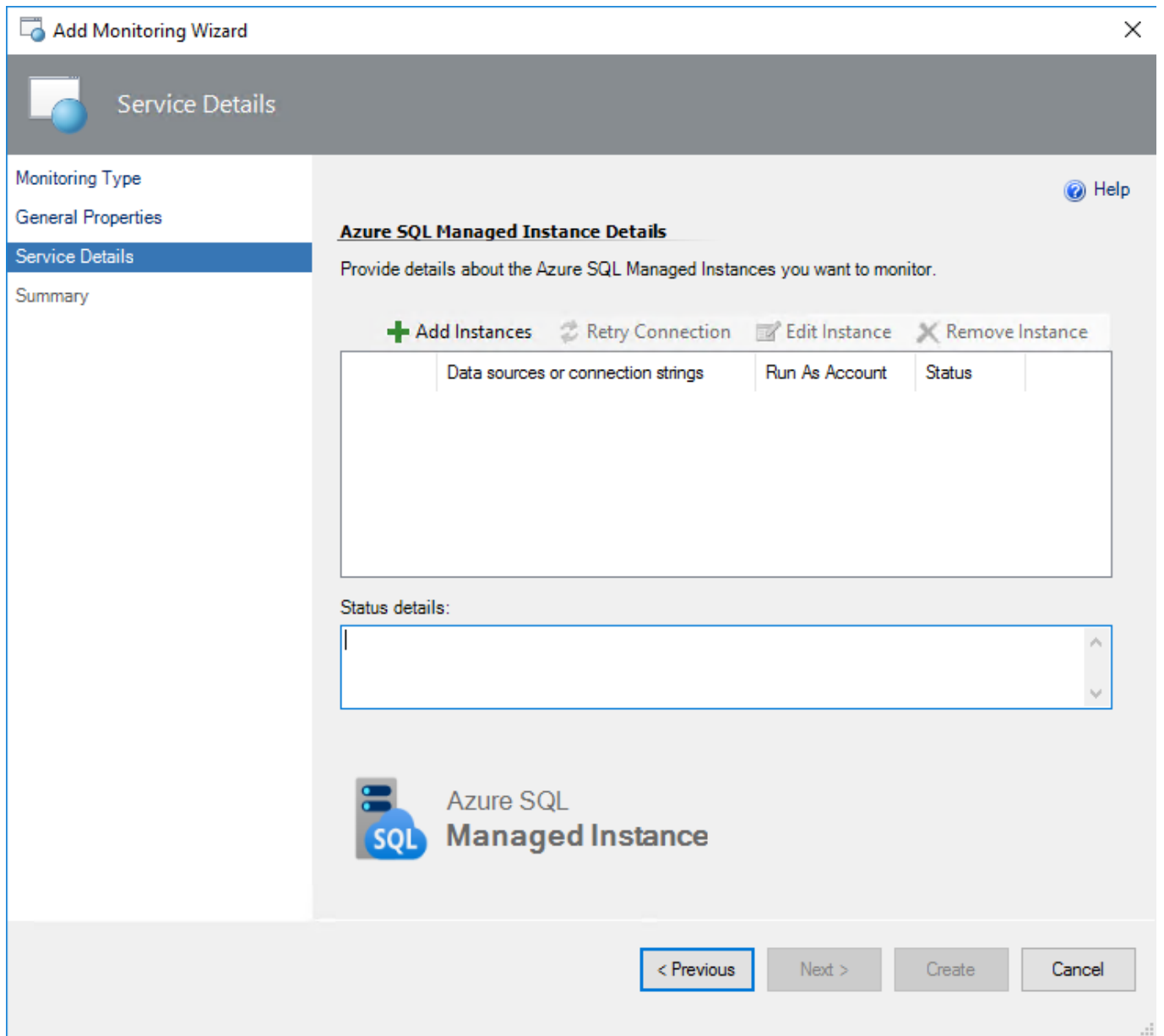
< Previous

Next >

Create

Cancel

In the **Service Details** window, you should provide the corresponding details about the instances you want to monitor.



Click the corresponding button to **Add Instances** for monitoring.

Select common Run As Account with SQL credentials

Note that selected Run As Account will be used for all connections.

Create Run As Accounts using User ID and Password from the connection strings.
 If User ID or Password keywords are missing, the selected common Run As Account will be used.

Enter data sources and connection strings

- Each data source/connection string is to be entered in a new line.
- You can add keywords to skip connection test for some lines at the end of the data source or connection string:
 <data source or connection string>

In this window, select a Run As Account with appropriate SQL credentials. Then, enter the data sources and (or) connection strings. Follow the instructions provided in this window to avoid errors.

