

Guide to System Center Management Pack for Microsoft Azure

Microsoft Corporation

Published: August 2022

Send feedback or suggestions about this document to [UserVoice link](https://feedback.azure.com/d365community/forum/2a49c9ee-4436-ec11-b6e6-00224824730c). Please include the management pack guide name with your feedback.

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.

© 2019 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

[Contents 3](#_Toc111213642)

[Guide to System Center Management Pack for Microsoft Azure 4](#_Toc111213643)

[Changes History 4](#_Toc111213644)

[Supported Configurations 12](#_Toc111213645)

[Upgrade 14](#_Toc111213646)

[Management Pack Scope 18](#_Toc111213647)

[Prerequisites 21](#_Toc111213648)

[The following requirements must be met to run this management pack: 21](#_Toc111213649)

[Azure MP Authentication 22](#_Toc111213650)

[Mandatory Configuration 23](#_Toc111213651)

[1. Import Management Pack 23](#_Toc111213652)

[2. Add Microsoft Azure Subscriptions 23](#_Toc111213653)

[3.Select Resources to Monitor in Wizard 31](#_Toc111213654)

[4.H5 Dashboard Views for Azure Management Pack 38](#_Toc111213655)

[Modified Alert Description in Operations Manager 44](#_Toc111213656)

[Features 46](#_Toc111213657)

[Availability tests in Application insights 46](#_Toc111213658)

[Azure Alerts in Operations Manager 47](#_Toc111213659)

[Azure Diagnostics and Guest Metrics on Virtual Machines, Web Roles, and Worker Roles 57](#_Toc111213660)

[Enable Grooming of Performance and Event Logs from Azure Table Storage 60](#_Toc111213661)

[Enable Disabled Monitors 61](#_Toc111213662)

[Write Rules to Collect Events and Performance from Azure Table Storage 61](#_Toc111213663)

[Monitor Large Number of Azure Instances 62](#_Toc111213664)

[Full Scan 70](#_Toc111213665)

[Files in this Management Pack 71](#_Toc111213666)

[Management Pack Purpose 71](#_Toc111213667)

[Monitoring Scenarios 72](#_Toc111213668)

[How Health Rolls Up 73](#_Toc111213669)

[Topology Dashboard 74](#_Toc111213670)

[Model Hybrid Applications via Distributed Application Template 75](#_Toc111213671)

[Endpoints 75](#_Toc111213672)

[Alert Severity Changes 76](#_Toc111213673)

[Impact on SCOM Health State based on the Alert 76](#_Toc111213674)

[Security Configuration 76](#_Toc111213675)

[Setting up Proxy Connection 77](#_Toc111213676)

[Low-Privilege Configuration 80](#_Toc111213677)

[Links 83](#_Toc111213678)

[System Center Operations Manager 83](#_Toc111213679)

[Appendix: Known Issues 84](#_Toc111213680)

[Appendix: Management Pack Contents 91](#_Toc111213681)

[Deprecated Workflows 103](#_Toc111213682)

Guide to System Center Management Pack for Microsoft Azure

This Guide is based on version 1.8.0.9 of the management pack for Microsoft Azure.

### Changes History

|  |  |
| --- | --- |
| Release Date | Changes |
| August 2022 (1.8.0.9 version) | Bug Fixes:   * ADAL Deprecation - update latest MSAL binaries. * Auto SPN creation is not working in Azure MP. * Removal of Azure MP Silverlight changes. * Not receiving alerts for Azure Web tests in SCOM while alerts are seen in Azure Portal. * Some SQR alerts are not changing its state from Healthy to Critical. * Azure MP - SCOM console is crashing while creating template. |
| September 2021 (1.8.0.8 version) | Bug Fixes:  • New “Service Type” dropdown added as a filter in “All Resources” H5 dashboard.  • Fixed: Status always showing healthy for Metric Alerts with Space.  • Fixed: App insight health state doesn’t change with corresponding Web Test status in SCOM.  • Fixed: Resource scan issues while creating authoring template.  • SQR and Metric Alert description now shows Impacted resources (assets) information.  Note: Upgrade is supported from v1.8.0.2 and v1.8.0.5. |
| September 2020 (1.8.0.5 version) | Bug Fixes:   * Performance Graph Mismatch between the data viewed in SCOM and azure Application Insights. * Bogus Event IDs 11424 and 11426 from Azure MP * Accessibility bugs in HTML5 Dashboard * Alerts display issue when alert rules are in one resource group & target entity in different resource group. * Performance data for the selected metrics is not collected.   Note: Upgrade is supported from v1.6.0.7, v1.7.0.0, v1.8.0.1 and v1.8.0.2.  Authoring template should be updated for UI changes to be reflected. Refer ***Upgrade Steps*** section. |
| February 2020 (1.8.0.2 version) | Improvements:   * H5Dashboard - New H5 Dashboards are created for Azure MP to help in easy filtering and navigation through Web console. * Alert Severity Changes - Change alert state and health state based on Azure alert severity.   Bug Fixes:   * Azure MP-Web Test Failure in SCOM - App Insights * Close of SQR and Activity Log alerts from SCOM console.  Note: Upgrade is supported from v1.6.0.7, v1.7.0.0 and v1.8.0.1.   Existing template will be honored. |
| November 2019 (1.8.0.1 version) | Improvements:   * Enabled Resource Group filtering for subscription. * Modified Alert description for all Alert types * Enabled multi-resource metric alerts support.   Bug Fixes:   * Fixed health state issue to be in sync with Azure portal. * Fixed ‘unknown’ state issue for metric alert. * Note: Upgrade is supported from v1.6.0.7 and v1.7.0.0. Existing template will be honored. |
| March 2019 (1.7.0.0 version) | This guide was updated to reflect the changes introduced with version 1.7.0.0 of this Management Pack:   * Added monitoring of Scheduled Query Rules and close its alerts Task with account that has Contributor/Owner permissions to subscription. * Added monitoring of Activity Logs Alerts Rules and close its alerts Task with account that has Contributor/Owner permissions to subscription. * At clean installation, all *Service types*now *unchecked* by default.   User should select services to monitor on Wizard configuration step.   * At clean installation *Metrics collection* for all services *unchecked* by default.   User can select metrics to collect on Wizard configuration step.   * On Upgrade, all previous customer settings will be preserved. * Updated section how to perform Upgrade from different versions. Follow “Upgrade” section for more details. * Improved Service types user interface in Wizard. Highlighted with grey services that are in less use * Full Scan option disabled by default. It is possible re-enable it in registry. Follow “Full Scan” section for more details. * Re-enabled Guest metrics collection for VMs in public Azure. Guest metrics should be added as a new extension to Azure. Guest collection has limitations by regions. For more information how enable Guest Metrics read “[Guest metrics monitoring](#_A_note_about)” section. * To obtain new Guest Metrics for Virtual Machines in Azure in Authoring- Azure MP wizard > press [Refresh data]. Guest metrics will appear in Metrics tab unchecked by default. * Updated section “Azure in China”. Added limitation: In China subscription Virtual machines metrics will not be collected. * All “Alert Rule” entries in descriptions were renamed to “Classic Metric Alerts”   Fixed bug when performance metrics stopped collecting while receive incorrect configuration from Azure |
| December 2018 (1.6.0.7) | * Fixed Health Service “Greyed Out” issue while monitor large number of Classic Alerts. * Added url string to Classic Alerts description for webtests * Updated list of known issues in Guide   + Full Scan issue. It is not recommended check “Full scan” in Wizard. All required services will be available out of the box with default configuration.   + Performance collection error issue on large number of instances   + Fixed typo for CLR Threads in registry values in section “Monitor a large number of Azure Instances” in guide |
| October 2018 (1.6.0.0) | * Fixed false errors about required access to DataAccess service when monitor classic alert rules in the Gateway configuration * Improved names and descriptions for workflows that responsible for metric alerts presentation in Operations Manager Console * Updated section “Azure Alerts in Operations Manager” in Guide * Changed alert names for warning alerts created on dynamic monitors. * Declare compatibility with System Center Operations Manager 1801 * Implemented validation on “the given key not present in the dictionary” issue * It is possible to upgrade from 1.5.30.26 CTP, but user is recommended to re-create Azure MP template in Authoring section to obtain new changes and perform modifications. |
| September 2018 (1.5.30.26 CTP) | * Implemented monitoring of Microsoft Azure Metric Alerts * Fixed issue when more than 6000+ instances could not be added for monitoring. * Implemented Waring in Wizard that will arise with recommendation to configure environment according to Guide if more than 2000 instances detected on subscription. * Fixed issue when SCOM workflows unloaded if selected empty metric for monitoring when select Alert if in Wizard. * Fixed issues on adding wrong SPN in edit mode. * Fixed null reference exception issue when it was unable to add subscription to monitor new Azure services. * To upgrade from 1.5.20.18 CTP it is important to re-create Azure MP template in Authoring section |
| June 2018 (version 1.5.20.18 CTP) | * Added the “Audience URI” field in the Endpoints Configuration for the Azure Subscriptions Wizard * Updated insights library to version 0.15.0.0 * Implemented monitoring of Non-classic storage account. * Implemented monitoring of Application gateway. * Fixed issue of obtaining data with Azure Data Factory * Implemented monitoring of Azure Data Factory * Metric collection for Classic storage account is not supported. * Implemented monitoring of Service Bus in SPN mode * Implemented monitoring support for Gateway Server |
| June 2017 (version 1.5.0.0) | * Fixed issue: Azure management pack Discovery Full Scan was failing with the following message: "One or more errors occurred. Unable to cast object of type 'Newtonsoft.Json.Linq.JValue' to type 'Newtonsoft.Json.Linq.JArray'.". * Fixed RDFE Cloud service discovery issue: Cloud Service did not match with the Azure portal data. * Fixed issue: Insights Incident Monitor did not change its state to critical after receiving alerts from the monitored Azure Web App. * Fixed Add Monitoring wizard issue: “Cannot access child value on Newtonsoft.Json.Linq.JValue” error was appearing while selecting a subscription. * Fixed issue: Azure Application Insights performance metrics could not be collected by SCOM; removed "request.rate" from the metrics’ list of the management pack. |
| January 2017 (version 1.4.4.0) | * Implemented automatic creation of the Service Principal Name * Updated and redesigned Add Subscription and Add Monitoring wizards; fixed duplication of metrics for SQL Databases, fixed editing the Exclude list. * Multi-factor authentication support is implemented. * Delay of Azure Application Insights alerts’ delivery is reduced. * Fixed issue: virtual machines did not have "OS Version" property populated. * Fixed issue: in SCOM, successfully completed tasks could have “Failed” status in the Task Output. * Improved the Add Monitoring wizard performance. * Fixed “Virtual Machine Turn Off Monitor” operational state names. * Updated the list of REST endpoints essential for Chinese instances. * For SPN mode, RDFE types are removed from the service types list. * Removed the need for SCOM Administrators to enter the password while creating/editing the monitoring configuration. Implemented a UI improvement that makes multiplication of the subscription administration easier: it provides a possibility to enroll multiple subscriptions using the same account without having to enter the credentials for every subscription * Fixed issue: alerts were not delivered if the discovered entity had an alert in the past (before SCOM discovered the entity) * Fixed issue: Azure Application Insights alerts were missing the links back to the Azure portal * Added a feature: if new Azure virtual machines are discovered or existing ones are removed, a corresponding alert is displayed in SCOM console. * Reduced the latency of event generation when a condition occurs in the Azure virtual machine. * Reduced the latency for virtual machines provisioned in Azure to show up in SCOM. * Implemented a task to query for inventory of all the Azure virtual machines. * Updated the display strings to match the recent changes. * Added a new section to the guide: “Appendix: Display Strings Changes History” |
| July 2016 (version 1.3.22.0) | * Fixed issue: due to the deadlock of Storage Account Capacity Probe threads, Storage Account Size Performance Collection rule did not work, and the corresponding performance counters were not collected. * Fixed issue: service type page did not display all instances in the Add Monitoring wizard when there were more than 1000 instances. * Fixed issue: storage account state view did not display non-classic storage accounts. * Fixed performance stability issue observed while monitoring large subscriptions (1000+ objects): all management pack components (objects monitoring, objects discovery and counters collection) did not work. * Added support for China subscriptions; for details, see the Azure in China and Azure for the US Government section * Fixed issue with “Add subscription” wizard pertaining to China subscriptions; added a corresponding guidance regarding the required user activity for China subscriptions monitoring, see the corresponding Note * Implemented monitoring of Azure Application Insights alerts for web tests; for more details, see the Application Insights Configuration section * The “Appendix: Known Issues” section of the guide is updated. * Updated information about Run As Profiles configuration: Run As Profile Proxy is to be configured manually; see the Security Configuration section for details |
| March 2016 (version 1.3.18.0) | * Added support for Virtual Machines (non-classic) in addition to Classic Virtual Machines supported previously. * Improved logging for the case when RDFE resources request is performed under SPN mode. * Fixed/added display names and Knowledge Base articles * Improved error logging * Fixed resource group name validation issue (underscore symbols in resource group names led to discovery fails) * Added the “Configure Proxy Connection” section to the guide. * Fixed Data Warehouse performance issue; added the main aggregation for performance metrics. * The “Appendix: Known Issues” section of the guide is updated |
| October 2015 (version 1.3.10.0) | The original release of this guide |

### Supported Configurations

This management pack requires System Center Operations Manager - SCOM 2016, SCOM 2019 and SCOM 2022.

Updated H5 dashboard for Azure MP (v1.8.0.2 and higher) requires SCOM 2019 UR1 at least.

Gateway Server Support – Gateway as a standalone Management Pool, Gateway, and Operations Manager in same Management Pool, 2 Gateways and Operations Manager in same Management Pool.

|  |  |
| --- | --- |
| Configuration | Support |
| System Center 2016, 1801 Operations Manager | Supported by this management pack |
| System Center 2019 Operations Manager | Supported by this management pack |
| Upgrade from previous versions of the management pack | See [**Upgrade**](#_Upgrade)section for more information. Upgrade from **6.1**.x.x versions of the System Center Management pack for Windows Azure Applications and **1.1**.x.x, **1.3.10.0, 1.3.18.0** versions of the System Center Management Pack for Windows Azure - **Not supported.** |
| Coexistence with previous versions of the management pack including:  **6.1**.x.x versions of the System Center Management pack for Windows Azure Applications  **1.1**.x.x, **1.3.10.0, 1.3.18.0, 1.5.x.x,1.8.x.x** versions of the System Center Management Pack for Windows Azure | Not supported |
| Internet connectivity to Microsoft Azure | Management Server Pool requires connectivity to Microsoft Azure.  The Operations Manager console used to configure the management pack requires connectivity to Microsoft Azure |
| Clustered servers | N/A |
| Agentless monitoring | Not supported |
| Virtual environment | N/A |
| .Net Framework | Management Server Pool requires .Net 4.5  The Operations Manager console used to configure the management pack requires .Net 4.5 |
| Gateway Server | Supported:  -Gateway as a standalone Management Pool  -Gateway and Operations Manager in same Management Pool - 2 Gateways and Operations Manager in same Management Pool  Configuration notes:   * It is important to install on a Gateway Server console of same version as Management Server has to avoid missing libraries issue. * DNS resolution is required for Gateway to communicate to SCOM server. * In Operations Manager Administration – Management servers –properties validate that “Allow this server act as a proxy” is checked for the Gateway server |

### Upgrade

|  |  |
| --- | --- |
| Upgrade from | Details |
| 1.8.0.8 | To upgrade to Azure MP with latest version (1.8.0.9), below steps should be followed.   * Install the Latest MSI from the [DLC](https://www.microsoft.com/en-us/download/details.aspx?id=58013) and import the Azure MP to the SCOM console. * To import newer version of MP in Operations Manager, go to Administration-> Installed Management packs-> select “Import Management Packs” in Tasks pane-> select ‘*Microsoft.SystemCenter.MicrosoftAzure.mpb*-> click on import. * Once new MP imported, run “**Obtain Service Types and Performance Counters Data**” task from Monitoring Pane > Task Status > Microsoft Azure Subscription Tasks. * Perform ‘*Refresh data*’ in Azure MP template. Since namespace data was not collected in previous template, this helps to collect it. * For the UI changes to be reflected, edit template data, and save it. |
| 1.8.0.5 | To upgrade to Azure MP with latest version (1.8.0.8), below steps should be followed.   * Install the Latest MSI from the [DLC](https://www.microsoft.com/en-us/download/details.aspx?id=58013) and import the Azure MP to the SCOM console. * To import newer version of MP in Operations Manager, go to Administration-> Installed Management packs-> select “Import Management Packs” in Tasks pane-> select ‘*Microsoft.SystemCenter.MicrosoftAzure.mpb*-> click on import. * Once new MP imported, run “**Obtain Service Types and Performance Counters Data**” task from Monitoring Pane > Task Status > Microsoft Azure Subscription Tasks.      * Perform ‘*Refresh data*’ in Azure MP template. Since namespace data was not collected in previous template, this helps to collect it. * For the UI changes to be reflected, edit template data, and save it. |
| 1.8.0.2 | To upgrade to Azure MP with latest version (1.8.0.5), below steps should be followed.   * Install the Latest MSI from the [DLC](https://www.microsoft.com/en-us/download/details.aspx?id=58013) and import the Azure MP to the SCOM console. * To import newer version of MP in Operations Manager, go to Administration-> Installed Management packs-> select “Import Management Packs” in Tasks pane-> select ‘*Microsoft.SystemCenter.MicrosoftAzure.mpb*-> click on import. * Once new MP imported, run “**Obtain Service Types and Performance Counters Data**” task from Monitoring Pane > Task Status > Microsoft Azure Subscription Tasks. * Perform ‘*Refresh data*’ in Azure MP template. Since namespace data was not collected in previous template, this helps to collect it. * For the UI changes to be reflected, edit template data, and save it. * Since the name is changed for H5 dashboard MP, we need to delete older version and then import 1.8.0.5 version if customer is using 1.8.0.2 version. * To delete older MP in Operations Manager, go to Administration-> Installed Management packs-> search for ‘*Microsoft.SystemCenter.HtmlCustomDashboard.mp*’-> right click-> select ‘delete’ * To import newer version of MP in Operations Manager, go to Administration-> Installed Management packs-> select “Import Management Packs” in Tasks pane-> select ‘*Microsoft.SystemCenter.MicrosoftAzure.HtmlCustomDashboard.mp*’-> click on import. |
| 1.8.0.1 | * Close and re-open SCOM console. * Perform ‘*Refresh data*’ in Azure MP template. Since namespace data was not collected in previous template, this helps to collect it. * For the UI changes to be reflected, edit template data, and save it. * We need to delete older version and then import 1.8.0.2 version if customer is using 1.8.0.1 version. * To delete older MP in Operations Manager, go to Administration-> Installed Management packs-> search for ‘*Microsoft.SystemCenter.HtmlCustomDashboard.mp*’-> right click-> select ‘delete’ * To import newer version of MP in Operations Manager, go to Administration-> Installed Management packs-> select “Import Management Packs” in Tasks pane-> select ‘*Microsoft.SystemCenter.MicrosoftAzure.HtmlCustomDashboard.mp*’-> click on import. |
| 1.7.0.0 | * Close and re-open SCOM console. * Perform ‘*Refresh data*’ in Azure MP template. Since namespace data was not collected in previous template, this helps to collect it. * For the UI changes to be reflected, edit template data, and save it. * We need to delete older version and then import 1.8.0.1 version if customer is using 1.7.0.0 version. * To delete older MP in Operations Manager, go to Administration-> Installed Management packs-> search for ‘*Microsoft.SystemCenter.HtmlCustomDashboard.mp*’-> right click-> select ‘delete’ * To import newer version of MP in Operations Manager, go to Administration-> Installed Management packs-> select “Import Management Packs” in Tasks pane-> select ‘*Microsoft.SystemCenter.MicrosoftAzure.HtmlCustomDashboard.mp*’-> click on import. |
| 1.6.0.7 | **Case 1:** Scheduled Query rule or Activity log alert or Metric alert objects discovered in previous version of management pack and/or displayed as NOT monitored.  **Upgrade Steps:**  Action is needed to re-generate template for supporting new introduced features that have been discovered before as NOT monitored.  For this, any checkbox in Service types tab needs to be unchecked or checked, and template saved.  In Authoring pane go to subscription Wizard >Service types tab > uncheck or check any greyed out service type (for example, for disks or schedules) and save template. Greyed out in Wizard services do not have metrics and pre-defined performance rules and action will have less impact on monitoring.  **Note.** Alternatively, you can uncheck related checkboxes for**: -**Scheduled Query rule  - Activity log alert  - Metric alert objects  Save template, await objects get undiscovered, and after upgrade enable checkboxes again.  **Case 2:**  Scheduled Query rules, Activity log alert, Metric alert objects are not present in management pack.  Upgrade will pass. No additional actions required. |
| 1.5.20.18 | **Case 1:**  Scheduled Query Rule or Activity Log Alert or Metric alert objects discovered in previous version of management pack and displayed as NOT monitored.  **Upgrade Steps:**  Action is needed to re-generate template for supporting new introduced features that have been discovered before as NOT monitored.  For this any checkbox in Service types tab needs to be unchecked or checked, and template saved.  1. In Authoring pane go to subscription Wizard >Service types tab > uncheck or check any greyed out service type (for example, disks or schedules) and save template. Action on greyed-out services in Azure MP Wizard will have less impact on monitoring.  2. Step 1 must be repeated for each subscription template that had metric alerts, scheduled query rules or activity logs alerts discovered before upgrade.  **Note.** Some temporary events might occur with event id 10801 in Operations Manager eventlog.  **Case 2:**  Scheduled Query rules, Activity log alert, Metric alert objects are not present in management pack.  Upgrade will pass. No additional actions required. |
| 1.5.0.0 | Import on top of previously installed MP will pass. It is **important** re-create template in Authoring pane. |
| Versions earlier than 1.5.0.0 | Not Supported.  Old Management pack should be uninstalled before installing new one. |

## Management Pack Scope

The management pack for Microsoft Azure enables you to monitor the availability and performance of Azure resources. The management pack runs on a specified server pool (Management Server or Gateway Server) and then uses Microsoft Azure REST APIs to remotely discover and collect performance information about Microsoft Azure resources.

