Contents

What is Impact Reporting?

6/19/2024 • 2 minutes to read

Azure Impact Reporting enables you to report issues with performance, connectivity, and availability impacting your Azure workloads directly to Microsoft. It is an additional tool you can leverage and a quicker way to let us know that something might be wrong. These reports are used by Azure internal systems to aid in quality improvements and regression detection.

What is an "Impact"?

In this context, an impact is any unexpected behavior or issue negatively affecting your workloads that has been root caused to the Azure platform.

Examples of impacts include:

- Performance Impact: Your application's performance degrades suddenly, you investigate and realize that database writes to your IaaS SQL virtual machine are unusually slow.
- Connectivity Impact: You're not able to successfully write to blob store despite having the right permissions
- Availability: Your Azure virtual machine unexpectedly reboots

Next steps

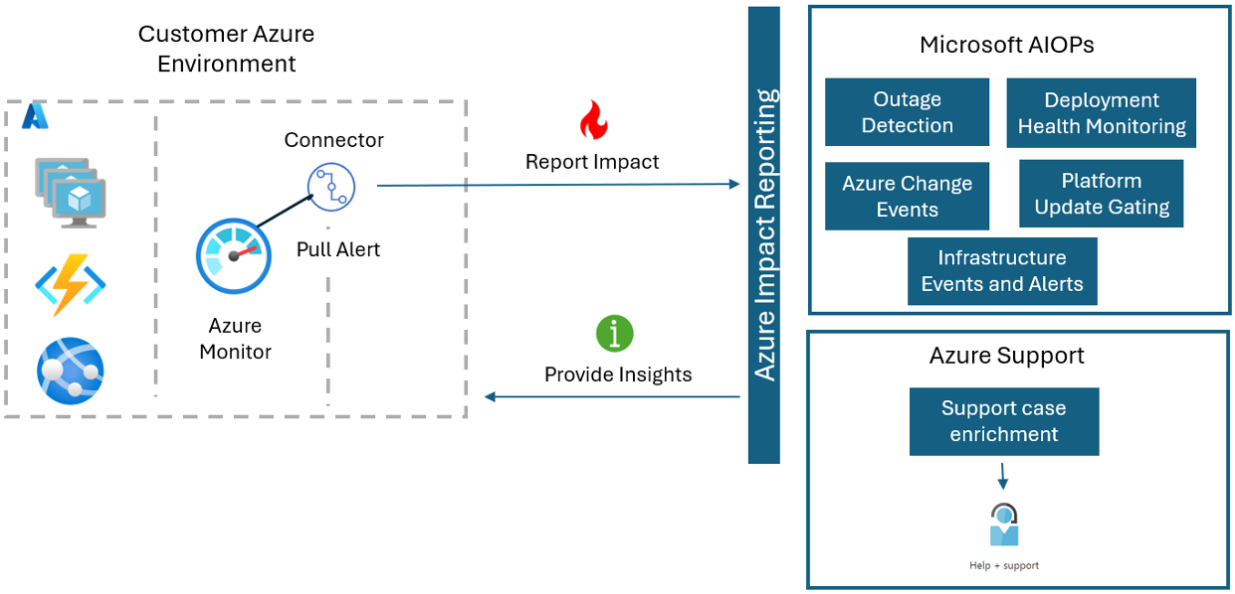
- File an impact report

What is the Impact Connector for Azure Monitor Alerts?

6/19/2024 • 2 minutes to read

The impact Connector for Azure Monitor alerts enables you to seamlessly report impact from an alert into Microsoft AIOps for change event correlation.

How Connectors work



When you create a connector, it is associated with a subscription. When alerts whose target resource reside in the specified subscription get fired, an Impact report is created through Azure Impact Reporting and sent to Microsoft AIOPs.

Create an Impact Connector for Azure Monitor Alerts

Below are steps needed to create an impact Connector for Azure Monitor Alerts

Pre-Requisites

TYPE	DETAILS
Azure RBAC Permissions	Ensure you have **contributor** access on the subscription you where the resources reside
Command line tools	Bash or Powershell (*not needed if you are using CloudShell*)
Subscription Id	A subscription ID, or a file containing a list of subscription IDs whose alerts are of interest

Steps

The deployment scripts does the following:

- Registers your subscription(s) for Azure Impact Reporting private preview (pre-requisite for using Connectors)

- Creates a connector resource (`microsoft.impact/connector`)
- This connector will report an impact whenever an alert from those subscriptions fires

1. Get the script

Go to the Impact Reporting samples githup repo and choose your script and choose either the bash or powershell script

2. Execute in your environment

You will need to execute this script in your Azure environment.

