

Guide to System Center Management Pack for Microsoft Azure Stack

Microsoft Corporation

Published: April 2019

If you have an idea or suggestion about this management pack, the Operations Manager team encourages you to share it at the [SCOM Feedback site](http://systemcenterom.uservoice.com/forums/293064-general-operations-manager-feedback/filters/top).

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](#_Toc5202445)

[Guide to System Center Management Pack for Microsoft Azure Stack 6](#_Toc5202446)

[Changes History 6](#_Toc5202447)

[Supported Configurations 8](#_Toc5202448)

[Upgrade 8](#_Toc5202449)

[Management Pack Scope 9](#_Toc5202450)

[Prerequisites 10](#_Toc5202451)

[Files in this Management Pack 11](#_Toc5202452)

[Management Pack Purpose 11](#_Toc5202453)

[Mandatory Configuration 11](#_Toc5202454)

[Add Azure Stack Deployment 11](#_Toc5202455)

[Edit Azure Stack Deployment 24](#_Toc5202456)

[Authentication 36](#_Toc5202457)

[Auto-Created SPN AAD deployment 36](#_Toc5202458)

[Create SPN Manually for AAD Deployment 38](#_Toc5202459)

[Create SPN for AD FS deployment 41](#_Toc5202460)

[Create Run As account in the Operations Manager manually 42](#_Toc5202461)

[Run As account and Run As Profile association 44](#_Toc5202462)

[How Health Rolls Up 44](#_Toc5202463)

[View the Information in the Operations Manager Console 45](#_Toc5202464)

[Microsoft Azure Stack Views 45](#_Toc5202465)

[Microsoft Azure Stack App Service Dashboard 46](#_Toc5202466)

[Microsoft Azure Stack Backup Dashboard 47](#_Toc5202467)

[Microsoft Azure Stack Capacity Dashboard 48](#_Toc5202468)

[Microsoft Azure Stack Health Dashboard 51](#_Toc5202469)

[Microsoft Azure Stack Infrastructure Role Dashboard 51](#_Toc5202470)

[Microsoft Azure Stack Marketplace Management Dashboard 52](#_Toc5202471)

[Microsoft Azure Stack Resource Provider Dashboard 53](#_Toc5202472)

[Microsoft Azure Stack Scale Unit Dashboard 54](#_Toc5202473)

[Microsoft Azure Stack Update Status Dashboard 55](#_Toc5202474)

[Microsoft Azure Stack Storage Performance Dashboards 56](#_Toc5202475)

[The Operations Manager Maintenance Mode 58](#_Toc5202476)

[Auto Maintenance Mode 60](#_Toc5202477)

[Region in Maintenance Mode 60](#_Toc5202478)

[Scale Unit Node in Maintenance Mode 62](#_Toc5202479)

[Storage Performance Metric Rules 62](#_Toc5202480)

[Storage Metric Time Grain 63](#_Toc5202481)

[App Service Role Available Workers Rule 65](#_Toc5202482)

[Alert on available workers rule 65](#_Toc5202483)

[Update Run State Monitor 66](#_Toc5202484)

[Health of update run 66](#_Toc5202485)

[Tasks 67](#_Toc5202486)

[Set Additional Information Task 67](#_Toc5202487)

[Force Refresh Tasks 68](#_Toc5202488)

[Auto Maintenance Mode Tasks 69](#_Toc5202489)

[Remaining subscription reads monitoring 72](#_Toc5202490)

[Security Configuration 72](#_Toc5202491)

[Role-Based Access Control Configuration 72](#_Toc5202492)

[Extended Logging 72](#_Toc5202493)

[Worker Task Limit 73](#_Toc5202494)

[Links 74](#_Toc5202495)

[System Center 2012 R2 - Operations Manager 74](#_Toc5202496)

[System Center 2016 - Operations Manager 74](#_Toc5202497)

[Appendix: Known Issues 75](#_Toc5202498)

[Appendix: Management Pack Contents 77](#_Toc5202499)

[Rules (alerting) 77](#_Toc5202500)

[Microsoft Azure Stack App Service Role 77](#_Toc5202501)

[Microsoft Azure Stack App Service Role Instance 79](#_Toc5202502)

[Microsoft Azure Stack Backup 80](#_Toc5202503)

[Microsoft Azure Stack Deployment 81](#_Toc5202504)

[Microsoft Azure Stack Infrastructure Role 84](#_Toc5202505)

[Microsoft Azure Stack Infrastructure Role Instance 85](#_Toc5202506)

[Microsoft Azure Stack Marketplace Management 87](#_Toc5202507)

[Microsoft Azure Stack Region 87](#_Toc5202508)

[Microsoft Azure Stack Resource Provider 103](#_Toc5202509)

[Microsoft Azure Stack Scale Unit 105](#_Toc5202510)

[Microsoft Azure Stack Scale Unit Node 106](#_Toc5202511)

[Microsoft Azure Stack Update 108](#_Toc5202512)

[Microsoft Azure Stack Update Run 110](#_Toc5202513)

Guide to System Center Management Pack for Microsoft Azure Stack

This guide is based on version **1.0.4.0** of the Management Pack for Microsoft Azure Stack.

### Changes History

| Release Date | Changes |
| --- | --- |
| April 2019 (version 1.0.4.0) | * Implemented the App Service Roles and the Role Instances monitoring, management, and the dashboard. * Added Restart Infrastructure Role Task * Implemented the Backup dashboard * Implemented the Marketplace Management dashboard * Alert on Failed Update Run now will only show up for latest update |
| February 2019 (version 1.0.3.11) | * Removed Stop Infrastructure Role Instance Task * Removed Shutdown Infrastructure Role Instance Task * Increased interval second value for Update Run State Monitor and Update State Monitor * Increased interval of re-discovering of Update Runs |
| December 2018 (version 1.0.3.7) | * Changed the processing of service names in monitors and tasks |
| April 2018 (version 1.0.3.0) | * Implemented “Auto-Created SPN” and “Manual SPN” for AAD environments that allows support multi-factor authentication. * Implemented the Storage Performance metrics collection and the dashboard. * Implemented the Resource Provider monitoring and the dashboard. * Implemented the Update monitoring, management, and the dashboard. * Implemented the Scale Unit and the Unit Node monitoring, management, and the dashboard. * Implemented the Infrastructure Roles and the Role Instances monitoring, management, and the dashboard. * Implemented the “Auto Maintenance Mode Monitoring Rule for Scale Unit Node” that allows enable maintenance mode for the node in the Operations Manager when node is in maintenance state. * Implemented “Remaining Subscription Reads Monitor” that checks the number of the remaining subscription reads to the Azure Stack API. * Added information about the last update to the Regions. |
| July 2017 (version 1.0.2.3) | * Implemented the “Edit Deployment” wizard. * Improved the authentication by means of Azure Active Directory (UPN authentication) and Active Directory Federation Services (UPN and AD FS SPN authentication). * Implemented UI improvements in the “Add Deployment” wizard. * Implemented the Capacity Dashboard. * Implemented the “Auto Maintenance Mode Monitoring Rule” that checks if any updates are run on Azure Stack regions and switches regions that are being updated to maintenance mode in the Operations Manager. Implemented the “Turn Off Auto Maintenance Mode” and the “Turn On Auto Maintenance Mode” tasks to manually disable and enable the Auto Maintenance Mode. * Implemented improvements to reflect changes in the API. * Updated the display strings. * Added a workaround to support Alert names and descriptions to be displayed in the Operations Manager Reports as a plain text. |
| April 2017 (version 1.0.1.0) | The Technical Preview release of this management pack. |

## Supported Configurations

This management pack requires System Center 2012 R2 Operations Manager, System Center 2016 Operations Manager, System Center 2019 Operations Manager or System Center Operations Manager 1801.

A dedicated Operations Manager management group is not required.

### Upgrade

Management pack supports upgrade from version 1.0.3.11 and higher.

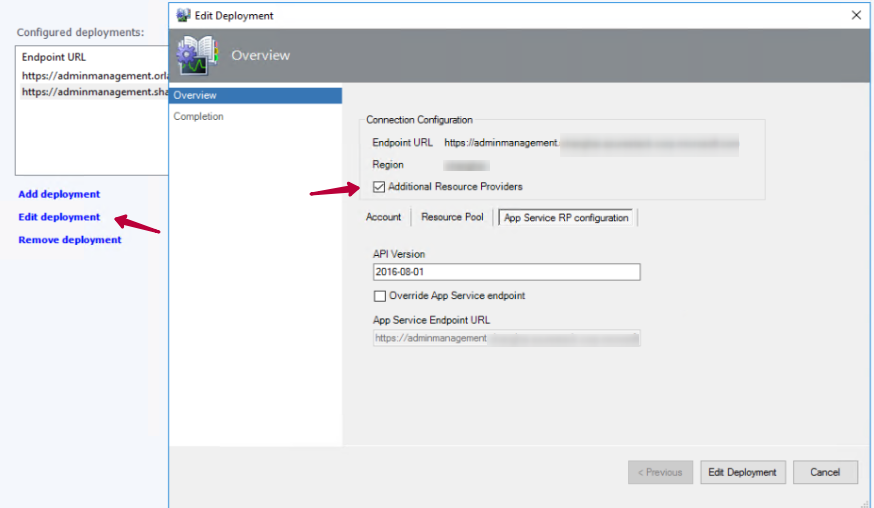
#### Known issues related to upgrade:

##### “The dashboard view has been deleted or no longer exists” message on App Service and Backup Dashboards.

**Resolution:** A lot of new objects discovered and data sources need to be reinitialized for data to be displayed on dashboards for the first time. Restart Operations Manager Console after upgrade. Dashboard view will be populated with discovered data.

##### No data is displayed on App Service Dashboard.

**Resolution:** In order to display monitoring data on App Service Dashboard, additional Resource Provider should be added to the Azure Stack deployment. In the Operations Manager **Edit Deployment Wizard** select “**Additional Resource Providers**” checkbox. For this go to Administration tab > Microsoft Azure Stack node.



## Management Pack Scope

The Management Pack for Microsoft Azure Stack is designed to monitor the availability and health state of the Azure Stack deployments, regions, resource providers, updates, update runs, scale units, unit nodes, infrastructure roles, backup states, app service roles and their instances (logical entities comprised of the hardware resources).

The Management Pack collects and displays actual capacity metrics for the Azure Stack deployment such as physical storage, physical memory and public IP pools usage and actual storage performance metrics for blob, table and queue services.

The Management Pack runs on a selected server pool and uses Azure Stack REST APIs to remotely discover and collect information about the specified Azure Stack deployment.

|  |
| --- |
| * **Important:**   Concurrent monitoring of multiple regions has not been tested. |

## Prerequisites

Before running this management pack, you must manually ensure that the following prerequisites are met:

* You must have version 1809 of the Azure Stack installed.
* You must have an Operations Manager 2012 R2 or later environment installed external to Azure Stack.
* For deployments using Azure Active Directory, the management server requires communication with Microsoft Azure. In this case, the workstation with the Operations Manager console that will be used to configure Azure Stack monitoring must have a connection to the Internet during the initial configuration process.
* The management pack is supported to monitor up to 15 deployments and up to 15 regions per deployment.
* All management servers in your management server pool and the workstation with the Operations Manager console must have .NET framework 4.5 or later installed.
* The same SSL certificate must be installed in the Trusted Root Certificate Authority Store on the computer with the management pack installed, that was provided for the Azure Stack deployment of Azure Resource Manager.
* If an AD FS Service Principal Name (SPN) is used for authentication, the corresponding certificate created along with the SPN must be installed on the computer where the management pack is used. For more details, see the [Create and Configure AD FS SPN](#_Create_SPN_for) section.
* In order to create a Service Principal Name via PowerShell, you must [install](https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-powershell-install) PowerShell modules for Azure Stack; [download](https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-powershell-download) Azure Stack tools from GitHub repository and [configure](https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-powershell-configure-admin) an environment based on the Azure Stack online tutorial.
* A user that creates SPN application on the Azure portal must have **Owner** permissions to the subscription on the Azure Stack administrator portal.
* The Azure Stack Service Administrator account credentials or other user credentials that have **Owner** or **Contributor** rights to the Default Provider Subscription are required by this management pack.

For more information, visit the [Azure Stack deployment prerequisites](https://docs.microsoft.com/azure/azure-stack/azure-stack-deploy) page.

## Files in this Management Pack

The Management Pack for Microsoft Azure Stack includes the following files:

* Microsoft System Center Management Pack for Microsoft Azure Stack.msi
* Microsoft Azure Stack Management Pack Guide.docx

## Management Pack Purpose

For details on the discoveries, rules, monitors, tasks, and views contained in this management pack, see [Appendix: Management Pack Contents](#zf475f3cc57b84a049d89cda7b1f37ba8).

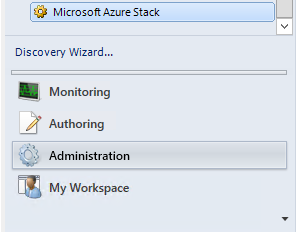
## Mandatory Configuration

This section explains how to configure the Management Pack for Microsoft Azure Stack to discover and monitor your deployments. The management pack does not discover or monitor Azure Stack on import. To monitor Azure Stack deployments, you must add Azure Stack deployments that you want to monitor. Adding a deployment via the “Add Deployment” wizard is described in the section below.

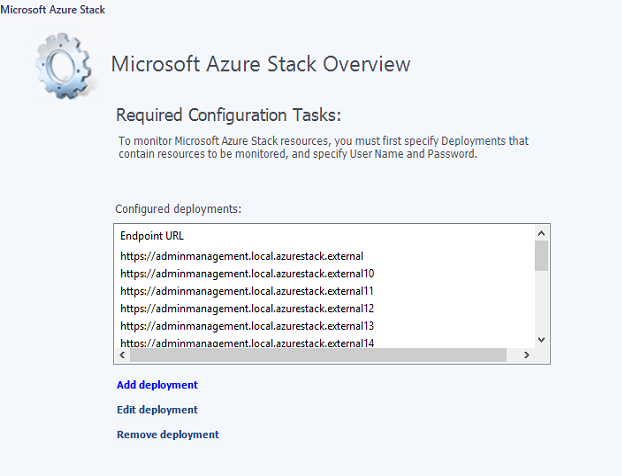
### Add Azure Stack Deployment

To configure monitoring of your Azure Stack deployments, you must run the corresponding “Add Deployment” wizard. This procedure assumes that you have already imported the Management Pack for Microsoft Azure Stack into the Operations Manager. Then, perform the following steps.

In the Operations Manager console, open the **Administration** workspace, and then click the **Microsoft Azure Stack** node:

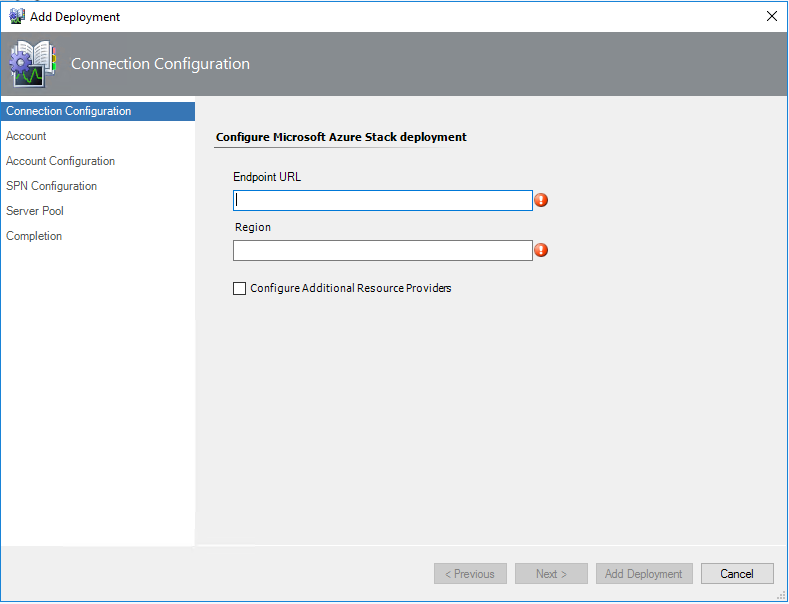


To start the wizard, click **Add deployment** in the **Microsoft Azure Stack Overview** window:



In the **Connection** **Configuration** window of the wizard, specify the following:

* + The endpoint URL of the Resource Manager API (<https://adminmanagement.local.azurestack.external> for the development kit environment).
  + Any region of your Azure Stack deployment.

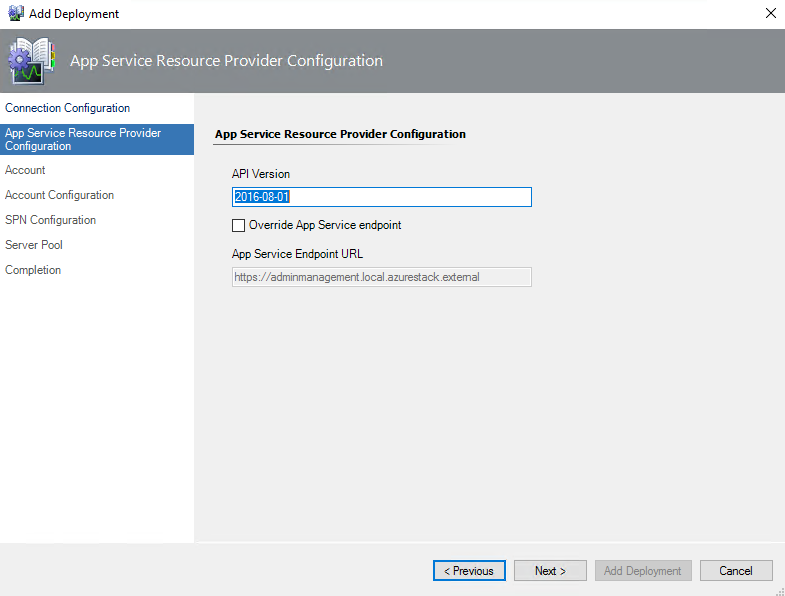


#### Configure Additional Resource Providers

Enable checkbox **Configure Additional Resource Providers** to monitor and manage **App Service Roles** and **Role Instances** from SCOM

Click the **Next** button to configure **App Service Resource Providers**. In this window, perform the following:

* + In the **API Version** text field, type the desired value (API Version by default: **2016-08-01**)
  + You can override **App Service Endpoint URL** by clicking on the checkbox (**App Service Endpoint URL** is the same as **Endpoint URL** by default)

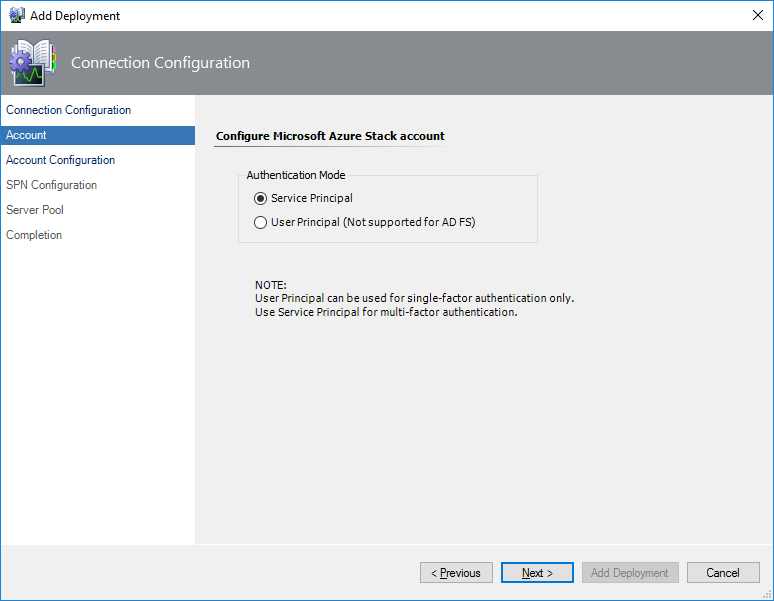


#### Account configuration

In the **Account** window, select whether to use **Service Principal** or **User Principal** for authentication.