This management pack focuses on the collection of performance metrics made available by Azure Services that use Azure Resource Manager.

Azure Active Directory is used for authenticating Azure REST API calls.

1.8.0.5 version of Azure MP MSI also includes H5 Dashboard MP that provides a light-weight interface with essential functionality to view the monitoring data of subscriptions, resource groups, service types, active alerts, and performance metrics at-a-glance. Within the network, H5 dashboard can be accessed from anywhere via browser URL. No need to connect to Operations console explicitly.

This management pack queries Azure REST APIs to enumerate the resources running in the Azure subscription and the performance metrics available for each resource.

Some service types might not have any metrics or any pre-defined monitors in SCOM, but still can be monitored through the relationships that Azure MP builds.

Examples of services that can be discovered, and whether performance counters are available for collection, are presented in the table below.

| **Service** | **Discovered** | **Performance Counters** | **Notes** |
| --- | --- | --- | --- |
| Application Insights | Yes | Yes |  |
| Automation | Yes | No |  |
| Backup | Yes | No |  |
| BizTalk | Yes | No |  |
| Cloud Service (web and worker roles) | Yes | No |  |
| Data Factory | Yes | Yes | Data factories version 1 only discovered, performance collection and monitoring for data factories version 1 is not supported |
| DocumentDB | Yes | No | Metrics are not available in the Add Monitoring wizard |
| Logic App | Yes | No |  |
| Media Services | Yes | No | Supported in UPN mode only. This RDFE resource is exposed by Azure Service Manager (ASM) that uses different deployment model also termed as Classic Deployment model |
| Mobile Services | Yes | Yes | Supported in UPN mode only. This RDFE resource is exposed by Azure Service Manager (ASM) that uses different deployment model also termed as Classic Deployment model |
| Networks | Yes | No | Supported in UPN mode only. This RDFE resource is exposed by Azure Service Manager (ASM) that uses different deployment model also termed as Classic Deployment model |
| Notification Hubs | Yes | No |  |
| Operational Insights | Yes | No |  |
| Redis Cache | Yes | Yes |  |
| Scheduler | Yes | No |  |
| Search | Yes | No |  |
| Service Bus | Yes | Yes |  |
| SQL Azure | Yes | Yes |  |
| Storage Accounts | Yes | Yes | Performance collection and monitoring for Classic storage accounts is not supported |
| Traffic Manager | Yes | No | Supported in UPN mode only. This RDFE resource is exposed by Azure Service Manager (ASM) that uses different deployment model also termed as Classic Deployment model |
| Virtual Machines | Yes | Yes | Virtual machines also appear as role instances for Cloud Services |
| Websites | Yes | Yes |  |
| Application Gateways | Yes | Yes |  |
| Event Hubs | Yes | Yes |  |
| SQL Servers | Yes | Yes |  |
| HDInsight clusters | Yes | Yes |  |

As soon as new Azure services are released (and older services are moved to the new Azure Resource Manager), they will be discovered automatically. As soon as the services expose performance counters via the metrics API, they will become available for collection.

Note that availability monitoring can be applied to the following monitors only:

* Subscription Certificate Monitor
* Virtual Machine (non-classic) Turnoff Monitor
* Classic Virtual Machine Turnoff Monitor
* Hosted Service Certificate Monitor
* Insights Classic Metric Alert Monitor
* Insights Metric Alert Monitor
* Insights Activity Log Alert Monitor
* Insights Scheduled Query Rule Monitor

Virtual Machine (non-classic) Turnoff, Classic Virtual Machine Turnoff, Hosted Service Certificate, Classic Metric Alert, Insights Metric Alert, Insights Activity Log Alert and Insights Scheduled Query Rule monitors extend the possibility of availability monitoring to Cloud Service via health roll-up.

Insights Scheduled Query Rules, Insights Activity Logs and Insights Metric Alert are **highly recommended for selection**, as they provide integration of Azure Alerts in SCOM.

## Prerequisites

User must manually ensure that the prerequisites are met.

### The following requirements must be met to run this management pack:

* User must have an Operations Manager SCOM 2016, SCOM 2019 and SCOM 2022 or later environment. This management pack will not import on Operations Manager 2007 R2 or Operations Manager 2012.
* Due to certain performance issues, a separate management server should be dedicated for this management pack.
* All management servers in the management server pool must have a connection to the Internet to communicate with Microsoft Azure.
* All management servers in your management server pool must have .Net framework 4.5 or newer installed.

The management pack has a monitoring rule, which detects .Net framework version on Management Servers. You can find Management Servers with .Net 4.5 missing by looking to “Active Alerts” view in “Microsoft Azure” folder.

* The workstation with the Operations Manager console, which will be used to configure Microsoft Azure monitoring, must have a connection to the Internet in order to communicate with Microsoft Azure during the initial configuration process.
* The workstation with the Operations Manager console, which will be used to configure Microsoft Azure monitoring must have .Net framework 4.5 or newer installed.
* For collecting event and performance data from Azure VMs, Web roles and Worker roles, Microsoft Azure Diagnostics must be enabled.   
  For more information about Microsoft Azure Diagnostics, see the [Collect Logging Data by Using Windows Azure Diagnostics](https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-dotnet-diagnostics) article
* Microsoft Azure Diagnostics must be configured to forward diagnostic data to a Microsoft Azure storage. For more information about configuring Microsoft Azure Diagnostics, see the [Store and view diagnostic data in Azure Storage](https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-dotnet-diagnostics-storage) article.

## Azure MP Authentication

Azure MP requires either Azure Active directory user or Application in Azure.

Azure Management Pack supports two authentication modes: Azure Active Directory User Principal Name (UPN) and Service Principal Name (SPN).

**NOTE: We strongly recommend using Service Principal Name mode of authentication. Service Principal Name can be auto created using Azure MP through SCOM.**

To create SPN manually, follow steps below.

#### Create Azure Active Directory Service Principal Name (SPN)

SPN works in any environment and allows assigning permissions in a more flexible way. Using a service principal allows the management pack to be used in environments with multi-factor authentication. For more details on Azure Active Directory Service Principal Name, click [here](https://docs.microsoft.com/en-us/powershell/azure/create-azure-service-principal-azureps?view=azps-3.0.0).

Go to Azure Active directory in azure portal. Go to app registrations. Create SPN by using new registration. After that grant at-least reader permission to the SPN in the Azure subscription.

For more details, click [here](https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal).

Note: User should grant at-least reader permission to the SPN in the Azure subscription to use it in Authoring wizard in SCOM console.

#### Create Azure Active Directory User Principal Name

UPN is simpler to configure, but it does not work when multi-factor authentication is enforced. For more details on Azure Active Directory User Principal Name, click [here](https://docs.microsoft.com/en-us/powershell/module/azuread/?view=azureadps-2.0#users).

**Note:** To monitor RDFE resources or run some service tasks directly from Operations Manager Console, user account requires co-administrator permissions on subscription.

## Mandatory Configuration

Azure MP requires Azure subscription details and monitoring template to monitor your Azure resources. This section explains how to configure Management Pack for Microsoft Azure to discover and monitor Azure resources.

The following steps are essential:

1. Import management pack.
2. Add Microsoft Azure Subscriptions in the Operations Manager **Administration** pane.
3. Add resources for monitoring by the wizard in the Operations Manager **Authoring** pane.

### 1. Import Management Pack

In Operations Manager go to Administration > Installed Management packs>select “Import Management Packs” in Tasks pane.

### 2. Add Microsoft Azure Subscriptions

To add a new Microsoft Azure Subscription, go to the Operations Manager console, navigate to the Administration pane, and then select “Microsoft Azure” node.

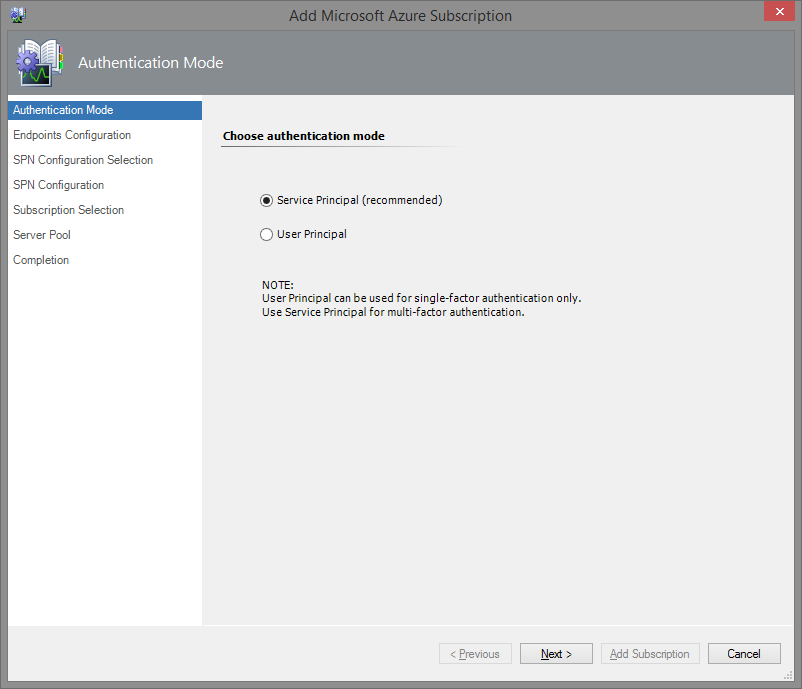
A screenshot of a cell phone

Description automatically generated A screenshot of a social media post

Description automatically generated

Click “**Add subscription**” to connect the Operations Manager with Microsoft Azure subscription. As a result, **Authentication Mode** window of Add Microsoft Azure Subscription wizard will be displayed. In this window, select the preferred authentication mode. To configure the monitoring, Service Principal Name or User Principal Name can be used.

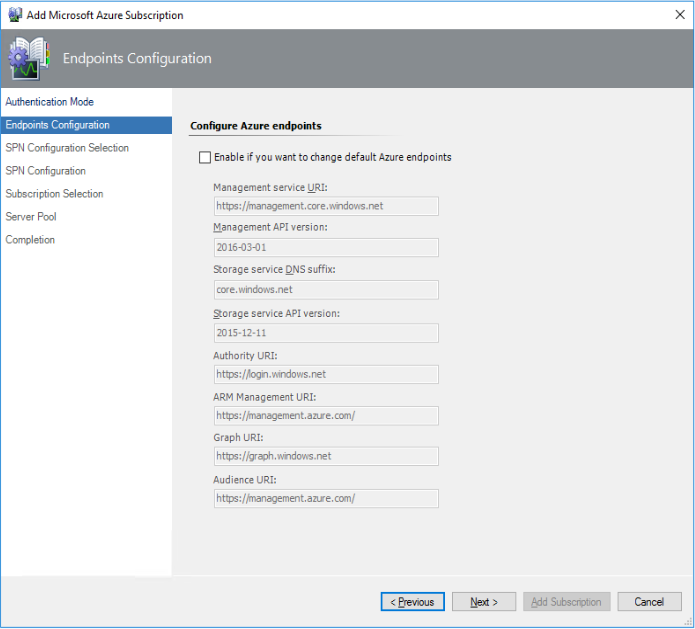
Since UPN can be used for single-factor authentication only, **it is strongly recommended to use SPN** for the monitoring.



Note: There is no limitation to number of subscriptions being monitored, however it is recommended to use maximum of 10 subscriptions in a single management server. Creation of template is limited to one for each Azure subscription.

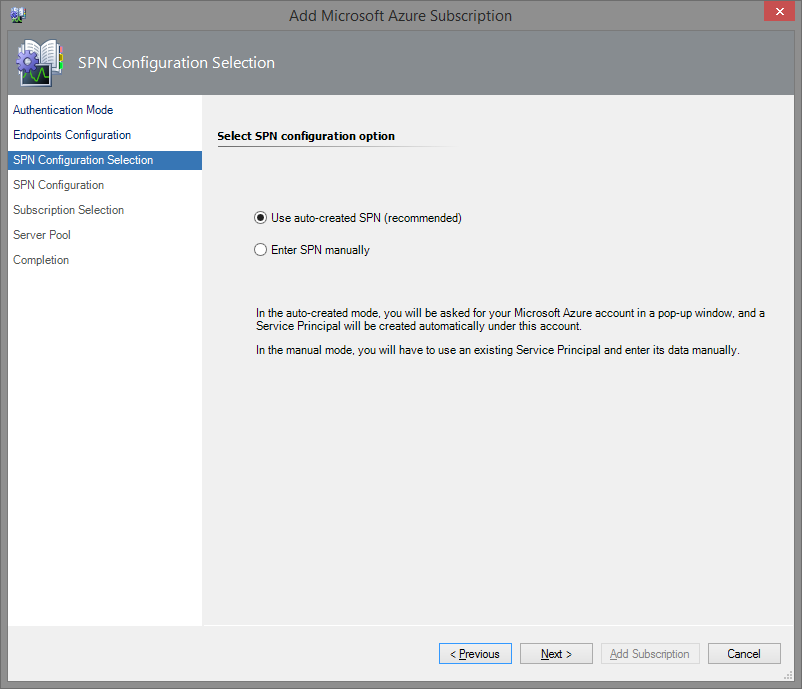
#### Azure Service Principal Authentication Mode

If Service Principal Authentication mode has been selected, **Endpoints Configuration** window will be displayed upon clicking the **Next** button.

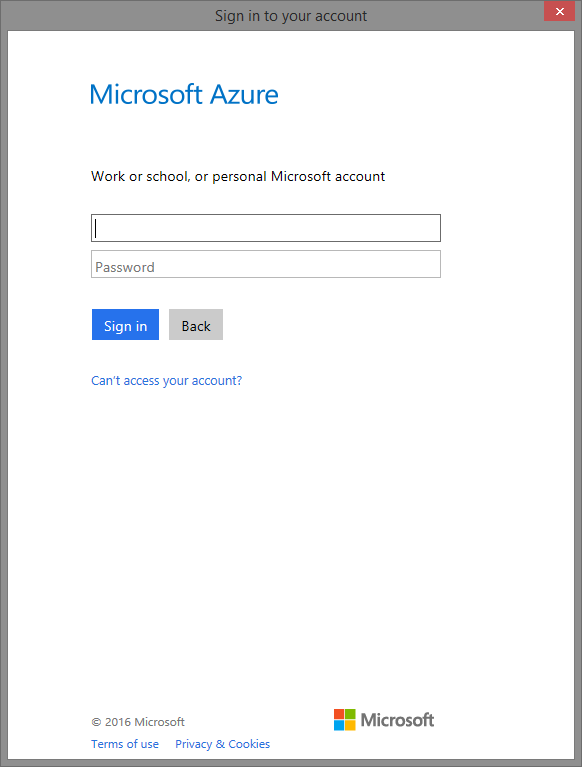


**Note:** Default Endpoints are hardcoded and displayed in Endpoints configuration view.

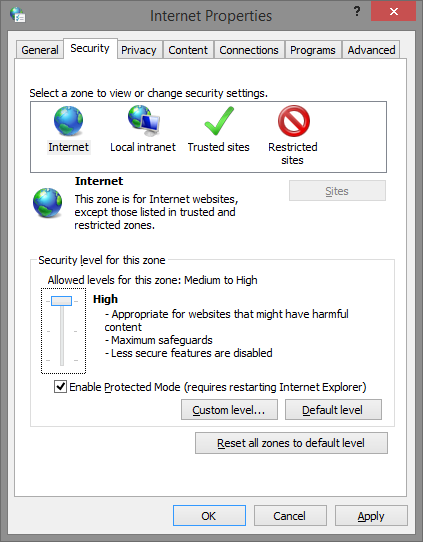
If user wants to change the default Azure endpoints, user should check the corresponding checkbox. In the following **SPN Configuration Selection** window, user should choose whether to create an SPN in automatic mode or to enter existing SPN data manually.



If you choose to create an SPN automatically, the Microsoft Azure sign-in window will be displayed upon clicking the Next button. In this window, fill in your work, school or personal Microsoft account credentials and click Sign in button.



Note: If you use Internet Explorer as a default Internet browser, you may receive multiple security alerts on this step. To solve this issue, go to the Security section of the Internet Properties and lower the security level for the Internet zone.



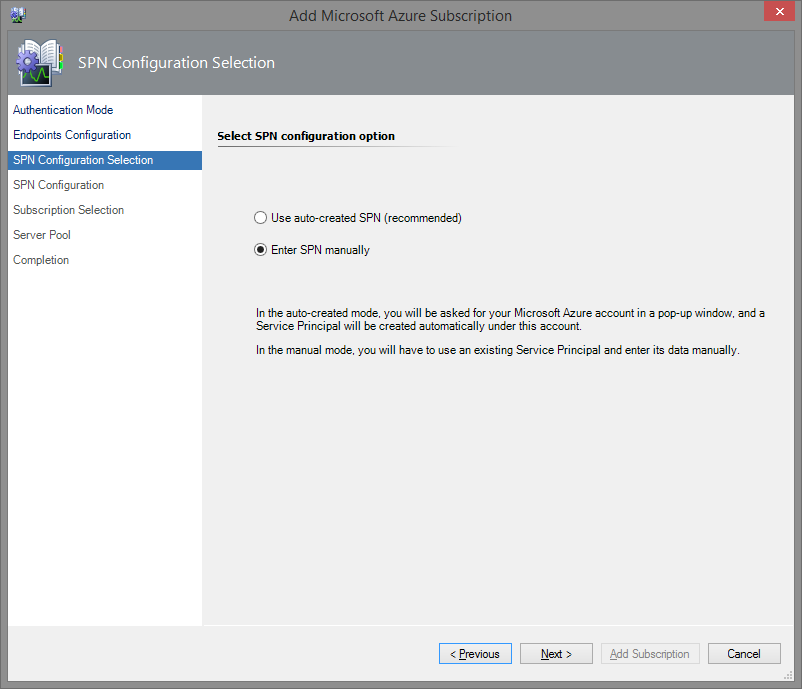
Upon successful creation of the application, the corresponding authentication data will be displayed in the **SPN Configuration** window.

A screenshot of a cell phone

Description automatically generated

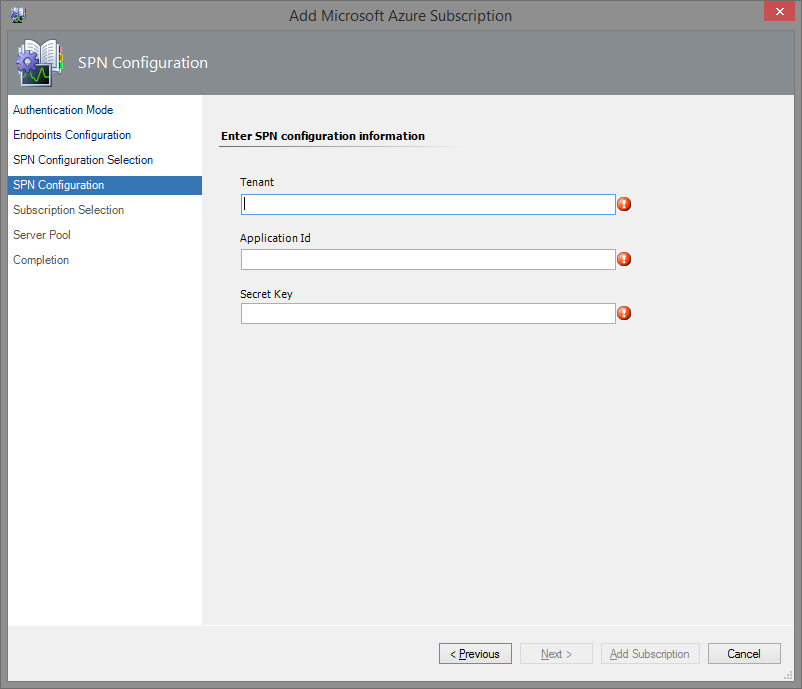
**Important: it is strongly recommended to save this data for further usage!**

If you choose to enter your existing SPN data manually, select the corresponding option.