Powershell

- Single Subscription: `./CreateImpactReportingConnector.ps1 -SubscriptionId <subid>`
- Multiple subscriptions from file: `./CreateImpactReportingConnector.ps1 -FilePath './subscription_ids'`

Bash

- Single Subscription: `./create-impact-reporting-connector.sh --subscription-id <subid>`
- Multiple subscriptions from file: `./create-impact-reporting-connector.sh --file_path './subscription_ids'`

Next steps

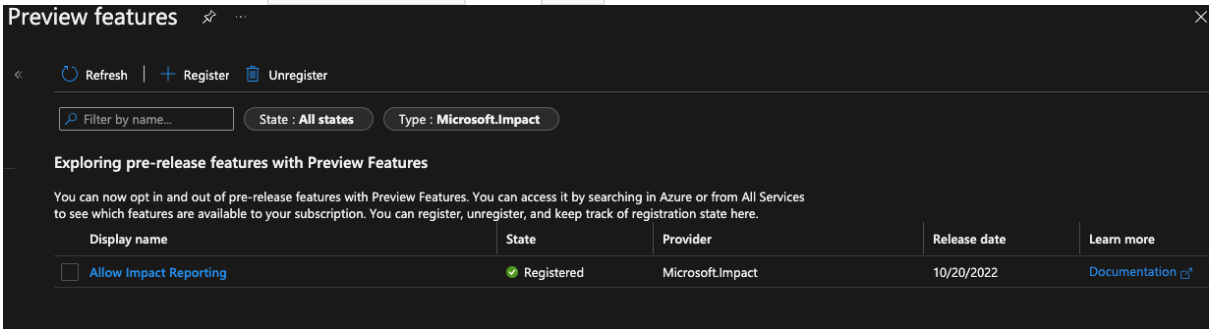
- View Reported Impacts and Insights

Register your Subscription for Impact Reporting Feature

6/19/2024 • 2 minutes to read

Follow the steps below to register your subscription for Impact Reporting.

1. Navigate to your subscription
2. Under the `Settings` tab section, go to `Preview Features`
3. Under this tab, filter for `Microsoft.Impact` in the `type` section



4. Click on `Allow Impact Reporting` feature and register
5. After approval, please go to `Resource providers`, search for `Microsoft.Impact` and register

Once your request is approved, you will have the ability to report Impact to your Azure workloads.

Register your Subscription for Impact Reporting Feature - Script

To onboard multiple subscriptions, please use the following script.

> **WARNING**
> Please note that the following script is offered with no guaranty from Microsoft.

```
#!/bin/bash

# List of your subscription IDs
SUBSCRIPTIONS=("sub_Id", "sub_Id2")

# Resource provider namespace to register, e.g., 'Microsoft.Compute'
PROVIDER_NAMESPACE="Microsoft.Impact"

# Feature name
FEATURE_NAME="AllowImpactReporting"

# AppId/MI id that needs "Impact Reporter" role
APP_ID="app_Id"

# role name that's used to grant access to appId/MI to be able to report impacts
ROLE_NAME="Impact Reporter"

# Loop through each subscription
for SUBSCRIPTION_ID in "${SUBSCRIPTIONS[@]}"
do
    # Select the subscription
    az account set --subscription "$SUBSCRIPTION_ID"

    # register resource provider
    az provider register --namespace "$PROVIDER_NAMESPACE" --wait

    # register preview feature
    az feature register --namespace "$PROVIDER_NAMESPACE" --name "$FEATURE_NAME"

    # Grant the role to the app ID or managed identity
    az role assignment create --assignee "$APP_ID" --role "$ROLE_NAME"

    echo "Registered $PROVIDER_NAMESPACE in $SUBSCRIPTION_ID"
done
```

[HPC] Register your Subscription for Impact Reporting Feature - Script

> **IMPORTANT**
>
> The following script is intended to be used for HPC Guest Health Reporting scenario customers.