Microsoft Azure Stack Management Pack supports two authentication scenarios using User Principal Name (UPN) and Service Principal Name (SPN). UPN is simpler to configure, but it does not work when multi-factor authentication is enforced.

On the other hand, 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.

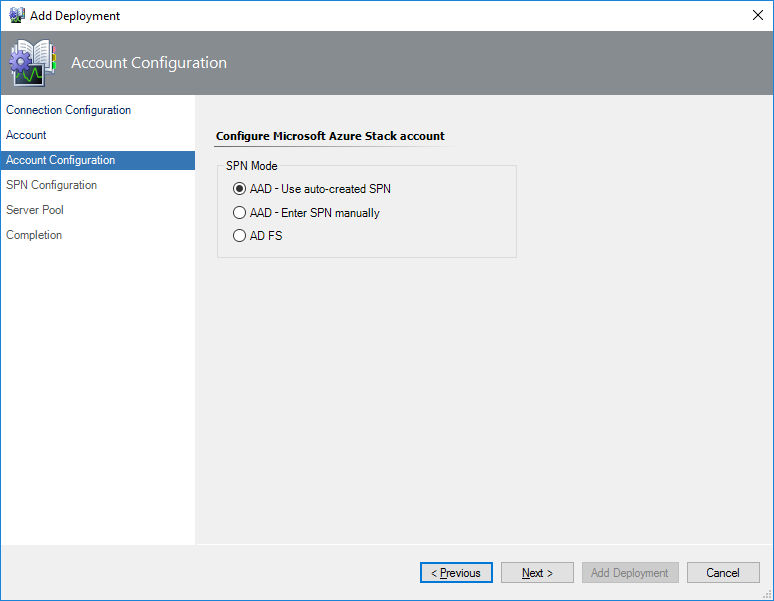


#### SPN Modes:

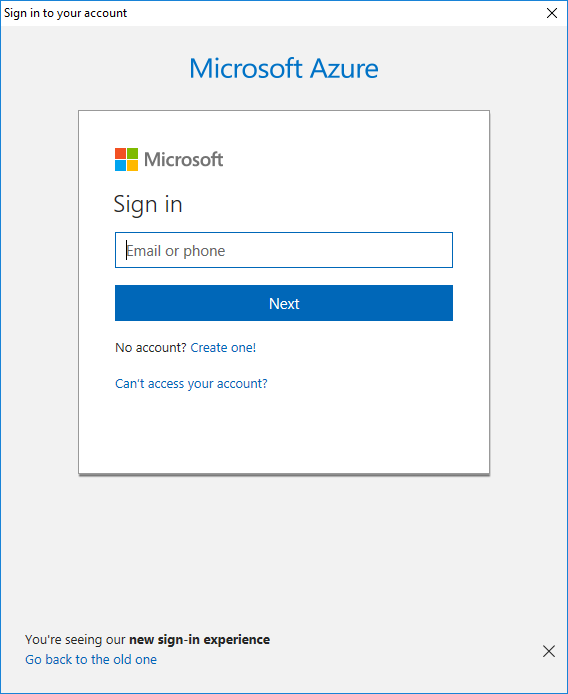
If you select the **Service Principal** option, you must decide whether you are going to use AAD (Azure Active Directory) mode, or Azure AD FS (Active Directory Federation Services) mode.

##### Auto-Created SPN AAD Mode

The wizard provides a possibility to create an AAD Service Principal Name in automatic mode. Therefore, you may select **AAD – Use auto-created SPN** mode and create a new SPN:

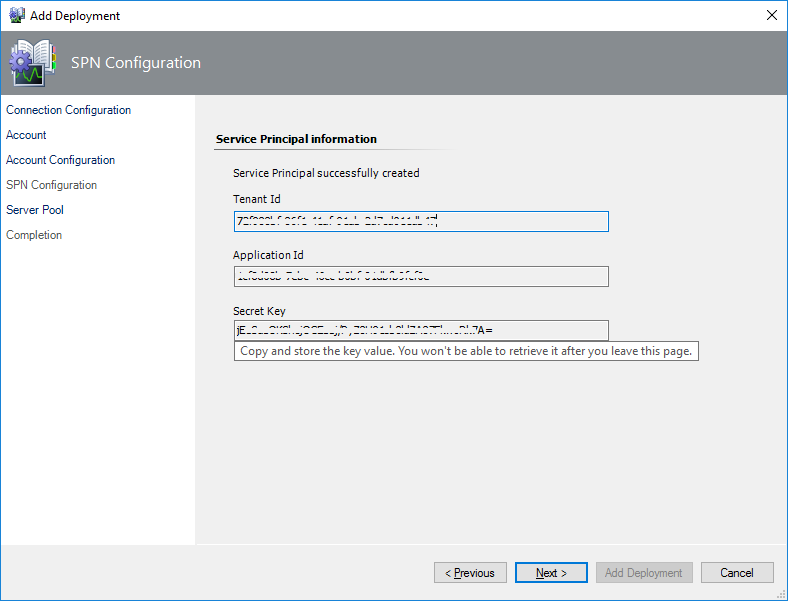


The Microsoft Azure sign-in window will be displayed by clicking the **Next** button:



In this window, sign in to your Microsoft account, which has **Owner** permissions to the default Provider subscription on the Azure Stack administrator portal.

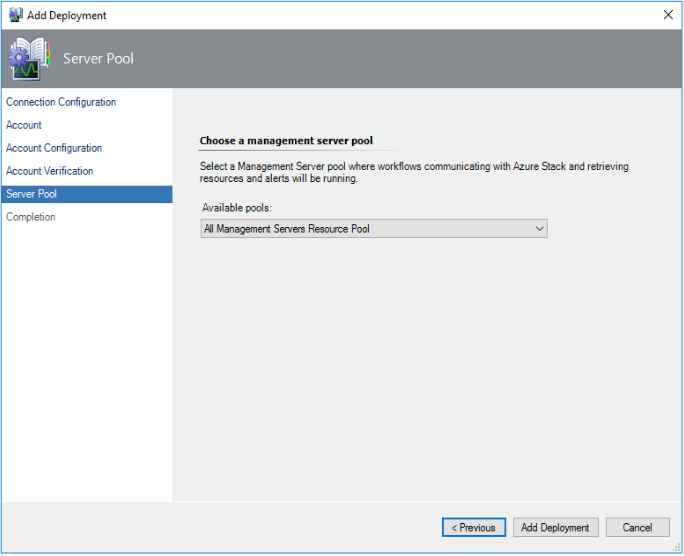
Upon a successful sign in, an application is created in Azure Active Directory, and the Service Principal information will be displayed in the **Service Principal Information** window:



|  |
| --- |
| * **Important:**   It is strongly recommended to save the SPN information data presented in this window for further usage! |

Click the **Next** button to continue to the **Server Pool** window. In this window, perform the following:

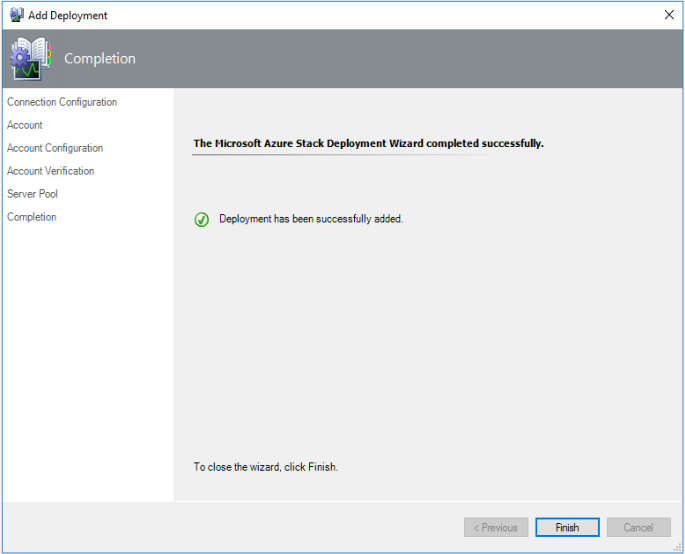
* + In the **Available pools** list, select a management pool where the deployment object must be created.
  + Click the **Add Deployment** button to start the deployment creation process. Note that creation of a deployment may take some time.



|  |
| --- |
| * **Important:**   Adding a deployment may fail with a "Could not establish trust relationship" error because of an SSL certificate validation failure (the Certificate Root Authority that issued the certificate is not trusted by the server). In this case, ask your system administrator to obtain a valid SSL certificate.  In some cases, restarting the Operations Manager console, reboot machine or clear Operations Manager cache might help. Also, please check if all Infrastructure role instances are up and running. |

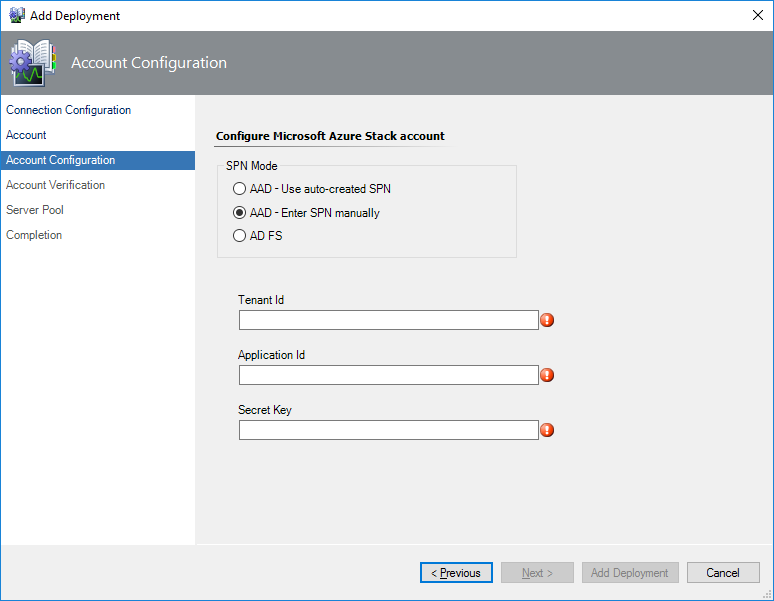
Upon successful completion of the wizard, the associated Run As account will be created in the **Accounts** section of the Operations Manager.

Click the **Finish** button to close the wizard.



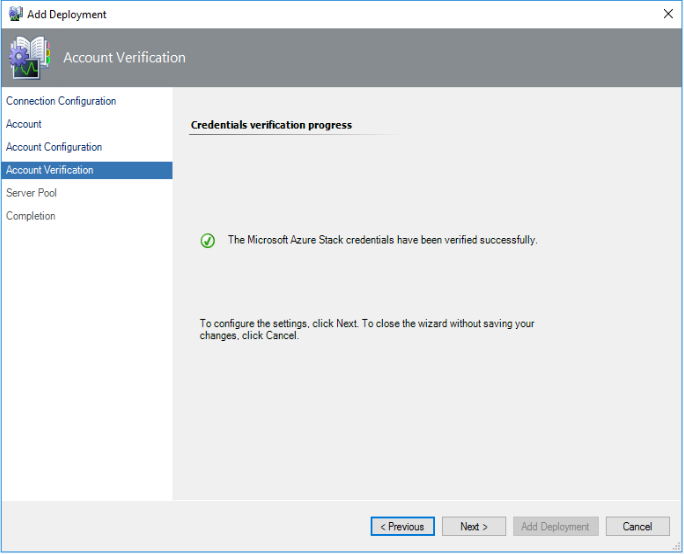
##### Manual SPN AAD Mode

If you select **AAD** **– Enter SPN manually** mode, you must enter your SPN Tenant ID, Application ID, and Secret Key:



**Note:** if you do not have an SPN or you do not know where to find your SPN Application ID, Tenant ID, Secret Key or Certificate Thumbprint, please review the [Authentication](#z5a9ff008734b4183946f840ae0464ab0) section of this guide.

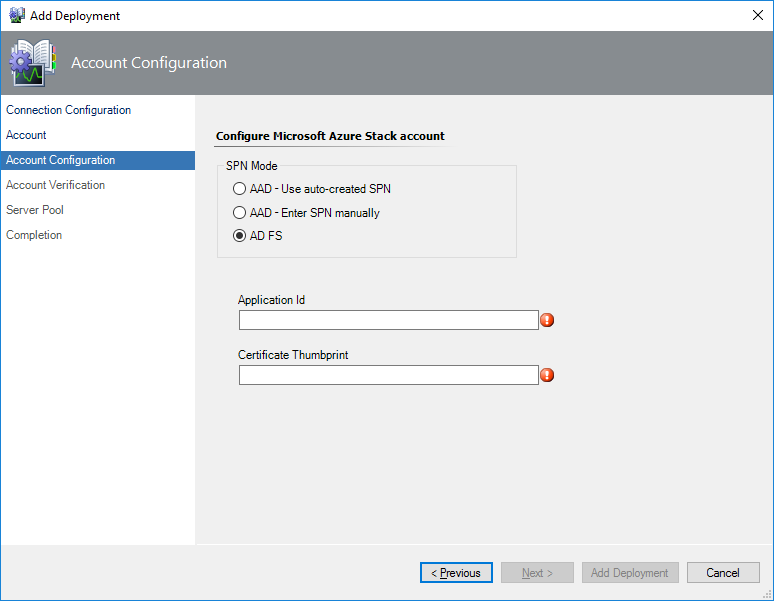
When the **Next** button is clicked, the wizard validates the entered data and obtains an authentication token.



If the validation succeeds, the last wizard steps will be similar to [Auto-Created SPN AAD Mode](#_Auto-Created_SPN_AAD_1) configuration.

##### SPN AD FS Mode

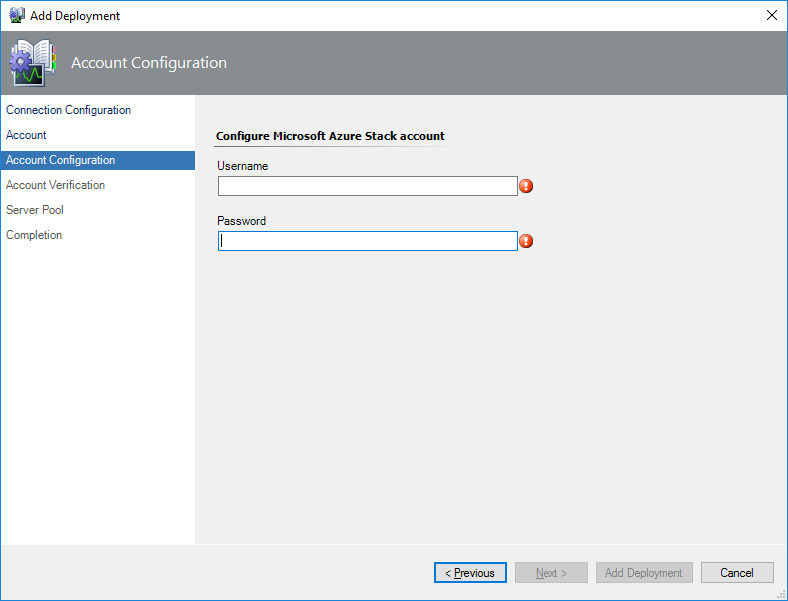
If you select **AD FS** mode, you must enter your SPN Application ID and Certificate Thumbprint:



#### UPN Mode

If you select **User Principal** option, you must enter credentials for the Azure Stack Service Administrator account or an account that has **Owner** or **Contributor** rights to the Default Provider Subscription (username and password).

**Note:** UPN authentication in the management pack is applicable for Azure Active Directory (AAD) environments only.



The last wizard steps will be similar to [Manual SPN AAD Mode](#_Manual_SPN_AAD_2) configuration.

### Edit Azure Stack Deployment

Edit Deployment option allows to change account and resource pool to communicate with Azure Stack API. Monitoring account can be changed to account with same authentication type (for example, from UPN mode to UPN mode) or to account with different authentication type if it is supported by configuration (for example, from UPN mode to SPN mode).

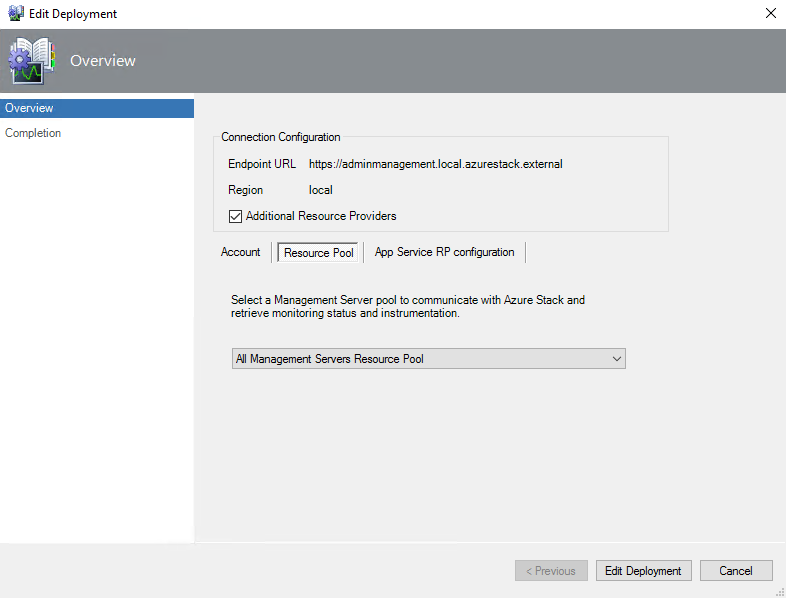
To edit your Azure Stack deployments, you must run the corresponding **Edit Deployment** wizard. To do so, perform the following steps:

In the Operations Manager console, open the **Administration** workspace, and then click the **Microsoft Azure Stack** node.

In the **Microsoft Azure Stack Overview** window, select the deployment you want to edit and click **Edit deployment**.

#### Edit Resource Pool

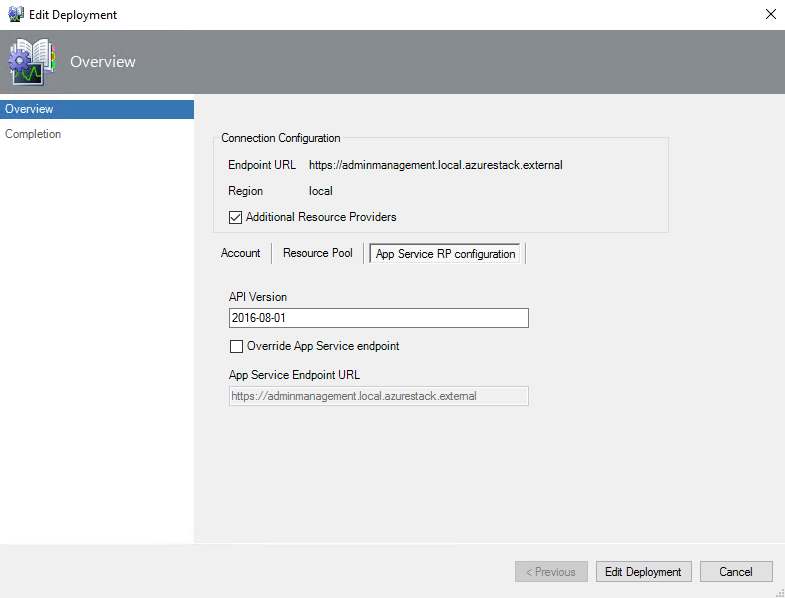
You can change the resource pool of the deployment by selecting the **Resource Pool** tab:



**Note:** The Management Server pool can also be changed in the Run As Account properties (in the **Distribution** tab).

#### Edit App Service Resource Provider configuration

You can enable checkbox **Additional Resource Provider** to monitor **App Service Roles**. To change **App Service Resource Providers** settings, click the tab **App Service RP configuration**.