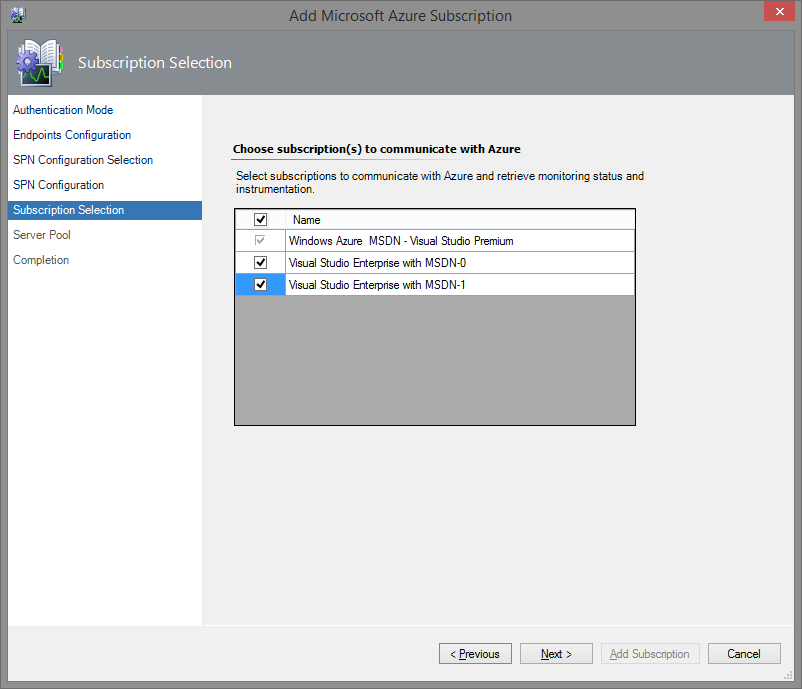


In this case, you must enter your SPN data manually in the following **SPN Configuration** window.

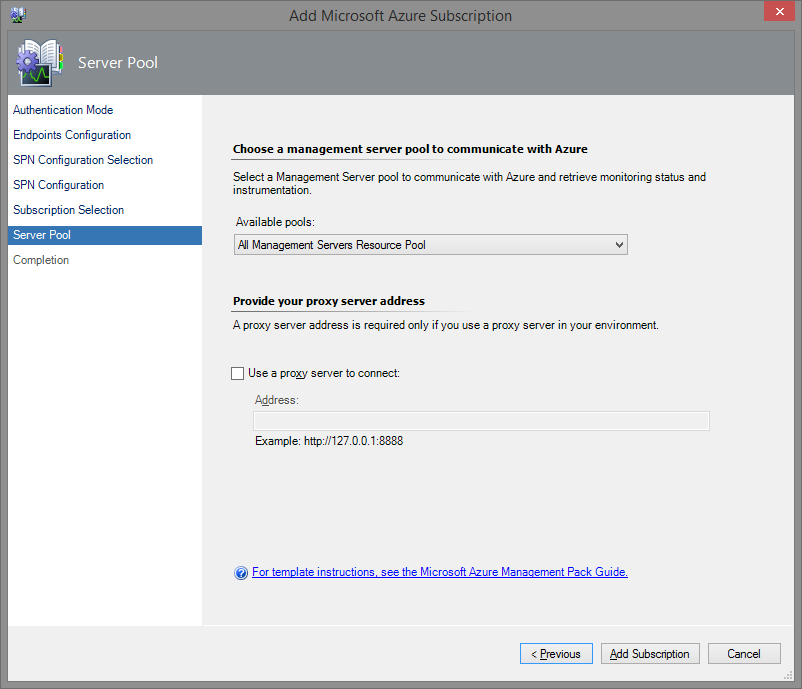
**Note:** If you want to create a new SPN, see the [Create Azure Active Directory Service Principal](#_Creating_Azure_Active_1) section for details.



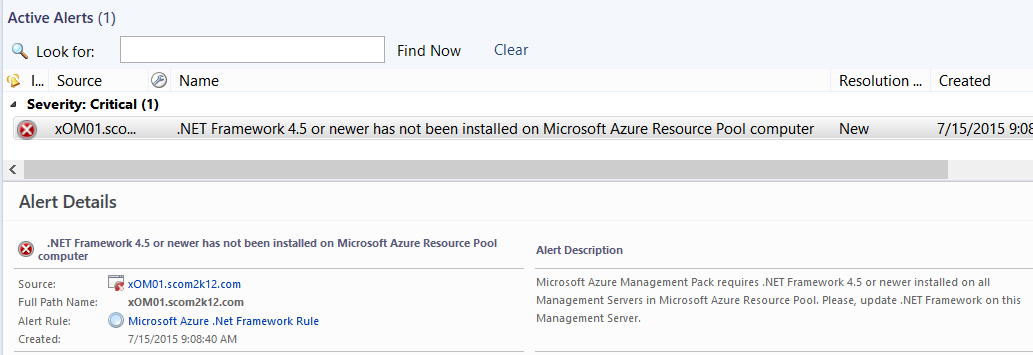
The next steps of the wizard are the same for both options mentioned above. In the **Subscription Selection** window, select subscriptions to communicate with Azure and retrieve the monitoring status and instrumentation.



In the **Server Pool** window, you should select a Management Server pool from the dropdown list to communicate with Azure. If you use a proxy, you can also configure the proxy server settings in this window.



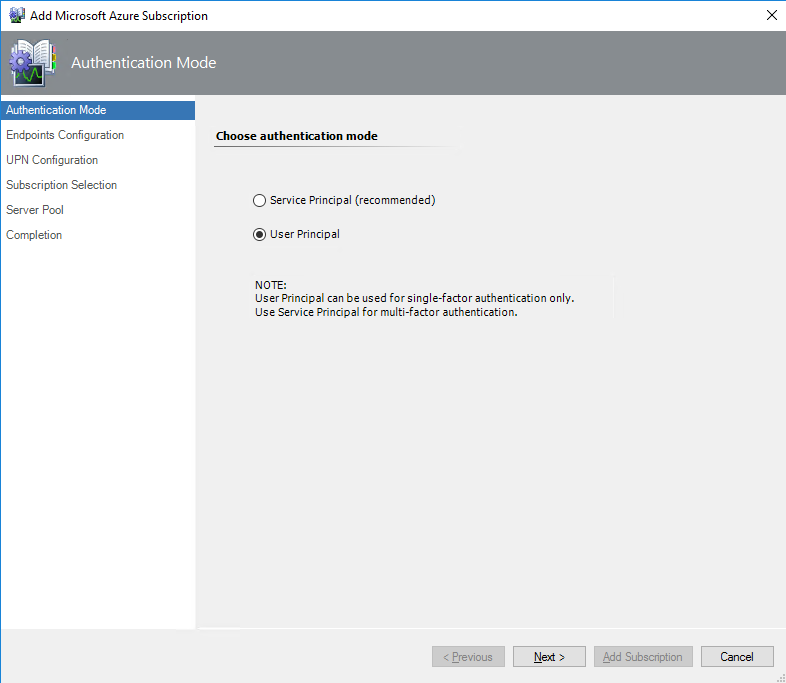
**Note:** If you select a management server pool that does not have .Net 4.5.2 installed, you will receive an alert notifying you of the missing/incorrect .Net version.



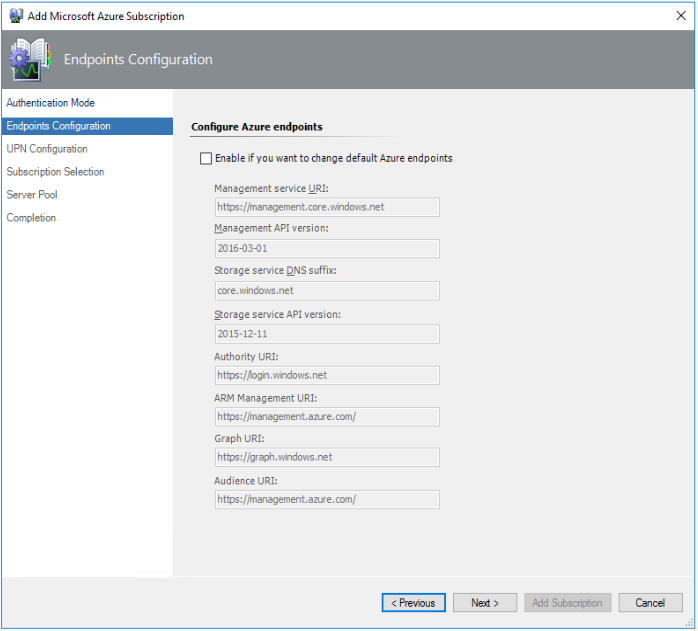
Upon clicking the Add Subscription button, the configuration will be completed.

#### Azure User Principal Authentication Mode

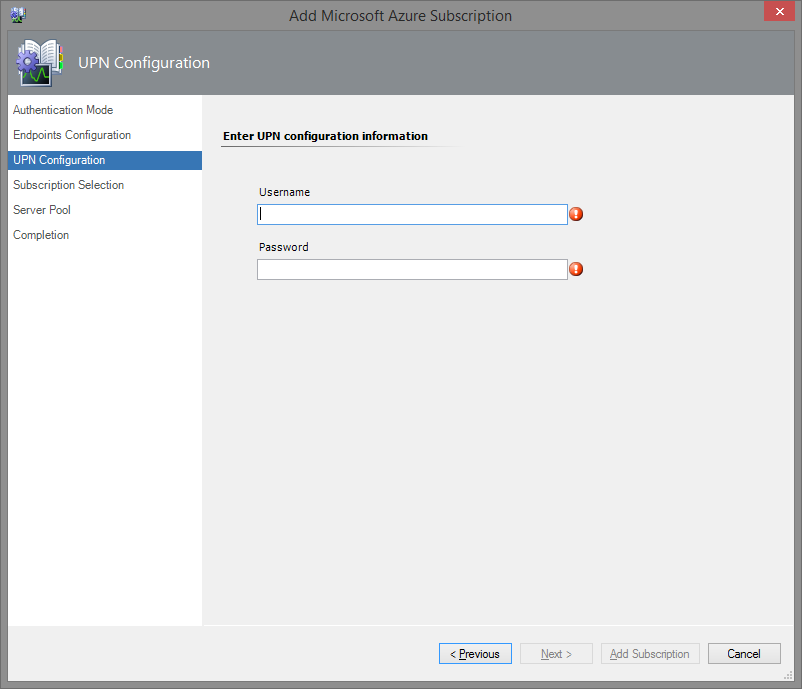
If you want to use User Principal Name for monitoring, select the corresponding option in the **Authentication Mode** window.



The **Endpoints Configuration** window will be displayed upon clicking the **Next** button.



In the following **UPN Configuration** window, enter your existing User Principal Name credentials.



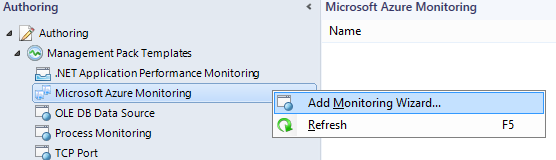
**Note:** If you want to create a new UPN, see the [Create Azure Active Directory User Principal Name](#_Creating_Azure_Active) section for details.

The rest configuration steps are the same as in the section above.

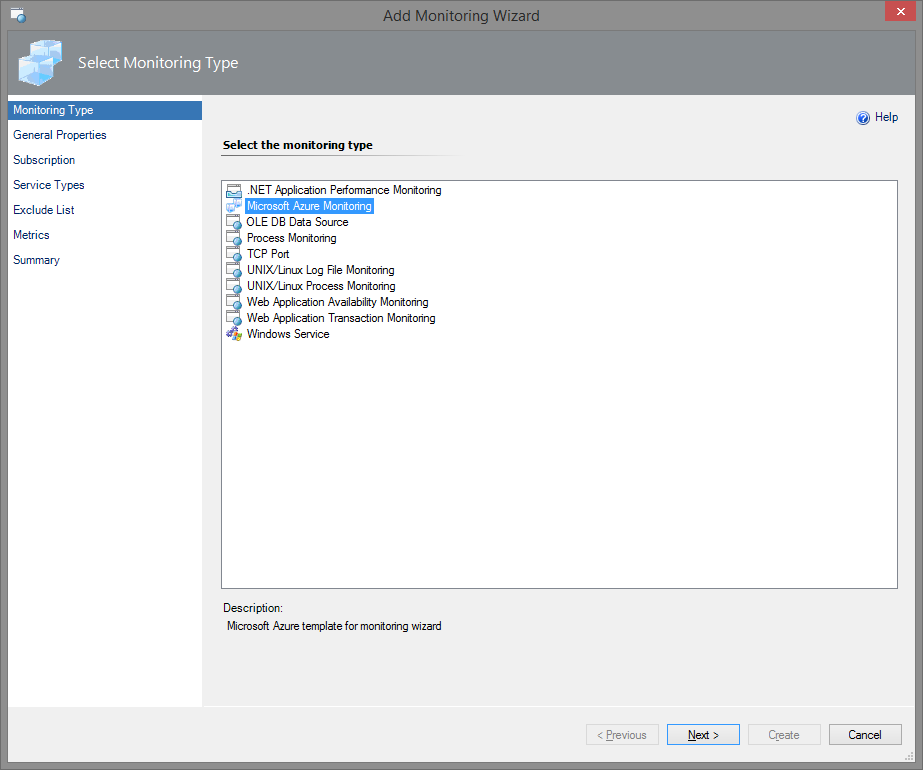
### 3.Select Resources to Monitor in Wizard

After you have completed the “Add Subscription” wizard, you will need to specify the Microsoft Azure Resources you want to discover and monitor. To do that, perform the following steps:

Navigate to **Authoring** Pane of the Operations Manager Console and select the “Microsoft Azure Monitoring” template.



As a result, the **Monitoring Type** window of the wizard will be displayed.



Select the “Microsoft Azure Monitoring” option and click the **Next** button.

#### Create a New Management Pack to Store Subscription Configuration

In the General **Properties** window, enter a name and a corresponding description for the new management pack template instance.

A screenshot of a social media post

Description automatically generated A screenshot of a social media post

Description automatically generated

Choose **New…** destination for the management pack to store the information about the template instance of the management pack. Enter the details for the new destination management pack and click the **Next** button. Click the **Create** button to create the new destination management pack.

**Recommendation:** Save the template for each subscription into a separate management pack. This will let you export the management packs into a different Operations Manager environment and simplifies customization.

#### Select a Subscription to Monitor

In the **Subscription** window, select a subscription.

A screenshot of a social media post

Description automatically generated

Note. Warning might occur in Wizard with recommendation to set up Operations Manager server if more than 1000 instances monitored.

Selection Mode:

* Service type flow will allow you to monitor all instances of service type for the subscription. For example, if you want to monitor all the virtual machines under your subscription, irrespective of what resource groups they are in, select this mode.

A screenshot of a social media post

Description automatically generated

* Resource group mode will allow you to monitor resources which are grouped under resource groups for the selected subscription.

#### Select Resource Groups to Monitor

For the selected subscription you will see all the Resource Groups. You can select resource groups that you want to monitor. For the selected resource groups, relevant resources will be displayed in next screen.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

Azure Portal Resource Group View Azure MP Resource Group View

#### Select Service Types to Monitor

* Select specific service types for the selected resource group(s) to monitor
* For the selected service types, health state and Azure alerts will be displayed in SCOM.

For the service types which are greyed out, any alert configured in portal would be visible in SCOM. However, there will be no performance data for such service types.

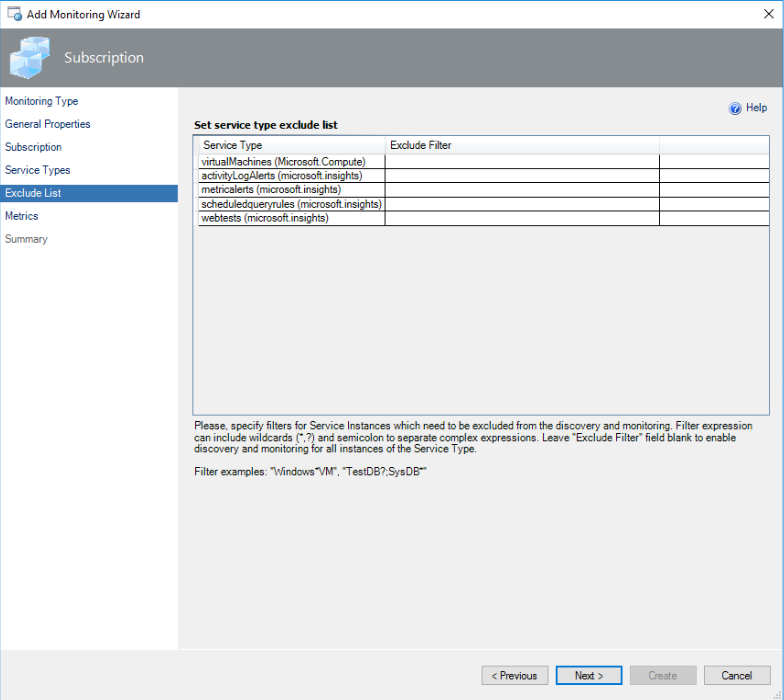
Relations can be investigated in the Operations Manager health rollups based on services selected in Wizard. For example, in DEMO-LAB Resource Group, we have 2 VM in portal and SCOM shows 2 instances of these VM. If you will select Virtual Machine, both Virtual Machine in DEMO-LAB Resource Group will be monitored along with Azure alerts configured on these VMs.

A screenshot of a cell phone

Description automatically generated A screenshot of a social media post

Description automatically generated **Azure Portal Resources View** **SCOM Resources View**

#### Configure the Exclude List

By default, all instances of a service are discovered and monitored. If there are instances of services you do not want to collect metrics for, you can exclude them from discovery and monitoring in the **Exclude List** window. You can use wildcards (\*,?) to pattern match on the instance name and use a semicolon (;) to specify multiple instances to exclude.**Note:** Instances of the services discovered by means of the older versions of the Service Management API cannot be excluded.

#### Select Metrics to Monitor

In the next window, review the list of **Metrics** available for the selected service types. It is grouped by service type. For each metric, there are the following properties available:

* Metric Title
* Metric Units
* Aggregation Type (e.g. “Total”, “Average”, etc.)

Note: To collect performance metrics for the selected service type, check ‘Collect Data’ checkbox.

To receive a SOCM alert for the collected performance metrics, check ‘Alert If’ check box and define the threshold value.

A screenshot of a social media post

Description automatically generated

**Note:** Monitoring artifacts will be generated even if the “Alert If” checkboxes are not enabled; though, they will be displayed as disabled.

The ‘Summary’ page shows the service types and performance metrics details.

A screenshot of a cell phone

Description automatically generated

A progress indicator will be displayed until the monitoring rules are generated.

A special group of objects is added to the created template. Each of the objects receives its own property containing the subscription ID.

### 4.H5 Dashboard Views for Azure Management Pack

Azure Management Pack dashboard requires web console. Install web console with steps given:

Step1. Import **Microsoft.systemcenter.HtmlCustomDashboard** MP that is part of Azure MP msi.

Step2: Log into http://<XXX>/OperationsManager/#/monitoring/view -> where XXX is SCOM server.

A screenshot of a cell phone

Description automatically generatedOnce the web console is setup, you can browse to Monitor Azure Dashboard as shown in image.

**All H5 Azure dashboards adhere to Pagination, Sorting and Column resizing options.**

**Subscriptions Dashboard:** This Dashboard shows you the summary of your configuration. So, you can quickly check the **Health state and Alerts summary** for each subscription.A screenshot of a cell phone

Description automatically generated

**Resource Groups dashboard**: A view which displays all the “Resource Groups” across subscriptions. When filtered for Subscription, the corresponding Resource groups for the filtered subscription are displayed. This can be further filtered to choose a resource group or health state.

**A screenshot of a cell phone

Description automatically generated**

**All Resources dashboard**: A consolidated view to display all the Azure resources in SCOM. In the below image resources are filtered for “SCOM MP Test Infra” subscription.

Name column shows the Azure resource name, Type shows the resource type and Resource Group shows under which resource group this resource is available.

If you want to monitor All the critical Virtual machines which start with TestVM in Subscription X and Resource Group ABC, then you can do it with the provided filters.

Graphical user interface, text, email, website

Description automatically generated  
Graphical user interface, text, application

Description automatically generated

You can choose to further drill down for a resource and see the active alerts and performance data as shown in the image.

**A screenshot of a social media post

Description automatically generated**

**Active Alerts dashboard**: This dashboard lists all active alerts from added subscriptions. Name column shows the alert name, Signal Type shows either the alert is Metric\Activity Log\Log\SCOM Alert, Age column display alert’s age, Last Modified column shows when the alert is last modified. This list also shows Affected Resource Count and Affected resources.

Filtering option is also available to filter alerts based on subscription\Signal Type\Severity along with Name filter.

A screenshot of a cell phone

Description automatically generated

You can choose to further drill down for an alert and see alert information as shown in the image.

A screenshot of a social media post

Description automatically generated

### Modified Alert Description in Operations Manager

To ensure that SCOM is not flooded with Azure alerts, SCOM has modified the way alerts are displayed in SCOM.

If multiple “Log-based alert” and “Activity log alerts” are fired in Azure on same resource, then we will increase the alert count and not show a new alert every time.

A screenshot of a social media post

Description automatically generated

**Support for** [**multi-resource target alert**](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-overview#monitoring-at-scale-using-metric-alerts-in-azure-monitor)

When an alert is defined for multi-resource, portal shows many alerts. While Azure MP will only show one alert and the alert description will show all the target resource name for which the alert is fired. This feature helps to not fill SCOM with redundant alerts. The health state of only the target resource for which alert is fired will change to critical.

A screenshot of a cell phone

Description automatically generated

## Features

This section contains information about management pack features configuration.

