Procedure to Forward Azure Activity Logs to Datadog

Overview

Platform:	Azure
Owner of this SOP:	Fully Managed POD A
Cloud Services:	Azure Logs and Datadog

Problem

When requesters are asking to Azure collect activity/resource logs .

tester	Reviewer
@ Suresh Potlapalli (Deactivated)	

Solution

Raise a Normal Change Request

Please open a Normal SNOW request and get it approved before collecting activity logs and resource, And respective stake holders and application owners should be informed prior to this activity as new resources are required.

Note:

- The Event Hub must be in the same Location as the resource you want to submit logs from. For activity logs or other account-wide log sources, you can choose any region.

Summary

- This document explains how to forward Azure activity/resource logs to Datadog monitoring using Azure Event hub.
- The best method for submitting logs from Azure to Datadog is with the Agent or Daemon Set.
- For some resources it may not be possible. In these cases, Datadog recommends **creating a log forwarding pipeline using an Azure Event Hub** to collect Azure platform logs.

Prechecks:

- Datadog API key to integrate with Azure.
- Access to create the resources in Azure subscription.

General process:

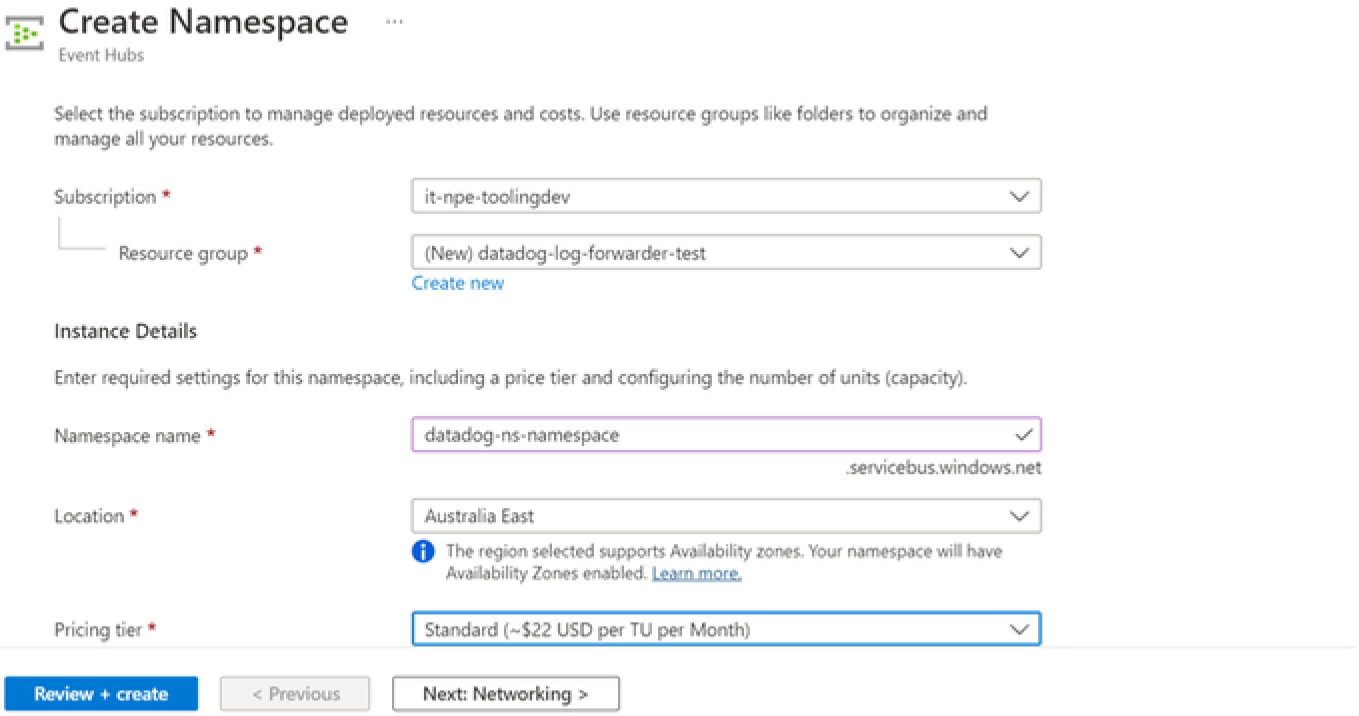
- Create an Azure Event Hub.
- Setup the Datadog-Azure function with an Event hub trigger to forward logs to Datadog.
- Configure your Azure services to stream logs to the Event Hub by creating a diagnostic setting.