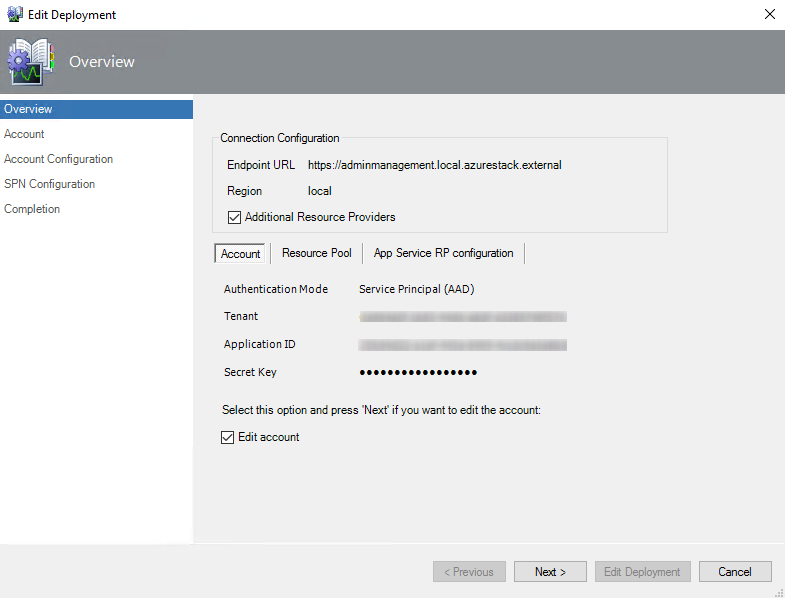
To edit the account properties, select the **Account** tab, check the “Edit account” box and click the **Next** button.

#### Edit SPN mode

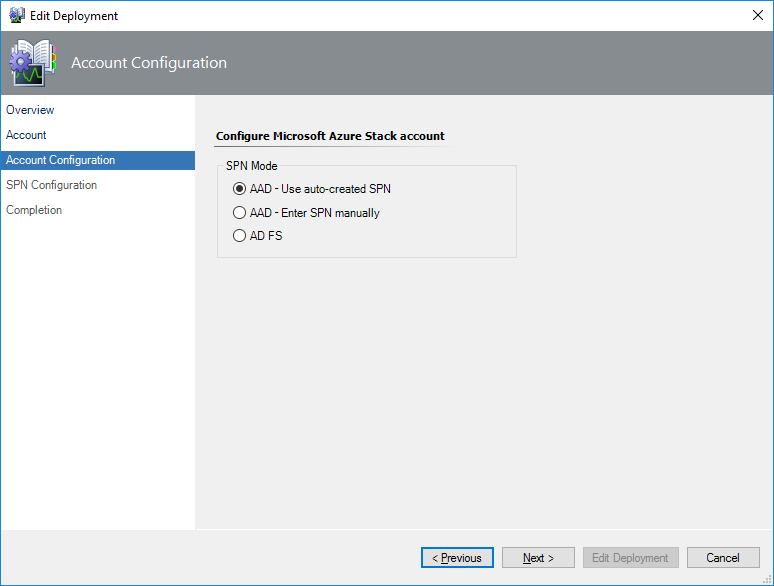
##### Edit Auto-Created SPN AAD Mode

By means of **AAD – Use auto-created SPN** mode, the management pack searches for an application in Azure Active Directory on the Azure portal or creates one if such application does not exist. Then, it obtains Application Id and Secret Key for authentication and grants the application **Contributor** permissions to the subscription on the Azure Stack administrator portal in automatic mode.

If the selected deployment is using the SPN authentication option, the **Edit Deployment** window is displayed as follows:



Click **Edit account** checkbox to make changes.



After clicking the **Edit Deployment** button, the introduced changes will be saved and an associated Run As account will be created in the **Accounts** section of the Operations Manager.

|  |
| --- |
| * **Important:** When an auto-created SPN is removed, its associated Run As account will not be removed in the Operations Manager; it is necessary to remove the Run As account manually. For more information, please refer to the [Auto-Created SPN for AAD](#_Auto-Created_SPN_AAD) section. |

In the next window of the wizard, you can edit your credentials.

##### Edit Manual SPN AAD Mode

To create an AAD SPN deployment manually, you will need your existing SPN **Tenant Id**, **Application Id**, and **Secret Key**. For more information, please see the [Create SPN Manually](#_Create_SPN_Manually_1)  section.



**Note:** If the Run As account of the manually-created SPN is removed via the Operations Manager, its application still remains on the Azure portal and is to be removed manually.

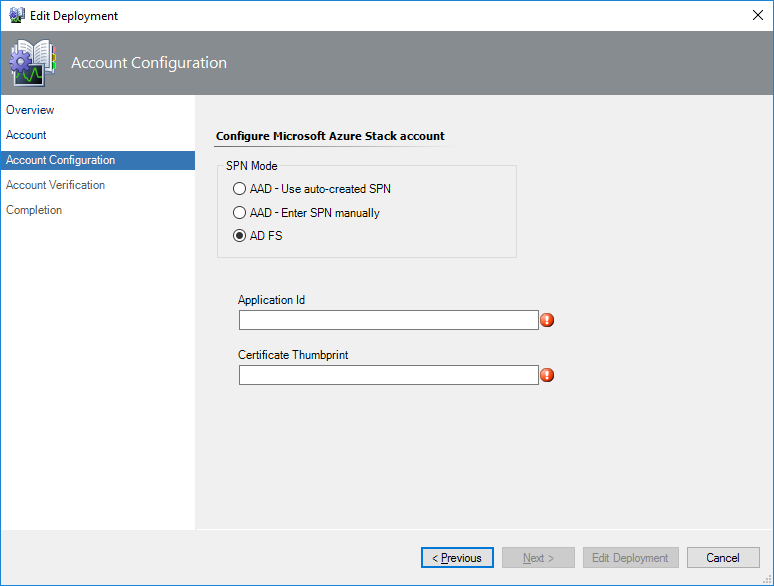
##### Edit SPN AD FS Mode

If the selected deployment is using SPN AD FS authentication option, the following window will be displayed:



Click **Edit account** checkbox to make changes.

In AD FS SPN Mode credentials are presented by **Application Id** (as a Name) and **Certificate Thumbprint** (as a Password).

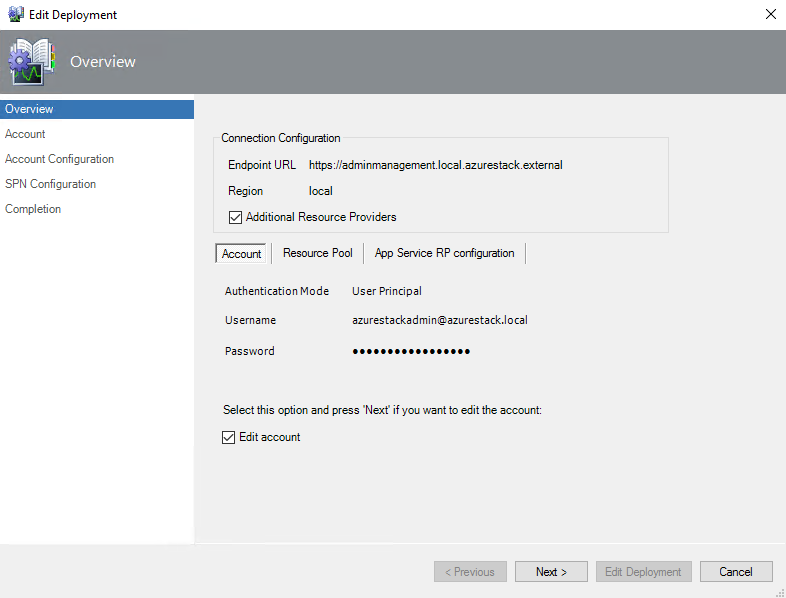


After clicking the **Edit Deployment** button, the introduced changes will be saved and the associated Run As account will be created in the **Accounts** section of the Operations Manager.

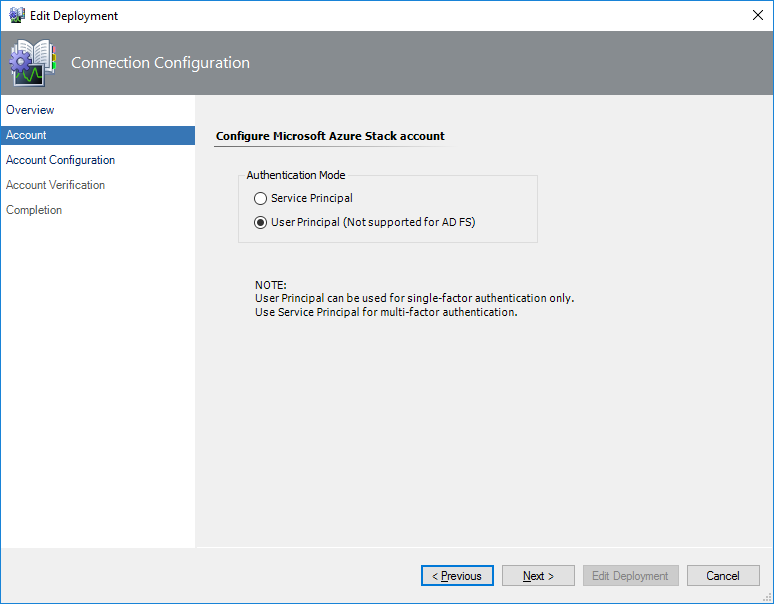
**Note:** The changes you make in this window will not affect the data stored in Active Directory.

#### Edit UPN mode

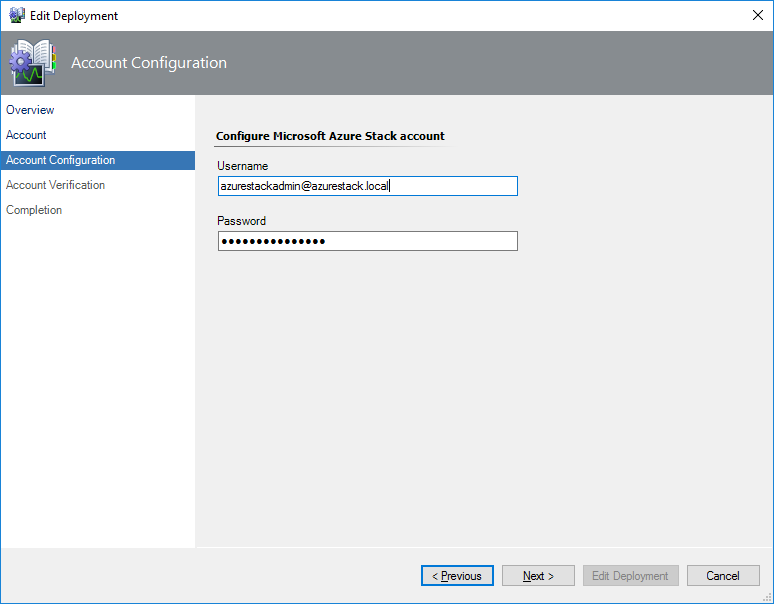
If the selected deployment is using UPN authentication option, the following window will be displayed:



Click **Edit account** checkbox to make changes.

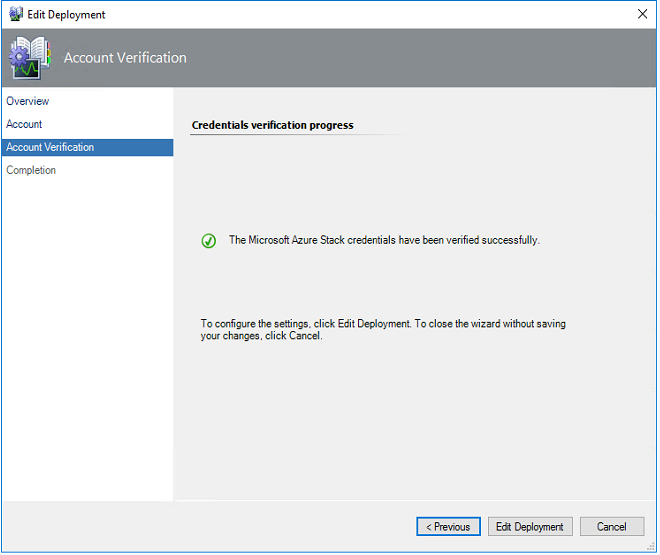


Select the **User Principal (Not supported for AD FS)** option and click the **Edit Deployment** button. At that, the **Account Configuration** window will be opened:

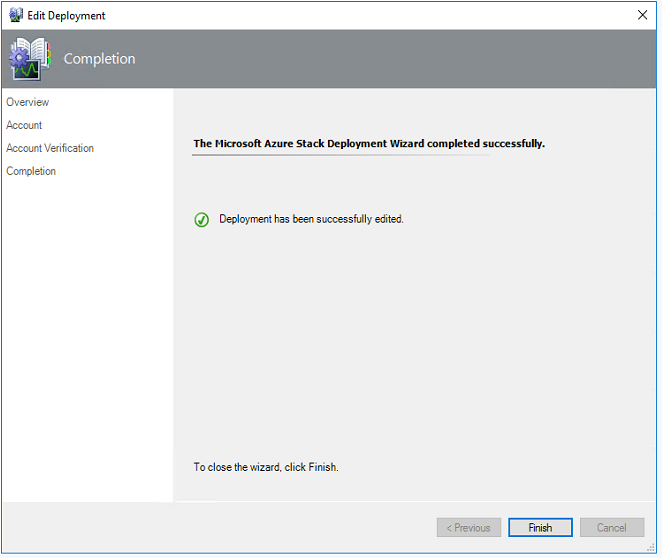


**Note:** The changes you make in this window will not affect the data stored in Active Directory.

Click the **Next** button to continue to the **Account Verification** window:



Upon successful account verification, click the **Edit Deployment** button to apply the changes. Then, click the **Finish** button to exit the wizard:



**Note:**  You can also edit credentials of your deployments in the Run As Account properties in Operations Manager Administration pane.

## Authentication

In this section, you can find guidance on how to create a Service Principal for Azure Active Directory or for Active Directory Federation Services deployments.

### Auto-Created SPN AAD deployment

With Auto-Created SPN option, the management pack automatically creates an application on the Azure portal and then registers this application on the Azure Stack administrator portal with the **Contributor** role.

When the application is created, you can find it on the Azure Stack administrator portal.

To do this, perform the following steps:

1. Go to the **Subscriptions** sectionof the Azure Stack administrator portal.
2. Select the particular subscription and choose the **Access Control (IAM)** option.
3. Search the application by name.

A new auto-created application will have the following format:

Azure Stack SCOM\_{SCOMManagementGroupID\_UserID}

where:

SCOMManagementGroupID *–* ID of the SCOM management group where the management pack is installed;

UserID– ID of the user account on the Azure portal that was used to create Service Principal in automatic mode.

When the application is created, the associated Run As account is created in the Operations Manager.  
An Auto-Created SPN Run As account has the following format:

Azure Stack Run As Account credentials\_AAD\_SPN\_Auto\_{ApplicationID}

where:

ApplicationID – ID of the application created on the Azure portal.

|  |
| --- |
| Important iconImportant:  If an auto-created SPN is no longer used (for example, the deployment is removed, the account is replaced or the management pack is uninstalled), the associated Run As account is still remaining in the Operations Manager and can be reused, as long as the corresponding application remains on the Azure Portal.  If you need to entirely remove an Auto-Created SPN application, log in to the **Azure portal** – **App registrations** and remove the application manually.  The Run As account can be removed in the Operations Manager **Administration** – **Run As Configuration** – **Accounts** pane. |

**Note:** If a Run As account is no longer used, it will be automatically removed by the Management Pack in other authentication scenarios such as UPN, manually created SPN and ADFS SPN.

**Note.** Uninstallation of the MP does not remove associated Run As account.

### Create SPN Manually for AAD Deployment

A Service Principal can be created using either PowerShell cmdlets or via the Azure administrator portal.

##### Create SPN with PowerShell

In order to create SPN with PowerShell, review the corresponding [article](https://azure.microsoft.com/en-us/documentation/articles/resource-group-authenticate-service-principal/) to obtain all the necessary information.

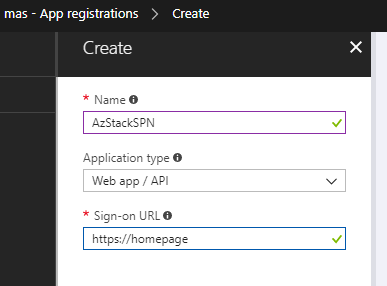
If you want to add a Service Principal Name to an Azure Stack administrator subscription, the following syntax is to be used:   
  
New-AzureRmRoleAssignment -RoleDefinitionName Contributor -ServicePrincipalName $app.ApplicationId.Guid –Scope “/subscriptions/<subscriptionId>”

For the detailed information, see the [New-AzureRmRoleAssignment](https://msdn.microsoft.com/en-us/library/mt603580.aspx) article.

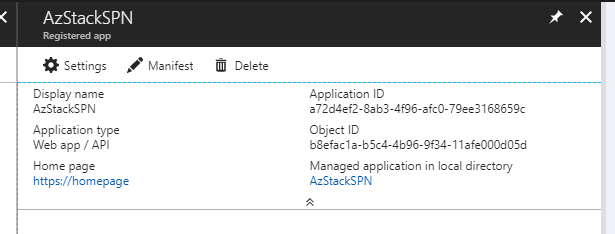
##### Create SPN Manually via the Azure Portal and the Azure Stack Administrator Portal

Follow the steps described below to create an Azure Active Directory SPN via the Azure portal and assign a role to the application on the Azure Stack administrator portal manually.