### Availability tests in Application insights

Management pack allows user to monitor notifications on issues with [Availability tests](https://docs.microsoft.com/en-us/azure/application-insights/app-insights-monitor-web-app-availability) (webtests) performed by Azure Application Insights. Health state of a web test in SCOM depends on Insights Incident Monitor state that checks information about alerts configuration through Azure REST API.

Below an example of a web test configuration with Near-Realtime alert (Metric Alert) :

* Open portal.azure.com in the browser, log in and navigate to "Application Insights" category
* Add a new Application Insight in Azure portal:
* Click "Add"
* For "Application Type" choose "ASP.NET web application"
* For "Subscription" choose a current active subscription
* Select a previously created "Resource group" or create a new one
* Select "location" and click "Create"
* Add a new Webtest in Azure portal:
* Click "Availability" tile on the Insight's dashboard
* Click "Add test"
* For “Test name” it is recommended to add “webtest” ending that will allow distinguish webtest alert rule from other alert rules in Azure.   
  Example: mysitenamewebtest
* For "Test Type" choose "URL ping test" or “Multi-step web test”
* For "URL" Enter the URL for ping test or Upload a file for “Multi-step web test”
* For "Success Criteria" choose values that will lead webtest to success
* Select "Alert type": Near-realtime (Metric Alert). This option will automatically create new Alert rule in Azure.
* Select Near-realtime alert status “Enabled”. This will enable alert notification.
* Choose optional values for other preferences and click "Create"
* Obtain Alert rule and it’s state in the Operations Manager:
* In Operations Manager alert rule will be discovered as a resource of type microsoft.insights/metricalerts
* Open Operations Manager Console and navigate to Monitoring > Microsoft Azure > Service State, filter results to find an expected microsoft.insights/components, /webtests, and /metricalerts objects. Check State (initial), Name, Service Type, and Service Location.
  + Healthy conditions.

If the web test is available from all the configured locations it’s state in Operations Manager will be Healthy, /metricalerts object that represents Enabled alert rule on Azure portal will also be in Heathy state.

* + Unhealthy conditions.

If the web test, for which alert rule enabled, is unavailable from the configured locations and threshold conditions has been exceeded, the state of the web test on Azure portal will be changed to Warning. Alert rule on Azure portal will have “Fired” monitor condition.   
In Operations Manager microsoft.insights/meritcalerts object for “Fired” alert rule condition will change state to Critical. Critical alert will arise in Operations Manager Console in Monitoring > Active Alerts view.

### Azure Alerts in Operations Manager

This section explains how user can obtain alerts for Azure resources in the Operations Manager.

There are several options to configure Operations Manager to raise alerts on the same service:

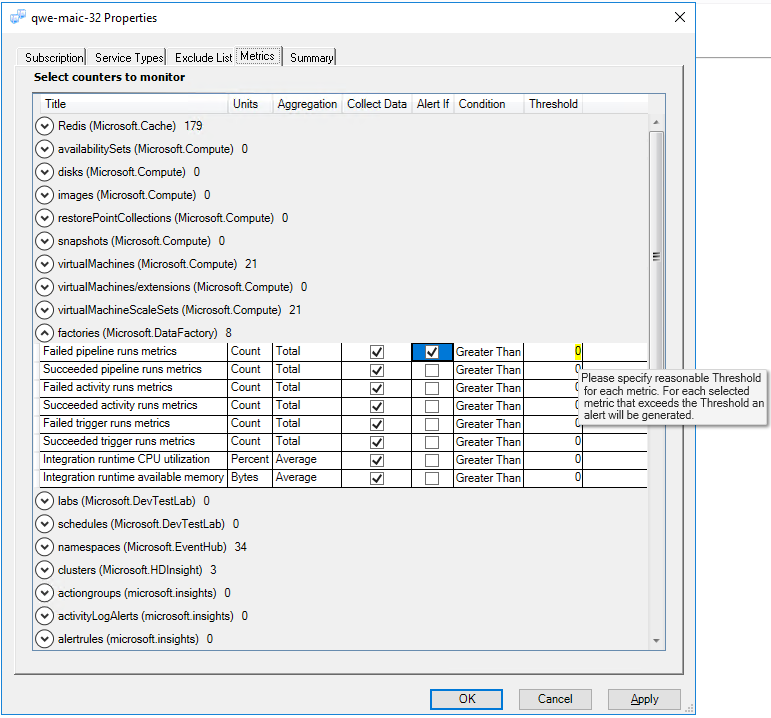
* “Alert if” condition in the Operations Manager Wizard that dynamically creates monitors on service performance Metrics in SCOM
* Using Insights rules on Metrics (recommended):
* Metric Alerts (alternative to “Alert if”)
* Classic Metric Alerts (alternative to “Alert if”, planned to be deprecated in June,2019 )
* Insights Scheduled Query Rules
* Insights Activity Log Alerts

#### “Alert if” Metric Alerts in SCOM Wizard

Alert on metric notifications can be configured through Wizard during initial management pack configuration or, if a template has already been created, double click on it in Authoring pane and open Metrics tab in the Operations Manager Console.

“Alert if” option in Wizard unchecked by default. It is made to avoid alert storming issue. If the threshold is left with ‘0’ value, all monitors, for which metrics exceeded the condition, will raise Warning alert.

The user is advised to configure a reasonable threshold.



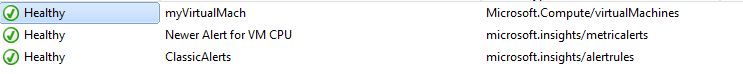
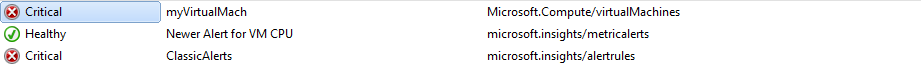
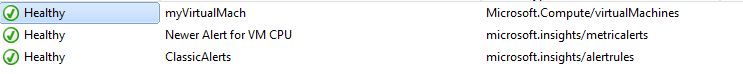
#### Metric Alerts and Classic Metric Alerts in Azure

Metric Alerts configured on Azure portal for a specific service metric have more flexibility in configuration and return more information about an issue to the Operations Manager.

For example, virtual machine has been created and a non-classic alert and classic metric alerts were [configured](https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitor-alerts-unified-usage) to notify once the CPU average usage crosses

* 80% threshold for metric alert
* and 40% threshold for classic alert.

In the Operations Manager:

1. [Import Azure Management Pack](#_1._Import_Management)
2. [Add subscription](#_Adding_Microsoft_Azure)
3. [Select Resources to Monitor](#_Select_Resources_to)  
    On “Service Types” tab in Wizard *“virtualMachines/(Microsoft.Compute)”*, “*alertrules (microsoft.Insights)*” type and “*metricalerts (microsoft.insights)*” type should be visible. “*Alertrules*” goes for classic metric alerts and “*Metricalerts*” goes for newer alerts type. Select them both.  
   
4. After a couple of minutes depending on how many services have been selected to monitor, Operations Manager will discover service instances
5. Initially, all services are healthy (CPU usage < 40% on virtual machine)  
   
   1. Once CPU usage is greater than 40% but less than 80% classic alert will switch health state to unhealthy and virtual machine to which this rule applies also will switch state, and Operations Manger will generate alert with more detailed information (Monitoring — Microsoft Azure — Active Alerts)  
      
   2. Once CPU usage is greater than 80% both classic alert and metric alert will switch their health states to unhealthy and virtual machine will also obtain unhealthy state and Operations Manager will generate alert with more detailed information (Monitoring — Microsoft Azure — Active Alerts)  
      
   3. Once CPU usage lowers to less than 40% all alerts will close themselves and health state will switch to Healthy  
      

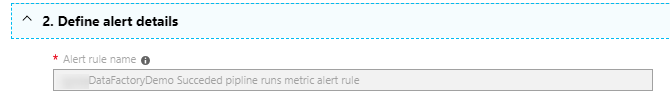
Alerts on metric mechanism is supported by many services in Azure (e.g. SQL Azure, Storage Accounts, Application Gateways …) and the list of services is growing. For each service in Azure where user can create metric alert, its state can be obtained in the Operations Manager.

##### Metric Alert Naming Convention

Metric Alert rule object in the Operations Manager does not contain information for which service and for which metric it is created until alert conditions applied. In order to simplify Azure alert rule monitoring scenarios in Operations Manager it is recommended to create alert rules name in Azure using following format:

<Resource name> <MetricName> metric alert rule

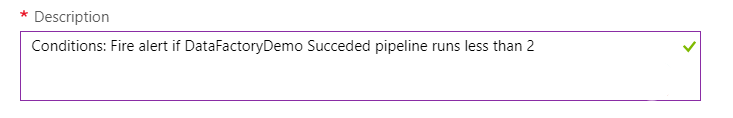
Example: <DataFactoryDemo> <Succeeded pipeline runs> metric alert rule



In Operations Manager console Monitoring tab >Microsoft Azure>Service State metric alert object name will be displayed with a corresponding alert rule name in Azure.

While the Alert rule name cannot be changed in Azure portal, the Description field is still available to edit. It is recommended to specify rule **conditions** in the textbox.  
Example:

*Conditions: Fire alert if DataFactoryDemo Succeeded pipeline runs less than 2*



##### Metric Alerts by Resource Group

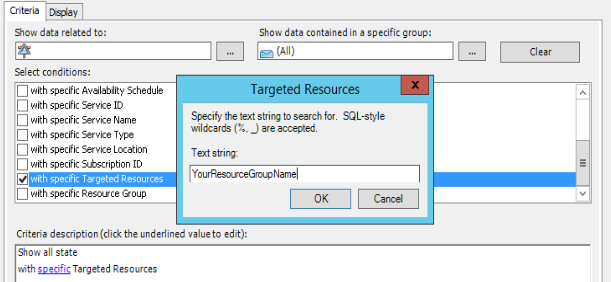
To see the resource name for which metric alert rule has been created, you can configure Custom Views in the Operations Manager.

Please note about known limitation on creating custom views:  
*“Job Failed” when trying to uncheck selected services in Wizard if custom views configured in Operations Manager* ***for management pack that created for the template****.* For detailed information see list of known issues section.

Resource groups containing services are called **targeted resources.** Metric alerts objects created for a specific service metric, for example, for Virtual Machine metrics, Datafactory metrics, Availability test availability metric or any other Azure service metric belong to a specific resource group in Azure where these services reside.

In order to see servicesfor which **Metric Alert** objects are targeted create custom *StateView* and target it to ***Microsoft.SystemCenter.MicrosoftAzure.Insights.MetricAlert*** class.

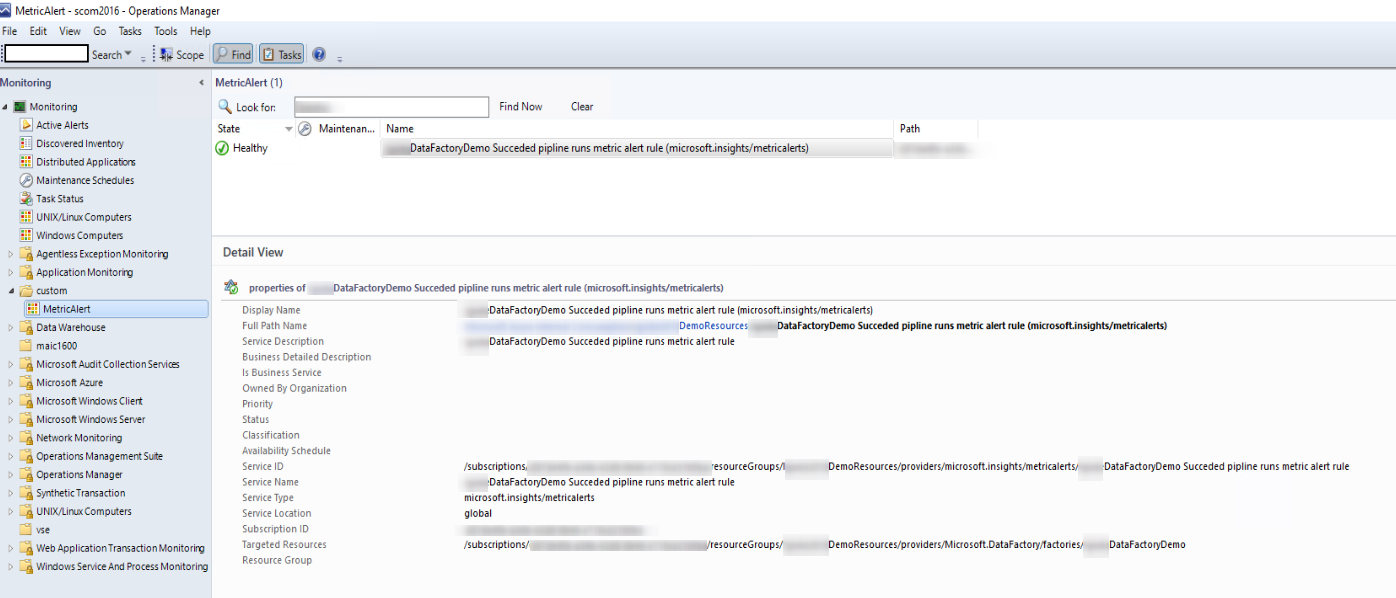
In order to obtain metric alert rules information for the defined Resource Group go to **[Criteria] tab> Select conditions,** check “**with specific Targeted Resources”**checkboxand specify Resource Group Name.



**Custom MetricAlert State View**

Below is an example of custom MetricAlert State View.

For DataFactory service metric “Succeeded pipeline runs” created metricalert object. In **Detail View- Targeted Resources** it is possible to see that metric alert created for service of Microsoft.Datafactory class, datafactory service name “DataFactoryDemo”



##### Alerts on Metrics for Disabled rule in Azure

If Metric Alert rule disabled on Azure portal and still has not closed alerts, metricalert object that replicates its state in SCOM will change state to **Healthy** regardless of remaining Fired alerts left behind in Azure.

Note: Alerts in SCOM console are dependent on alert condition and not on user response. If alert condition is fired, then the alerts will be in active state in console.Known issues related to Metric Alerts monitoring:

###### Issue: Metric Alerts monitoring in management pack for Dynamic conditions type returns 0 threshold value. Resolution: No resolution available.

###### Azure Issue: Rule that created more than 30 days ago in Azure and still Unhealthy might not display alerts in Azure. Resolution: Make changes for the rule threshold in Azure portal and save changes. Alert on rule will re-appear in Azure portal again within filter interval: last 30 days.

#### “Alert if” vs Metric Alerts

For alerts on Metrics user have a choice whether configure various rules on Azure portal or use “Alert if” option in management pack Wizard, or both. If a user configures both to the same metric and both meet the condition, he gets two alerts in case if condition exceeded Threshold. For each option there are separate monitor created in the Operations Manager and both configurations can coexist without conflict.

Alerts created through “Alert if” condition in the management pack Wizard have “Warning” severity in the Operations Manager. Metric Alerts and Classic Metric Alerts configured on Azure portal have “Critical” severity in the Operations Manager. If user configured both options he can see Warning and Critical alert to the same metric in the Operations Manager Active Alerts view.

All services that do not have monitored metrics will obtain a “Not monitored” state (green circle without a check mark) in the Operations Manager Monitoring > Microsoft Azure > Service State view

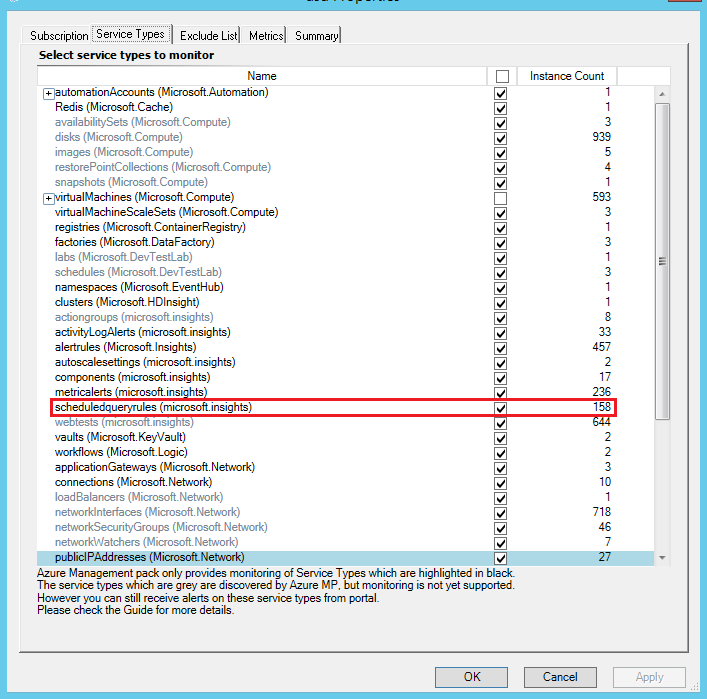


#### Scheduled Query Rule Alerts

##### Health calculation

Log queries are intended to retrieve any log data from Azure Monitor. For each Scheduled Query Rule in the management pack implemented monitor that calculates how many alerts for rule has been created during the past 30 days and whether they were not marked as “Closed”. If there is at least one not Closed alert for the Azure rule, Scheduled Query Rule monitor in SCOM changes state to Critical and raises an alert.

In order to enable monitoring of [Scheduled Query Rules](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview), select them in the Service Types tab :



##### Scheduled Query Rule Naming Convention

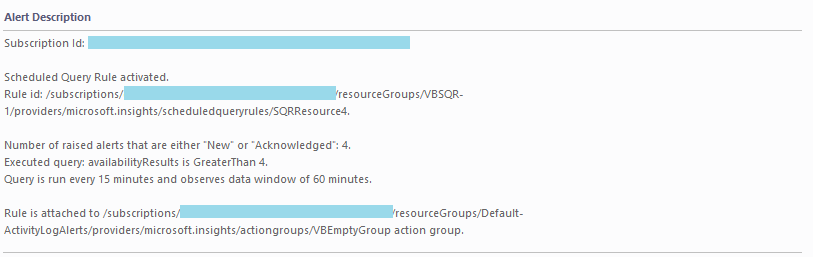
Scheduled query rule object in the Operations Manager does not contain information for which service it is created until alert conditions applied. In order to simplify Azure alert rule monitoring scenarios in Operations Manager it is recommended to create rule names in Azure using following format:

*<Targeted Resource name> <Signal Type> <Monitor Service> scheduled query rule*

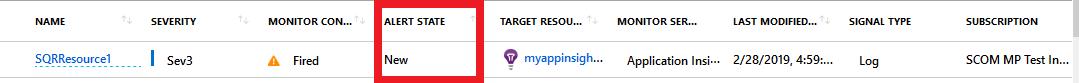
Example: <AppInsightsComponent1> <LogSearch> <ApplicationInsights> scheduled query rule

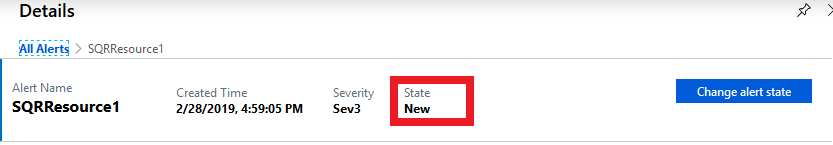
##### Scheduled Query Rule Description in Operations Manager

Once monitor becomes unhealthy you will receive SCOM alert in the following format:



Below is an example of alert state in Azure:





##### Log Analytics Scheduled Query Rules

Alert description for Log Analytics rules whose Log Analytics workspace uses legacy Log Alerts API doesn’t include details like **Rule Query, Threshold, Frequency, Action Group**. To make these details present in alert description you should switch Log Analytics workspace to new scheduledQueryRules API. You may find how to do it in the following article: [Switch API preference for Log Alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log-api-switch).

##### Notifications suppression

“Suppression” option in Azure allows stop sending notifications through Action Group for some time (emails, webhooks etc.). Please note, that only notifications are suppressed for the case. Azure Alerts will still be emitted, and because of that, objects in SCOM will change their states.

##### Alerts from Scheduled Query rules for Disabled rule in Azure

If Scheduled query (Log search) rule disabled on Azure portal and still has not closed alerts for the past 30 days, monitor that replicates its state in SCOM will be in Critical state until alerts for the rule closed in Azure. It is recommended to close all alerts for the rule on portal.

##### Close Scheduled Query Rule Alerts Task

It is possible to close all alerts generated by Azure Scheduled Query rule in SCOM console using “Close all alerts” task. Minimum required permissions in Azure for SCOM Action Account to run the task must be Contributor or Higher.

#### Activity Log Alerts

##### Health calculation

Activity Log Alerts are used to audit activities in the Azure subscription and serve the purpose to send notifications when specific operation or health event occurs on the Azure resource. For each Azure Activity Log Alert rule in management pack implemented monitor that counts how many [alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview) for rule has been created during the past 30 days and whether they were not marked as “Closed”. If there is at least one not Closed alert for the Azure rule Activity Log Alert monitor in SCOM changes state to Critical and raises an alert.

