# Monitoring and Alerting Framework Solution Design for Azure

## Overview

The monitoring and alerting framework is designed to meet the following requirements:

* Flexible and minimizes tag maintenance effort
* Support for one or more teams to be notified for a particular type of alert, without notifying teams that shouldn’t be notified
* Fully automated so that when new resources are created that require monitoring and alerting, the applicable alert rule sets are automatically created for that resource if it has been tagged.
* When broadscale changes are required to an alert trigger condition (eg. across hundreds of resources), the change can be rolled out automatically for all affected resources.

## Solution design

The Azure native components used by the framework are:

* Action Groups which define who or what to notify (ie. contact information for a support team member, an Azure runbook or Azure Function, etc)
* Alert Rules which define the conditions under which the alert should trigger, as well as which Action Groups to notify.
* Azure resource group and resource level tags. The tags described below will be used to control which Action Groups are notified as well as which Alert Rules sets apply for a particular resource.

Related sets of Alert Rules are grouped into “alert rule sets” (this is our own concept). Each resource type in azure will have a corresponding default set of alert rules.

The following resource types and alert rule sets are supported by the current version of the framework:

|  |  |
| --- | --- |
| **Azure Resource Type** | **Supported Alert Rule Set Names** |
| Azure Linux Virtual Machines | linuxVMStandard, linuxVMStandardLogAnalyticsQueries,linuxVMResourceHealthStandard |
| Azure Windows Virtual Machines | windowsVMStandard,windowsVMStandardLogAnalyticsQueries,windowsVMResourceHealthStandard, sqlServerIaaSLogAnalyticsQueries |
| Azure App Service Application Insights | applicationInsightsStandard |
| Azure Virtual Machine Scale Sets | vmScaleSetStandard |
| Azure App Service Plan | appServicePlanStandard |

By browsing the repository structure, you can see the various alert rules that are included in each alert rule set (see below).

The solution uses resource level and resource group level tags to define whether alerting should be enabled, what alert rules should be applied, and which support team to notify.

The tags that are used are as follows:

1. The **alert** tag, which when set to True enables alerting for an individual resource or all resources in a resource group (see table below for more details).
2. The **alertRuleExtensions** tag, which defines which alert rule extension sets that should be created for a particular resource in addition to the standard set of alert rules corresponding to the resource. For example, the sqlServerIaaSLogAnalyticsQueries extension set defines a set of alert rules for SQL Server performance metrics for the tagged resource.
3. The **alertActions** tag, which defines which support teams (defined via Action Groups) should be notified for one or more alert rule sets. This tag can be defined at the individual resource level and/or the resource group level (see table below for more details).
4. The **alertRulesExclusions** tag, which defines any standard alert rule sets and/or individual alert rules that shouldn’t be created for this resource. This may be used in cases where a customization is required to a particular alert rule; the alert rule would be created as per normal on the initial run of the script, modified manually, and then excluded using this tag from further script runs to ensure that the customized configuration isn’t overwritten.

Each resource type has an associated standard set of alert rule sets. These are implicit and do not need to be specified in the alertRuleExtensions tag (eg. windowsVMStandard, applicationInsightsStandard, etc).

There are 3 different types of alert rules:

1. Metric alert rules based on Azure Monitor supported metrics. These alert rule are scoped to a particular resource (eg. a particular VM, app service, application insights instance, etc).
2. Metric alert rules based on Log Analytics Workspace metrics. These alert rules are scoped to the log analytics workspace that a resource is logging to. The names of log analytics metric alert rules must terminate with “LogAnalyticsMetrics”.
3. Log analytics query based alert rules. These alert rules are scoped to the log analytics workspace that a resource is logging to. The names of log analytics query alert rules must terminate with “LogAnalyticsQueries”.

### Repository structure

|  |  |
| --- | --- |
| **Folder** | **Description** |
| activity-log-alert-rules | Alert rule template parameter files for activity log based alerts |
| log-analytics-query-alert-rules | Alert rule template parameter files for log analytics query based alerts |
| metric-alert-rules | Alert rule template parameter files templates for metric based alerts |
| scripts | Powershell scripts to create the alert rules based on tagging |
| templates | ARM templates used by the powershell scripts to create the alert rules |

### Alert Rule template definitions

There are 3 Alert Rule templates defined in the templates folder:

1. metric-alert-rule-template.json which is a parameterized ARM template for creating metric alert rules
2. log-analytics-query-alert-rule-template.json which is a parameterized ARM template for creating log analytics query based alert rules
3. activity-log-alert-rule-template.json which is a parameterized ARM template for creating activity log based alert rules

### Alert Rule set definitions

The trigger conditions for alert rules are stored in JSON parameter files, and referenced when deploying the alert rule ARM template.