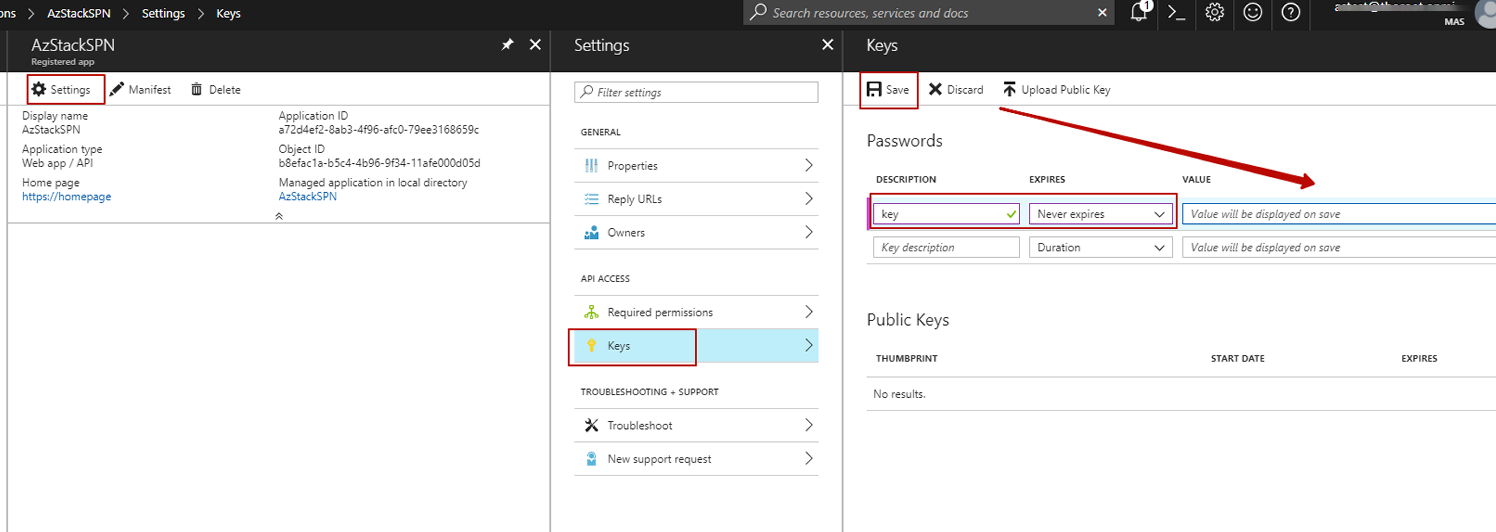
1. Login to <https://portal.azure.com> as an administrator or user with the **Owner** role to the subscription on the Azure Stack administrator portal.
2. Go to **Active Directory** – **App registrations** and select the **New application registration** option.
3. Create an application:

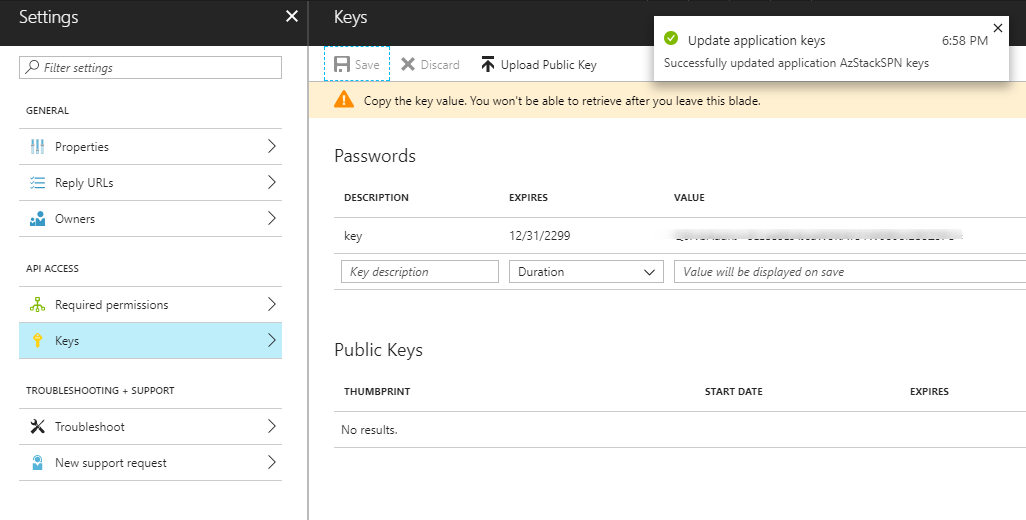


1. Copy the Application ID:

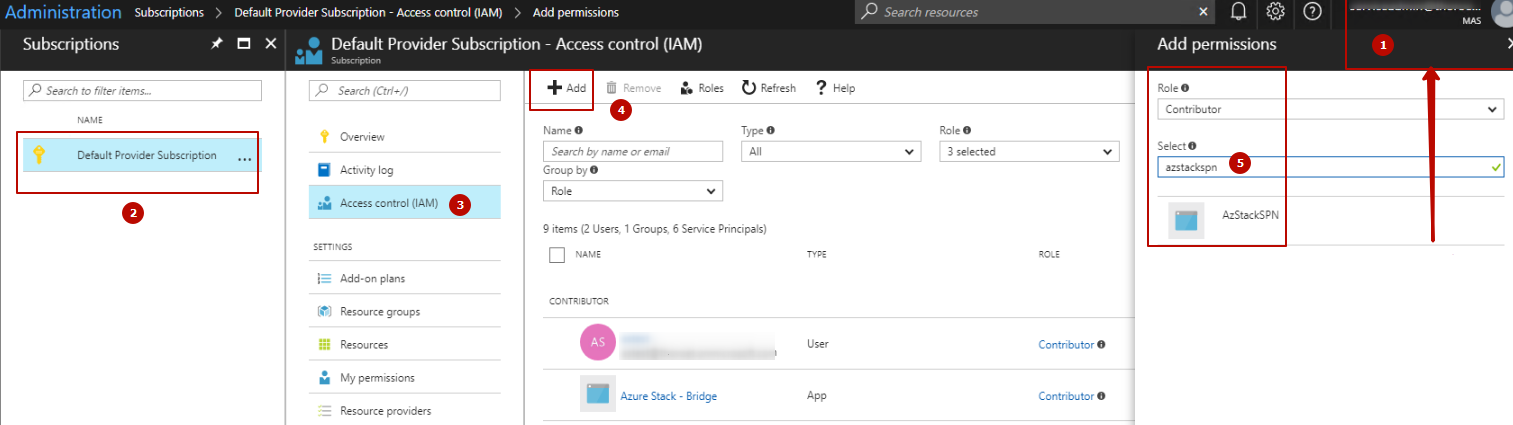


1. Generate the key by clicking the **Save** button:





1. On the Azure portal, go to **Help** – **Show diagnostics** and find the Tenant ID in the json file.
2. Log in to the Azure Stack administrator portal. Go to **Subscriptions – Access control – Add.** Add the SPN to the **Contributor** or **Owner** role.



Now, when you have SPN **Tenant Id**, **Application Id**, and **Secret Key**,you can go to the Azure Stack “Add Deployment” wizard in the Operations Manager and [create SPN manually](#_Create_SPN_Manually_1).

The associated Run As account for a manually created SPN will have the following format:

Azure Stack Run As Account credentials\_AAD\_SPN\_{ApplicationID}

### Create SPN for AD FS deployment

To create an AD FS Service Principal Name, perform the following steps:

1. Follow the instructions provided on [this page](https://docs.microsoft.com/en-us/azure/azure-stack/azure-stack-create-service-principals) to create an SPN.
2. Upon completion of the SPN creation, copy and save the Application Id and Certificate Thumbprint from the output of the cmdlet.
3. Open the Certificate Manager tool (Certmgr.exe) and find the created SPN certificate in the list of Current User personal certificates. Export it to a file (together with the private key) and then import it to the Local Machine personal certificates of the computer where the management pack is used (both Operations Manager console and Management Server). To import the certificate, double-click the corresponding certificate file and follow the wizard steps.
4. Login to the Microsoft Azure Stack Administrator Portal with the **Owner** permissions to the subscription. Add the created SPN to the Access Control list of the subscription with the **Owner** or **Contributor** role.
5. Now, you can configure the management pack by means of an SPN. Enter the Application Id and Certificate Thumbprint of the SPN in the corresponding window of the Azure Stack “Add Deployment” wizard.

The associated Run As account for AD FS SPN has the following format in the Operations Manager:

Azure Stack Run As Account credentials\_ADFS\_SPN\_{ApplicationID}

### Create Run As account in the Operations Manager manually

In some cases, a Service Principal application can remain on the Azure administrator portal while its Run As account is deleted in the Operations Manager. The Azure Stack wizard queries to the portal, finds the application related to this Operations Manager, but cannot authenticate.

In this case, the user can either remove the application from the Azure portal or recreate the missing Run As account for it. The below steps describe how to recreate a Run As account in the Operations Manager console.

##### Auto-created SPN Run As Account

###### Create a Run As account

1. Log on to the Operations Manager console with an account that is a member of the Operations Manager Administrators role.

1. In the Operations Manager console, click Administration.
2. In the Administration workspace, right-click Accounts, and then click Create Run As Account.
3. In the Create Run As Account Wizard, click Next in the Introduction window.
4. In the General Properties window, do the following:
   * 1. Select Basic Authentication in the Run As Account type: list.
     2. Type a display name in the Display Name text box.

|  |
| --- |
| **Title: Important iconImportant:**  For an Auto-Created SPN displayname, it is mandatory to have the following format (syntax is important):  Azure Stack Run As Account credentials\_AAD\_SPN\_Auto\_{Applicationid}  Example: *Azure Stack Run As Account credentials\_AAD\_SPN\_Auto\_9532009c-65e5-4f34-80c0-1ec9c3e4dc12* |

* + 1. Optionally, type a description in the Description box.
    2. Click Next.

1. In the Credentials window, enter a username and its password, where the Auto-Created SPN **Account name** has the following format:{applicationid\_tenantid}; and the **Password** is a **Secret Key** for the application.
2. Click Next.
3. In the Distribution Security window, select the Less secure or More secure option as appropriate.
4. Click Create.
5. In the Run As Account Creation Progress window, click Close.

###### Re-use Auto-Created SPN with a manually created Run As Account

1. Go to **Administration** – **Microsoft Azure Stack** node.

2. Re-run the **Add Deployment Wizard** and select the **SPN AAD – Use auto-created SPN** mode.

Auto-Created Service Principal becomes found.

3. Finish steps by assigning Management Pool to communicate with Azure Stack administrator portal and close the wizard.

###### Validate that the Run As Account is Assigned Correctly

1. Go to **Profiles** – **Microsoft Azure Stack Run As Profile AD Credentials**

2.Double-click the profile and check in **Run As accounts** account name that was assigned to the deployment.

##### **Manually created SPN Run As account**

Run As account for manual SPN is created the same way as for [Auto-Created SPN](#_Auto-created_SPN_Run) with **Basic Authentication** type.   
**Displayname** for manually created SPN can have **any supported format** allowed by Operations Manager (for example: “Azure Stack manual SPN”).

##### **Manually created UPN Run As account**

Run As account for UPN created with **Basic Authentication** type. **Displayname** for manually created UPN can have any supported format allowed by Operations Manager (for example: “Azurestack User”). In the **Distribution** tab specify managed servers that will receive Run As account credentials.

### **Run As account and Run As Profile association**

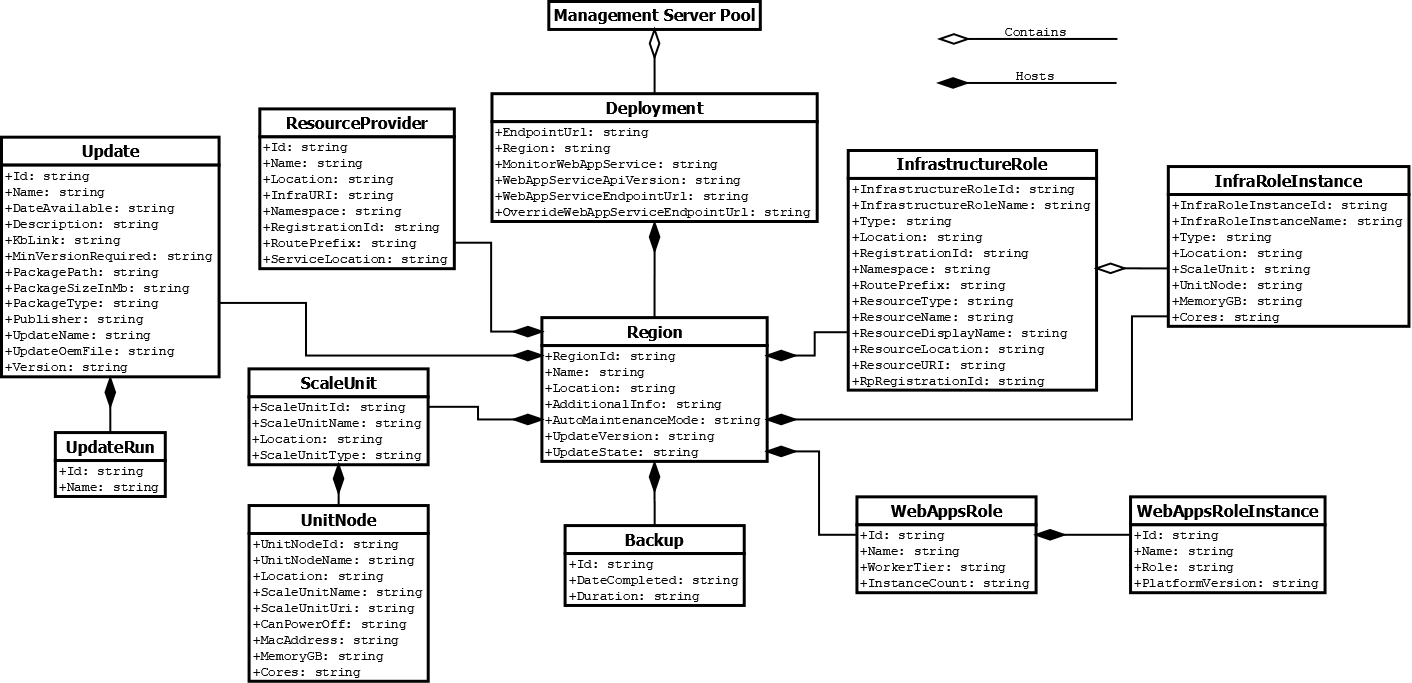
Besides using Azure Stack “Add Deployment” wizard, Run As Account can be manually assigned to the deployment with Operations Manager Run As account.

For this go to **Profiles** – **Microsoft Azure Stack Run As Profile AD Credentials** and associate the selected Run As account with the deployment you want to monitor.

|  |
| --- |
| **Title: Important iconImportant:**  Manual association of Run As Account with Run As Profile for the deployment suggested as the last option to use.  Association creates dependencies that causes issue with Azure Stack Management Pack uninstallation. Please see [unable uninstall management pack known issue](#Upgrade) for more information. |

## How Health Rolls Up

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



## View the Information in the Operations Manager Console

### Microsoft Azure Stack Views

The management pack introduces a comprehensive set of views. You can find them in the **Microsoft Azure Stack** folder:

 Microsoft Azure Stack

 Active Alerts

App Service Dashboard



 Backup Dashboard

 Capacity Dashboard

 Deployments

 Health Dashboard

 Infrastructure Role Dashboard

 Marketplace Management Dashboard

 Regions

 Resource Provider Dashboard

 Scale Unit Dashboard

 Update Status Dashboard

 Storage Performance

 Blob Dashboard

 Queue Dashboard

 Table Dashboard

#### Icon Legend

 Folder

 Alert

 State

 Dashboard

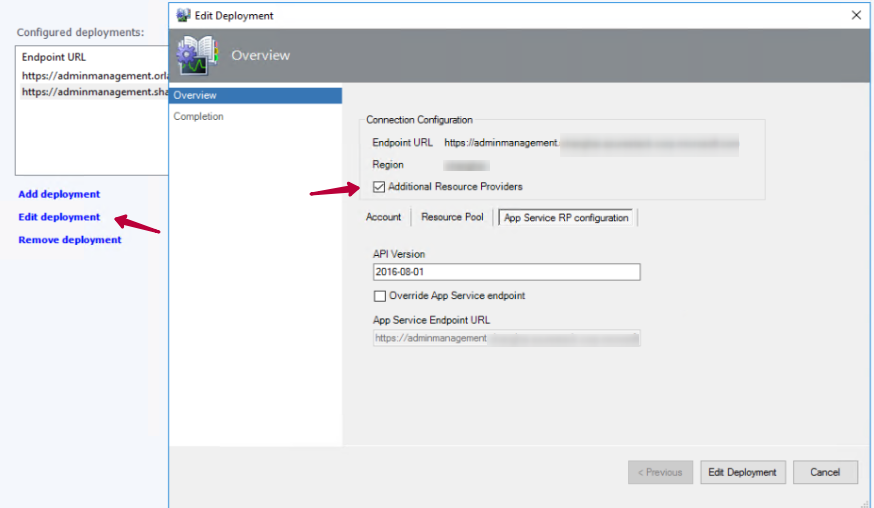
### Microsoft Azure Stack App Service Dashboard

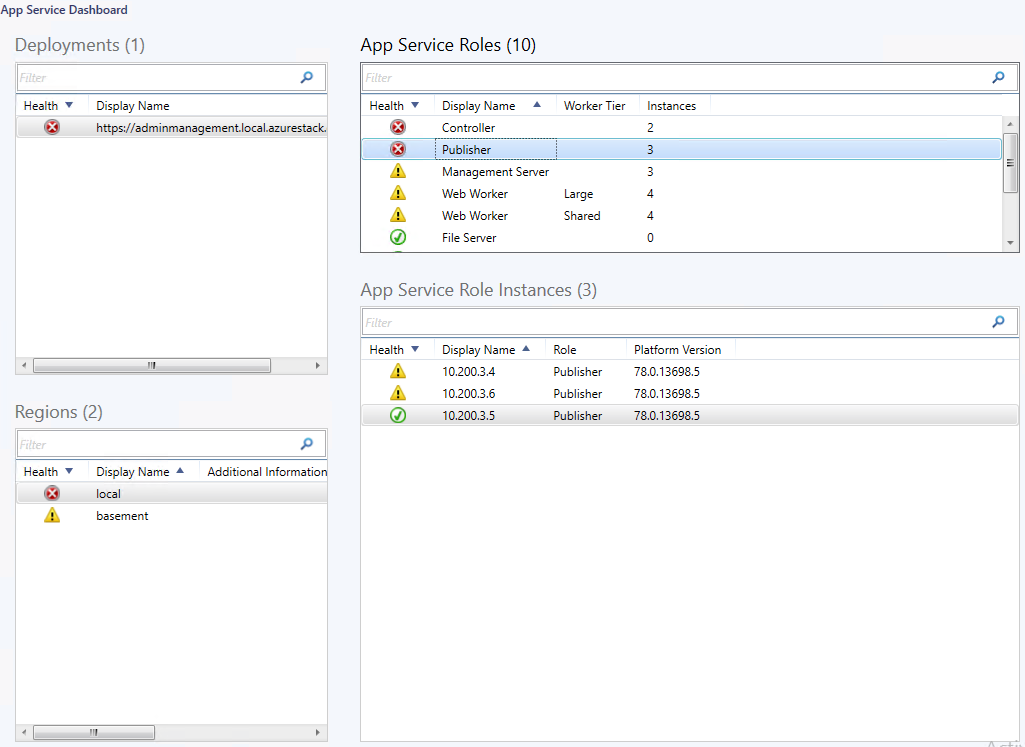
This management pack includes an app service dashboard, which provides detailed information about Azure Stack app service roles. The app service dashboard displays the following information by means of the Operations Manager widgets:

* List of discovered deployments
* List of discovered regions
* List of discovered app service roles
* List of discovered app service role instances

Important iconImportant:

In order to enable App Service Roles and role instances monitoring **Additional Resource Providers** must be configured for the Deployment. For this go to **Administration > Microsoft Azure Stack pane > Edit Deployment Wizard >** check **Additional Resource Providers** checkbox**.** Make additional changes in **App Service RP configuration** tab if needed.