##### Activity Log Alert Rule Naming convention

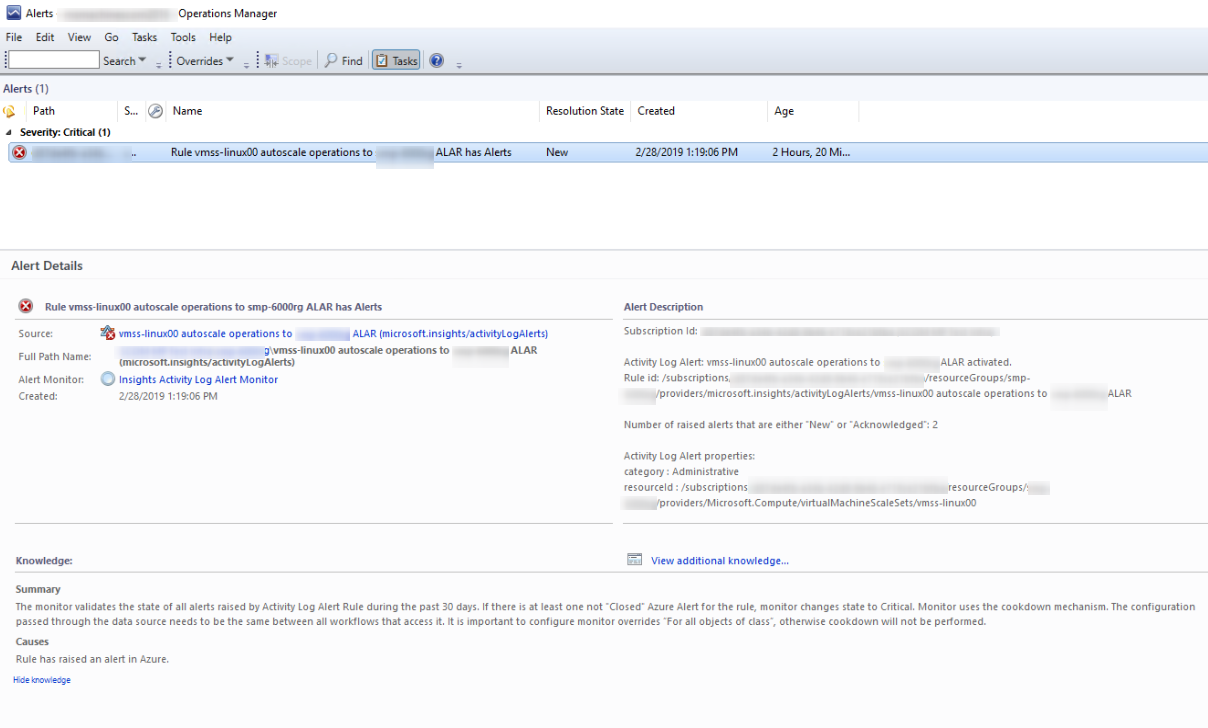
Activity Log Alert rule object in Operations Manager does not contain information for which service it is created until alert conditions applied. In order to simplify alert rule monitoring scenarios in Operations Manager it is recommended to create rule name in Azure using following format:

*<Targeted Resource name> <Signal Type> <Monitor Service> Activity Log Alert rule*

Example: <VM1> <Activity Logs> <PowerON VirtualMachine> Alog rule

##### **Activity Log Alert Description in Operations Manager**

Below is an example of alert description for Activity Log Alert rule that has alerts.



##### Alerts from Activity Log Rules for Disabled rule in Azure

If Activity Log rule disabled on Azure portal and still has not closed alerts for the past 30 days, monitor that replicates its state in SCOM will be in Critical state until alerts for the rule closed in Azure.

##### Close Activity Log Alert Task

It is possible to close all alerts generated by Azure Activity Log Alert rule in SCOM console using “Close all alerts” task. Minimum required permissions in Azure for SCOM Action Account to run the task must be Contributor or Higher.

##### Known issues related to Activity Log Alerts monitoring:

###### **Issue: Activity Log Alert rules created on All Administrative operations in LogAnalytics workspace (Solution in LogAnalytics) will not trigger an alert in Azure, hence no alert will arise in SCOM.** Resolution: No resolution available.

###### Issue: In case when second Activity Log Alert rule that has alerts targeted to First Activity Log Alert rule that targeted to a specified Azure Resource, in SCOM monitor that represents Second Activity Log Alert rule will rollup health to both First Activity Log Alert rule monitor and to a Resource monitor that it is not targeted to. Resolution: In Azure Activity Log Alert rule can be targeted to another Activity Log Alert rule. Relationships between classes of same type are not supported for health rollup mechanism in the Operations Manager.

### Azure Diagnostics and Guest Metrics on Virtual Machines, Web Roles, and Worker Roles

To collect additional performance counters and events from Virtual Machines, web roles, and worker roles, Azure diagnostics should be enabled.

For more information about Microsoft Azure Diagnostics, see the [Collect Logging Data by Using Windows Azure Diagnostics](https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-dotnet-diagnostics) article.

Microsoft Azure Diagnostics must be configured to forward the diagnostic data to a Microsoft Azure storage and to Azure Monitor. For more information about configuring Microsoft Azure Diagnostics, see the [Store and view diagnostic data in Azure Storage](https://docs.microsoft.com/en-us/azure/cloud-services/cloud-services-dotnet-diagnostics-storage) article and [VM Guest to metric store](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-custom-metrics-guestos-resource-manager-vm) article.

#### Guest Metrics Monitoring

Starting Azure MP 1.7.0.0 collection of Guest OS metrics for Virtual Machines require additional configuration steps to be performed in Azure.

Below Articles describe how configure and deploy Guest OS extension:

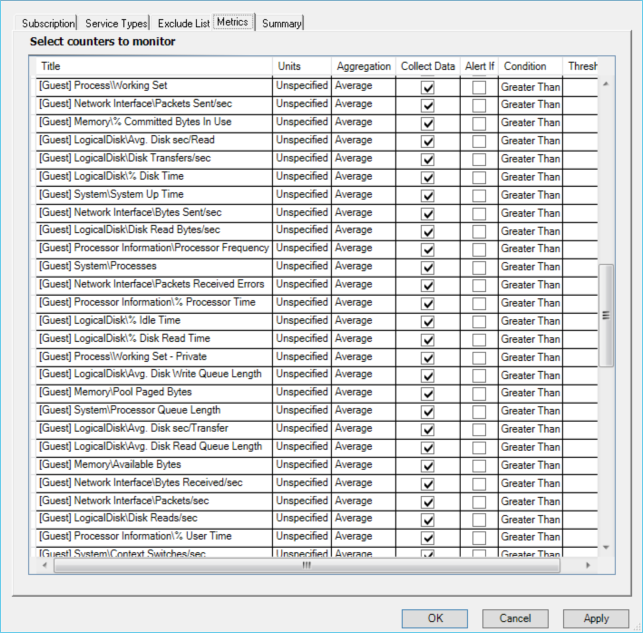
[For **Linux VMs**](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-custom-metrics-linux-telegraf)

[For **Windows VMs**](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-custom-metrics-guestos-resource-manager-vm)

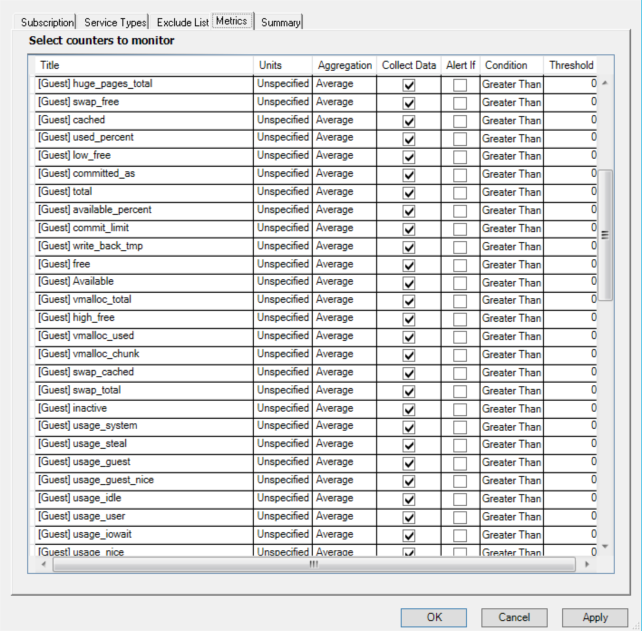
Alternative, a **Tool** to enable Guest extensions for Windows Virtual machines might be used from [**this GitHub repository.**](https://github.com/VIAcode/Azure-Toolbox/tree/master/VM%20guest%20metrics)

Once configuration done and metrics collected for Virtual Machines in Azure, it is possible to obtain them in the Azure Management pack. For this Go to **Authoring** pane > select Azure Management pack subscription **template**>Subscription tab>press **[Refresh Data]** button.  
After refresh completed go to **Metrics** tab. New Guest OS metrics will appear under **Virtual machines** section.

Below is an example of metrics view in Azure MP wizard for the **Windows VMs**:



For the **Linux VMs**:



**Note:** It is recommended to do a reasonable selection of Guest Metrics for monitoring and exclude those that are not required.

Below in table described test results of Operations Manager Database size growing for Virtual Machines Metrics collection when all metrics selected by default. Operations Manager database size grew up to 3,3 Gigabytes for 15 hours of data collection.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | Number of monitored metrics for VMs | Time in hours | Number of Virtual Machines | Operations Manager database size grew up to in Gb |
| SQL Server 2016 SP1, SCOM 2016  Azure Management pack version: 1.7 CTP | 128 Total:   * 35 Host * 93 Guest | 15 | 679 Total:   * 503 with Guest Metrics and Host Metrics collection enabled ( 250 Linux, 253 Windows) * 176 with Host Metrics collection enabled | 3,3 Space available:   * Start time: 12,187 Gb * End time: 8,888 Gb |

##### Known issues while monitoring Guest Metrics:

###### Issue: After upgrade Guest Metrics did not appear in Metrics tab in Wizard. Resolution: Press [Refresh data] in Azure MP Wizard > Subscription tab to fetch data. By default all new metrics unselected. Select metrics to monitor and save template.

###### Issue: Events “no parent resource was found for … extensions” might occur every 4 hours in event log. Resolution: Uncheck checkbox for VirtualMachines/extensions to reduce number of events.

### Enable Grooming of Performance and Event Logs from Azure Table Storage

Microsoft Azure Diagnostics writes performance and event information to Azure storage but does not delete it. This means that the tables in the Microsoft Azure storage will continue to grow unless the data is groomed. The management pack for Microsoft Azure provides three rules that control the data grooming:

 Microsoft Azure Storage NT Event Log Grooming

 Microsoft Azure Storage Performance Counter Grooming

 Microsoft Azure Storage.NET Trace Grooming

By default, these grooming rules are disabled. To enable the Operations Manager to periodically groom the data from Microsoft Azure storage, use overrides to enable the rules. By default, the enabled rules run every 24 hours.

The event log can be used to track the data grooming on the root management server. Event 34023 is logged when the grooming starts. Event 34014 is logged when the grooming is completed, and the event includes the count of deleted rows and the time when the grooming occurred.

### Enable Disabled Monitors

The following monitors are disabled by default and need to be manually enabled:

* Microsoft Azure Subscription Certificate Expiration Monitor
* Microsoft Azure Cloud Service Certificate Expiration Monitor

### Write Rules to Collect Events and Performance from Azure Table Storage

Microsoft Azure Diagnostics can write event logs and performance counters to Azure table storage.

Refer to Azure.AlertExample.xml file included with this management pack for an example of how to generate an alert for an event logged to Azure storage. This file is for Classic Virtual Machines only.

**Note:** These samples are purely illustrative of how to create custom monitoring. They are not intended for use “as-is”.

This example looks for an Event with ID 7036 and generates an Alert. One rule is targeted to Virtual Machines, and the second one is targeted to Web and Worker Roles (Azure.AlertExample.Role.EventID.AlertRule)

If you have Azure diagnostics configured to collect Informational Events from the System event log, this example management pack will generate an alert whenever Service Control Manager detects a service has stopped or started.

In web roles, these events are generated quite frequently.

For each virtual machine that does not have diagnostics enabled (or if diagnostics are enabled but no data is specified to be collected), the following message will be logged in the Operations Manager event log on the management server:

Provider = Health Service Modules

EventID = 34024

Level = 3 (Warning)

Storage account for Windows Azure Diagnostics is not specified.

Subscription ID: <Azure subscription guid>

Service name: <virtual machine name>

Deployment ID: <deployment guid>

Deployment slot: Production

Role name: <virtual machine name>

Workflow name: Azure.AlertExample.EventID.AlertRule

Instance name: <virtual machine name> (Microsoft.ClassicCompute/virtualMachines)

Instance ID: {guid}

Management group: <management group name>

#### Custom Performance Rules

Refer to Azure.CustomPerformanceMonitoring.xml file included with this management pack for an example of how to collect performance counters for Virtual Machines and web/worker roles transferred to Azure storage. Note that this file is for Classic Virtual Machines only.

This example collects the ISAPIExtensionRequestsPerSec counter.

### Monitor Large Number of Azure Instances

#### Monitor large number of Azure services instances

Below provided an example of how to configure monitoring of many Virtual Machines. It is recommended to apply the similar approach (increase interval of workflows based on your environment configuration) to monitor many other service instances.

To monitor a large number of Virtual Machines, perform the following configuration:

1. Increase the number of Maximum CLR threads in the system registry (see Minimal recommended configuration section).
2. Create override with 3600 seconds interval for each Virtual Machines Performance Collection rule.

For this scope rules to *Microsoft Azure virtualMachines (Microsoft.Compute) for <YourSubscriptionID>* and set override for each.

A screenshot of a social media post

Description automatically generated

1. Create override with 900 seconds interval for *Microsoft Azure Virtual Machine Turn Off Monitor for <YourSubscriptionID>.*

A screenshot of a computer

Description automatically generated

1. Be careful to enable Monitoring of all Virtual Machines metrics from the Azure MP in Authoring Wizard. Specify reasonable thresholds and select only desired metrics.

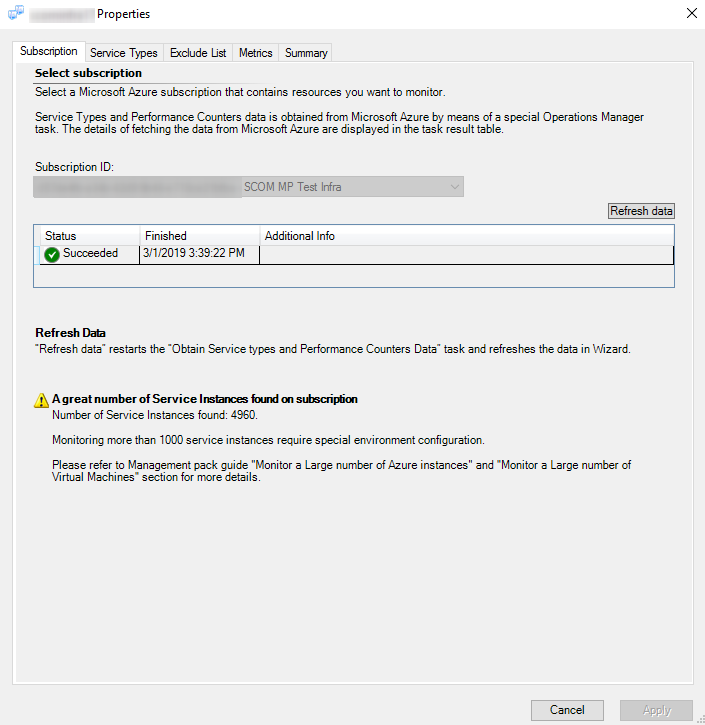
A screenshot of a social media post

Description automatically generated

Azure REST API itself has the following limitation[: **12000 read requests per hour**.](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-request-limits) You can calculate minimum monitoring interval as 10 minutes for every 2000 monitored entities. For example, if the cloud contains 6000 databases, the minimal interval for all rules and monitors should be (6000/2000) \*10 = 30 minutes.

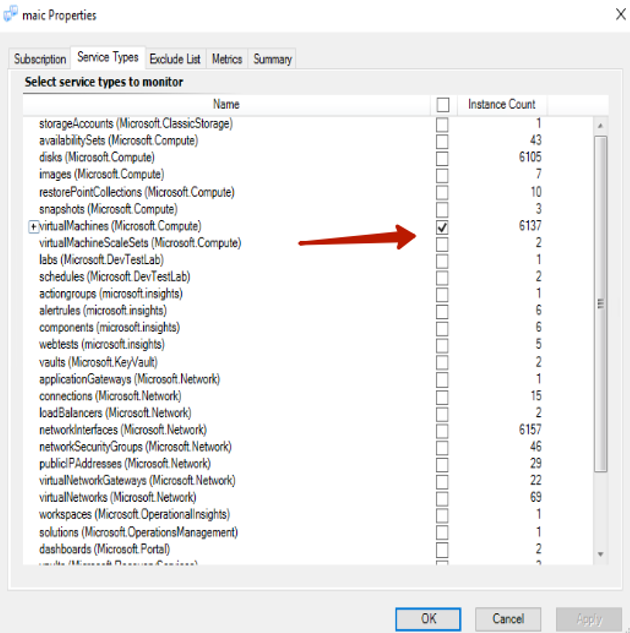
For Azure Subscription that contains more than 1000 instances Warning will pop up in Wizard with recommendation to check SCOM pre-requisites configuration.

Note: Due to certain performance issues, a separate management server should be dedicated for this management pack.



* **Important:** Do not monitor more than 6500 instances at once.   
  Adding more instances to monitoring will result in Operations Manager performance issues.

For example, in Service Types dialog subscription has 6137 Virtual Machines and 6157 Network Interfaces. To monitor 6137 Virtual Machines leave only this checkbox checked.



#### Known issues while monitoring a large number of Azure instances

##### Issue: Management Pack State Views in Operations Manager Monitoring is in “Loading …” state up to 5 minutes before objects appear in it.

**Resolution:** Alternative, you can create [Dashboard View](#_How_create_Dashboard) and specify objects you want to monitor.

##### Issue: Health Service Private Bytes exceeded threshold of 1500 MB when monitor large number of instances with Azure Management pack. Management Server health is Critical.

**Resolution:** To monitor several thousands of instances Health Service running a lot of rules and monitors that causes it to consume more resources. In order to meet Operations Manager default threshold values user needs to define priorities of what instances and what metrics are in most demand for monitoring, and perform following actions:

* disable monitoring of less used metrics and services in management pack Wizard
* increase default intervals for monitoring workflows. Please, see an example in “Monitor a large number of Virtual Machines” section.

Alternative, user can configure Health Service Private Bytes Threshold monitor to trigger Critical state on higher Threshold value( for example to 3,000MB for 6000 instances) .

##### Issue: “An error occurred while sending the request” warning with event id 11422 from MS Azure MP Module

**Resolution:** Issue periodically might occur when monitor large number of instances because of too many requests have been made to Azure API. Resolution – increase interval of workflows for monitored objects or exclude some services from monitoring in Azure Wizard.

##### Azure Issue: When start simultaneously 100 or more Virtual machines on Azure Portal actual state for some Virtual Machines will not be changed in SCOM Console

**Resolution:** Issue happens because some state change events on bulk start returned with unexpected values for Virtual Machines states from the Azure API. Resolution – stop and start individual Virtual Machines that did not change their state on previous bulk run.

##### SCOM Issue: Console crashes when bulk remove large number monitored objects in Azure subscription. “Object reference not set to an instance of an object” error.

**Resolution:** Restart Console and refresh state view. Number of objects will be updated with their actual state in subscription.

##### Issue: Too many OpsMgr SDK Warnings with id 26373 in event log

**Resolution:** Issue periodically might occur when monitor large number of instances. Resolution – increase interval of workflows for monitored objects or exclude some services from monitoring in Azure Wizard.

##### Issue: Intermittent error “Unexpected Error occurred. Module name: ArmPerformanceCollectionProbe” with Event id: 6420 and error Level: Warning while monitoring more than 1000 instances.

**Resolution:**The following recommendations should minimize load:  
1. Increase interval for all performance collection rules from 900 seconds up to 3600. Interval depends on number of instances monitored, hardware used and can vary from 900 to 3600 based on user priorities.

2. In *Azure Wizard ->Services* tab uncheck services that are not required to be monitored.

3. In *Azure Wizard ->* *Metrics tab –> Collect Data* column uncheck metrics that are not required to be collected.

4. Increase number of CPU cores.

#### Minimal recommended configuration for monitoring 1000+ objects is as follows:

* SCOM 2016 / 2019
* Windows Server 2012 R2 as a server OS and higher
* A dedicated Run As account for “Microsoft Azure Run as Profile Proxy.”
* A dedicated server for the SCOM Operations DB SQL Server (minimum database file size is 10 000 MB and auto-growth enabled)
* A dedicated server for the SCOM DW DB SQL Server (minimum database file size is 10 000 MB and auto-growth enabled)
* A dedicated SCOM Management server for the Azure management pack:
* 4 (V)CPU 2.0 GHz (or more)
* 16 GB RAM (or more)
* A dedicated Separate HDD formatted with 64K Cluster Size for the SCOM Health Service State folder; one SSD recommended. See **“Move Health Service State folder to new location”** section.
* It is recommended to update/create the registry settings on the dedicated SCOM Management Server (watcher node) as follows:
* Increase the number of Maximum CLR threads in pool via registry.

For this create “Thread Pool CLR Max Thread Count Min” DWORD (32-bit) parameter:

“HKLM\System\CurrentControlSet\Services\HealthService\Parameters\Thread Pool CLR Max Thread Count Min” and set Decimal value from 150-512 (512 is maximum) depending on your Server configuration (10 threads per CPU core; for example if you have 48 cores, set the value to 480; if you have 50 cores and more, set the value to 512; for 8 cores, set max value to 80-512).