The data is to be entered in the Standard Security connection string format:

```
Server=<ServerAddress>;Database=<DatabaseName>;
```

You can get the connection string for a managed instance using Azure Portal.

If you would like to create a Run As account from the connection string, then use the following format:

```
Server=<ServerAddress>;Database=<DatabaseName>;User Id=<UserName>;Password=<Password>;
```

You can also create a new Run As account by clicking the **New...** button.

Create new Run As Account

Account name:

Login:

Password:

Confirm password:

OK Cancel

In the corresponding window, enter an account name and connection credentials for your Managed Instance.

After clicking the **OK** button in **Add Instances** window, testing of the connection to the selected instance will be performed.

Add Monitoring Wizard

Service Details

Monitoring Type

General Properties

Service Details

Summary

Azure SQL Managed Instance Details

Provide details about the Azure SQL Managed Instances you want to monitor.

+ Add Instances ↻ Retry Connection ✎ Edit Instance ✕ Remove Instance

Data sources or connection strings	Run As Account	Status
tcp: [redacted].36c954d642c6.data...	fk_azure	Processing

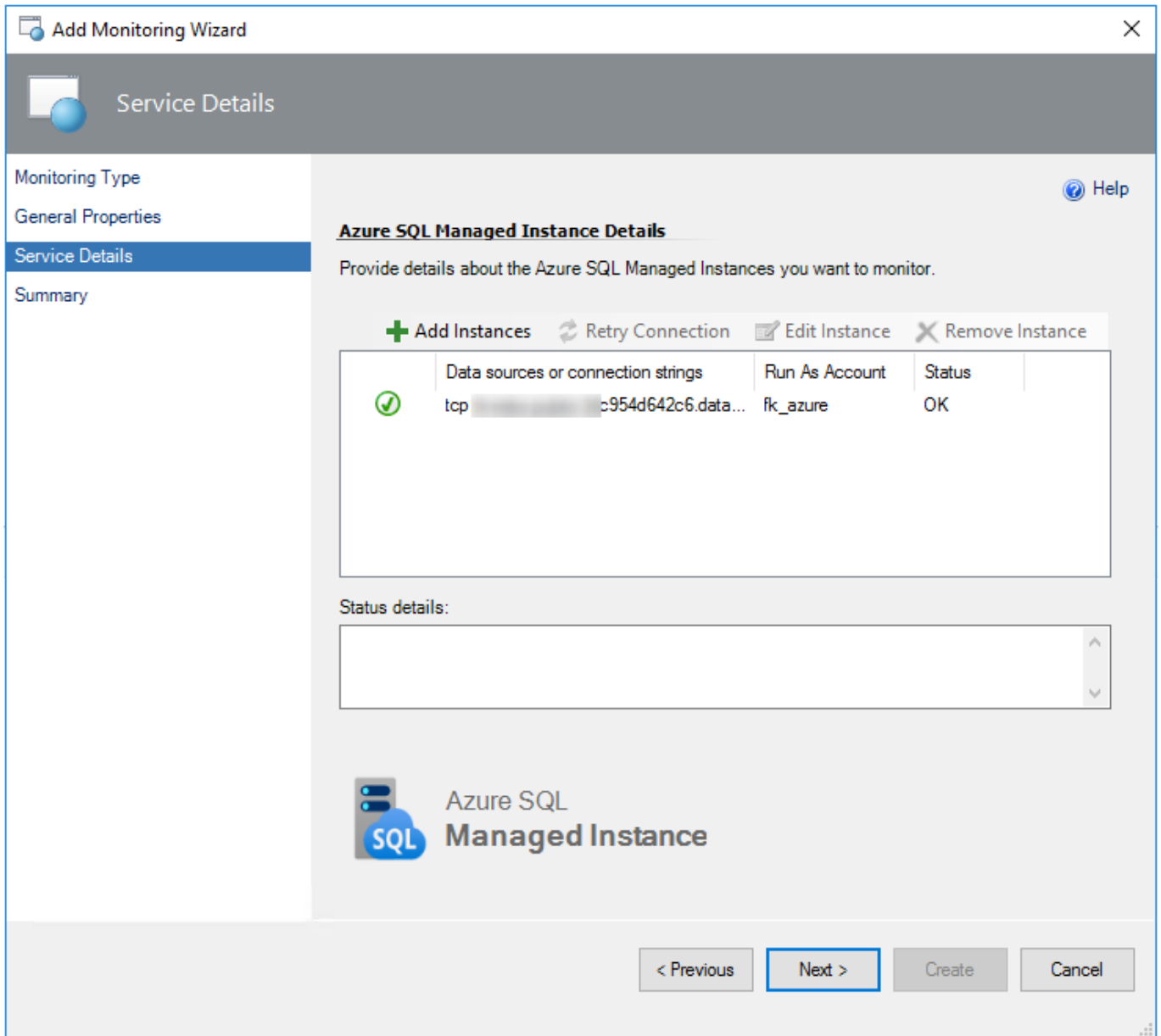
Status details:

Testing connection using "tcp: [redacted].36c954d642c6.database.windows.net,3342". 1 try out of 12

Azure SQL Managed Instance

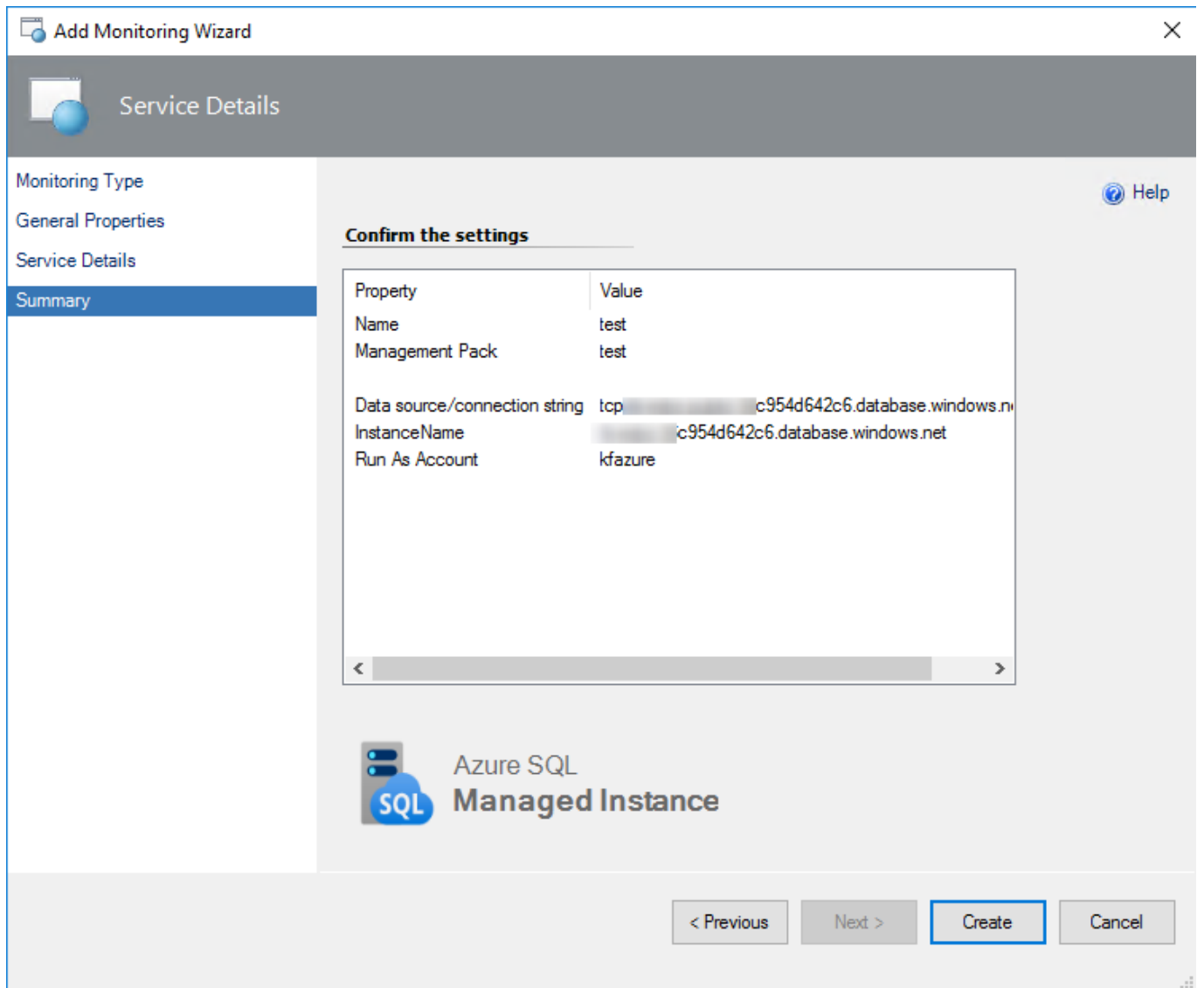
< Previous Next > Create Cancel

When the connection testing is completed, you can view and edit properties of the added instance. To do that, select the instance and click the **Edit Instance** button.