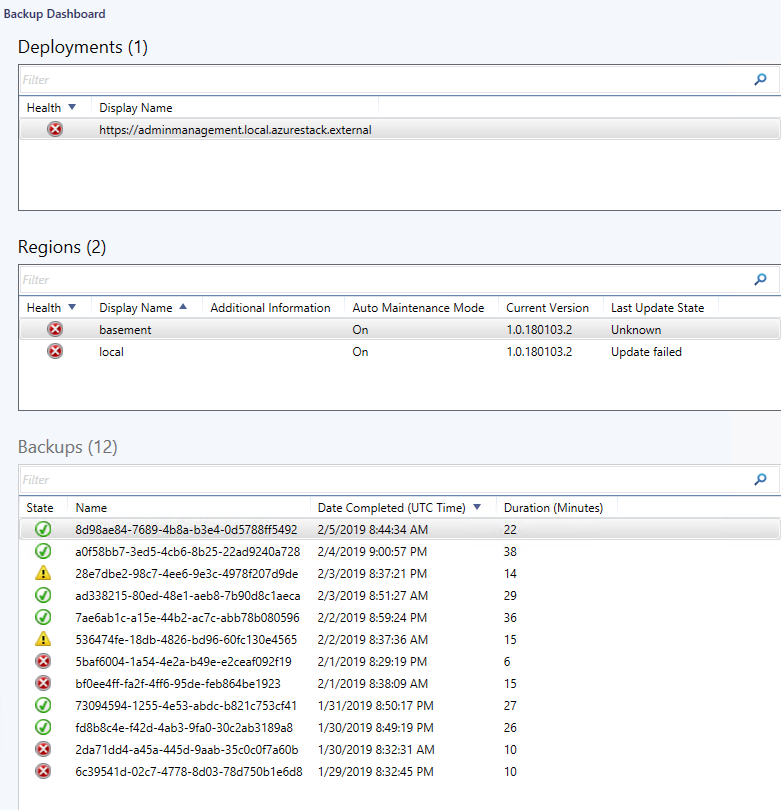




### Microsoft Azure Stack Backup Dashboard

This management pack includes a backup dashboard, which provides detailed information about Azure Stack Backups. The backup dashboard displays the following information by means of the Operations Manager widgets:

* List of discovered deployments
* List of discovered regions
* List of discovered backups

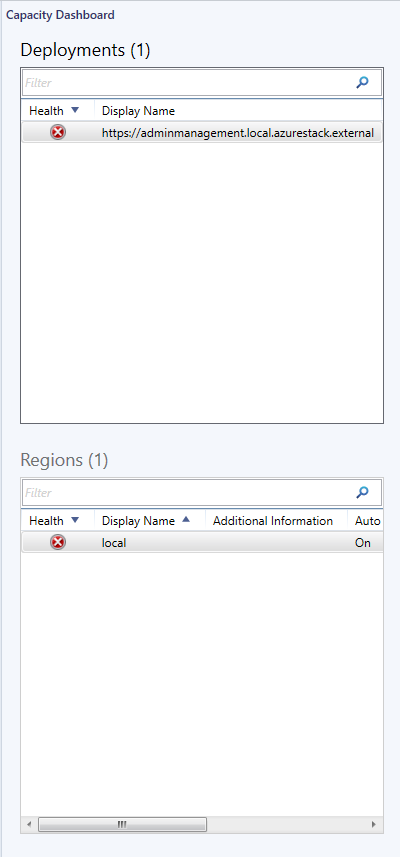


**Note.** Backup monitor does not generate alerts.

### Microsoft Azure Stack Capacity Dashboard

This dashboard provides detailed dynamic information about the capacity of the Azure Stack instances based on the data received via the corresponding performance rules. The capacity dashboard displays the following information by means of the Operations Manager widgets:

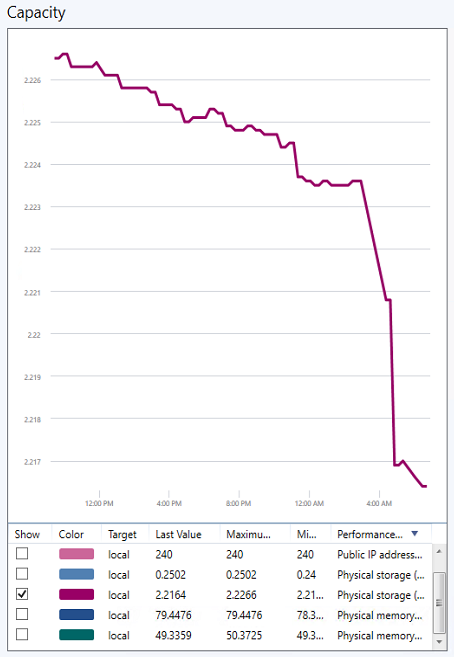
* List of discovered deployments
* List of discovered regions per selected deployment
* Capacity diagrams



For each selected region, you can view dynamic diagrams regarding the following capacity readings:

* Physical memory usage
* Physical memory availability
* Physical storage usage
* Physical storage availability
* Public IP address pool usage
* Public IP address pool availability

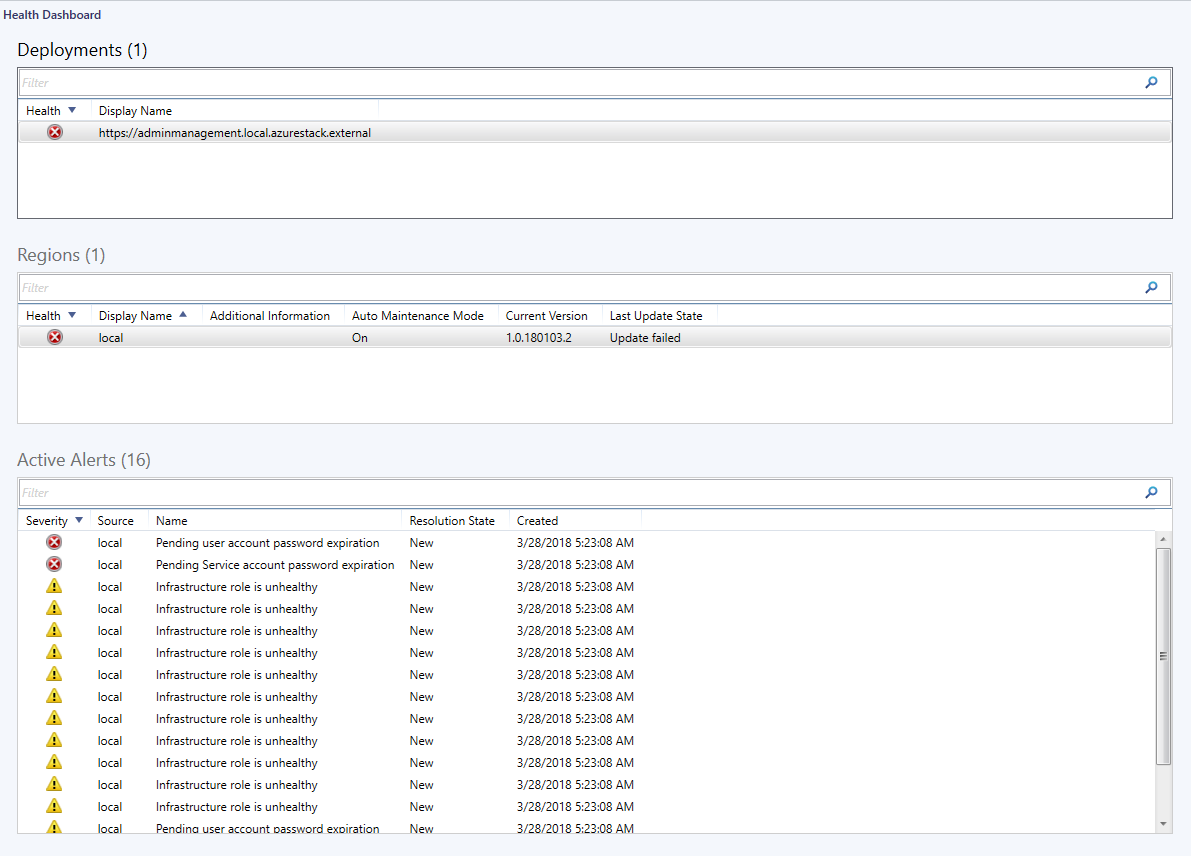
At that, you can select only necessary readings to be displayed:



### Microsoft Azure Stack Health Dashboard

This management pack includes a health dashboard, which provides detailed information about Azure Stack instances. The health dashboard displays the following information by means of the Operations Manager widgets:

* List of discovered deployments
* List of discovered regions
* List of active Azure Stack alerts

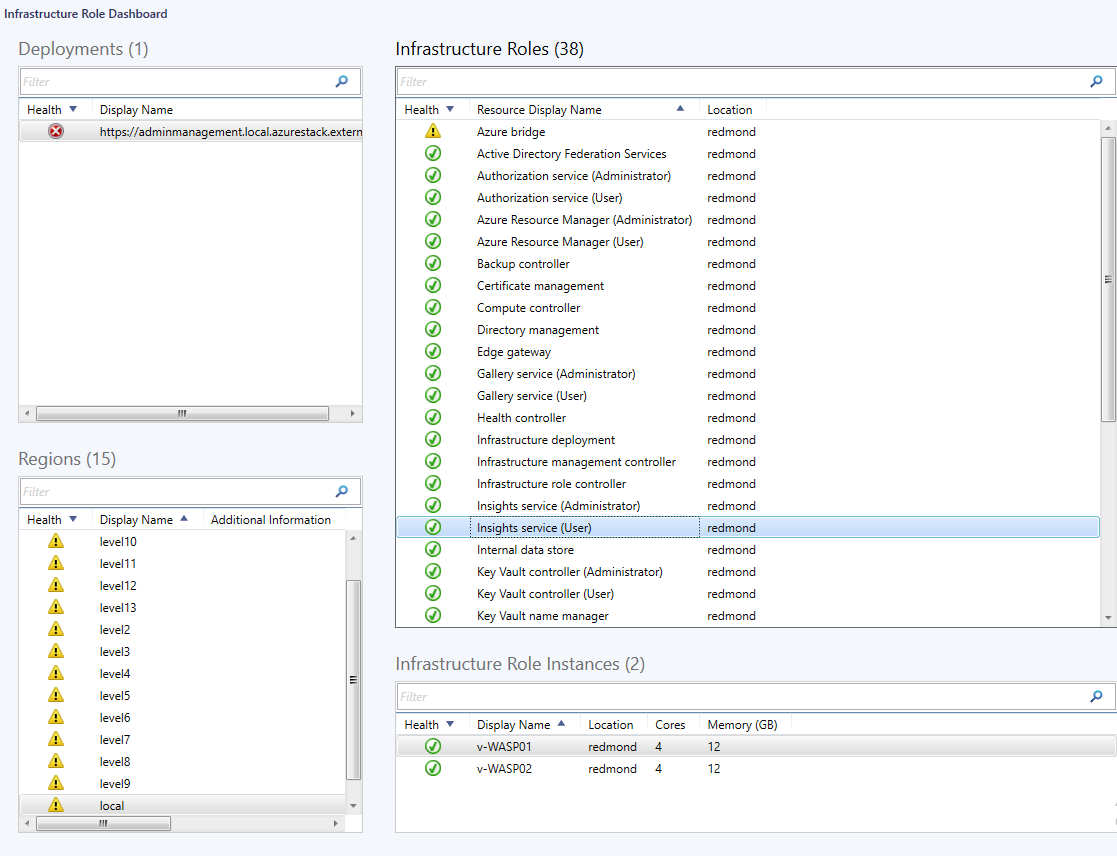


You can select and close active Azure Stack alerts in the health dashboard.

### Microsoft Azure Stack Infrastructure Role Dashboard

This management pack includes an infrastructure role dashboard, which provides detailed information about Azure Stack infrastructure roles. The infrastructure role dashboard displays the following information by means of the Operations Manager widgets:

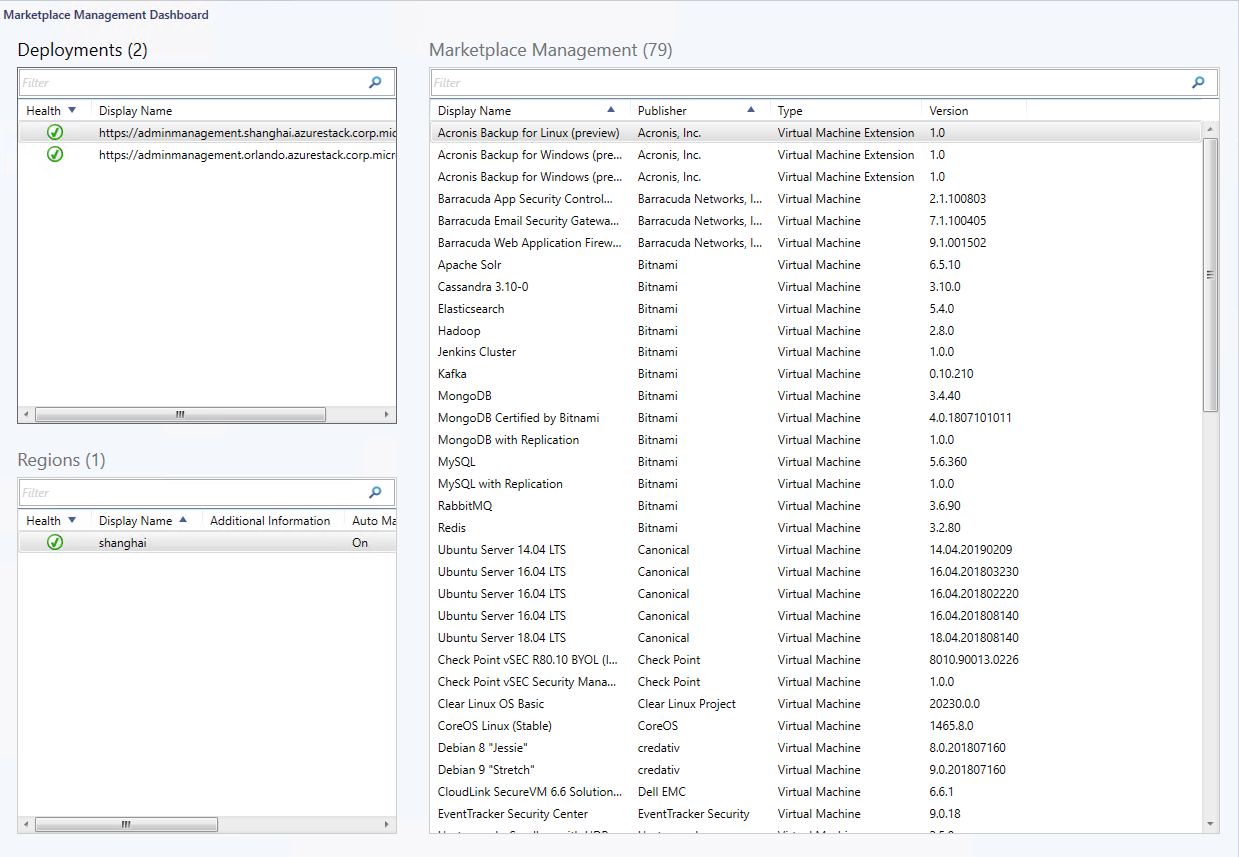
* List of discovered deployments
* List of discovered regions
* List of discovered infrastructure roles
* List of discovered infrastructure role instances



### Microsoft Azure Stack Marketplace Management Dashboard

This management pack includes a marketplace management dashboard, which provides detailed information about Azure Stack marketplace management. The marketplace management dashboard displays the following information by means of the Operations Manager widgets:

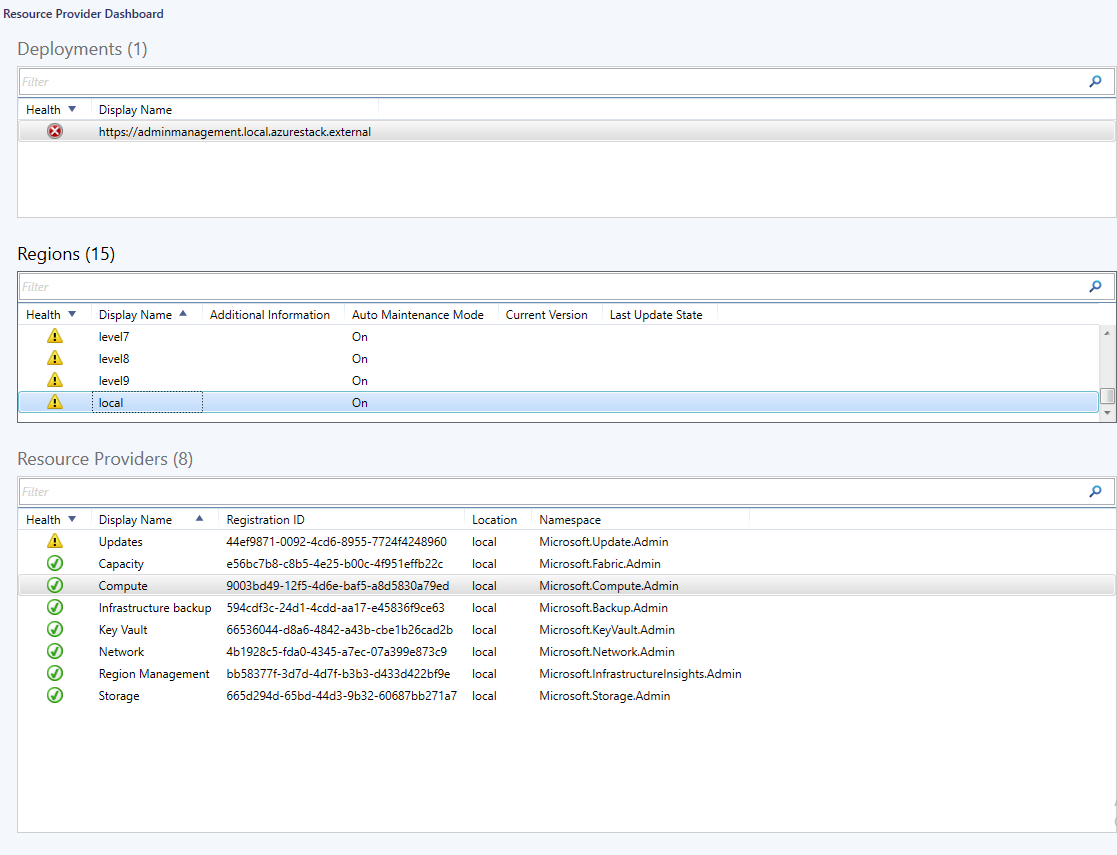
* List of discovered deployments
* List of discovered regions
* Discovered marketplace management



### Microsoft Azure Stack Resource Provider Dashboard

This management pack includes a resource provider dashboard, which provides detailed information about Azure Stack resource providers. The resource provider dashboard displays the following information by means of the Operations Manager widgets:

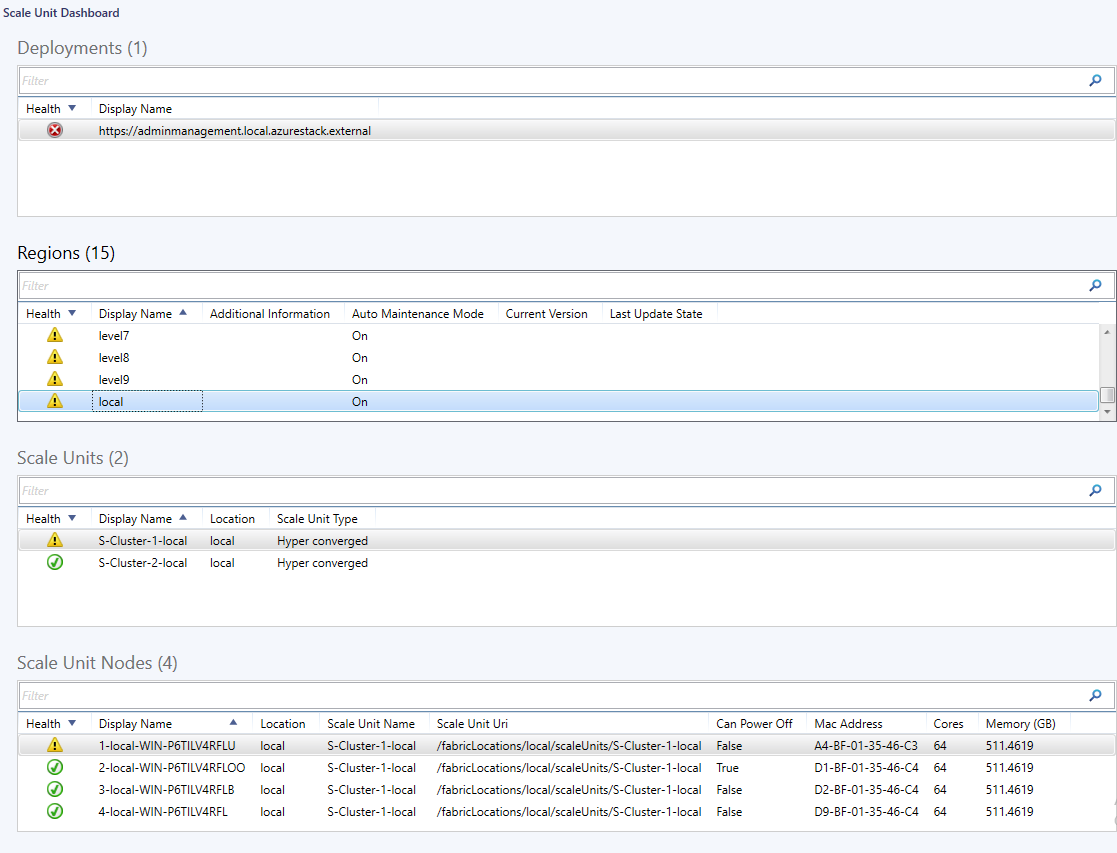
* List of discovered deployments
* List of discovered regions
* List of discovered resource providers