> **WARNING**
>
> Please note that the following script is offered with no guaranty from Microsoft.

```
#!/bin/bash

# List of your subscription IDs
SUBSCRIPTIONS=("sub_Id1")

# Resource provider namespace to register, e.g., 'Microsoft.Compute'
PROVIDER_NAMESPACE="Microsoft.Impact"

# Feature name
FEATURE_NAME="AllowImpactReporting"

# HPC Feature name
HPC_FEATURE_NAME="AllowHPCImpactReporting"

# AppId/MI id that needs impact reporter role
APP_ID="app_Id"

# role name that's used to grant access to appId/MI to be able to report impacts
ROLE_NAME="Impact Reporter"

# Loop through each subscription
for SUBSCRIPTION_ID in "${SUBSCRIPTIONS[@]}"
do
    # Select the subscription
    az account set --subscription "$SUBSCRIPTION_ID"

    # register resource provider
    az provider register --namespace "$PROVIDER_NAMESPACE" --wait

    # register preview feature
    az feature register --namespace "$PROVIDER_NAMESPACE" --name "$FEATURE_NAME"

    # register preview feature
    az feature register --namespace "$PROVIDER_NAMESPACE" --name "$HPC_FEATURE_NAME"

    # Grant the role to the app ID or managed identity
    az role assignment create --assignee "$APP_ID" --role "$ROLE_NAME"

    echo "Registered $PROVIDER_NAMESPACE in $SUBSCRIPTION_ID"
done
```

Next steps

- File an impact report

Report Impact

6/19/2024 • 2 minutes to read

You can call our REST API to file an impact report.

> **TIP**
> Since most workloads have monitoring in place to detect failures, we recommend creating an integration through a logic app or Azure Function to file an impact report when your monitoring identifies a problem that you think is caused by the infrastructure.

Report Impact via Azure REST API

Please review our full REST API reference for more examples.

```
{
  "properties": {
    "impactedResourceId":
"/subscriptions/<Subscription_id>/resourcegroups/<rg_name>/providers/Microsoft.Compute/virtualMachines/<vm_n
ame>",
    "startDateTime": "2022-11-03T04:03:46.6517821Z",
    "endDateTime": null, //or a valid timestamp if present
    "impactCategory": "Resource.Availability", //valid impact category needed
    "workload": { "name": "webapp/scenario1" }
  }
}
```

```
az rest --method PUT --url
"https://management.azure.com/subscriptions/<Subscription_id>/providers/Microsoft.Impact/workloadImpacts/<im
pact_name>?api-version=2022-11-01-preview"  --body <body_above>
```

--coming soon: file an impact report via azcli and Azure portal.