⚠ Monitoring Template Wizard may show the "An error occurred discovery: A connection was successfully established with the server, but then an error occurred during the login process" or "Monitoring error" exception while checking connection. See [A Managed Instance is not discovered and Discovery error or Monitoring error alerts appeared](#) to work this issue out.

In **Summary** window, you can view you monitoring settings and confirm them by clicking the **Create** button.



After that, your monitoring template will be successfully created.

Configuring Azure SQL Managed Instance Monitoring Pool

The monitoring pool is available for configuration in the Operations Manager. To configure the monitoring pool, navigate to **Administration | Resource Pools**, right-click **Azure SQL MI Monitoring Pool** in the list of Resource Pools and check **Manual Membership** option. Then, select **Properties** action. As a result, **Azure SQL MI Monitoring Pool Properties** window will be displayed.

Azure SQL MI Monitoring Pool Properties

Enter the Name and Description for the Resource Pool

General Properties

Pool Membership

Summary

Completion

Enter a friendly name and description

Name:

Azure SQL MI Monitoring Pool

Description (optional):

< Previous Next > Save Cancel

In this window, enter a name and description for the Resource Pool and click the **Next** button. As a result, the **Pool Membership** window will appear.

Azure SQL MI Monitoring Pool Properties

Choose members for this Resource Pool

General Properties



Pool Membership

Summary

Completion


Resource pool members

Choose the resources that you want in this pool. Two or more members are required for high availability.

 Add...  Remove

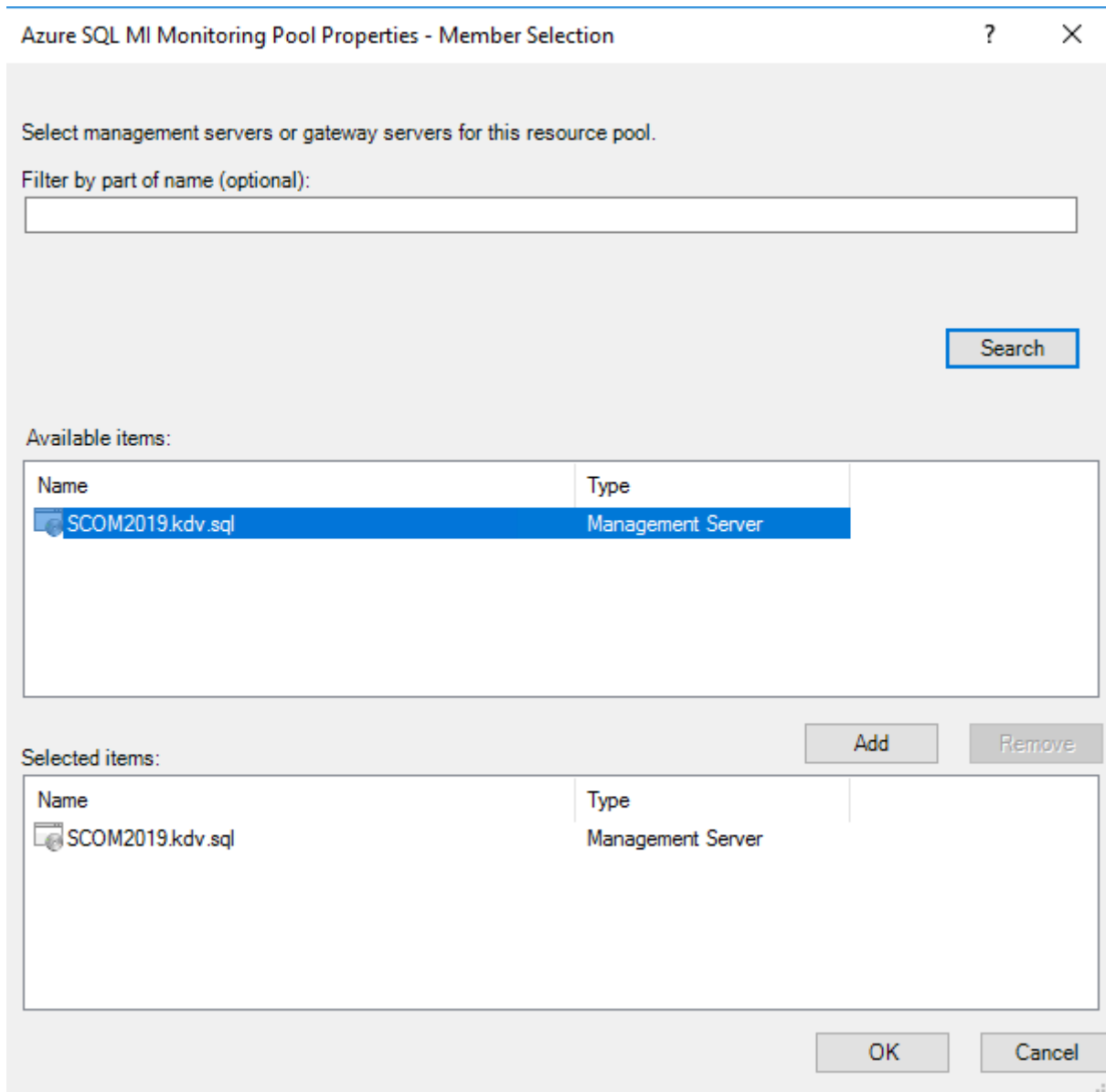
Pool members:

Name	Type
------	------

 [More about adding resources to a pool](#)

< Previous Next > Save Cancel

In this window, click the **Add...** button to populate the monitoring pool.



Click the **OK** button to complete the procedure.

Note: If the pool remains empty, it mirrors the contents of All Management Servers pool. The pool can be populated with either Gateways or Management Servers, but they should not be added to the pool together.



Choose members for this Resource Pool

General Properties



Pool Membership

Summary

Completion


Resource pool members

Choose the resources that you want in this pool. Two or more members are required for high availability.

 Add...  Remove

Pool members:

Name	Type
SCOM2019.kdv.sql	Management Server

 [More about adding resources to a pool](#)

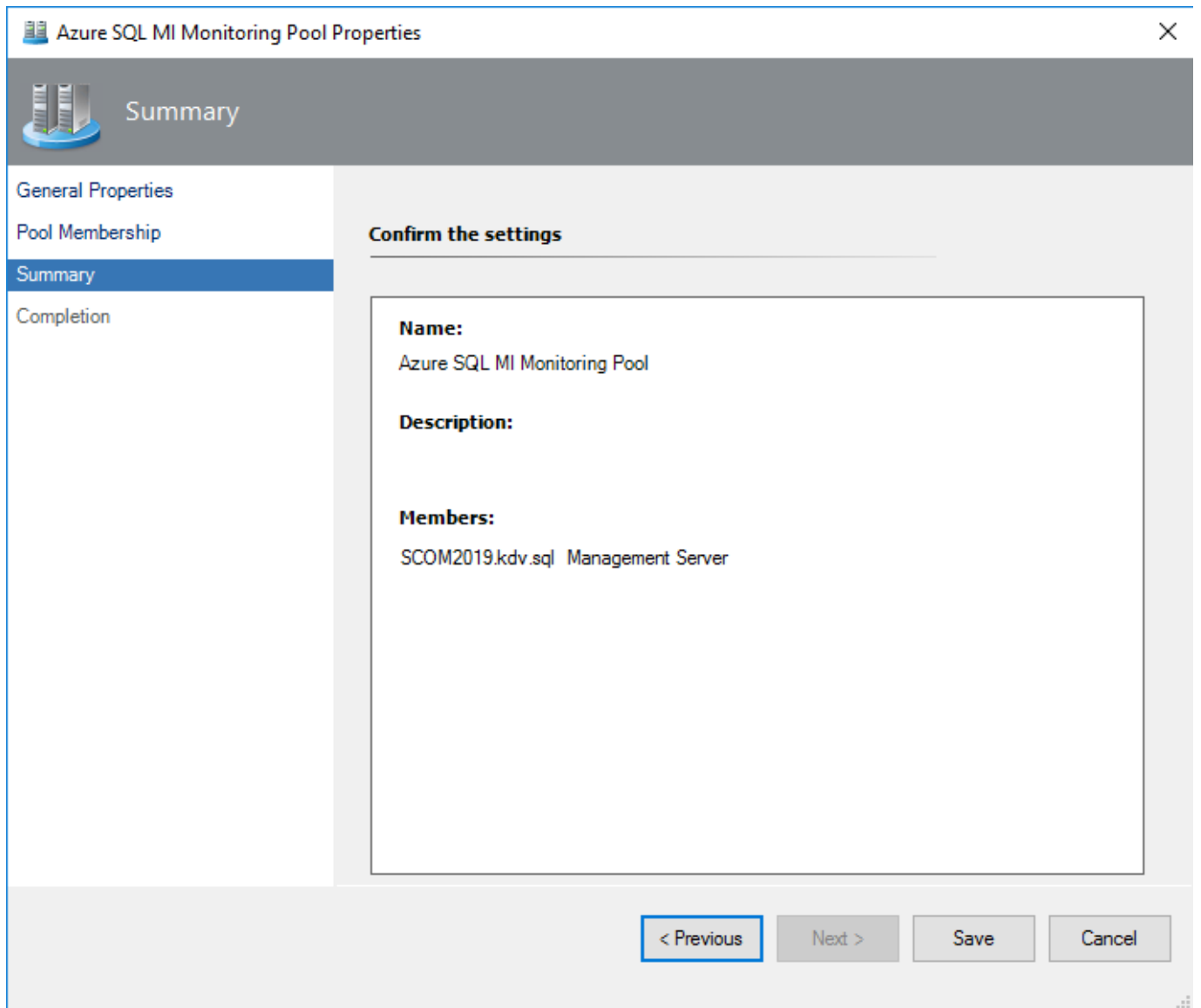
< Previous

Next >

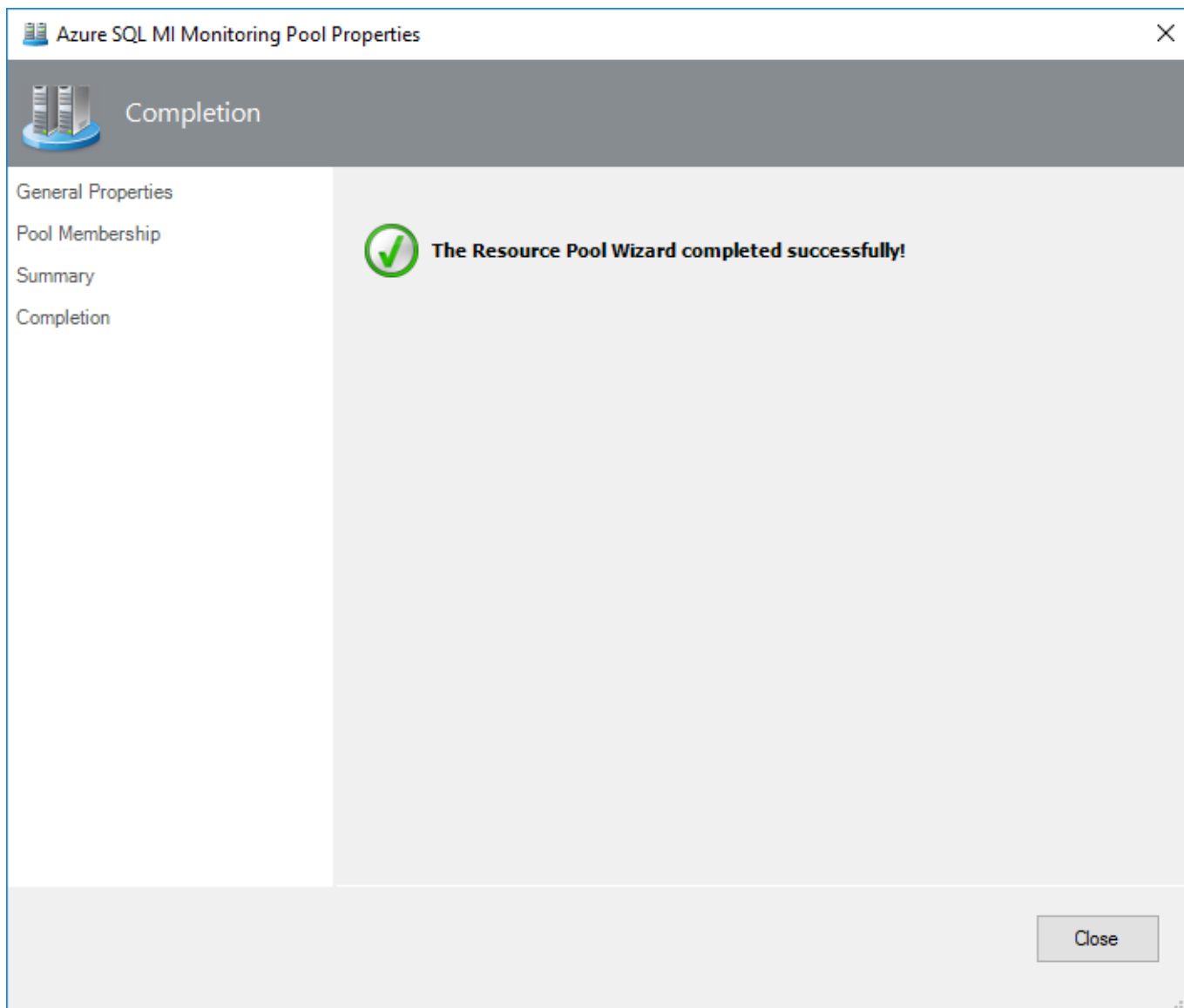
Save

Cancel

Click the **Next** button to view the **Summary** window.



In this window, check the applied settings and click the **Save** button if they are correct. Otherwise, click the **Previous** button and make necessary corrections.



Close the final **Completion** window by clicking the corresponding button.

Security Configuration

A monitoring account—SQL account or AAD principal used by this management pack for monitoring—should have enough permissions on each Managed Instance that is covered by a particular monitoring template. Every Managed Instance has to have a login for the monitoring account, and this login should be granted with:

- Sysadmin rights;
- Or the minimum level of permissions that allows the management pack to operate (so-called least-privilege configuration).

The latter is explained below.

Least-Privilege Configuration

To configure the least-privilege monitoring, we suggest you use the following three scripts as an example. The first should be run against every managed instance, and the second against every user database on each managed instance. With deploying new managed instances, make sure to run both scripts for them. You don't need to run the second script for each new database that you have created after the initial execution as the

first script updates the model database so that later created databases will have the required user. But you need to run the second script for every database attached or restored after the initial execution of the scripts.

The third script adds the monitoring account to the db_owner role which may be not allowed. The db owner permissions are required to enable the management pack tasks for running DBCC checks to work. If you don't need these tasks, don't give these permissions.

```
--First script that
-- - grants server-level permissions to the monitoring account
-- - creates a user in the master and msdb databases and grants the required
permissions to it
-- - creates a user in the model database
USE [master]
CREATE LOGIN [MILowPriv]
GRANT VIEW SERVER STATE TO [MILowPriv]
GRANT VIEW ANY DEFINITION TO [MILowPriv]
GRANT VIEW ANY DATABASE TO [MILowPriv]
GRANT ALTER ANY DATABASE TO [MILowPriv]
CREATE USER [MILowPriv] FOR LOGIN [MILowPriv]
GRANT EXECUTE ON xp_readerrorlog TO [MILowPriv]
GRANT EXECUTE ON xp_instance_regread TO [MILowPriv]
GRANT EXECUTE ON xp_sqlagent_enum_jobs TO [MILowPriv]
GRANT EXECUTE ON sp_enumerrorlogs TO [MILowPriv]

USE [msdb]
CREATE USER [MILowPriv] FOR LOGIN [MILowPriv]
ALTER ROLE [db_datareader] ADD MEMBER [MILowPriv]
ALTER ROLE [db_owner] ADD MEMBER [MILowPriv]
ALTER ROLE [SQLAgentReaderRole] ADD MEMBER [MILowPriv]
GRANT EXECUTE ON sp_help_job TO [MILowPriv]
GRANT EXECUTE ON sp_help_jobactivity TO [MILowPriv]
GRANT SELECT ON sysjobschedules TO [MILowPriv]
GRANT SELECT ON backupset TO [MILowPriv]

USE [model]
CREATE USER [MILowPriv] FOR LOGIN [MILowPriv]
```

```
--Second script that creates a user in a user database.
--This script should be run for each user database on all managed instances
USE [<DATABASE NAME>]
CREATE USER [MILowPriv] FOR LOGIN [MILowPriv]
```

```
--Third script that adds MILOWPriv user to db_owner role
--This script should be run for the model database and each user database on all
managed instances
--This is only to enable running DBCC checks right on SCOM (Check Catalog, Check
Database, Check Disk)
--If you don't need this functionality, don't run this script
```

```
USE [<DATABASE NAME>]
ALTER ROLE [db_owner] ADD MEMBER [MILowPriv]
```

Monitor “Securables Configuration Status”

This monitor checks if each of the required Managed Instance securables is accessible under the configured monitoring account. Here's the complete list of securables that are checked by the monitor.