### Microsoft Azure Stack Scale Unit Dashboard

This management pack includes a scale unit dashboard, which provides detailed information about Azure Stack scale units. The scale unit dashboard displays the following information by means of the Operations Manager widgets:

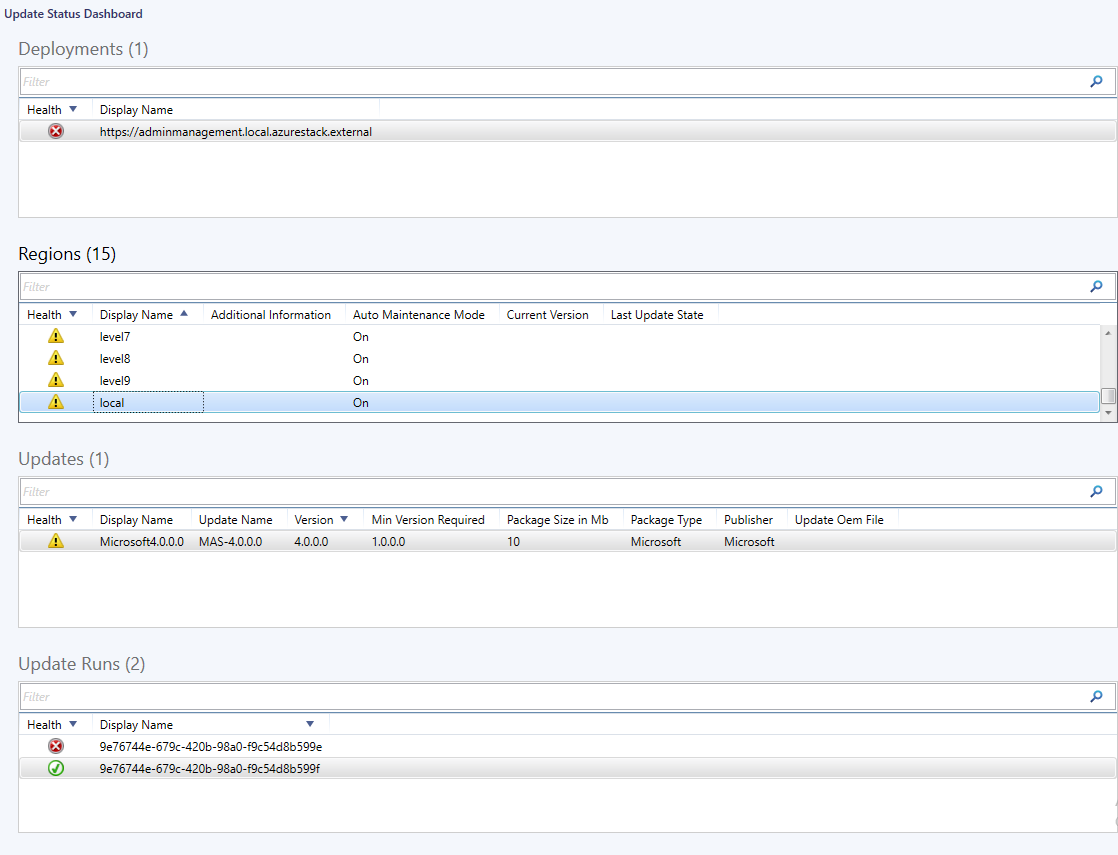
* List of discovered deployments
* List of discovered regions
* List of discovered scale units
* List of discovered scale unit nodes



### Microsoft Azure Stack Update Status Dashboard

This management pack includes an update status dashboard, which provides detailed information about Azure Stack updates. The update status dashboard displays the following information by means of the Operations Manager widgets:

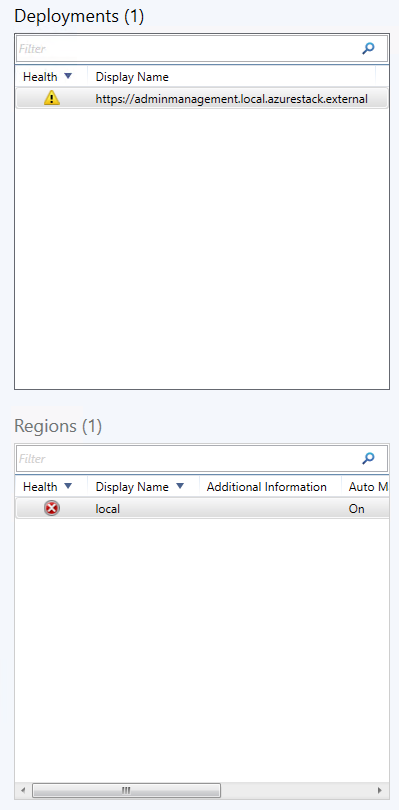
* List of discovered deployments
* List of discovered regions
* List of discovered updates
* List of discovered update runs



### Microsoft Azure Stack Storage Performance Dashboards

Storage Performance dashboards provide detailed dynamic information about the capacity of the Azure Stack storage services based on the data received via the corresponding performance rules. The storage dashboards have a common design and display the following information by means of the Operations Manager widgets:

* List of discovered deployments
* List of discovered regions per selected deployment
* Storage capacity diagrams



Each dashboard for each selected region provides dynamic diagrams regarding the following capacity readings:

#### Blob Dashboard

* Server latency (BlobService)
* Total requests (BlobService)
* Availability (BlobService)

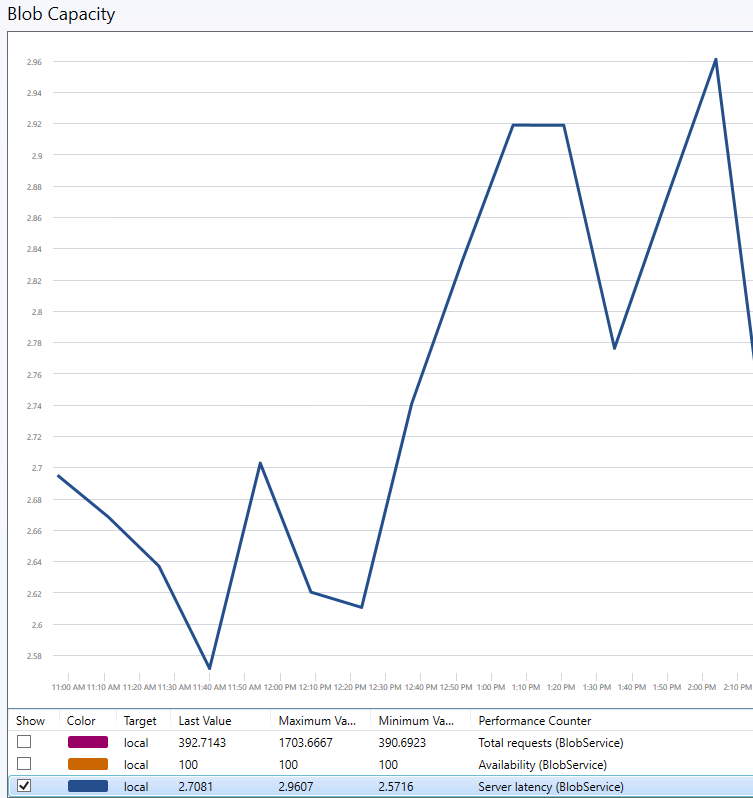
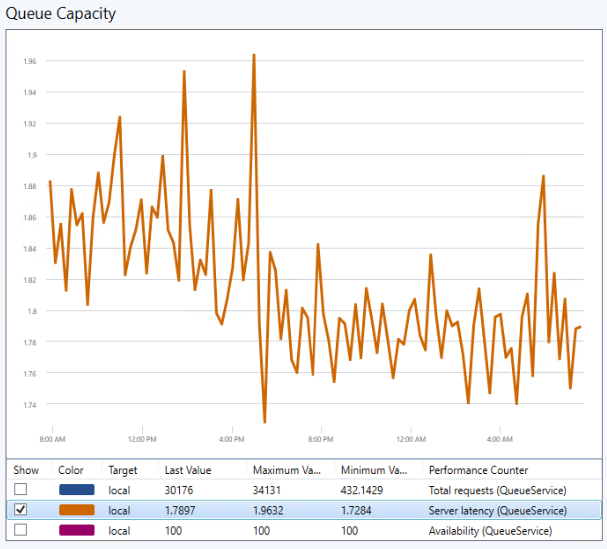
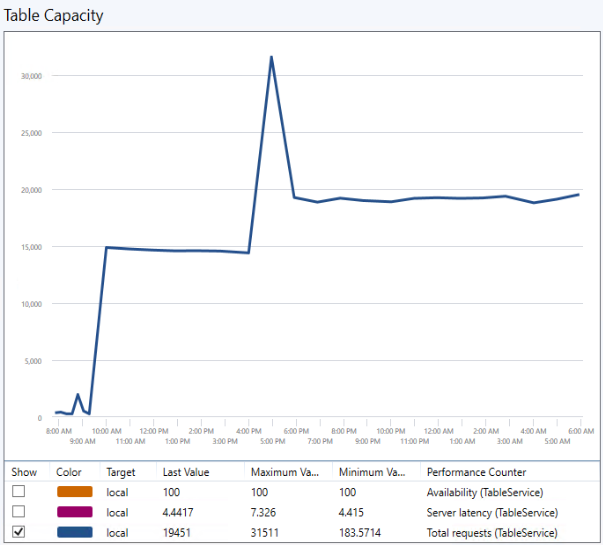
#### Queue Dashboard

* Server latency (QueueService)
* Total requests (QueueService)
* Availability (QueueService)

#### Table Dashboard

* Server latency (TableService)
* Total requests (TableService)
* Availability (TableService)

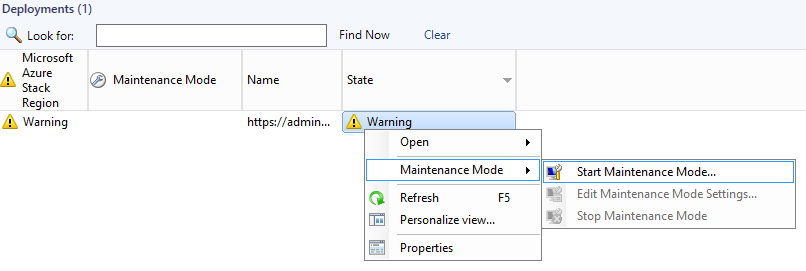
At that, you can select only necessary metrics to be displayed:

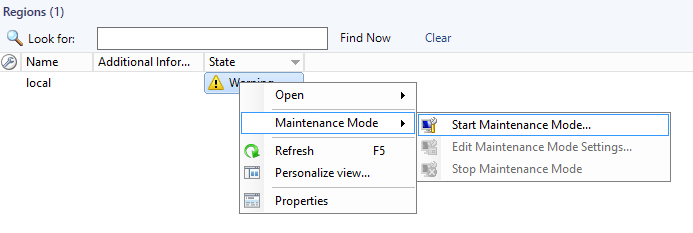
  

## The Operations Manager Maintenance Mode

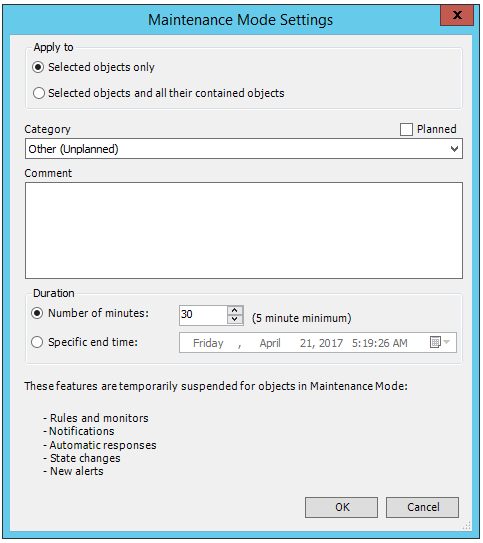
The Maintenance Mode is a feature in the Operations Manager that suspends the monitoring of an object during maintenance activities.

Maintenance mode provides a possibility to switch instances into maintenance mode manually. To do so, right-click the required instance in the **Monitoring** workspace of Operations Manager and select the **Start Maintenance Mode** option.





In the **Maintenance Mode Settings** window, apply the mode either to **Selected objects only** or **Selected objects and all their contained objects**. Then, specify the duration of the set maintenance mode by selecting the corresponding **Duration** option and entering a specific period or end time value.



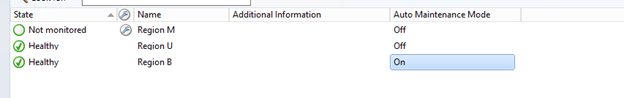
For more details, see the [How to suspend monitoring temporarily by using maintenance mode](https://technet.microsoft.com/en-us/library/hh212870(v=sc.12).aspx) article.

## Auto Maintenance Mode

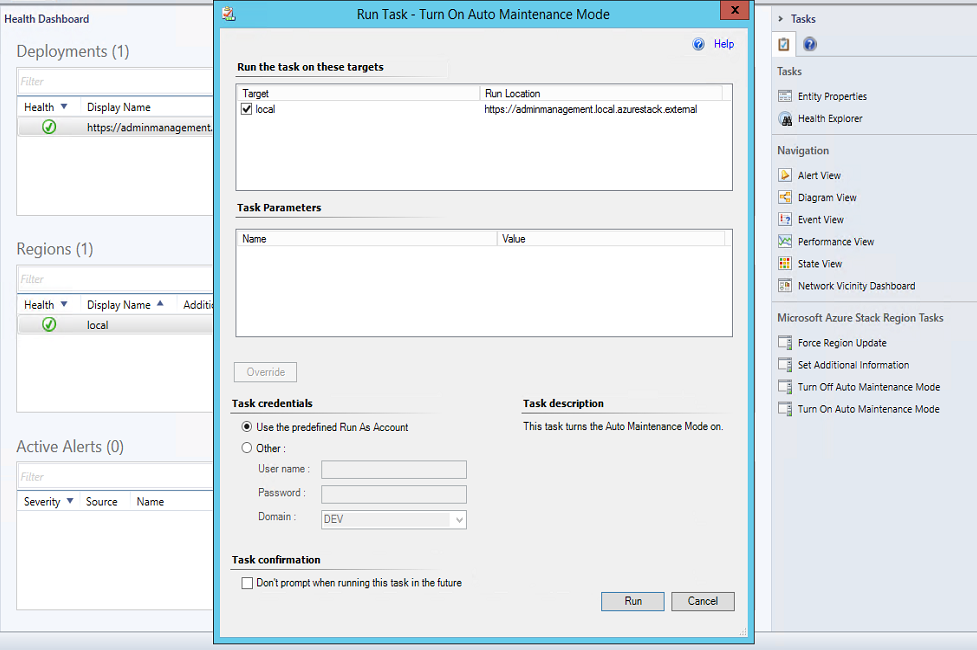
In order to suspend monitoring during maintenance activities maintenance mode activation was implemented in Operations Manager for the region and for the scale unit node.

### Region in Maintenance Mode

The Auto Maintenance mode monitoring rule for the region automatically checks the status of the regions in Azure Stack. If a region goes into a process of an update, the region is automatically switched to maintenance mode in the Operations Manager. Therefore, this mode helps prevent multiple alerts and errors when a monitored object is taken offline for maintenance.



The interval of the status check is 10 minutes. This mode is enabled by default. It can be switched off by the [Turn Off Auto Maintenance Mode Task](#_Turn_Off_Auto). To switch the mode on, use the [Turn On Auto Maintenance Mode Task](#_Turn_On_Auto).

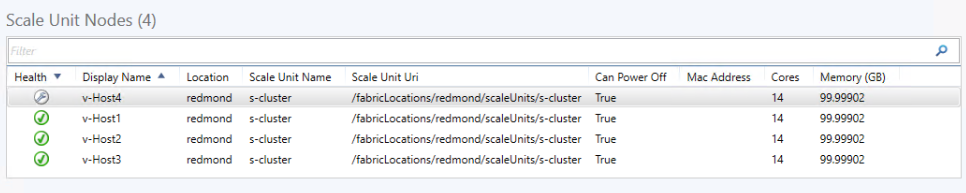


**Note:** If a deployment is switched to maintenance mode, all the corresponding regions and their objects will be switched to maintenance mode accordingly.

|  |
| --- |
| Important:  It is not recommended to switch deployments to maintenance mode manually in the Operations Manager if the Auto Maintenance Mode is on. The Auto Maintenance Mode is controlled by the Microsoft Azure Stack Auto Maintenance Mode Monitoring Rule which is targeted to deployment. Maintenance mode disables workflows, and if the rule has run earlier and not yet disabled, maintenance mode for the deployment is stopped. |

### Scale Unit Node in Maintenance Mode

When scale unit node is taken offline for maintenance in the Azure Stack the Auto Maintenance mode monitoring rule for scale unit node activates maintenance mode for the node in the Operations Manager.



## Storage Performance Metric Rules

The Azure Stack management pack provides metrics for Azure Stack Storage services using the following performance rules:

* Server latency (BlobService)
* Total requests (BlobService)
* Availability (BlobService)
* Server latency (QueueService)
* Total requests (QueueService)
* Availability (QueueService)
* Server latency (TableService)
* Total requests (TableService)
* Availability (TableService)

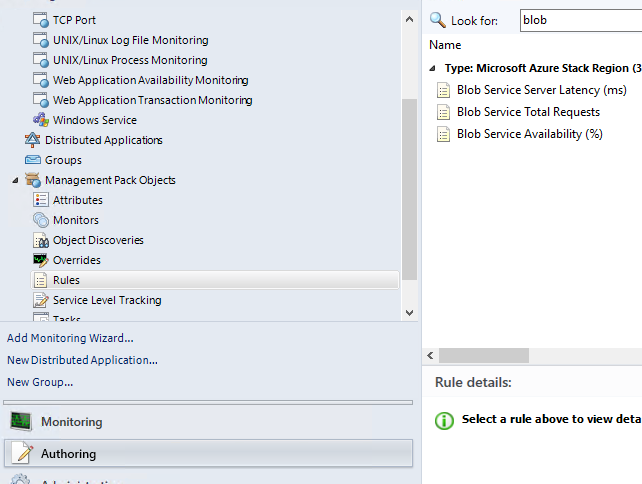
### Storage Metric Time Grain

All rules get metric definitions for storage services. By default, metric values are queried according to the minimal time grain of each metric definition. The time grain specifies the aggregation period of the metric values.

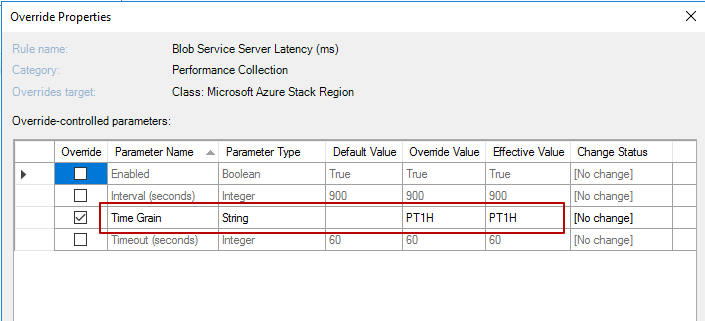
For each of these rules, the time grain may be configured via the corresponding overridable parameter.

#### How to Set a Custom Time Grain

1. In the Operations Manager console, open the Authoring workspace; then, find the storage service performance rule (for example, Blob Service Server Latency (ms)):



1. In the **Override Properties** window, set a time grain value (use ISO 8601 duration format).



If the override value is set not in ISO 8601 duration format, greater than the rule interval value or does not exist in the metric availabilities for the resources, the minimal time grain from the metric availabilities will be applied by default.

#### Troubleshooting Time Grain issues

Below are common troubleshooting events that help resolve issue with Time Grain configuration in rule’s overrides:

Event with **ID 4457** will appear in the Operations Manager event log in the Event Viewer if the time grain is in an incorrect format.

Event with **ID 4458** will appear in the Operations Manager event log in the Event Viewer if the time grain is more than the rule interval.