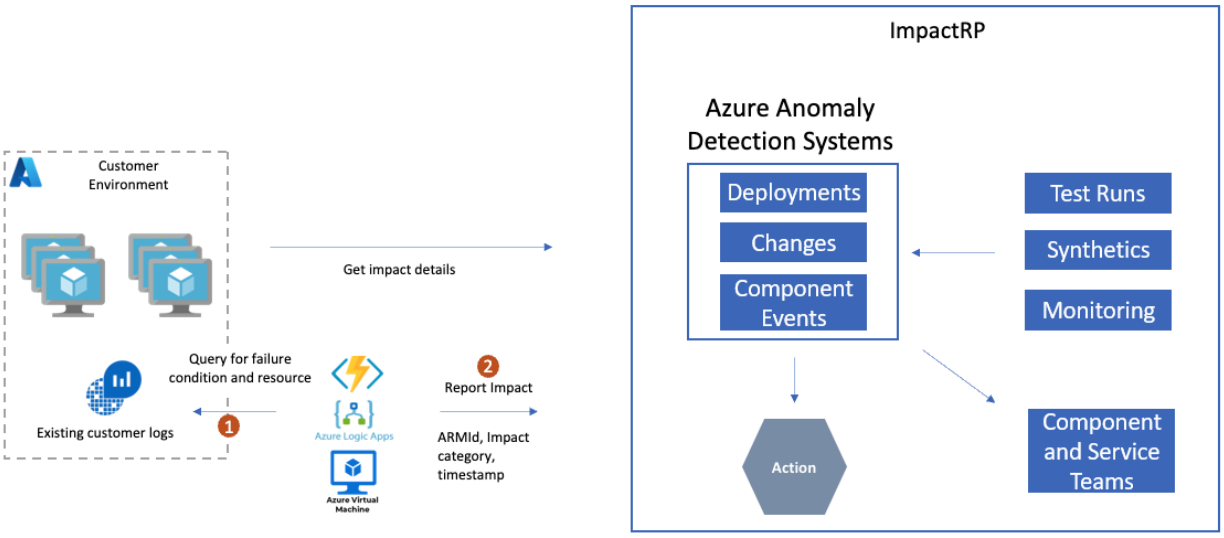
Next steps

- Get allowed impact category list

Quickstart: Onboard to Azure Impact Reporting

6/19/2024 • 2 minutes to read

> **NOTE**
>
> Please visit the API Docs to learn more about available impact management actions.

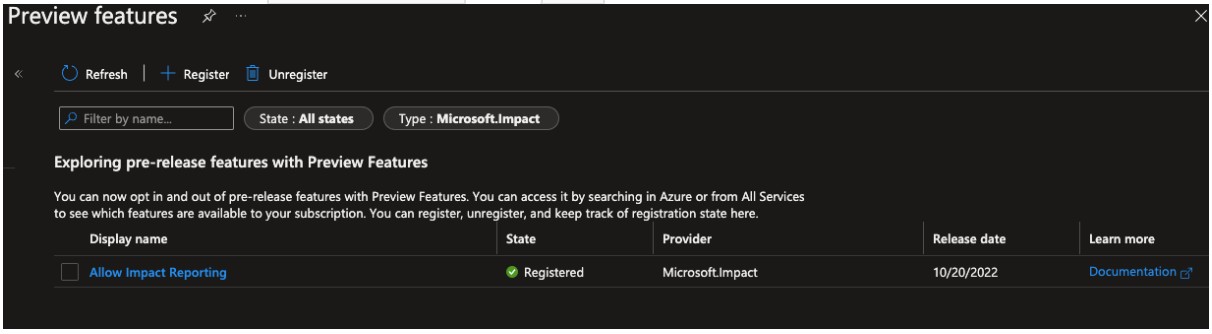


Register your Subscription for Impact Reporting Feature

> **NOTE**
>
> Please remember to also send the subscription list to `impactrp-preview@microsoft.com`.

Follow the steps below to register your subscription for Impact Reporting.

1. Navigate to your subscription
2. Under the `Settings` tab section, go to `Preview Features`
3. Under this tab, filter for `Microsoft.Impact` in the `type` section



4. Click on `Allow Impact Reporting` feature and register
5. After approval, please go to `Resource providers`, search for `Microsoft.Impact` and register

Once your request is approved, you will have the ability to report Impact to your Azure workloads.

Report Using Managed Identity

Grant Required Permissions

The principal reporting impacts needs to have the `Impact Reporter` Azure built-in role at the tenant, subscription, resource group, or resource level. This role provides the following actions:

```
"Microsoft.Impact/WorkloadImpacts/*",
```

Report Using curl or Powershell

Below are some examples on how you may report impact from the cli. Please note that in this case the user reporting impact needs to have the `Impact Reporter` Azure resource role assigned at the right scope.

- Powershell
- cURL

```
# Log in first with Connect-AzAccount if not using Cloud Shell

$azContext = Get-AzContext
$azProfile =
[Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvider]::Instance.Profile
$profileClient = New-Object -TypeName Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient -
ArgumentList ($azProfile)
$token = $profileClient.AcquireAccessToken($azContext.Subscription.TenantId)
$authHeader = @{
    'Content-Type'='application/json'
    'Authorization'='Bearer ' + $token.AccessToken
}
$body = @"
{
  `"properties`": {
    `"impactedResourceId`": `"/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/resource-
rg/providers/Microsoft.Sql/sqlserver/dbservercontext`",
    `"startDateTime`": `"2022-06-15T05:59:46.6517821Z`",
    `"endDateTime`": null,
    `"impactDescription`": `"high cpu utilization`",
    `"impactCategory`": `"Resource.Performance`",
    `"workload`": {
      `"context`": `"webapp/scenario1`",
      `"toolset`": `"Other`"
    },
    `"performance`": [
      {
        `"metricName`": `"CPU`",
        `"actual`": 90,
        `"expected`": 60
      }
    ]
  }
}
"@


# Invoke the REST API
$restUri = 'https://management.azure.com/subscriptions/00000000-0000-0000-0000-
000000000000/providers/Microsoft.Impact/workloadImpacts/<impact_name>?api-version=2023-02-01-preview'
$response = Invoke-RestMethod -Uri $restUri -Method Put -Body $body -Headers $authHeader
```