* Increase the number of Minimum CLR threads in pool via registry.

For this create “Thread Pool CLR Min Thread Count” DWORD (32-bit) parameter:

“HKLM\System\CurrentControlSet\Services\HealthService\Parameters\Thread Pool CLR Min Thread Count” and set Decimal value to 50 or value calculated based on number of cores you have ( for example, if you have 4 cores, set value to 40) .

* **Important.** Restart Microsoft Monitoring agent upon a change of the registry settings.

|  |  |
| --- | --- |
| HKLM\SYSTEM\CurrentControlSet\services\HealthService\Parameters | Value in Decimal |
| Persistence Cache Maximum | 262144 |
| Persistence Version Store Maximum | 131072 |
| Persistence Page Hint Cache Size | 262144 |
| Persistence Checkpoint Depth Maximum | 20971520 |

##### Move Health Service State folder to new location.

To move folder the following steps can be performed:

* Stop HealthService with command “net stop healthservice”.
* Change path in registry. Folder location can be found under the following registry path: “HKLM\ SYSTEM\CurrentControlSet\Services\HealthService\Parameters\State Directory.”
* Move old folder data to new location to save old data (otherwise SCOM creates it from scratch in new location)
* Check that SYSTEM account has Modify writes to the new folder and all subfolders.
* Start HealthService with command “net start healthservice.”

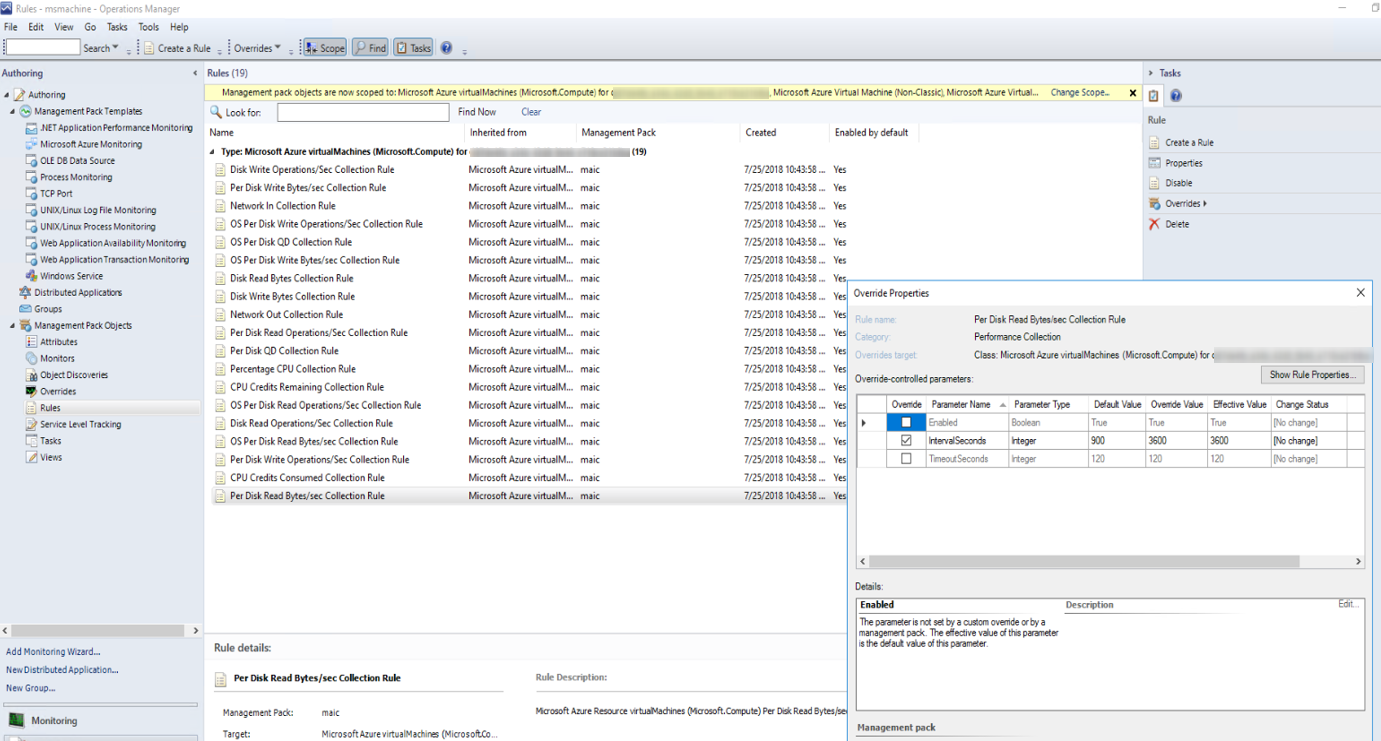
#### Monitor a Large number of Virtual Machines.

Below provided an example of how to configure monitoring of a large number of Virtual Machines. It is recommended to apply the similar approach (increase interval of workflows based on your environment configuration) to monitor a large number of other service instances.

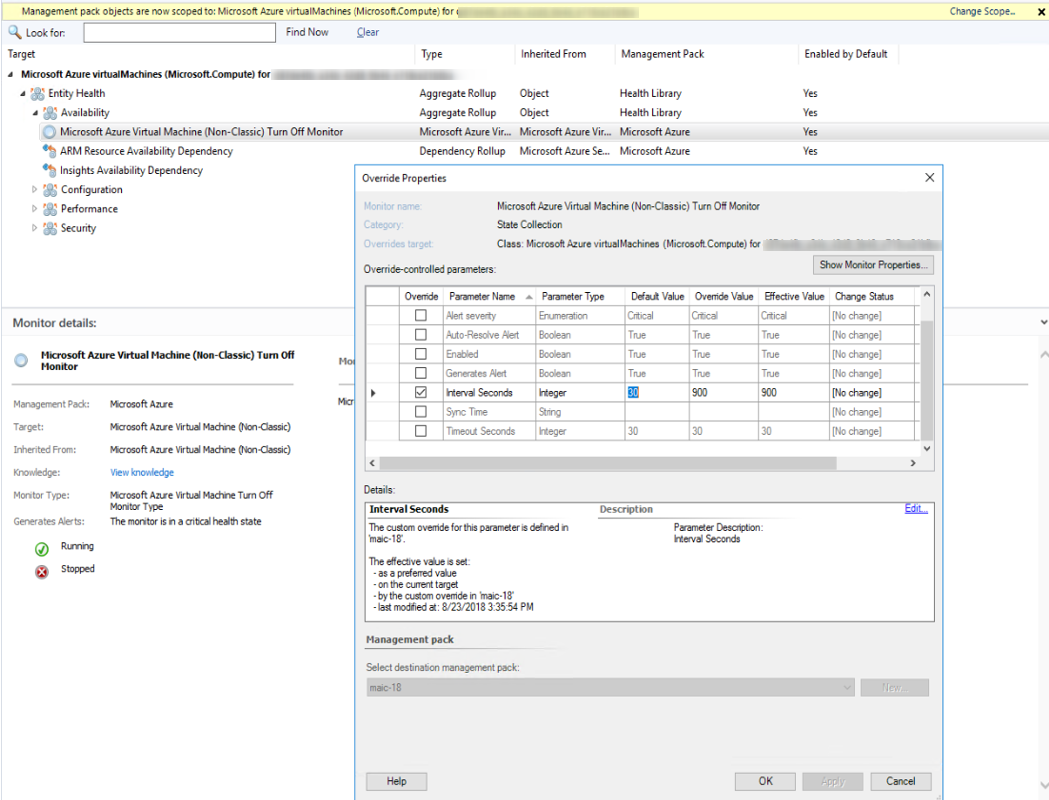
To monitor a large number of Virtual Machines perform the following configuration:

1. Increase the number of Maximum CLR threads in the system registry (see Minimal recommended configuration section).
2. Create override with 3600 seconds interval for each Virtual Machines Performance Collection rule.

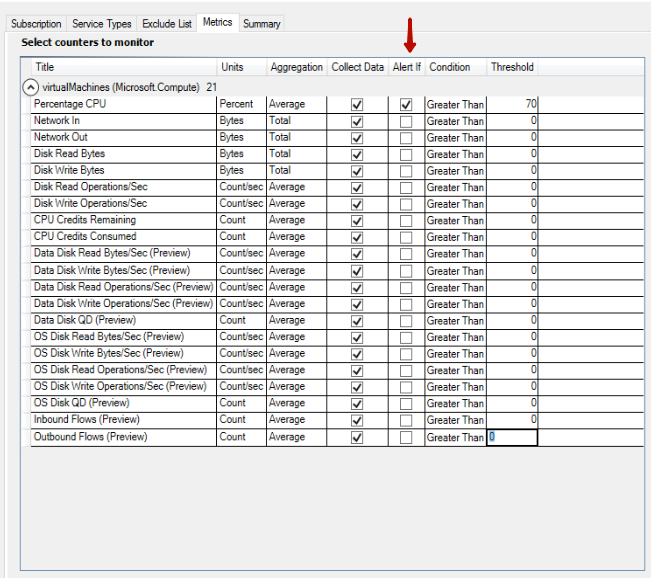
For this scope rules to *Microsoft Azure virtualMachines (Microsoft.Compute) for <YourSubscriptionID>* and set override for each.



1. Create override with 900 seconds interval for *Microsoft Azure Virtual Machine(Non-Classic) Turn Off Monitor for <YourSubscriptionID>.*



1. Be careful to enable Monitoring of all Virtual Machines metrics from the Azure MP in Authoring Wizard. Specify reasonable thresholds and select only desired metrics.

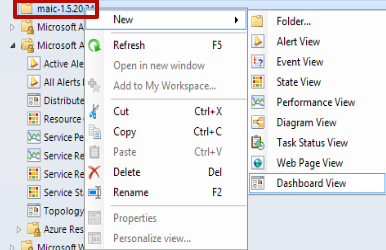


#### How create Dashboard View to monitor Azure objects

Below there are an example of how to create alternative Dashboard view in Operations Manager to monitor a state of Virtual Machines.

In Monitoring tab of Operations Manager select unsealed management pack that you created to monitor Azure resources

Select New - > Dashboard View



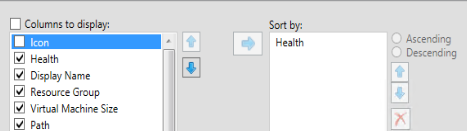
1. Dashboard and Widget Wizard will open. Configure it.

* Select Column Layout template
* Give a name to your view, for example “Virtual Machines State”
* For Column Count specify 1
* Create View

New Dashboard will appear with one column

1. In New Dashboard select “Click to add widget”

* Dashboard and Widget Wizard will open. Configure it.
* Select State Widget template
* Give a name to your widget, for example “Virtual Machines State widget”
* In Scope press […] under “Select a class to scope the members of the specified groups” and select *Microsoft Azure Virtual Machine*
* In the Criteria section leave all defaults and press [Next]
* In the Display section select columns to display: Health, Display Name, Resource Group, Virtual Machine Size, Path. Sort objects by Health

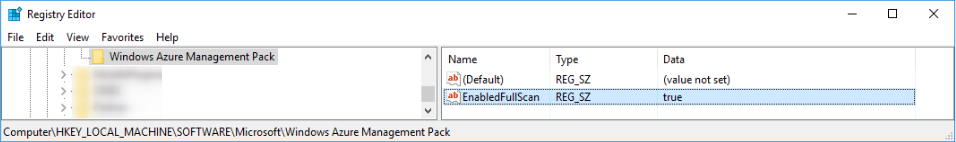


* Next leave all defaults configurations and press [Create]

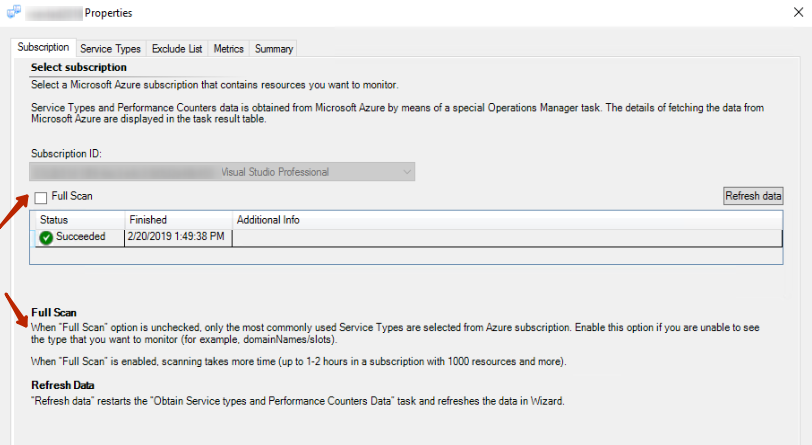
### Full Scan

In order to enable Full scan option the following registry key must be created on host with SCOM server installed:

|  |
| --- |
| HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\**Windows Azure Management Pack** String “**EnabledFullScan**”  value “**true**” |



Full Scan option will become available in Wizard.



**NOTE:**  There is a known issue with this feature and may not work as expected.

## Files in this Management Pack

The management pack for Microsoft Azure includes the following files:

* Microsoft.SystemCenter.MicrosoftAzure.mpb
* Microsoft.SystemCenter.MicrosoftAzure.SLA.mpb
* MicrosoftAzureManagementPackGuide.docx

## Management Pack Purpose

In this section:

 [Monitoring Scenarios](#z5a9ff008734b4183946f840ae0464ab0)

 [How Health Rolls Up](#zb8b3e32eb8154a8da8b18b606568e65d)

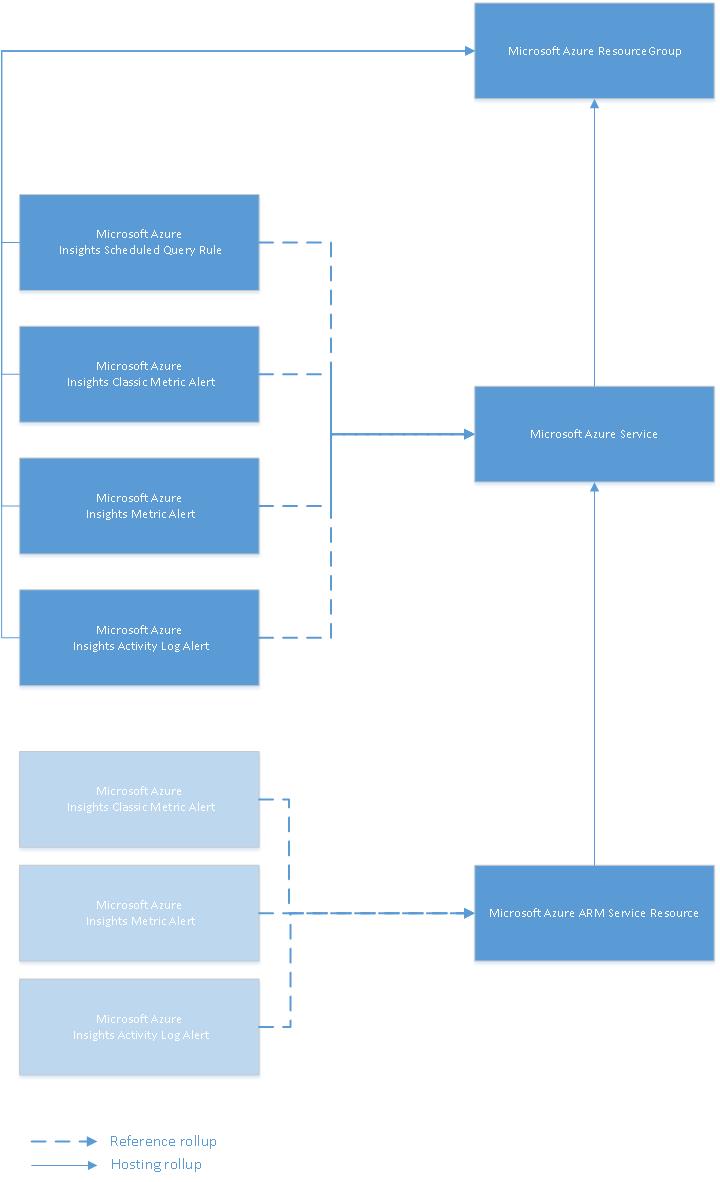
For details on the discoveries, rules, monitors, views, and reports contained in this management pack, see the Appendix: Management Pack Contents.

### Monitoring Scenarios

|  |  |
| --- | --- |
| Monitoring scenario | Description |
| Collect performance counters for Azure services | For all instances of a service, collect any performance counters exposed by the Azure service. The user can select not to collect specific counters and can exclude specific instances of a service. |
| Collect custom performance counters for web roles, worker roles, and Virtual Machines | For a web role, worker role, or virtual machine with Azure diagnostics enabled, collect custom performance counters. The performance counter must be collected by Azure diagnostics (and by Azure Monitor in case of Virtual Machines). |
| Generate an alert if a performance counter exceeds a specific threshold | For a collected performance counter, specify a greater than/less than the threshold, which will result in an alert being generated if the threshold is crossed. |
| Generate an alert based on an event log entry for a virtual machine, web role or worker role | For a web role, worker role or virtual machine with Azure diagnostics enabled, generate an alert for specific events.  The event must be collected by Azure diagnostics. |
| Generate an alert for an Azure notification | For each classic metric alert, metric alert, scheduled query rule and activity log alert in Azure, a corresponding monitor is created in the Operations Manager. When a notification is generated by Azure, a corresponding alert is created in the Operations Manager. |
| Monitor the health of a hybrid application | Use the distributed application designer to model an application that consists of components in Azure and on-premises. |
| View health of resources in the resource group | For each resource group, a rollup monitor is created that contains monitors for each resource instance in the resource group. |

### How Health Rolls Up

The following diagram shows, how the health states of objects roll up in this management pack.

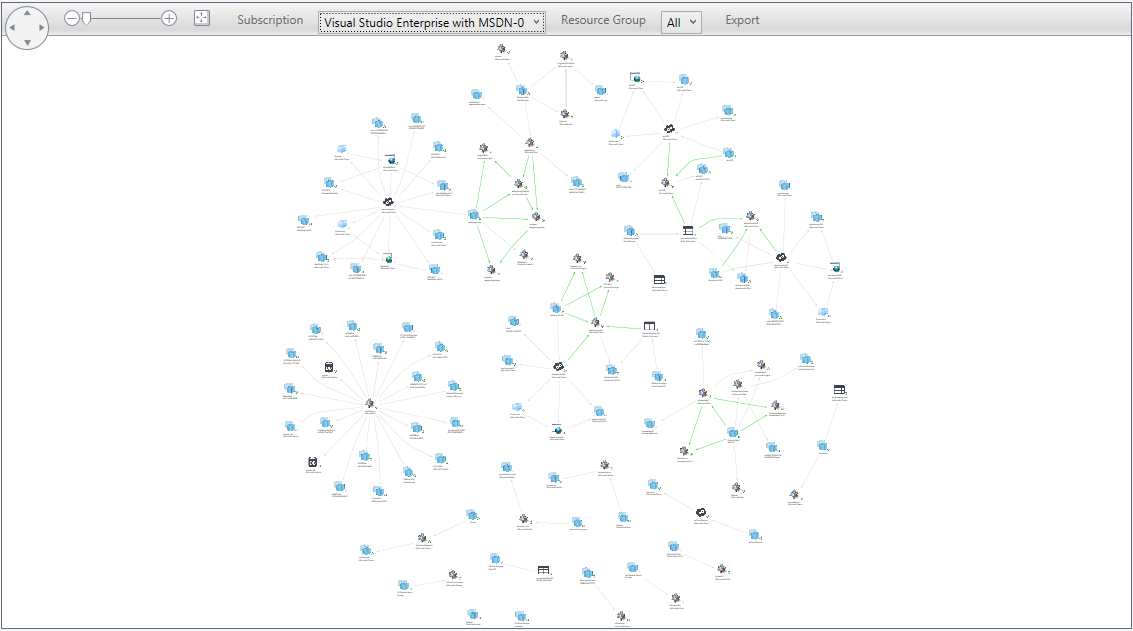


### Topology Dashboard

This management pack contains a Topology dashboard. The purpose is to show how the Azure objects in your subscriptions are related to each other. Note that it will show all discovered objects for all subscriptions you have configured, not only the “monitored” ones.

The dashboard has the following functionality:

* Displays of all Cloud Services contained by the Subscriptions you have defined.
* Discovers relationships between these cloud services and displays them in the dashboard as “connections.”
* Displays instance details of the cloud services.
* Ability to filter by a particular subscription.
* Ability to filter by a particular Resource Group.
* Ability to zoom and pan.
* Ability to drill into a Service Vicinity dashboard by selecting a particular service. This dashboard shows the instance details, as well as details of each connection.

A sample complex topology is shown below:

### Model Hybrid Applications via Distributed Application Template

The management pack contains a new Distributed Application template that enables you to model and monitor hybrid applications, i.e. applications that have some cloud-based resources, and some resources on premise.