The alert rule JSON parameter files are organized into folders matching the name of the corresponding alert rule set, as shown below:

log-analytics-query-alert-rules (*alert rule type*)

sqlServerIaaSLogAnalyticsQueries (*alert rule set name*)

lock-wait-time.json (*alert rule parameter file*)

…

metric-alert-rules (*alert rule type*)

windowsVMStandard (*alert rule set name*)

low-memory-alert.json (*alert rule parameter file*)

low-disk-space.json (*alert rule parameter file*)

…

linuxVMStandard (*alert rule set name*)

low-memory-alert.json (*alert rule parameter file*)

low-disk-space.json (*alert rule parameter file*)

…

…

activity-log-alert-rules (*alert rule type*)

linuxVMResourceHealthStandard (*alert rule set name*)

vm-unhealthy.json (*alert rule parameter file*)

windowsVMResourceHealthStandard (*alert rule set name*)

vm-unhealthy.json (*alert rule parameter file*)

The Azure Automation runbook powershell script can be found in the scripts folder and automatically creates Alert Rules as follows (at a high level):

* Reads the tags of resource groups and resources within those resource groups and determines for each resource what Alert Rules sets should be created and which Action Groups should be notified based on tag settings.
* For each Alert Rule set that applies, the script then loops through all Alert Rule JSON parameter files defined for that Alert Rule set does an ARM template deployment for each one by passing in the JSON parameter file and the corresponding Action Group Ids as parameters to create the Alert Rules.

Note that the powershell script will only create or update alert rules, it will not delete them, even if the “**alert**” tag is toggled from True to False. Alert rule deletion is anticipated to be rare, and as such will need to be done manually.

## Resource Group Level tagging

|  |  |  |  |
| --- | --- | --- | --- |
| **Tag name** | **Purpose** | **Format** | **Example** |
| alert | Indicates whether alerting should be enabled or disabled for all resources in the resource group. This setting can be overridden at the individual resource level. | String, with a value of True or False |  |
| alertActions | For one or more alert rule sets, defines who should be notified if one of the alerts in the set triggers. | JSON string of the format:  {  “comma separated list of alert rule set names 1”: “comma separated list of action group names”,  “comma separated list of alert rule set names 2”: “comma separated list of action group names”,  …  }  In place of a list of alert rule set names, a wildcard (\* character) can be used to designate “All Alert Rule Sets”. | An example value for the alertActions tag:  {  “\*”: “Resource Group XYZ Support Team”,  “windowsVMStandard,  linuxVMStandard,  windowsVmStandardLogAnalyticsMetrics,  linuxVmStandardLogAnalyticsMetrics”: “Infrastructure Support Team”  }  In the above example the Infrastructure Support Team will be notified if one of the standard Alert Rules for VMs triggers for any resource in the resource group, and the Resource Group XYZ Support Team will be notified if any Alert Rule for any resource in the resource group triggers. |

## Resource Level tagging

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tag name** | **Purpose** | **Format** | **Example** | **Notes** |
| alert | Indicates whether alerting should be enabled or disabled for the resource. If defined, it will override the setting at the resource group level. | String, with a value of True or False |  | If not defined at the resource level, it will default to the resource group’s “alert” tag value; otherwise if the tag is not defined at either level, a value of False is assumed |
| alertRuleExtensions | Names of any additional alert rule sets (ie. alert rule extensions) that should be applied in addition to the standard set. The standard set is derived based on resource’s resource type. | Comma separated list of alert rule set names. | For example, for a VM that is running SQL Server, the value could be set to **sqlServerIaaSLogAnalyticsQuery** in order to include alerting on SQL Server performance counters. | Not applicable |
| alertActions | For one or more alert rule sets, defines who should be notified if one of the alert rules in the set triggers for the resource. | JSON string of the format:  {  “comma separated list of alert rule set names 1”: “comma separated list of action group names”,  “comma separated list of alert rule set names 2”: “comma separated list of action group names”,  …  }  In place of a list of alert rule set names, a wildcard (\* character) can be used to designate “All Alert Rule Sets”. | An example value for the alertActions tag:  {  “sqlServerIaasLogAnalyticsQueries”: “SQL Server Support Team”  }  In the above example the  SQL Server Support Team is notified if one of the SQL Server Alert Rules trigger. | Any alert actions defined in the “alertActions” tag at the resource group level will be **additive** to those defined at the resource level. |
| alertRuleExclusions | List of alert rule sets and/or individual alert rules that should not be created for this resource. | Comma separated list of alert rule set names or alert rule parameter file names. | For example, a tag value of:  **low-disk-space.json,** **windowsVMStandard**  would exclude creating the low-disk-space alert rule and all the rule in the windowsVMStandard alert rule set for the tagged resource.  Sometimes resources have to be excluded from certain alerts to avoid generating too many spurious alert notification. |  |