Event with **ID 4459** will appear in the Operations Manager event log in the Event Viewer if there is no specified time grain in the Azure Stack metric definitions.

|  |
| --- |
| * **Important:**   It is strongly recommended to apply the same time grain for all storage performance rules and for each storage service. Different values of time grain for each storage service will break the cookdown mechanism in SCOM and will cause an increase of web-request count to Azure Stack REST API. For more details on how the cookdown works, see the [Cookdown](https://technet.microsoft.com/en-us/library/ff381335.aspx) article. |

## App Service Role Available Workers Rule

The Azure Stack management pack provides rule for Azure Stack App Service Web Worker roles.

### Alert on available workers rule

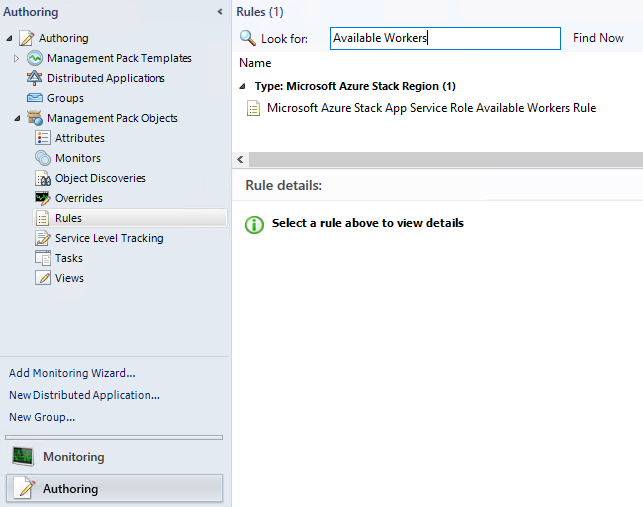
The rule checks an available worker count property in the web worker roles. If the percent of available worker count is less than or equal to critical threshold the rule will raise a critical alert. If the percent of available worker count is less than or equal to warning threshold and more than critical threshold the rule will raise a warning alert.

#### Set warning and critical thresholds

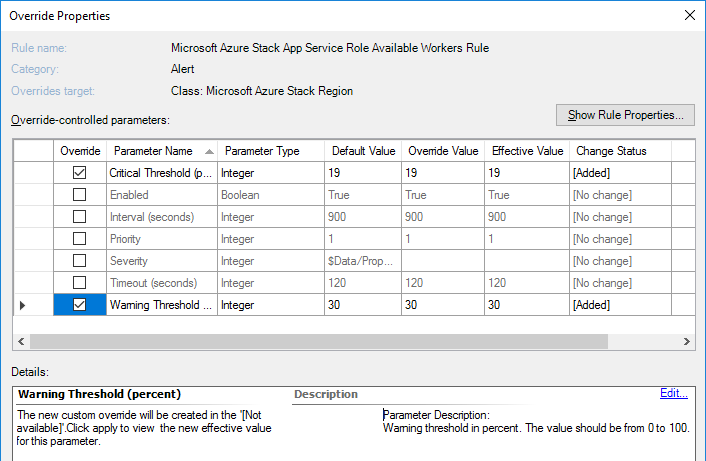
By default critical threshold equals to 19 percent and warning threshold equals to 30 percent. The threshold may be configured via the corresponding overridable parameter.

#### How to set warning and critical thresholds

1. In the Operations Manager console, open the Authoring workspace; then, find the app service role available workers rule:



1. In the **Override Properties** window, set warning and critical thresholds (values should be from 0 to 100).



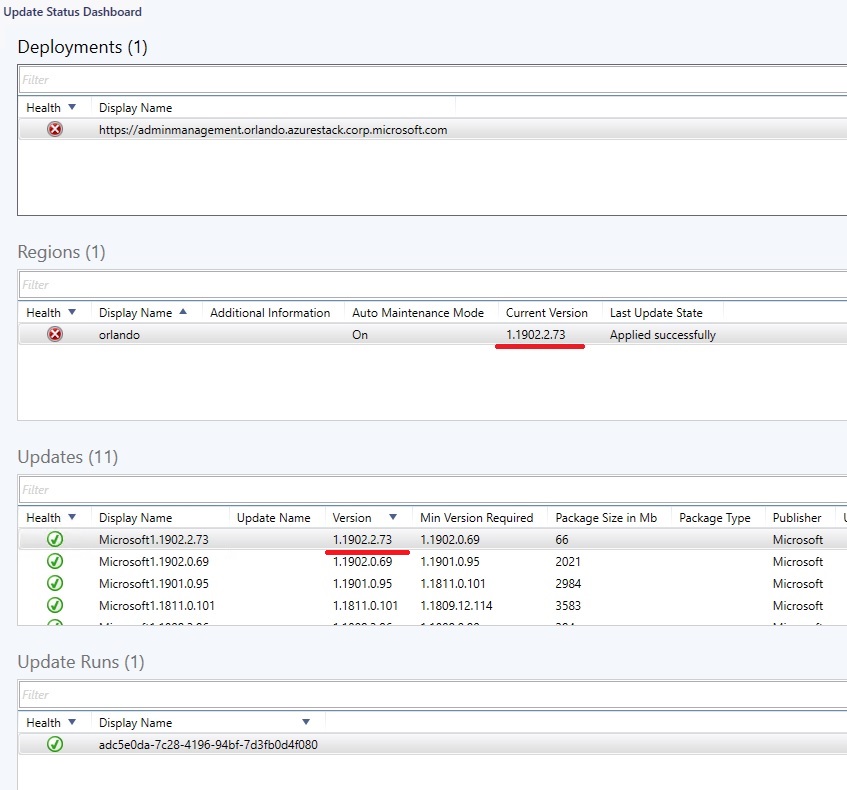
If the override values are set not from 0 to 100, the rule will work with these thresholds but it is recommended to set values from 0 to 100.

## Update Run State Monitor

The Azure Stack management pack provides monitor for Azure Stack Update Run.

### Health of update run

This monitor checks the state of the update run. By default, the monitor sends a request to Azure Stack to obtain update run state. But if the current version of the region is equal to the version of the latest update all update runs will be in healthy state and monitor won’t send the request.



## Tasks

There are several tasks that expand the possibilities of monitoring the Azure Stack objects.

### Set Additional Information Task

This task enables associating additional information with Azure Stack regions. You can enter any additional text information via the override; for example, the location of the region or contacts of the person responsible for it.

To use this task, select the desired region and run the task from the navigation pane list. Then, click **Override** and enter the additional information into the **Value** field. When the task is completed, select **Refresh** to update the information presented in the Operations Manager.

### Force Refresh Tasks

These tasks launches an immediate forced refresh of a certain object and can skip the corresponding workflows.

To use the tasks, select the desired object and run the corresponding task from the navigation pane list.

#### Force Deployment Refresh Task

This task forces the refresh of the deployment state, all regions for the selected deployment and the list of alerts for every region in the deployment.

#### Force Region Refresh Task

This task forces the refresh of the region state, all updates, resource providers, scale units, infrastructure roles and infrastructure role instances for the selected region and the list of alerts for the selected region in the deployment.

#### Force Update Refresh Task

This task forces the refresh of the update state and all runs of the selected update.

#### Force Update Run Refresh Task

This task forces the refresh of the update run state.

#### Force Resource Provider Refresh Task

This task forces the refresh of the resource provider state.

#### Force Scale Unit Refresh Task

This task forces the refresh of the scale unit state and all nodes of the selected scale unit.

#### Force Scale Unit Node Refresh Task

This task forces the refresh of the unit node state.

#### Force Infrastructure Role Refresh Task

This task forces the refresh of the states of all infrastructure roles.

#### Force Infrastructure Role Instance Refresh Task

This task forces the refresh of the states of all infrastructure role instances.

#### Force App Service Role Refresh Task

This task forces the refresh of the states of all app service roles.

#### Force App Service Role Instance Refresh Task

This task forces the refresh of the states of all app service role instances.

#### Force Backup Refresh Task

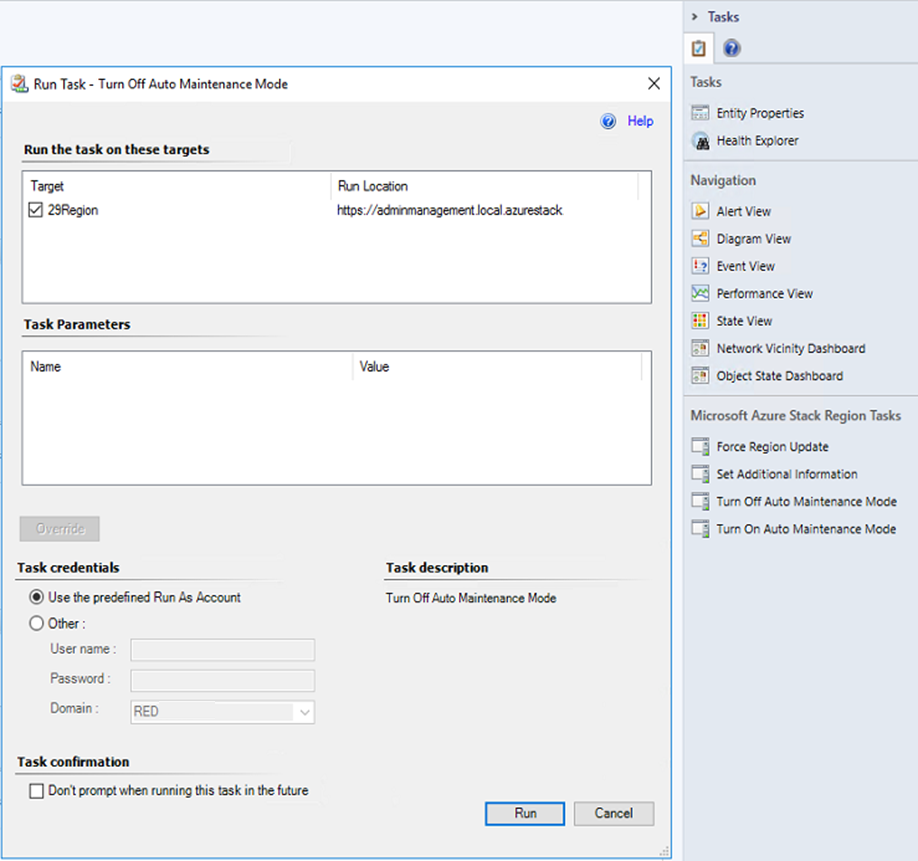
This task forces the refresh of the states of all region backups.

### Auto Maintenance Mode Tasks

#### Turn Off Auto Maintenance Mode Task

This task allows disabling the Auto Maintenance mode when necessary.

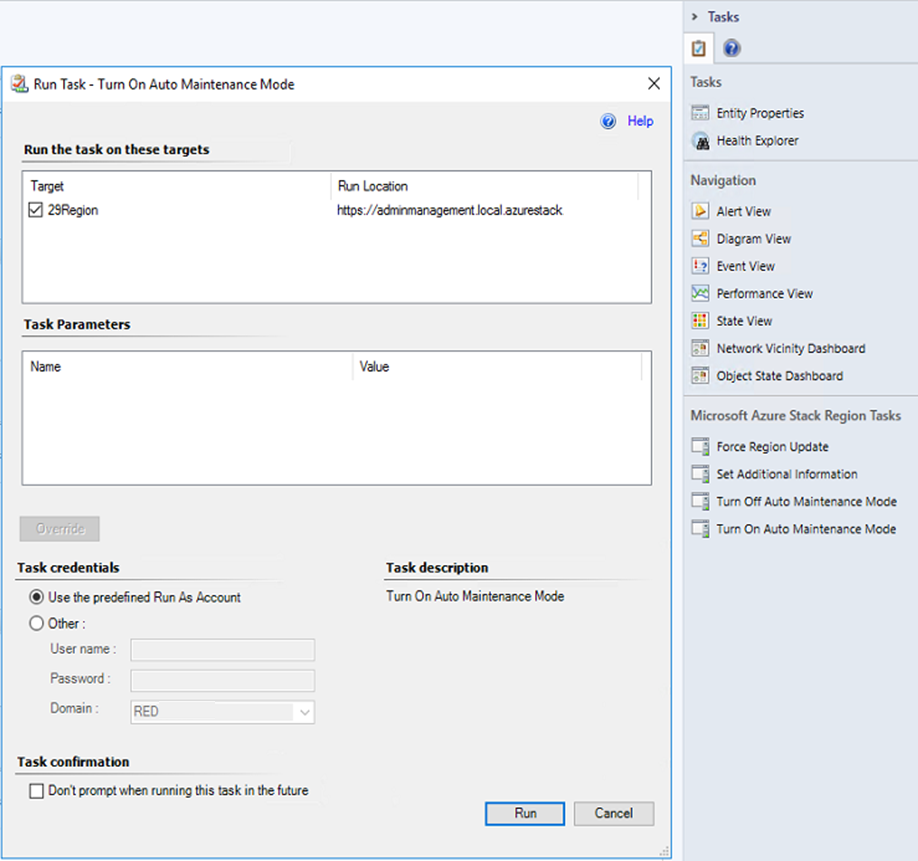
To use the tasks, select the appropriate region and run the corresponding task from the navigation pane list:



#### Turn On Auto Maintenance Mode Task

This task allows enabling the Auto Maintenance mode when necessary.

To use the tasks, select the appropriate region and run the corresponding task from the navigation pane list:



|  |
| --- |
| Important iconImportant:  Tasks will not refresh the Operations Manager state of the region that appears to be in maintenance mode until Force Deployment Refresh task is run. |

## Remaining subscription reads monitoring

Azure Stack API imposes a limit on a number of performed subscription reads per hour. That quantity is returned by an API in a header named *x-ms-ratelimit-remaining-subscription-reads*. Monitoring of this quantity was implemented in a Remaining Subscription Reads monitor.

The monitor has two thresholds: Warning Threshold and Critical Threshold. When remaining subscription read count becomes less than Warning Threshold then monitor switches to a warning state. When it becomes less than Critical Threshold then monitor switches to a critical state.

## Security Configuration

The **Azure Stack Run As Account AD Credentials** profile is configured automatically when you add a deployment using Wizard. You do not have to perform any additional configuration.

|  |  |
| --- | --- |
| Run As Profile Name | Notes |
| Azure Stack Run As Account AD Credentials | Holds the Azure Stack Active Directory credentials to authenticate with Azure Stack. |

## Role-Based Access Control Configuration

To perform managing actions like closing alerts, applying updates, perform actions with scale units and infrastructure roles in Azure Stack via the management pack in the Operations Manager console, it is important for the account to have the **Contributor** or **Owner** permissions to the subscription.

## Extended Logging

The extended logging allows collecting additional information about work of the managed modules in the management pack. It may be necessary for the investigation of an unexpected behavior or output of HTTP requests.

The extended logging is activated by creating the following registry value:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Azure Stack Management Pack\*

*Create string with name: ExtendedLogging*

*Set Value: On*

Any other values will be interpreted as “Off”.

After activation, the Azure Stack management pack will write additional information to the “Operations Manager” log in Windows Event Log with “MS Azure Stack MP Module” and the “Log Level Information” Event Source.

**Note.** In order to turn off extended logging we need switch flag to “Off” state and restart Health Service.

|  |
| --- |
| * **Important:**   Activation of the extended logging may cause growing up of the “Operations Manager” log size. It is strongly recommended to increase the size of the “Operations Manager” log before turning the extended logging on. |

## Worker Task Limit

The worker task limit allows increasing the speed of processing the requests to Azure Stack API.

By default, managed modules can use 6 instances of System.Threading.Tasks.Task class per MonitoringHost.exe process simultaneously.

In environments with many existing objects (more than 3 deployments, more than 50 hosted objects per deployment), the user can increase/decrease the amount of worker task instances by means of the following registry value:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft Azure Stack Management Pack\*

*Create string with name: MaxWorkerCount*

*Set Value: <required\_instance\_count>*

**Note:** Value for MaxWorkerCount must be greater than 0 and less than 20. Otherwise, the default value – 6 – will be applied.

After setting a new value of the MaxWorkerCount parameter, the user must restart the Health Service for applying this value in the managed modules.

|  |
| --- |
| * **Important:**   It is strongly recommended to change this parameter only in cases of increasing latency of processing the HTTP requests by the Azure Stack management pack or in cases of huge performance load of the SCOM server host machine by the MonitoringHost.exe process. |

## Links

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

### System Center 2012 R2 - Operations Manager

 [Management Pack Life Cycle](http://go.microsoft.com/fwlink/p/?LinkID=232986)

 [How to Import a Management Pack](http://go.microsoft.com/fwlink/p/?LinkID=219431)

 [Tuning Monitoring by Using Targeting and Overrides](http://go.microsoft.com/fwlink/p/?LinkID=217065)

 [How to Create a Run As Account](http://go.microsoft.com/fwlink/p/?LinkId=232988)

 [How to Export a Management Pack](http://go.microsoft.com/fwlink/p/?LinkId=232990)

 [How to Remove a Management Pack](http://go.microsoft.com/fwlink/p/?LinkId=232991)

### System Center 2016 - Operations Manager

* [Operations Manager Documentation](https://docs.microsoft.com/en-us/system-center/scom/?view=sc-om-1711)

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 Survival Guide](https://social.technet.microsoft.com/wiki/contents/articles/1280.system-center-survival-guide.aspx).

|  |
| --- |
| **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

**Total Requests counters for Blob, Queue and Table Storage Performance Dashboards are not the same as in Azure Stack administrator portal**

**Issue:** Management pack obtains default Time Grain intervals that are coming from the Azure Stack API. Time Grain for Total requests counter in the Azure Stack administrator portal differs from the default one that API returns.

**Resolution:** Manually change Time Grain and Interval overrides for all 3 rules: Blob Service Total Requests, Queue Service Total Requests, Table Service Total Requests to get identical results. For example, if on portal Time Grain is set to 1 hour, do the following changes in overrides: Time Grain: PT1H, Interval: 3700.

**Drained scale unit node parameters are not displayed on the initial discovery**

**Issue:** Initial discovery of scale unit which already has a drained scale unit node results in empty values of Cores and Memory field for corresponding scale unit node. **Resolution:** No resolution available.

**Some Infrastructure roles visible in Operations Manager console are not displayed on Azure Stack Administrator portal  
Issue:** In the Infrastructure Role Dashboard displayed more infrastructure roles than it is displayed in Azure Stack administrator portal. This happens because management pack displays all discovered Infrastructure roles that returned from the Azure Stack API.   
**Resolution:** No resolution available.

**Common Error rule alerts are not displayed in the Azure Stack Active alerts view**

**Issue:** Alerts from the Common Error rule are not displayed in the **Active alerts** view of the management pack.

**Resolution:** Common Error rule alerts are available in Main Operation Manager Сonsole Active Alerts view.

**Selection for a previously viewed region is not saved after switching to another deployment**

**Issue:** In the Health Dashboard, selection for a previously viewed Region is not saved in case of switching to another deployment. Upon return to the initial deployment, the selection is randomly switched to another region.

**Resolution:** No resolution is available.

**"No such host is known" exception is received when the Operations Manager console is opened by IP from a remote machine**

**Issue:** "No such host is known" exception is received when the Operations Manager console is opened from a remote machine by IP.

**Resolution:** No resolution is available.

**Alerts from the previously selected region may be displayed for the current region**

**Issue:** When you switch from one region to another in the Operations Manager, the alerts from the previously viewed region may be displayed for the currently selected region.

**Resolution:** No resolution is available.

**In some cases, invalid UPN/SPN credentials may be validated successfully**

**Issue:** In some cases, invalid UPN/SPN credentials are validated successfully in the “Add Deployment” and “Edit Deployment” wizards because the previously entered valid credentials were cached in the Operations Manager.

**Resolution:** Close and reopen the Operations Manager console.  The cache will be cleared and the wizard will throw an error if invalid credentials are entered.

**The management pack does not work for external domain users**

**Issue:** The management pack user must belong to the exact Azure Active Directory, which was used for the Azure Stack deployment.