To create a hybrid-distributed application, you should follow these steps:

1. Go to the authoring space in the Operations Manager console.
2. Right-click **distributed applications** and select **Create a new distributed application**.
3. Provide a name and description.
4. For a template, use the **Microsoft Azure Distributed Application** template
5. Provide a management pack to save the distributed application and click OK.
6. The distributed application consists of several component groups:
   1. A Client perspective component group. You can use this for any synthetic transactions (such as Global Service Monitor synthetic transactions) you have running against your application.
   2. A Cloud Services Components group for the Azure components.
   3. An SQL group for SQL databases (on-premise or in Azure).
   4. A Storage account group for Azure Storage accounts.
   5. A generic dependencies group for any other dependencies (on-premise or in Azure) that your application may have.
7. Add the relevant components to the right component group and save the distributed application.
8. To see the resulting distributed application, go to **Distributed ApplicationState** view in the Microsoft Azure folder in the monitoring section of the console.
9. From there, you can also navigate to 2 dashboards that show **Availability** of the application over time and compared to provided SLAs, as well as **capacity utilization** of the Azure-based components over time (CPU and memory utilization)

### Endpoints

The following endpoint are used by default for obtaining data from Microsoft Azure ARM REST API

|  |  |
| --- | --- |
| Endpoint name | Endpoint URI |
| Management service URI | https://management.core.windows.net |
| Authority URI | https://login.windows.net |
| ARM Management URI | https://management.azure.com |
| Graph URI | https://graph.windows.net |

### Alert Severity Changes

AzureMP 1.8.0.1 and its lower versions have a critical alert for every alert that is fired in Azure portal. In Azure portal an alert has multiple state, while in SCOM we only show Critical alert. To bring the experience closer to Portal, we display Alert severity as per the portal.

### Impact on SCOM Health State based on the Alert

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Azure Alert Severity | SCOM Alert Severity | SCOM Alert Priority | Health State of Alert Rule | Health State of Target Resource | Type of Azure Alert |
| 0 | Critical | High | Critical | Critical | Metric, Log, Activity Log |
| 1 | Critical | Medium | Critical | Critical | Metric, Log, Activity Log |
| 2 | Warning | Low | Warning | Warning | Metric, Log, Activity Log |
| 3 | Informational |  | Healthy | Healthy | Metric, Log, Activity Log |
| 4 | Verbose |  | Healthy | Healthy | Metric, Log, Activity Log |

## Security Configuration

Note that Microsoft Azure Run As Profile AD Credentials profile is configured automatically; when you add a subscription, there is no need to perform an additional configuration. As for Microsoft Azure Run As Profile Proxy, it is to be configured manually in the case when large subscriptions (1000+ objects) are monitored. For more details, see the [Managing Run As Accounts and Profiles](https://technet.microsoft.com/en-us/library/hh212714(v=sc.12).aspx) article.

|  |  |
| --- | --- |
| Run As Profile Name | Notes |
| Microsoft Azure Run As Profile AD Credentials | Holds the Azure Active Directory Credential to authenticate with Azure. |
| Microsoft Azure Run As Profile Proxy | Holds the credentials needed to authenticate with a proxy to reach Azure |

Setting up Proxy Connection

To use a proxy server for the connection, perform the following steps:

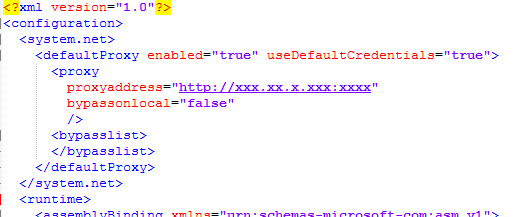
#### Edit Server configuration file

It can be found in the below location:

*C:\Program Files\Microsoft System Center <SCOM Version>\Operations Manager\Server\* *MonitoringHost.exe.config*

Add lines as shown in the screenshot below:

|  |
| --- |
| *<system.net>*  *<defaultProxy enabled="true" useDefaultCredentials="true">*  *<proxy*  *proxyaddress="http://xxx.xx.x.xx:xxxx"*  *bypassonlocal="false"*  */>*  *<bypasslist></bypasslist>*  *</defaultProxy>*  *</system.net>* |



**NOTE: Restart Health Service**

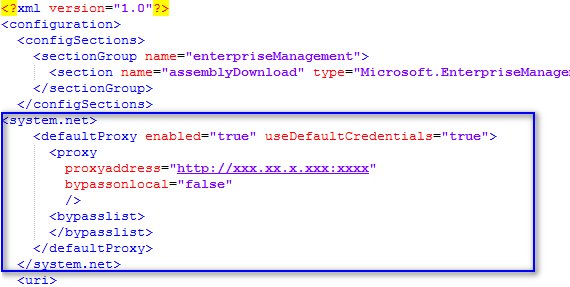
#### Edit Console configuration file.

In case Console installed separately from Server machine and proxy configured on console machine, Console config file must be updated to use proxy.

Console configuration ile can be found in the below location:

*C:\Program Files\Microsoft System Center <SCOM Version>\Operations Manager\Console\Microsoft.EnterpriseManagement.Monitoring.Console.exe.config*

Add lines as shown in the screenshot below:



**Note:**proxy address value must be entered in following format: http://ProxyIPaddress:Port, for example <http://192.168.0.200:8080>

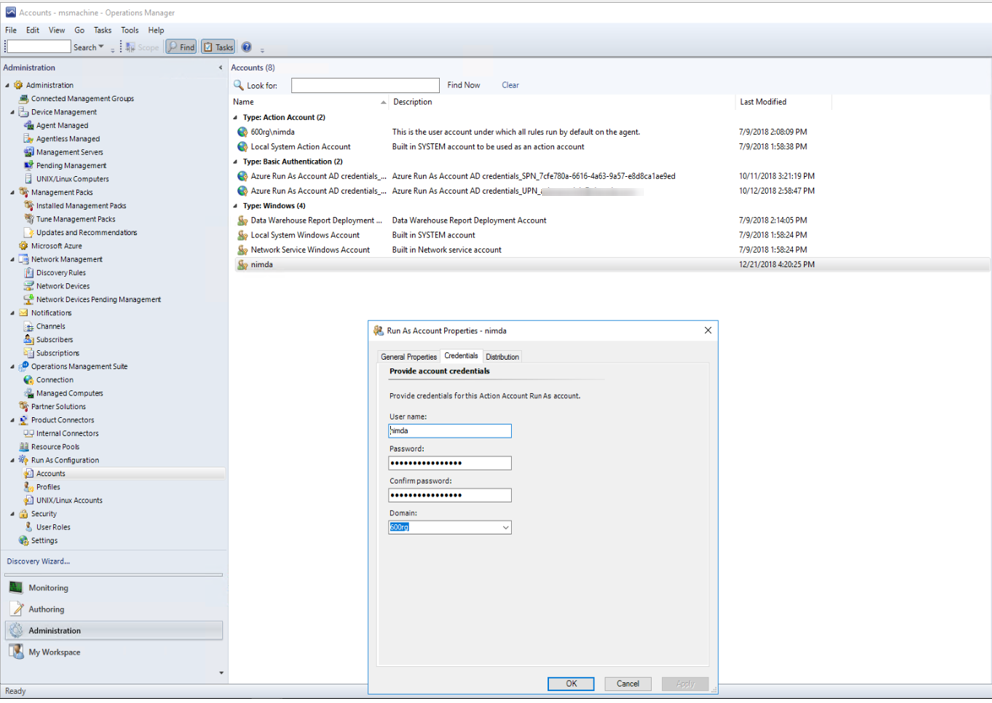
* **Restart the Operations Console**
* **Change IE settings to use the corresponding proxy**
* **Configure Management Server proxy settings:**

Enable “Use a proxy server for communication with Microsoft” option, enter the corresponding address, and port values.

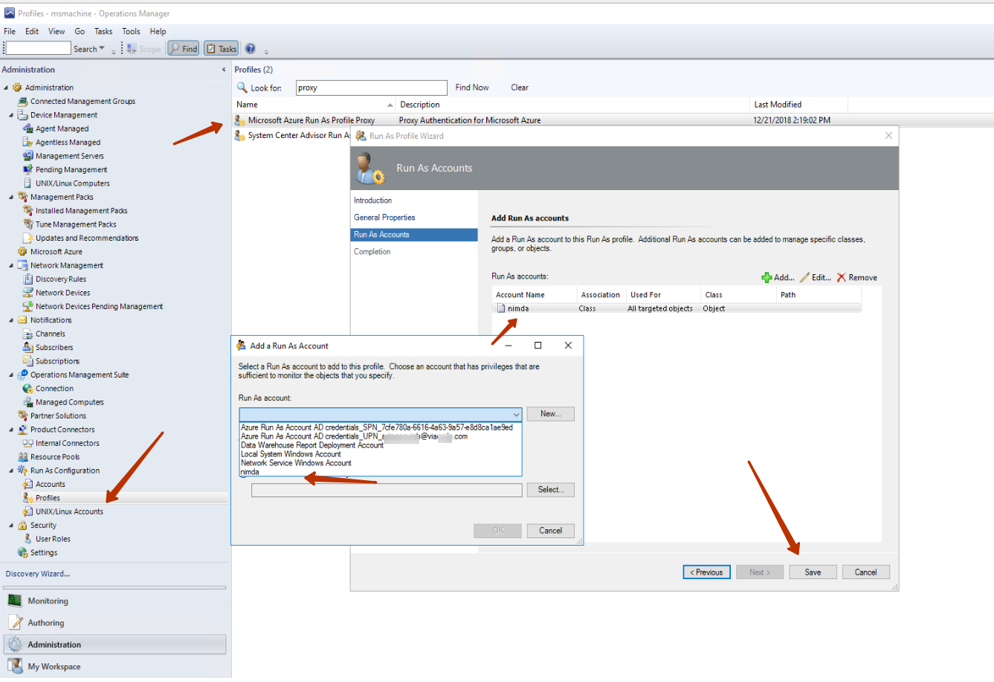
* **Create a Windows Run as Account with access to the proxy**

Add Run as Account to Microsoft Azure Run as Profile Proxy.

Create Windows Run As account: e.g. account of domain admin.



**Add this run as account to run as profile proxy for Azure**



CredentialCache DefaultCredentials Property (the DefaultCredentials property applies only to NTLM, negotiate, and Kerberos-based authentication.):

<https://msdn.microsoft.com/enus/library/system.net.credentialcache.defaultcredentials(v=vs.110).aspx>

WebProxy UseDefaultCredentials Property:

<https://msdn.microsoft.com/en-us/library/system.net.webproxy.usedefaultcredentials(v=vs.110).aspx>

**Note.** Basic proxy configuration via the Administration wizard is not available as long as ADAL library is not able to obtain token through the proxy.

### Low-Privilege Configuration

Azure Active Directory accounts can be configured to have read-only access to Azure Resource Manager resources.

To monitor older services (e.g. Mobile Services and RDFE resources), it is necessary to make the Azure Active Directory account used for monitoring a co-administrator on the subscription. You can find the corresponding instructions in the [How to add or change Azure administrator roles](https://docs.microsoft.com/en-us/azure/billing-add-change-azure-subscription-administrator) article (see the "Azure classic portal" section).

If you need an opportunity to run some service tasks directly from the Operations Manager Console, then you can configure the AAD account to have Owner or Contributor permissions to the below functionality:

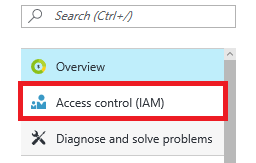
|  |  |
| --- | --- |
| Action | Functionality |
| Microsoft.ClassicStorage/storageAccounts/listKeys/action | Read Azure diagnostic logs from storage.  Groom Storage Accounts |
| Microsoft.ClassicCompute/virtualMachines/restart/action | Task: Restart Virtual Machine |
| Microsoft.ClassicCompute/virtualMachines/start/action | Task: Start Virtual Machine |
| Microsoft.ClassicCompute/virtualMachines/stop/action | Task: Stop Virtual Machine |
| Microsoft.ClassicCompute/virtualMachines/shutdown/action | Task: Shutdown Virtual Machine |
| Microsoft.ClassicCompute/domainNames/slots/write | Task: Scale Role |
| Microsoft.ClassicCompute/domainNames/swap/action | Task: Swap between environments |
| Microsoft.AlertsManagement/alerts/{alertId}/changestate?api-version= {apiVersion} | Task: Close All Scheduled Query Rule Alerts |
| Microsoft.AlertsManagement/alerts/{alertId}/changestate?api-version= {apiVersion} | Task: Close All Activity Log Alerts |

* **Important:** If your subscription is created via SPN, your application must have *Contributor* rights to perform the actions listed in the table above (including those related to Non-Classic Virtual Machines). To grant these rights to your application, you must perform the following steps:

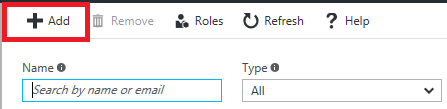
1. Go to Azure portal and find out the corresponding application display name in the “App Registrations” section of the “Azure Active Directory”.



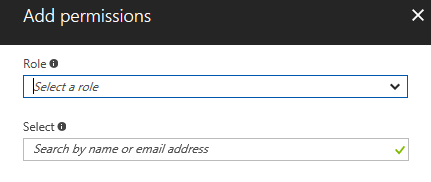
1. In the “Subscriptions” section, select your subscription and go to “Access control (IAM)” section:



1. Click the “Add” button in the middle section of the portal page:



1. In the right section of the portal page, enter your application display name in the “Select” field and choose the “Contributor” option in the “Role” field:



1. Click the “Save” button to apply the changes.

#### Telemetry Data

Below telemetry data is collected from AzureMP

* Azure MP version, number of subscriptions added\removed.
* No of resource groups, no of resources monitored, their type and metrics.
* Types of alerts monitored and their count including fired alerts.
* Service types and metrics in user's connected azure subscriptions

VMs data such as OS, publisher, and version.

## Links

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

### System Center Operations Manager

 [Management Pack Life Cycle](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-lifecycle?view=sc-om-2019)

 [How to Import a Management Pack](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-import-remove-delete?view=sc-om-2019)

 [Tuning Monitoring by Using Targeting and Overrides](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-create-unsealed-mp?view=sc-om-2019)

 [How to Create a Run As Account](https://docs.microsoft.com/en-us/system-center/scom/manage-security-create-runas-link-profile?view=sc-om-2019)

 [How to Export a Management Pack](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-import-remove-delete?view=sc-om-2019)

 [How to Remove a Management Pack](https://docs.microsoft.com/en-us/system-center/scom/manage-mp-import-remove-delete?view=sc-om-2019)

For questions about the Operations Manager and management packs, see the [System Center Operations Manager community forum](http://go.microsoft.com/fwlink/?LinkID=179635).

A useful resource is the [System Center Operations Manager Unleashed blog](http://go.microsoft.com/fwlink/?LinkId=246391), which contains “By Example” posts for specific management packs.

For additional information about the Operations Manager, see the [System Center 2012 - Operations Manager Survival Guide](http://go.microsoft.com/fwlink/?LinkId=246383).

Important iconImportant

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: Known Issues

##### Issue: Alerts on metrics for disabled rule in Azure

If metric alert rule disabled on Azure portal and still has not closed alerts, metric alert object that replicates its state in SCOM will change state to **Healthy** regardless of remaining Fired alerts left behind in Azure.

###### Issue: Rule that created more than 30 days ago in Azure and still Unhealthy might not display alerts in Azure. Resolution: Make changes for the rule threshold in Azure portal and save changes. Alert on rule will re-appear in Azure portal again within filter interval: last 30 days.

#### Issue: Empty status in Subscription and Service Types tab in Azure MP Wizard after Operations Manager database grooming (7 days by default)

**Resolution:** Press [Refresh data] in Wizard to obtain actual state of services in the subscription.

#### Issue: Sometimes, monitoring stopped if Azure failed to respond with errors 500, 504.

**Resolution:** In order to reestablish monitoring, user should go to Monitoring tab > Operations Manager> Management Server > Management Servers State dashboard, select server in Management Server State dashboard, in Tasks pane run “Flush Health Service State and Cache” task.

#### Issue: Sometimes, monitoring of Services stopped: no state changes

**Resolution:** Same as above.

Issue: If SQL Azure database monitoring is enabled, Event Log at SCOM machine will be filled with EventID: 11422 entries and the following message: “Message: ParentResourceNotFound: Cannot perform requested operation on nested resource”, because the resource provider does not return metrics for the master database.   
**Resolution:** To avoid this problem, add ‘master’ database to the exclude list.

##### Issue: Not monitoring resources when proxy is configured while adding SPN details.

**Resolution:** Uncheck proxy settings during SPN configuration.

##### Issue: Not monitoring activity log alerts when created with alert category – “All Administrative Operations” in Azure portal.

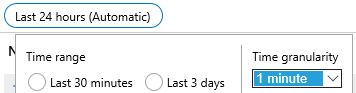
Resolution: Currently this version does not support monitoring of activity log alerts configured with ‘All Administrative Operations’.

#### Issue: Virtual Machine Guest metrics enabled with Azure Diagnostics default settings are not collected by the Azure management pack in the 1.5.20.18 CTP and higher

**Resolution:** Starting Azure MP 1.7.0.0 new way to collect Guest metrics implemented with Guest metrics extension. Follow “Guest Metrics for Virtual Machines” section for more information.

#### Issue: In Azure MP 1.5.30.26 and higher Storage account Transactions/Ingress/Egress has aggregation type SUM on portal and Total in SCOM, metrics mismatch.

**Resolution:** SUM aggregation type is displayed on portal, but actually Total aggregation is returned through REST API. In order to match metrics on portal and in Operations Manager user should specify Time granularity for the above metrics in graph on portal. Time granularity should be set to 1 minute.



#### Issue: “Could not load file or assembly” error when click on “Add Subscription” in Administration tab occurs sometimes after initial management pack installation

**Resolution:** Issue occurs because dlls were not yet initialized. Resolution: run “Flush Health Service state and cache” task. Restart console.

#### Issue: State column may disappear in the management pack State views after several management pack reinstallations

**Resolution:** Use the “Personalize view” context menu option to reset to the defaults.

#### Issue: Some performance counters are not available until they have a non-zero value. Resolution: No resolution is available.

Issue: The Distributed Application State view is empty by default.  
**Resolution:** Create a distributed application to see the resources here.

Issue: If SQL Azure database monitoring is enabled, Event Log at SCOM machine will be filled with EventID: 11422 entries and the following message: “Message: ParentResourceNotFound: Cannot perform requested operation on nested resource”, because the resource provider does not return metrics for the master database.   
**Resolution:** To avoid this problem, add ‘master’ database to the exclude list.

Issue: No performance counters are available in the Add Monitoring wizard for Mobile Services when the Operations Manager console is running at a computer using Windows 8.1 or newer.   
**Resolution:** Launch the wizard from a computer running the SCOM Server.

Issue: No performance counters are available in the Add Monitoring wizard for Mobile Services when the Operations Manager console is running at a computer using Windows 8.1 or newer.   
**Resolution:** Launch the wizard from a computer running the SCOM Server.

#### Issue: For classic (Microsoft.ClassicStorage provider) storage accounts, metrics are not collected.

**Resolution:** The performance counters are not available for classic (Microsoft.ClassicStorage provider) storage accounts via Azure ARM REST API.

#### Issue: Tags are not properly discovered for SQL Azure databases (Microsoft.Sql/servers/databases), because the resource provider does not expose tags in the corresponding /read operations.

Resolution:No resolution is available.

#### Issue: The Azure management pack cannot be removed due to a SCOM issue.

**Resolusion:** To remove the management pack manually, run the following code on the Operations Manager database:

*exec p\_TypeDeletePermanent 'E2169E37-FF79-4877-5AFF-987AAF0F9DBF'*

*go*

*exec [dbo].[p\_ManagementPackRemove] 'C7B2E0B6-A068-544D-CF8F-B26A3B6DDC52'*

*go*

#### Issue: Custom Events and performance counters for web and worker roles collected by Azure diagnostics for Virtual Machines (non-classic) are not supported. Resolution: No resolution is available.

**Issue**: **The Azure management pack does not support proxy for Storage Grooming Probe**, which is used by the following rules:

* + Windows Azure NT Event Log Grooming
  + Windows Azure Performance Counter Grooming
  + Windows Azure .NET Trace Grooming

Therefore, Microsoft.WindowsAzure.Storage.CloudStorageAccount is used in this probe, and it does not support proxy in practice.

#### Issue: Adding new subscriptions may fail if monitoring templates from the previous management pack installations (if there were any) are not removed.

Normally, they are removed automatically upon uninstallation of the management pack.

**Resolution:** Otherwise, remove those templates manually in order to avoid errors while adding the subscriptions.

#### **Issue**: The“Classic Virtual Machine Turn Off Monitor” does not work if the corresponding virtual machine is stopped via the old **Azure** portal. Alternatively, it will not work if the virtual machine is stopped via the new **Azure** portal and then started again via the old one.

**Resolution:** No resolution is available.

#### Issue: Properties of Microsoft Azure Generic Service class type objects are not populated. These objects are inherited from System.Service class; in this class, the properties exist but not populated by the management pack.

**Resolution:** No resolution is available.

#### Issue: The “[Host]” metrics of virtual machines cannot be selected in the Add Monitoring wizard; these metrics are not returned by the Azure Application Insights library. For classic virtual machines, these basic metrics are not [Host], and they are supported.

**Resolution:** No resolution is available.

#### Issue: The “DocumentDB (NoSQL)” metrics are not available in the Add Monitoring wizard due to a problem with the Microsoft.Azure.Insights dll library.