Payload Examples

- Connectivity

```
PUT https://management.azure.com/subscriptions/00000000-0000-0000-0000-
000000000000/providers/Microsoft.Impact/workloadImpacts/impact-001?api-version=2022-11-01-preview

{
  "properties": {
    "impactedResourceId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/resourceSub/providers/Microsoft.sql/sqlservers/db1",
    "startDateTime": "2022-06-15T05:59:46.6517821Z",
    "endDateTime": null,
    "impactDescription": "conection failure",
    "impactCategory": "Resource.Connectivity",
    "connectivity": {
      "protocol": "TCP",
      "port": 1443,
      "source": {
        "azureResourceId": "/subscriptions/00000000-0000-0000-0000-
000000000000/resourceGroups/resourceSub/providers/Microsoft.compute/virtualmachines/vm1"
      },
      "destination": {
        "uri": "https://www.microsoft.com"
      }
    },
    "workload": {
      "context": "webapp/scenario1",
      "toolset": "Other"
    }
  }
}
```

Performance

```
PUT https://management.azure.com/subscriptions/00000000-0000-0000-0000-
000000000000/providers/Microsoft.Impact/workloadImpacts/impact-002?api-version=2022-11-01-preview

{
  "properties": {
    "impactedResourceId": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/resource-
rg/providers/Microsoft.Sql/sqlserver/dbservercontext",
    "startDateTime": "2022-06-15T05:59:46.6517821Z",
    "endDateTime": null,
    "impactDescription": "high cpu utilization",
    "impactCategory": "Resource.Performance",
    "workload": {
      "context": "webapp/scenario1",
      "toolset": "Other"
    },
    "performance": [
      {
        "metricName": "CPU",
        "actual": 90,
        "expected": 60
      }
    ]
  }
}
```

Next steps

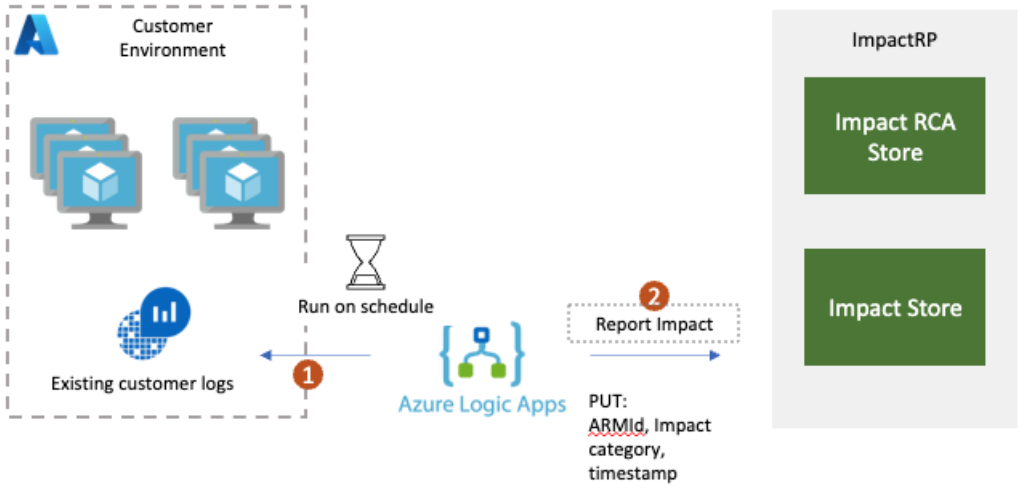
File an impact report

Report Impacts Using a Logic App

6/19/2024 • 3 minutes to read

NOTE

Please visit the API Docs to learn more about available impact management actions.