**Resolution:** Use the right Azure Active Directory user account.

**Operations Manager issue: checkboxes become selected after the capacity dashboard refreshing**

**Issue:** When the capacity dashboard is refreshed, the checkboxes become randomly selected.

**Resolution:**  Apply sorting by any column.

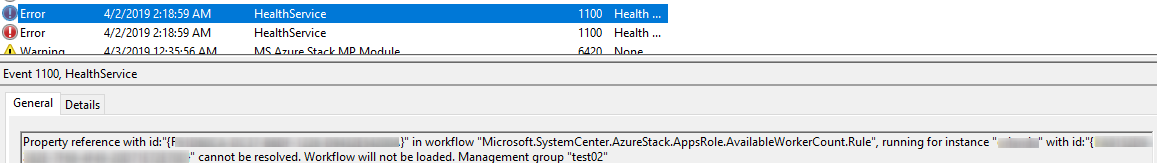
**Operations Manager issue: unable to uninstall the management pack after manually associating the Run As account with the Run As profile**

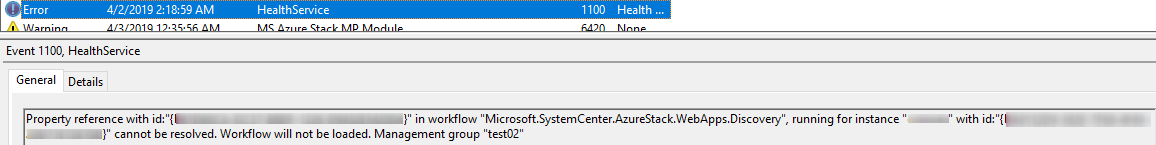
**Issue:** If manually associate Run As account with Microsoft Azure Stack Run As Profile AD Credentials and attempt to delete the Azure Stack management pack, it fails with a message that the Microsoft.SystemCenter.SecureReferenceOverride pack depends on the Azure Stack management pack.

**Resolution:**  Export the Microsoft.SystemCenter.SecureReferenceOverride pack, find the section with the Azure Stack management pack secure reference and manually remove it. Then, import the Microsoft.SystemCenter.SecureReferenceOverride pack again. See the [SCOM R2: Not able to remove a MP when a profile is set](http://thoughtsonopsmgr.blogspot.ru/2010/05/scom-r2-not-able-to-remove-mp-when.html) article for detailed instructions.

**Operations Manager issue: Temporary 1100 error in Event Viewer after upgrade 1.0.3.11 to 1.0.4.0**

**Issue:** After upgrade to version 1.0.4.0, next errors would be appeared in Event Viewer:





**Resolution:** Issue is temporary and wouldn’t affect further monitoring. Ignore errors and wait until SCOM updates these workflows.

## Appendix: Management Pack Contents

### Rules (alerting)

**Microsoft Azure Stack Common Error Rule**

The rule generates an alert when a common exception has been thrown.

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

### Microsoft Azure Stack App Service Role

An App Service Role for a Microsoft Azure Stack region.

#### Microsoft Azure Stack App Service Role – Discoveries

|  |
| --- |
| **Microsoft Azure Stack App Service Discovery** |
| Discovery of all Microsoft Azure Stack App Service Roles and Role Instances per region. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  | |  |  |  | |

#### Microsoft Azure Stack App Service Role - Unit monitors

|  |
| --- |
| **Microsoft Azure Stack App Service Role State Monitor** |
| Microsoft Azure Stack App Service Role state monitor. This monitor checks the App Service Role state. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 90 | |  | |  |  |  | |

#### Microsoft Azure Stack App Service Role - Dependency (rollup) monitors

|  |
| --- |
| **Microsoft Azure Stack App Service Role Instance Dependency Monitor** |
| Microsoft Azure Stack App Service Role availability depends on App Service Role Instance availability. **Azure Stack App Service Role Instance Dependency** monitor disabled by default by design. Health rollup mechanism for App Service role calculated in **Microsoft Azure Stack App Service Role State Monitor.** |

#### Microsoft Azure Stack App Service Role – Tasks

|  |
| --- |
| **Force App Service Role Refresh** |
| This task provides forced refresh of the App Service Roles state. |

### Microsoft Azure Stack App Service Role Instance

An App Service Role Instance for a Microsoft Azure Stack region.

#### Microsoft Azure Stack App Service Role Instance – Discoveries

|  |
| --- |
| **Microsoft Azure Stack App Service Discovery** |
| Discovery of all Microsoft Azure Stack App Service Roles and Role Instances per region. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  | |  |  |  | |

#### Microsoft Azure Stack App Service Role Instance - Unit monitors

|  |
| --- |
| **Microsoft Azure Stack App Service Role Instance State Monitor** |
| Microsoft Azure Stack App Service Role Instance state monitor. This monitor checks the App Service Role Instance state. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  | |  |  |  | |

#### Microsoft Azure Stack App Service Role Instance – Tasks

|  |
| --- |
| **Stop App Service Role Instance** |
| This task stops app service role instance. |
|  |
| **Repair App Service Role Instance** |
| This task repairs app service role instance. |
|  |
| **Start App Service Role Instance** |
| This task starts app service role instance. |
|  |
| **Force App Service Role Instance Refresh** |
| This task provides forced refresh of the App Service Role Instances state. |

### Microsoft Azure Stack Backup

Microsoft Azure Stack Backup

#### Microsoft Azure Stack Backup – Discoveries

|  |
| --- |
| **Microsoft Azure Stack Backup Discovery** |
| Discovery of all Microsoft Azure Stack Backups per region. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  | |  |  |  | |

#### Microsoft Azure Stack Backup - Unit monitors

|  |
| --- |
| **Microsoft Azure Stack Backup State Monitor** |
| Microsoft Azure Stack backup state monitor. This monitor checks the Backup state. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | False | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  | |  |  |  | |

#### Microsoft Azure Stack Backup – Tasks

|  |
| --- |
| **Force Backup Refresh** |
| This task provides forced refresh of the backup state. |

### Microsoft Azure Stack Deployment

A Microsoft Azure Stack deployment including logical entities comprised of the hardware resources.

#### Microsoft Azure Stack Deployment - Unit monitors

**Microsoft Azure Stack Deployment Connectivity Monitor**

Microsoft Azure Stack deployment connectivity monitor. This monitor checks deployment availability.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Microsoft Azure Stack Remaining Subscription Reads Monitor**

Microsoft Azure Stack remaining subscription reads monitor. This monitor checks the remaining subscription reads.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Critical Threshold | The monitor will change the state to Critical if the value drops below this threshold. | 500 | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | | Warning Threshold | The monitor will change the state to Warning if the value drops below this threshold. | 2000 | |  |
|  |  |  |

#### Microsoft Azure Stack Deployment - Dependency (rollup) monitors

**Microsoft Azure Stack Region Dependency Monitor**

Microsoft Azure Stack Deployment availability depends on Region availability.

#### Microsoft Azure Stack Deployment - Rules (non-alerting)

**Microsoft Azure Stack Auto Maintenance Mode Monitoring Rule**

The rule checks the update state of the regions on Azure Stack portal within the configured interval. When updates are run on an Azure Stack region, the region is switched to maintenance mode in SCOM.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 30 | |  |
|  |  |  |

#### Microsoft Azure Stack Deployment - Tasks

**Force Deployment Refresh**

This task provides forced refresh of the deployment state, configuration and regions list along with forced refresh of state and list of alerts for every region in the deployment.

#### Microsoft Azure Stack Deployment - Console Tasks

|  |
| --- |
| **Open Microsoft Azure Stack Portal** |
| This task opens Microsoft Azure Stack Portal. |

### Microsoft Azure Stack Infrastructure Role

Microsoft Azure Stack infrastructure role.

#### Microsoft Azure Stack Infrastructure Role - Discoveries

**Microsoft Azure Stack Infrastructure Discovery**

Discovery of all Microsoft Azure Stack infrastructure roles, infrastructure role instances and relations between them per region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

#### Microsoft Azure Stack Infrastructure Role - Unit monitors

**Microsoft Azure Stack Infrastructure Role State Monitor**

Microsoft Azure Stack infrastructure role state monitor. This monitor checks the status of the Infrastructure Role.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Infrastructure Role - Tasks

**Force Infrastructure Role Refresh**

This task provides forced refresh of the infrastructure role state and configuration.

**Restart Infrastructure Role**

This task only restarts the Infrastructure Role in which the Infrastructure Role Instance names contain XRP.

### Microsoft Azure Stack Infrastructure Role Instance

Microsoft Azure Stack infrastructure role instance.

#### Microsoft Azure Stack Infrastructure Role Instance - Discoveries

**Microsoft Azure Stack Infrastructure Discovery**

Discovery of all Microsoft Azure Stack infrastructure roles, infrastructure role instances and relations between them per region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 300 | |  |
|  |  |  |

#### Microsoft Azure Stack Infrastructure Role Instance - Unit monitors

**Microsoft Azure Stack Infrastructure Role Instance State Monitor**

Microsoft Azure Stack Infrastructure Role Instance State Monitor. This monitor checks the status of the Infrastructure Role Instance.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Infrastructure Role Instance - Tasks

**Force Infrastructure Role Instance Refresh**

This task provides forced refresh of the infrastructure role instance state and configuration.

**Restart Infrastructure Role Instance**

This task restarts infrastructure role instance.

**Start Infrastructure Role Instance**

This task starts infrastructure role instance.

### Microsoft Azure Stack Marketplace Management

Microsoft Azure Stack Marketplace Management.

#### Microsoft Azure Stack Marketplace Management – Discoveries

|  |
| --- |
| **Microsoft Azure Stack Marketplace Management Discovery** |
| Microsoft Azure Stack Marketplace Management discovery. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  | |  |  |  | |

### Microsoft Azure Stack Region

A separate Microsoft Azure Stack instance (e.g. an instance set on some separate hardware) included in a Microsoft Azure Stack deployment.

#### Microsoft Azure Stack Region - Discoveries

**Microsoft Azure Stack Region Discovery**

Discovery of all Microsoft Azure Stack regions per deployment.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

**Microsoft Azure Stack Region Set Additional Information Property**

By means of this discovery, you can set additional information property for Azure Stack regions via the override. This discovery contains additional properties that allow storing information about a region in the Operations Manager, such as associating additional customer details and displaying the current flag of the automatic maintenance mode state.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Additional Information | Additional Information |  | | Auto Maintenance Mode | Auto Maintenance Mode | On | |  |
|  |  |  |

#### Microsoft Azure Stack Region - Unit monitors

**Microsoft Azure Stack Region Connectivity Monitor**

Microsoft Azure Stack region connectivity monitor. This monitor checks the region availability.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 300 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Microsoft Azure Stack Region Alert Count Monitor**

Microsoft Azure Stack alert count monitor for the regions. Monitors the health state of the regions and checks for current alerts.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Critical Count Threshold | The monitor will change the state to Critical if the value drops below this threshold. | 1 | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | | Warning Threshold | The monitor will change the state to Warning if the value drops below this threshold. | 1 | |  |
|  |  |  |

#### Microsoft Azure Stack Region - Dependency (rollup) monitors

|  |
| --- |
| **Microsoft Azure Stack Update Dependency Monitor** |
| Microsoft Azure Stack Region availability depends on Update availability. |
|  |
| **Microsoft Azure Stack Infrastructure Role Dependency Monitor** |
| Microsoft Azure Stack Region availability depends on Infrastructure Role availability. |
|  |
| **Microsoft Azure Stack Resource Provider Dependency Monitor** |
| Microsoft Azure Stack Region availability depends on Resource Provider availability. |
|  |
| **Microsoft Azure Stack Scale Unit Dependency Monitor** |
| Microsoft Azure Stack Region availability depends on Scale Unit availability. |
|  |
| **Microsoft Azure Stack App Service Role Dependency Monitor** |
| Microsoft Azure Stack Region availability depends on App Service Role availability. |

#### Microsoft Azure Stack Region - Rules (alerting)

|  |
| --- |
| **Microsoft Azure Stack App Service Role Available Workers Rule** |
| Microsoft Azure Stack App Service Role Available Workers Rule. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Critical Threshold (percent) | The monitor will change the state to Critical if the value drops below this threshold. | 19 | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | $Data/Property[@Name='Severity']$ | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | | Warning Threshold | The monitor will change the state to Warning if the value drops below this threshold. | 30 | |  | |  |  |  | |

**Microsoft Azure Stack Alerts Sync Rule (Azure Stack to Operations Manager)**

Microsoft Azure Stack alerts synchronization rule creates alerts related to the regions and initiates closure of the alerts closed in Azure Stack.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Priority | Defines Alert Priority. | 1 | | Severity | Defines Alert Severity. | $Data/Property[@Name='SeverityInteger']$ | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 30 | |  |
|  |  |  |

#### Microsoft Azure Stack Region - Rules (non-alerting)

**Blob Service Availability (%)**

This rule collects blob service availability in percentage terms.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Physical Memory Available (GB)**

This rule collects the current amount of free physical memory available on the region in gigabytes.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Queue Service Availability (%)**

This rule collects queue service availability in percentage terms.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Physical Storage Used (TB)**

This rule collects the amount of physical storage currently used on the region in terabytes.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Physical Memory Used (GB)**

This rule collects the amount of physical memory currently used on the region in gigabytes.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Table Service Total Requests**

This rule collects total requests of table service.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Public IP Address Pools Used Count**

This rule collects the amount of free public IP address pools currently used on the region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Physical Storage Available (TB)**

This rule collects the current amount of free physical storage available on the region in terabytes.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Public IP Address Pools Available Count**

This rule collects the current amount of free public IP address pools available on the region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Blob Service Server Latency (ms)**

This rule collects blob service server latency in milliseconds.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Queue Service Total Requests**

This rule collects total requests of queue service.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Blob Service Total Requests**

This rule collects blob service total requests.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Table Service Availability (%)**

This rule collects table service availability in percentage terms.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Table Service Server Latency (ms)**

This rule collects latency of table service server in milliseconds.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

**Queue Service Server Latency (ms)**

This rule collects latency of queue service server in milliseconds.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 900 | | Time Grain | Time grain allows to specify metric value aggregation interval.  Examples of time grains are: PT1M (1 min), PT1H (1 hour), P1D (1 day). |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Region - Rules (non-alerting)

**Microsoft Azure Stack Alerts Sync Rule (Operations Manager to Azure Stack)**

Microsoft Azure Stack alerts synchronization rule initiates closure of the alerts closed in the Operations Manager.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 30 | | Synchronization Time | The synchronization time specified by using a 24-hour format. May be omitted. |  | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 30 | |  |
|  |  |  |

#### Microsoft Azure Stack Region - Tasks

|  |
| --- |
| **Set Additional Information** |
| This task provides a possibility to set additional information for Microsoft Azure Stack region: you can enter any additional text information via the override. |
| |  |  |  | | --- | --- | --- | |  |  |  | |  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Additional Information | Additional Information |  | |  | |  |  |  | |
| **Disable Automatic Backups** |
| This task provides possibility to disable automatic backups. |
|  |
| **Turn Off Auto Maintenance Mode** |
| This task turns the Auto Maintenance Mode off. |
|  |
| **Force Region Refresh** |
| This task provides forced refresh of the region state, configuration and updates along with forced refresh of state for every update and every resource provider for the region. |
|  |
| **Enable Automatic Backups** |
| This task provides possibility to enable automatic backups. |
|  |
| **Backup Now** |
| This task provides possibility to make a backup. |
|  |
| **Turn On Auto Maintenance Mode** |
| This task turns the Auto Maintenance Mode on. |

### Microsoft Azure Stack Resource Provider

A resource provider of a Microsoft Azure Stack region.

#### Microsoft Azure Stack Resource Provider - Discoveries

**Microsoft Azure Stack Resource Provider Discovery**

Discovery of all Microsoft Azure Stack resource providers per region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

#### Microsoft Azure Stack Resource Provider - Unit monitors

**Microsoft Azure Stack Resource Provider State Monitor**

Microsoft Azure Stack resource provider state monitor. This monitor checks the resource provider state.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Resource Provider - Tasks

**Force Resource Provider Refresh**

This task provides forced refresh of the resource provider state and configuration.

### Microsoft Azure Stack Scale Unit

Microsoft Azure Stack scale unit.

#### Microsoft Azure Stack Scale Unit - Discoveries

**Microsoft Azure Stack Scale Unit Discovery**

Discovery of all Microsoft Azure Stack scale units per region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

#### Microsoft Azure Stack Scale Unit - Dependency (rollup) monitors

**Microsoft Azure Stack Scale Unit Node Dependency Monitor**

Microsoft Azure Stack Scale Unit availability depends on Unit Node availability.

#### Microsoft Azure Stack Scale Unit - Rules (non-alerting)

**Microsoft Azure Stack Auto Maintenance Mode Monitoring Rule for Scale Unit Node**

The rule checks the state of the scale unit nodes on Azure Stack portal within the configured interval. When it founds difference between maintenance mode on the portal and in SCOM, the maintenance mode in SCOM is switched to the state present on the portal.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | No | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Scale Unit - Tasks

**Force Scale Unit Refresh**

This task provides forced refresh of the scale unit state and configuration.

### Microsoft Azure Stack Scale Unit Node

Microsoft Azure Stack scale unit node.

#### Microsoft Azure Stack Scale Unit Node - Discoveries

**Microsoft Azure Stack Unit Node Discovery**

Discovery of all Microsoft Azure Stack unit nodes per scale unit.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 86400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

#### Microsoft Azure Stack Scale Unit Node - Unit monitors

**Microsoft Azure Stack Scale Unit Node State Monitor**

Microsoft Azure Stack scale unit node state monitor. This monitor checks the Scale Unit Node Status.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 180 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Scale Unit Node - Tasks

**Resume Scale Unit Node**

This task allows to stop maintenance mode for the scale unit node.

**Force Unit Node Refresh**

This task provides forced refresh of the scale unit node state and configuration.

**Drain Scale Unit Node**

This task is putting a node into maintenance mode along with distributing it's workloads among remaining nodes in the particular scale unit.

**Power Off Scale Unit Node**

This task powers off the scale unit node.

**Shutdown Scale Unit Node**

This task allows to shut down the scale unit node.

**Power On Scale Unit Node**

This task powers on the scale unit node.

### Microsoft Azure Stack Update

An update for a Microsoft Azure Stack region.

#### Microsoft Azure Stack Update - Discoveries

**Microsoft Azure Stack Update Discovery**

Discovery of all Microsoft Azure Stack updates per region.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 14400 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

#### Microsoft Azure Stack Update - Unit monitors

**Microsoft Azure Stack Update State Monitor**

Microsoft Azure Stack update state monitor. This monitor checks the update state.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Update - Tasks

**Apply Update Package**

This task applies update package if it is available.

**Force Update Refresh**

This task provides forced refresh of the update state, configuration and update runs along with forced refresh of state for every run of the update.

### Microsoft Azure Stack Update Run

A run of a Microsoft Azure Stack update.

#### Microsoft Azure Stack Update Run - Discoveries

**Microsoft Azure Stack Update Run Discovery**

Discovery of all Microsoft Azure Stack update runs per update.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 120 | |  |
|  |  |  |

#### Microsoft Azure Stack Update Run - Unit monitors

**Microsoft Azure Stack Update Run State Monitor**

Microsoft Azure Stack update run state monitor. This monitor checks the state of the update run.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | |  |  |  | | --- | --- | --- | | **Name** | **Description** | **Default value** | | Enabled | Enables or disables the workflow. | Yes | | Generate Alerts | Defines whether the workflow generates an Alert. | True | | Interval (seconds) | The recurring interval of time in seconds in which to run the workflow. | 3600 | | Timeout (seconds) | Specifies the time the workflow is allowed to run before being closed and marked as failed. | 60 | |  |
|  |  |  |

#### Microsoft Azure Stack Update Run - Tasks

**Restart Update Run**

This task reruns the update run.

**Force Update Run Refresh**

This task provides forced refresh of the update run state and configuration.