**Resolution:** No resolution is available.

#### Issue: The output of the “Obtain Service Types and Performance Counters Data” task may seem incomprehensible.

**Resolution:** This is an internal task, and it should not be run manually.

#### Issue: The “Change Number of Role Instances”, “Swap Staging And Production Slots”, “Start Deployment Slot”, “Suspend Deployment Slot” tasks may fail silently without providing information about the failure.

**Resolution:** To resolve the issue, the Azure Cloud services should be configured correctly. Create a cloud service instance and deploy at least one web/worker role. For the “Swap Deployment Slots” task, you should configure two slots for Cloud service: staging and production.

#### Issue: the “ArmPerformanceCollectionProbe” module may throw the "Period is less than timegrain" exception to the event log. It can happen if interval parameter value of the corresponding performance collection rule is overridden with a small value, or if timegrain parameter value of the metric is large.

**Resolution**: To avoid this error, make sure that the Interval value is greater than the timegrain value.

Issue: Custom WAD metrics do not appear in the performance view, and there are no custom WAD events’ alerts. This issue is accompanied by the "Atom format is not supported" warnings in the Event Log saying that the requests to WAD Performance Counters and WAD Events tables failed.

**Resolution:** To avoid this issue, the "Storage service API version" should be changed to an earlier date than it is set by default in order to make custom XMLs working (the path is as follows: SCOM Console->Administration->Azure->Edit Subscription->Endpoint-> Storage service API version).

#### Issue: The “Restart” task does not start a virtual machine (whether it is classic or non-classic) if its status is “Stopped” or “Stopped (deallocated)”. Moreover, it is not recommended to use this task for virtual machines with the above statuses, as long as it may lead to monitoring issues.

**Resolution:** No resolution is available.

#### Issue: Upon upgrade of the management pack from version 1.3.22.0 and higher, monitoring may be broken and the following errors may occur in the Operations Manager event log: “Microsoft.SystemCenter.Azure.Modules.RoleInstanceStatusProbeModule.VirtualMachineStatusDS module type cannot be found.”, “Invalid module configuration”.

**Resolution:** To resolve the issue, perform the following steps:

* Stop the Operations Manager Health Service.
* Remove the SCOM folder containing the cache (by default, the path is as follows: C:\Program Files\Microsoft System Center 2016\Operations Manager\Server\Health Service State).
* Start the Operations Manager Health Service.

#### Issue: The “NoRegisteredProviderFound: No registered resource provider found for location 'centralus' and API version '2014-04-01' for type 'namespaces/notificationHubs'.” exception may occur in the Operations Manager event log.

Resolution: No resolution is available.

#### Issue: The “Requested value 'Milliseconds' was not found” exception may occur in the Operations Manager event log.

**Resolution:** No resolution is available.

#### Issue: Multiple “Microsoft.ClassicStorage:ResourceUnknown: Exception of type 'Microsoft.WindowsAzure.Management.Monitoring.Rest.MonitoringServiceException' was thrown.” warnings may occur in the Operations Manager event log.

**Resolution:** No resolution is available.

#### Issue: Errors may occur in the event log while collecting Azure Application Insights performance metrics.

**Resolution**: Issue might occur after upgrade if old information stored in cache and can not be updated. In the Operations Manager Console, go to Authoring – Microsoft Azure Monitoring, and double-click the template for your subscription. Click the “Refresh Data” button in the “Subscription” tab.

#### Issue: “Full scan” in Azure Wizard has been selected and no objects are discovered, warning with id 33333 and error with id 10801 appear in Event Log.

**Resolution**: Some hidden services such as networkinterfaces/ipConfigurations, networkSecurityGroups/defaultSecurityRules, networkSecurityGroups/securityRules, virtualNetworks/subnets that obtained with Full Scan might cause discovery failures. Uncheck additional services and their parents in *Service types tab*, **uncheck** “Full scan” checkbox in *Subscription tab* and press [Refresh Data].

#### SCOM Issue: “An object of class was not found” or “Object reference not set to an instance of an object” .Net unhandled exception might occur in Operations Manager console on Azure MP views when more than 100 services are deleted or added at once.

**Resolution:** Restart Console. Additionally, you can set up opening the Operations console with /clearcache parameter. More information can be found in [Operations Manager documentation.](https://docs.microsoft.com/en-us/system-center/scom/manage-clear-healthservice-cache?view=sc-om-1807)

#### Issue: “Job Failed” when trying to uncheck selected services in Wizard if custom views configured in Operations Manager for management pack that created for the template.

**Resolution**: When user adds resources to monitor in the Authoring tab, new management pack is created for this. It is not allowed to create custom views for this management pack in Monitoring tab in the Operations Manager Console. If user has targeted custom view to this management pack and then tries to uncheck services from monitoring in Wizard, classes could not be deleted as they are in use, hence “Job Failed” error occurs. Resolution: Create custom views targeted to **new** created unsealed management pack.

#### Issue: ArmPerformanceCollectionProbe issues in eventlog.

**Resolution**: Issue may occur once a day or once in a few days in Operations Manager Event log. If metrics collection on some services stopped it is recommended restart Health Service.

#### Issue: “Service returned error. Check inner exception for more details” error in Azure MP Wizard on click [Refresh data]

**Resolution**: Issue may happen because proxy configured incorrectly. Please refer to proxy configuration section in guide.

#### SCOM Issue: Uncheck or check in Wizard service types that have Metrics (e.g. Virtual Machines, Storage accounts) and save template causes temporary errors in EventLog with id: 10860 from Health Service Module “Insert statement conflicted” for ruleids, id: 10840 for monitorids.

**Resolution**: Issue can temporary happen when SCOM is still running workflows, but they are not present in OperationsManager database any more. No resolution available.

#### SCOM Issue: Too many events with ids 31400, 31401, 31405 related to group membership calculation about deleted objects might occur after management pack upgrade or reinstall same Management pack several times during a short time. Issue can temporary happen and can last for 3 days in case if class relationships changed in version of Management pack (for example, class ancestor changed for metricalert class). Deleted objects marked with “IsDeleted=1” setting in OperationsManager database BaseManagedEntity table, but still remain in the database. Issue will occur until SCOM runs standard data grooming to delete records that marked “IsDeleted” in the Operations Manager database. Resolution: run script against Operations Manager database to force delete records right away.

|  |
| --- |
| DECLARE    @TimeGenerated DATETIME,    @BatchSize INT,    @RowCount INT  SET @TimeGenerated = GETUTCDATE() -- now - purge everything deleted  SET @BatchSize = 10000  EXEC p\_DiscoveryDataPurgingByRelationship @TimeGenerated, @BatchSize, @RowCount  EXEC p\_DiscoveryDataPurgingByTypedManagedEntity @TimeGenerated, @BatchSize, @RowCount  EXEC p\_DiscoveryDataPurgingByBaseManagedEntity @TimeGenerated, @BatchSize, @RowCount |

#### Issue: “Failed to find metric configuration for provider” Warning on specific metrics with event id 6400 occurs each 15 minutes.

Issue may happen because some resources fail to return metrics from Azure, for example web/sites (CPUTime) or publicIPAddresses metrics.

**Resolution**: Check if metric available and collected for specified service on Azure portal. If metric cannot be configured uncheck this metric in Azure MP Wizard > Metrics tab or add service instance to Exclude list.

## Appendix: Management Pack Contents

**Operations Manager Management Service**

**- Rules (alerting)**

**Microsoft Azure Invalid AD Credentials**

Alert generating rule for when the AD credentials for the Management API are not valid

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | Yes | | Priority |  | 2 | | Severity |  | 2 | |  |
|  |  |  |

**Microsoft Azure HTTP Operation Exception**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | Yes | | Priority |  | 2 | | Severity |  | 2 | |  |
|  |  |  |

**Microsoft Azure Module Initialization Failure**

Alert generating rule for when Microsoft Azure Monitoring module failed to initialize

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | Yes | | Priority |  | 2 | | Severity |  | 2 | |  |
|  |  |  |

**Microsoft Azure Storage Table Not Found**

Alert generating rule for when the target storage table does not exist

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | Yes | | Priority |  | 1 | | Severity |  | 1 | |  |
|  |  |  |

**Microsoft Azure .Net Framework Rule**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | Yes | | Priority |  | 2 | | Severity |  | 2 | |  |
|  |  |  |

**Compute VM Removed Information Alert Rule**

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | No |
| Generate Alerts |  | Yes |
| Priority |  | 0 |
| Severity |  | 0 |

**Compute VM Added Information Alert Rule**

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | No |
| Generate Alerts |  | Yes |
| Priority |  | 0 |
| Severity |  | 0 |

**Microsoft Azure Invalid AD Credentials**

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | No |
| Generate Alerts |  | Yes |
| Priority |  | 0 |
| Severity |  | 0 |

**Classic Compute VM Removed Information Alert Rule**

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | No |
| Generate Alerts |  | Yes |
| Priority |  | 0 |
| Severity |  | 0 |

**Classic Compute VM Added Information Alert Rule**

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | No |
| Generate Alerts |  | Yes |
| Priority |  | 0 |
| Severity |  | 0 |

**Microsoft Azure ARM Service Resource**

Class representing all Microsoft Azure ARM (Azure Resource Manager) service resources

**Microsoft Azure ARM Service Resource - Dependency (rollup) monitors**

**Insights Classic Alert Rule for ARM Resource Performance Dependency**

Microsoft Azure ARM Resource performance depends on Insights Alert Rule Performance.

**Insights Classic Alert Rule for ARM Resource Availability Dependency**

Microsoft Azure ARM Resource availability depends on Insights Alert Rule Performance.

**Insights Classic Alert Rule for ARM Resource Configuration Dependency**

Microsoft Azure ARM Resource configuration depends on Insights Alert Rule Performance.

**Insights Classic Alert Rule for ARM Resource Security Dependency**

Microsoft Azure ARM Resource security depends on Insights Alert Rule Performance.

**Insights Metric Alert for ARM Resource Availability Dependency**

Microsoft Azure ARM Resource availability depends on Insights Metric Alert Availability.

**Insights Metric Alert for ARM Resource Security Dependency**

Microsoft Azure ARM Resource security depends on Insights Metric Alert Security.

**Insights Metric Alert for ARM Resource Performance Dependency**

Microsoft Azure ARM Resource performance depends on Insights Metric Alert Performance.

**Insights Metric Alert for ARM Resource Configuration Dependency**

Microsoft Azure ARM Resource configuration depends on Insights Metric Alert Configuration.

**Insights Activity Log Alert for ARM Resource Availability Dependency**

Microsoft Azure ARM resource availability depends on Insights Activity Log Alert availability.

**Microsoft Azure Distributed Application - Rules (non-alerting)**

**Collect Availability of Manageability Service**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | No | | Interval in Seconds |  | 3600 | | Sync Time |  | 12:15 | | Timeout Seconds |  | 3600 | |  |
|  |  |  |

**Microsoft Azure Domain Name**

Microsoft Azure Domain Name

**Microsoft Azure Domain Name - Unit monitors**

**Microsoft Azure Cloud Service Certificate Expiration Monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 432000 | | Number of days | Number of days | 10 | | Sync Time | Sync Time |  | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Microsoft Azure Domain Name - Tasks**

**Swap Staging And Production Slots**

Swaps the staging slot to the production slot.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | swap | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Microsoft Azure Insights Classic Metric Alert**

**Microsoft Azure Insights Classic Metric Alert - Unit monitors**

**Insights Classic Metric Alert Monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 300 | | Sync Time | Sync Time |  | | Timeout Seconds | Timeout Seconds | 30 | |  |
|  |  |  |

**Microsoft Azure Insights Metric Alert**

**Microsoft Azure Insights Metric Alert - Unit monitors**

**Insights Metric Alert Monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 300 | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  | **Microsoft Azure Insights Scheduled Query Rule**  **Microsoft Azure Insights Scheduled Query Rule - Unit monitors**  **Insights Scheduled Query Rule Monitor**   |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 300 | | Timeout Seconds | Timeout Seconds | 300 | | Time Range Hours | Parameter allows setting up how far in the past to look for Azure Alerts. The Minimum value is 1 hour, the Maximum value is 720 hours (30 days) | 720 | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Microsoft Azure Insights Scheduled Query Rule – Tasks**  Task changes the state of all alerts to "Closed" for the corresponding rule. "Time Range Hours" option defines the period of time in the past over which Azure Alerts are looked for. Default Maximum Time range — 30 days (720 hours).   |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | Close All related alerts | | Time Range Hours | Time Range Hours | 720 | | Timeout Seconds | Timeout Seconds | 300 |   **Microsoft Azure Insights Activity Log Alert**  **Microsoft Azure Insights Activity Log Alert- Unit monitors**  **Insights Activity Log Alert Monitor**   |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 300 | | Timeout Seconds | Timeout Seconds | 30 | | Time Range Hours | Parameter allows setting up how far in the past to look for Azure Alerts. The Minimum value is 1 hour, the Maximum value is 720 hours (30 days) | 720 | |  |

**Microsoft Azure Insights Activity Log Alert – Tasks**

Task changes the state of all alerts to "Closed" for the corresponding rule. "Time Range Hours" option defines the period of time in the past over which Azure Alerts are looked for. Default Maximum Time range — 30 days (720 hours).

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | Yes |
| Operation Name | The name of operation to perform at resource | Close All related alerts |
| Time Range Hours | Time Range Hours | 720 |
| Timeout Seconds | Timeout Seconds | 300 |

**Microsoft Azure Resource Group**

**Microsoft Azure Groups and Resources Discovery for <subscriptionID>**

By default, management pack rediscovers Azure resources on the specified subscription within 4 hours interval.

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Default value** |
| Enabled |  | Yes ( for <subscriptionid> |
| Interval Seconds | Interval Seconds | 14400 |
| Timeout Seconds | Timeout Seconds | 120 |

**Microsoft Azure Resource Group - Dependency (rollup) monitors**

**Resource Performance Dependency**

Microsoft Azure Resource Group performance depends on Resource Performance.

**Resource Availability Dependency**

Microsoft Azure Resource Group availability depends on Resource Availability.

**Microsoft Azure Role**

**Microsoft Azure Role - Discoveries**

**Microsoft Azure Role Diagnostic Storage Account Property Discovery**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Interval Seconds | Interval Seconds | 14400 | | Storage Account Override | Diagnostic Storage Account Override |  | | Timeout Seconds | Timeout Seconds | 120 | |  |
|  |  |  |

**Microsoft Azure Role - Tasks**

**Change Number of Role Instances**

Increase or decrease the number of role instances

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Role Instance Count | Role Instance Count | 2 | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Microsoft Azure Service**

Microsoft Azure Service In Resource Group

**Microsoft Azure Service - Dependency (rollup) monitors**

**ARM Resource Security Dependency**

Microsoft Azure ARM Service security depends on ARM Service Resource Security.

**ARM Resource Availability Dependency**

Microsoft Azure ARM Service availability depends on ARM Service Resource Availability.

**ARM Resource Performance Dependency**

Microsoft Azure ARM Service performance depends on ARM Service Resource Performance.

**ARM Resource Configuration Dependency**

Microsoft Azure ARM Service configuration depends on ARM Service Resource Configuration.

**Insights Classic Alert Rule for ARM Service Performance Dependency**

Microsoft Azure ARM Service performance depends on Insights Alert Rule Performance.

**Insights Classic Alert Rule for ARM Service Availability Dependency**

Microsoft Azure ARM Service availability depends on Insights Alert Rule Performance.

**Insights Classic Alert Rule for ARM Service Configuration Dependency**

Microsoft Azure ARM Service configuration depends on Insights Alert Rule Performance.

**Insights Classic Alert Rule for ARM Service Security Dependency**

Microsoft Azure ARM Service security depends on Insights Alert Rule Performance.

**Insights Metric Alert for ARM Service Availability Dependency**

Microsoft Azure ARM Service availability depends on Insights Metric Alert Availability.

**Insights Metric Alert for ARM Service Security Dependency**

Microsoft Azure ARM Service security depends on Insights Metric Alert Security.

**Insights Metric Alert for ARM Service Performance Dependency**

Microsoft Azure ARM Service performance depends on Insights Metric Alert Performance.

**Insights Metric Alert for ARM Service Configuration Dependency**

Microsoft Azure ARM Service configuration depends on Insights Metric Alert Configuration.

**Insights Activity Log Alert for ARM Service Availability Dependency**

Microsoft Azure ARM Service availability depends on Insights Activity Log Alert availability.

**Insights Scheduled Query Rule for ARM Service Availability Dependency**

Microsoft Azure ARM service availability depends on Insights Scheduled Query Rule availability.

**Microsoft Azure Storage Account**

**Microsoft Azure Storage Account - Rules (non-alerting)**

**Microsoft Azure Storage .NET Trace Grooming**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | No | | Grace Period Hours | The diagnostics data will be deleted if its timestamp is not within the grace period hours based on the time when the rule is running. | 24 | | Interval Seconds | Interval Seconds | 86400 | | Maximum Data Items to Process | The rule will delete at most Maximum Data Items to Process entities per run. | 0 | | Timeout Seconds | Timeout Seconds | 600 | |  |
|  |  |  |

**Microsoft Azure Storage Performance Counter Grooming**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | No | | Grace Period Hours | The diagnostics data will be deleted if its timestamp is not within the grace period hours based on the time when the rule is running. | 24 | | Interval Seconds | Interval Seconds | 86400 | | Maximum Data Items to Process | The rule will delete at most Maximum Data Items to Process entities per run. | 0 | | Timeout Seconds | Timeout Seconds | 600 | |  |
|  |  |  |

**Microsoft Azure Storage NT Event Log Grooming**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | No | | Grace Period Hours | The diagnostics data will be deleted if its timestamp is not within the grace period hours based on the time when the rule is running. | 24 | | Interval Seconds | Interval Seconds | 86400 | | Maximum Data Items to Process | The rule will delete at most Maximum Data Items to Process entities per run. | 0 | | Timeout Seconds | Timeout Seconds | 600 | |  |
|  |  |  |

**Microsoft Azure Storage Account - Rules (non-alerting)**

**Microsoft Azure Storage Account Size Performance Collection rule**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | No | | Interval Seconds | Interval Seconds | 900 | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Microsoft Azure Subscription**

**Microsoft Azure Subscription - Unit monitors**

**Microsoft Azure Subscription Certificate Expiration Monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | No | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 43200 | | Number of days | Number of days | 10 | | Sync Time | Sync Time |  | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Microsoft Azure Subscription - Tasks**

**Get Excluded Resources**

Microsoft Azure Subscription Get Excluded Resources Task

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Timeout Seconds | Timeout Seconds | 600 | |  |
|  |  |  |

**Microsoft Azure Virtual Machine Classic**

**Microsoft Azure Virtual Machine Classic - Unit monitors**

**Microsoft Azure Classic Virtual Machine Turn Off Monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 30 | | Sync Time | Sync Time |  | | Timeout Seconds | Timeout Seconds | 30 | |  |
|  |  |  |

**Microsoft Azure Virtual Machine Classic - Tasks**

**Shutdown Virtual Machine**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | shutdown | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Start Virtual Machine**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | start | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Restart Virtual Machine**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | restart | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Stop Virtual Machine**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | stop | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Microsoft Azure Virtual Machine (Non-Classic)**

**Microsoft Azure Virtual Machine (Non-Classic) - Unit monitors**

**Microsoft Azure Virtual Machine (Non-Classic) Turn Off Monitor**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Generate Alerts |  | True | | Interval Seconds | Interval Seconds | 30 | | Sync Time | Sync Time |  | | Timeout Seconds | Timeout Seconds | 30 | |  |
|  |  |  |

**Microsoft Azure Virtual Machine (Non Classic) - Tasks**

**Restart Virtual Machine**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | restart | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Start Virtual Machine**

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | start | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

**Power Off Virtual Machine**

Note that the virtual machine will continue to be billed.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled |  | Yes | | Operation Name | The name of operation to perform at resource | powerOff | | Request Content | Body of the request. Optional. |  | | Request type | Http request type. Valid values: get, put, post, delete | post | | Timeout Seconds | Timeout Seconds | 300 | |  |
|  |  |  |

## Deprecated Workflows

The following workflows are considered deprecated and disabled by default:   
  
**Rules:**

* Manageability Test Performance Collection Rule

**Unit Monitors:**

* Manageability Test State Monitor
* Manageability Test Performance Monitor

**Dependency Monitors:**

* Client Perspective Dependency
* Azure Dependency
* Azure Distributed Application Service Configuration Dependency
* Azure Distributed Application Service Performance Dependency
* Azure Distributed Application Service Security Dependency
* Azure Distributed Application Service Availability Dependency
* SQL Dependency
* Database Dependency
* Azure Database Availability Dependency
* Azure Database Performance Dependency
* Azure Database Configuration Dependency
* Azure Database Security Dependency
* Azure Storage Accounts Availability Dependency
* Azure Storage Accounts Performance Dependency
* Azure Storage Accounts Configuration Dependency
* Azure Storage Accounts Security Dependency
* Dependency
* Perspective Dependency
* Perspective Performance Dependency
* Perspective Configuration Dependency
* Perspective Security Dependency
* Database Performance Dependency
* Database Configuration Dependency
* Database Security Dependency
* Entity Availability Dependency
* Entity Performance Dependency
* Entity Configuration Dependency
* Entity Security Dependency