Prerequisites

Please first see Onboarding for steps on enabling private preview API access for your subscription.

A managed identity with PUT access to the ImpactRP API and read access to the data source for the workload is required. Additionally, a query with a 1 minute or greater polling interval for the data source to generate the following fields is needed:

- ImpactName
- ImpactStartTime
- ImpactedResourceId
- WorkloadContext
- ImpactCategory

This guide will use a Kusto cluster as an example data source with the following query:

```
ExampleTable
| where Status =~ "BAD" and ingestion_time() > ago(1m)
| distinct  ImpactStartTime=TimeStamp, ImpactedResourceId=ResourceId, WorkloadContext=Feature,
ImpactCategory="Resource.Availability", ImpactName = hash_sha1(strcat(TimeStamp, ResourceId , Feature,
Computer, ingestion_time()))
```

> **NOTE**
>
> Please replace the above query with a query to a datastore or source that is supported by Logic Apps that returns the same columns. If all of these columns are not readily available, additional steps must be added to the workflow to generate the missing fields.

Steps

1. Create a new Logic Apps in Azure Portal with the following settings:
   - Publish: Workflow
   - Region: Central US
   - Plan: Standard
2. (Optional) Under the "Monitoring" section, set "Enable Application Insights" to "Yes". This will allow for failure monitoring. Additional steps will be at the bottom of this document.
3. Review and Create the Logic App. Once created, open the Logic App and navigate to "Settings" -> "Identity" in the side pane. In the "User assigned" section, click "Add" and select the managed identity created in the prerequisites. Click "Save" to save the changes.
4. Navigate to "Workflows" -> "Connections" and click on the "JSON View" tab. Create a connection for your data source. The following is an example for Kusto with managed identity, but any data source supported by Logic Apps can be used:

```
{
    "managedApiConnections": {
        "kusto": {
            "api": {
                "id":
"/subscriptions/<subscription_id>/providers/Microsoft.Web/locations/<region>/managedApis/kusto"
            },
            "authentication": {
                "type": "ManagedServiceIdentity"
            },
            "connection": {
                "id":
"/subscriptions/<subscription_id>/resourceGroups/<rg_name/providers/Microsoft.Web/connections/<connec
tion_name>"
            },
            "connectionProperties": {
                "authentication": {
                    "audience": "https://kusto.kustomfa.windows.net",
                    "identity":
"/subscriptions/<subscription_id>/resourcegroups/<rg_name>/providers/Microsoft.ManagedIdentity/userAs
signedIdentities/<managed_identity_name>",
                    "type": "ManagedServiceIdentity"
                }
            },
            "connectionRuntimeUrl": "<kusto_connection_runtime_url>"
        }
    }
}
```

   Click "Save" to save the changes.
5. Navigate to "Workflows" -> "Workflows". Click "Add" and create and new blank workflow with "State Type" set as "Stateful".
6. Click on the newly created workflow. Navigate to to "Developer" -> "Code" and replace the contents of