- Server-Level permissions
 - VIEW SERVER STATE
 - VIEW ANY DEFINITION
 - VIEW ANY DATABASE
 - ALTER ANY DATABASE
- SELECT permission on dynamic management views
 - sys.dm_os_performance_counters
 - sys.dm_tran_active_transactions
 - sys.dm_tran_session_transactions
 - sys.dm_exec_sessions
 - sys.dm_exec_requests
 - sys.dm_exec_connections
 - sys.dm_os_sys_info
 - sys.dm_os_host_info
 - sys.dm_os_ring_buffers
 - sys.dm_os_volume_stats
 - sys.dm_os_threads
 - sys.dm_hadr_database_replica_states
 - sys.dm_hadr_fabric_partition_states
 - sys.dm_hadr_fabric_config_parameters
 - sys.dm_hadr_fabric_continuous_copy_status
 - sys.dm_db_xtp_checkpoint_files
 - sys.dm_db_xtp_table_memory_stats
 - sys.dm_db_xtp_hash_index_stats
 - sys.dm_internal_resource_governor_resource_pools
- SELECT permission on catalog views
 - sys.databases
 - sys.database_files
 - sys.tables
 - sys.filegroups
 - sys.syscolumns
 - sys.sysprocesses
 - sys.configurations
 - sys.syslanguages
 - sys.server_resource_stats

- msdb.dbo.sysjobschedules
- msdb.dbo.backupset
- EXECUTE permission on stored procedures
 - sys.sp_enumerrorlogs
 - sys.xp_readerrorlog
 - sys.xp_instance_regread
 - msdb.dbo.sp_help_jobactivity
 - msdb.dbo.sp_help_job

Appendix: Known Issues and Troubleshooting

Rules and monitors may provide incorrect data if default interval override values are changed

Issue: If the value of Interval (seconds) overridable parameter is set lower than the default value, rules and monitors may provide incorrect data.

Resolution: Make sure that Interval (seconds) overridable parameter is set no lower than the default value.

If a Managed Instance is not available, multiple errors occur in the watcher node event log

Issue: If a Managed Instance is not available, multiple errors appear in the watcher node event log. The errors will keep coming until the Managed Instance is available.

Resolution: No resolution available.

When an instance is not available, Module.Monitoring.Performance.SqlOsPerfCounterReaderHelper exception is received in the event log

Issue: When an instance is not available, Module.Monitoring.Performance.SqlOsPerfCounterReaderHelper exception is received in the event log. This exception will keep coming until the instance is available. The interval of this exception coming is equal to the lowest interval set for the performance rules.

Resolution: No resolution.

Odd behavior of the monitors' operational states

Issue: If the resource pool contains more than one management server, the operational states of all the monitors will be changing according to the failover settings of the resource pool.

Resolution: No resolution.

Extended discovery intervals

Issue: In case of using a resource pool with several watcher nodes, the discovery intervals may be significantly extended.

Resolution: No resolution.

Some error messages may appear in the Operations Manager events after adding a new database to already monitored MI

Issue: Some error messages may appear in the Operations Manager events after adding a new database to already monitored MI during the discovery process:

- Skipping the default startup of the database because the database belongs to an availability group.
- The database cannot be opened due to inaccessible files, insufficient memory or lack of disk space.

Resolution: No resolution.

Memory-Optimized Data Stale Checkpoint File Pairs Ratio monitor may not change its state

Issue: Memory-Optimized Data Stale Checkpoint File Pairs Ratio monitor may not change its state from Warning to Success.

Resolution: Reset health state of the monitor.

Error messages may appear in the event log right after monitoring template creation

Issue: "Windows logins are not supported in this version of SQL Server" or "SQL credentials are not set" error messages may appear in the Operations Manager event log after the creation of a monitoring template."

Resolution: These are temporary issues related to management pack workflows initialization.

A Managed Instance is not discovered and Discovery error or Monitoring error alerts appeared

Issue: "Discovery error" or "Monitoring error" alerts are arisen with the message "Object reference not set to an instance of an object" right after the creation of a monitoring template, and error event 4225 is thrown in the OpsMan log. No managed instances are discovered. Most likely, these errors indicate that the resource pool "Azure SQL MI Monitoring Pool" has not been discovered yet, and Managed Instance cannot be bound to it.

Resolution: Wait until discovered managed instance appear on Managed Instances state view (it can take up to few hours), then close "Azure SQL MI Instance: Discovery error" and/or "Azure SQL MI: Monitoring error" alerts generated by rules. To speed up the discovery process, decrease the intervals for both "Azure SQL MI: Generic Monitoring Pool Watcher Discovery" and "Discover All Management Servers Pool Watcher" discoveries to force them to run right away, give it 10 minutes and then restore the default intervals.