the JSON with the following:

```
{
    "definition": {
        "$schema": "https://schema.management.azure.com/providers/Microsoft.Logic/schemas/2016-06-
01/workflowdefinition.json#",
        "actions": {
            "For_each": {
                "actions": {
                    "HTTP": {
                        "inputs": {
                            "authentication": {
                                "identity":
"/subscriptions/<subscription_id>/resourcegroups/<rg_name>/providers/Microsoft.ManagedIdentity/userAs
signedIdentities/<managed_identity_name>",,
                                "type": "ManagedServiceIdentity"
                            },
                            "body": {
                                "properties": {
                                    "endDateTime": null,
                                    "impactCategory": "@{items('For_each')?['ImpactCategory']}",
                                    "impactedResourceId": "@{items('For_each')?
['ImpactedResourceId']}",
                                    "startDateTime": "@{items('For_each')?['ImpactStartTime']}",
                                    "workload": {
                                        "context": "@{items('For_each')?['WorkloadContext']}"
                                    }
                                }
                            },
                            "method": "PUT",
                            "retryPolicy": {
                                "count": 5,
                                "interval": "PT30M",
                                "maximumInterval": "PT24H",
                                "minimumInterval": "PT30M",
                                "type": "exponential"
                            },
                            "uri": "@{concat('https://management.azure.com/subscriptions/',
split(item().ImpactedResourceId, '/')[2], '/providers/Microsoft.Impact/workloadImpacts/',
item().ImpactName, '?api-version=2022-11-01-preview')}"
                        },
                        "runAfter": {},
                        "type": "Http"
                    }
                },
                "foreach": "@body('Run_KQL_query')?['value']",
                "runAfter": {
                    "Run_KQL_query": [
                        "Succeeded"
                    ]
                },
                "type": "Foreach"
            },
            "Run_KQL_query": {
                "inputs": {
                    "body": {
                        "cluster": "https://examplecluster.eastus.kusto.windows.net/",
                        "csl": "ExampleTable\n|where Status =~ \"BAD\" and
ingestion_time()>ago(1m)\n|distinct  ImpactStartTime=TimeStamp, ImpactedResourceId=ResourceId,
WorkloadContext=Feature, ImpactCategory=\"Resource.Availability\", ImpactName =
hash_sha1(strcat(TimeStamp, ResourceId , Feature, Computer, ingestion_time()))",
                        "db": "exampledb"
                    },
                    "host": {
                        "connection": {
                            "referenceName": "kusto"
                        }
                    },
```

```
                    "method": "post",
                    "path": "/ListKustoResults/false"
                },
                "runAfter": {},
                "type": "ApiConnection"
            }
        },
        "contentVersion": "1.0.0.0",
        "outputs": {},
        "triggers": {
            "Recurrence": {
                "recurrence": {
                    "frequency": "Minute",
                    "interval": 1
                },
                "type": "Recurrence"
            }
        }
    },
    "kind": "Stateful"
}
```

Click "Save" to save the changes.

7. Navigate to "Developer" -> "Designer". Click on the "Run KQL Query" block. Replace "Cluster URL" and "Database" with the target Kusto cluster and database. Replace the "Query" with the query from the prerequisites. Next, click on the blue "Change connection" link underneath the query textbox. Set "Authentication" to Managed Identity and set "Managed identity" to the managed identity created in the prerequisites with an appropriate "Connection Name" and click "Create".

   > **NOTE**
   > If using a source other than Kusto, replace the "Run KQL Query" block with the appropriate block for your data source. The "For Each" block will need to be updated to iterate over the results of the query and the "HTTP" block will need to be updated to use the appropriate data from the query results.

8. (Optional) If the polling interval for the query is greater than 1 minute, click on the "Recurrence" block and set the "Interval" to the polling interval in minutes.
9. Click on the "HTTP" block and update the "Authentication" to the managed identity created in the prerequisites. Click "Save" to save the changes.
10. Navigate to "Overview" and click "Run" to test the flow. Results will be displated under "Run History".
11. (Optional) Return to the Logic App screen in Azure Portal. Navigate to "Settings" -> "Application Insights" and click on the hyperlink to the Application Insights resource. Navigate to "Monitoring" -> "Alerts". Click "Create" -> "Alert Rule". From here, you can create an alert rule to notify on failures.

Viewing Impact Reports and Insights in Azure Resource Graph Explorer

6/19/2024 • 2 minutes to read

Permissions needed

You need either the "Impact Reporter" role or read action on `Microsoft.Impact/WorkloadImpact/*` at the right scope (root, subscription, or resource group)

Queries

To run these queries, go to the Azure Portal ARG query blade

Get all Impact reports that have Insights

> This query retrieves all Impact reports with Insights, displaying key details such as the resource ID and impact properties.

```
impactreportresources
|where ['type'] =~ 'microsoft.impact/workloadimpacts'
|extend startDateTime=todatetime(properties["startDateTime"])
|extend impactedResourceId=tolower(properties["impactedResourceId"])
|join kind=inner hint.strategy=shuffle (impactreportresources
|where ['type'] =~ 'microsoft.impact/workloadimpacts/insights'
|extend insightCategory=tostring(properties['category'])
|extend eventId=tostring(properties['eventId'])
|project impactId=tostring(properties["impact"]["impactId"]), insightProperties=properties, insightId=id) on
$left.id == $right.impactId
|project impactedResourceId, impactId, insightId, insightProperties, impactProperties=properties
```

For a resource URI, Find all reported Impacts and Insights

> Given a resource Id, this query retrieves Impact reports and Insights that include the specified resource Id.

```
impactreportresources
|where ['type'] =~ 'microsoft.impact/workloadimpacts'
|extend startDateTime=todatetime(properties["startDateTime"])
|extend impactedResourceId=tolower(properties["impactedResourceId"])
|where impactedResourceId =~ '<***resource_uri***>'
|join kind=leftouter  hint.strategy=shuffle (impactreportresources
|where ['type'] =~ 'microsoft.impact/workloadimpacts/insights'
|extend insightCategory=tostring(properties['category'])
|extend eventId=tostring(properties['eventId'])
|project impactId=tostring(properties["impact"]["impactId"]), insightProperties=properties, insightId=id) on
$left.id == $right.impactId
|project impactedResourceId, impactId=id, insightId, insightProperties, impactProperties=properties
|order by insightId desc
```

Next steps

- Get allowed Impact category list

Impact Categories

6/19/2024 • 2 minutes to read

> **NOTE**
> All Azure resource types are currently supported for impact reporting.

Please review our full list of categories in our REST API reference.

Category list

CATEGORY NAME	PROBLEM DESCRIPTION
ARMOperation.CreateOrUpdate	Use this to report problems related to creating a new azure virtual machines such as provisioning or allocation failures
ARMOperation.Delete	Use this to report failures in deleting a resource.
ARMOperation.Get	Use this to report failures in querying resource metadata.
ARMOperation.Start	Use this to report failures in starting a resource.
ARMOperation.Stop	Use this to report failures in stopping a resource.
ARMOperation.Other	Use this to report Control Plane operation failures that don't fall into other ARMOperation categories.
Resource.Performance	Use this to report general performance issues. For example, as high usage of CPU, IOPs, disk space, or memory
Resource.Performance.Network	Use this to report performance issues which are networking related. For example, degraded network throughput.
Resource.Performance.Disk	Use this to report performance issues which are disk related. For example, degraded IOPs
Resource.Performance.CPU	Use this to report performance issues which are CPU related.
Resource.Performance.Other	Use this to report issues that don't fall under other Resource.Performance sub-categories.
Resource.Connectivity	Use this to report general connectivity issues to or from a resource.
Resource.Connectivity.Inbound	Use this to report inbound connectivity issues to a resource.
Resource.Connectivity.Outbound	Use this to report outbound connectivity issues from a resource.

CATEGORY NAME	PROBLEM DESCRIPTION
Resource.Connectivity.Other	Use this to report issues that don't fall into under other Resource.Connectivity sub-categories
Resource.Availability	Use this to report general unavailability issues
Resource.Availability.Restart	Use this to report if an unexpected virtual machine restarts
Resource.Availability.Boot	Use this to report virtual machines which are in a non-bootable state, not booting at all or is on a reboot loop
Resource.Availability.Disk	Use this to report availability issues related to disk
Resource.Availability.UnResponsive	Use this to report a resource that is not responsive now or for a period of time in the past
Resource.Availability.Storage	Use this to report availability issues related to storage.
Resource.Availability.Network	Use this to report network availability issues.
Resource.Availability.DNS	Use this to report DNS availability issues.
Resource.Availability.Other	Use this to report issues that don't fall into under other Resource.Availability sub-categories

Next steps

View previously filed impact reports

Azure impact Reporting FAQ

6/19/2024 • 2 minutes to read

Is this a replacement for opening a support ticket?

No. Azure Impact Reporting is simply another tool that enables you to inform Microsoft that something may be wrong. In addition to being analyzed by different service teams, your impact reports are correlated with ongoing deployments to determine what action should be taken.

What do I get as response to filing an Impact report?

Every Impact report is ingested by our internal correlation tools to help Microsoft provide you with better services and ease your pain. When there's a correlation, this will be indicated in the impact report.

Who do I reach out to if I need to learn more about a previously filed Impact report?

Please email `impactrp-preview@microsoft.com`

What Azure resource types are enabled for Impact reporting?

All Azure resource types are enabled for impact reporting.

Next steps

- File an impact report