Steps to follow:

- The instructions below walk through a basic, initial setup using the Azure Portal.
- All of these steps can be also performed with the **Terraform Components**, CLI, or PowerShell

Create Event Hub Namespace:

- In the Azure portal, navigate to the Event Hubs overview and click create
- Enter the name, pricing tier, subscription, and resource group and location details



Create Namespace

Event Hubs

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * it-npe-toolingdev

Resource group * (New) datadog-log-forwarder-test

Create new

Instance Details

Enter required settings for this namespace, including a price tier and configuring the number of units (capacity).

Namespace name * datadog-ns-namespace

.servicebus.windows.net

Location * Australia East

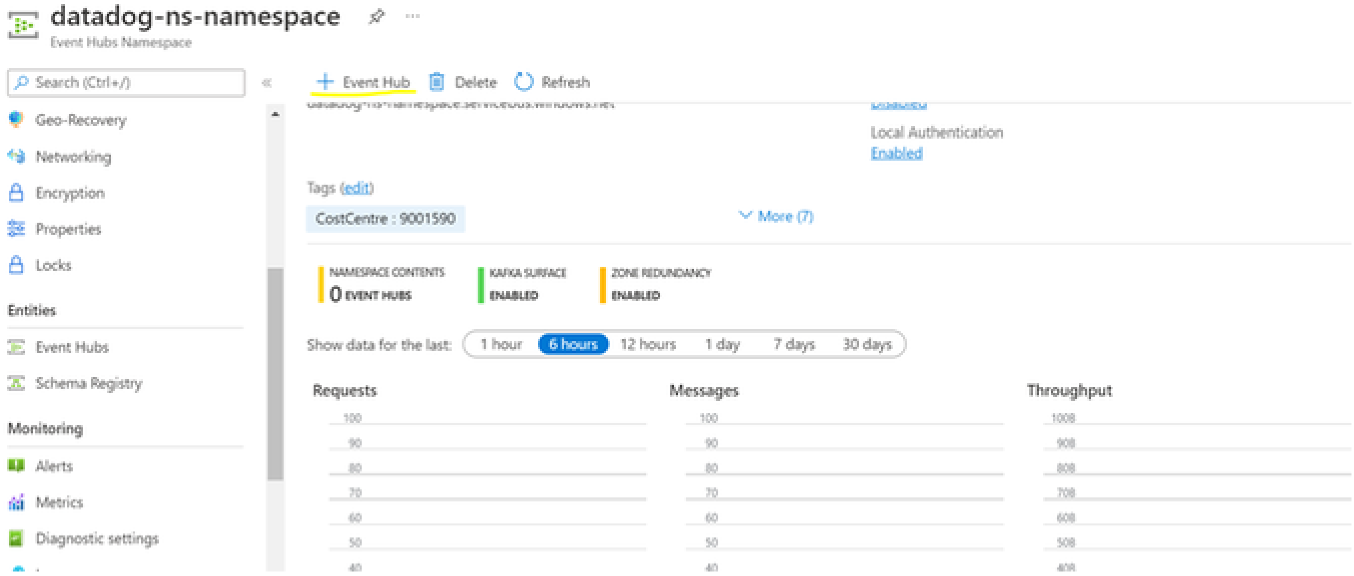
The region selected supports Availability zones. Your namespace will have Availability Zones enabled. Learn more.

Pricing tier * Standard (~$22 USD per TU per Month)

- Select your desired options for throughput units, pricing and networking. Click **Create**

Add Event hub to the Event Hub namespace:

- In the Azure portal, navigate event hub namespace. Click + Event Hub
- Select your desired options for name, partition-count, and message-retention. Click Create



datadog-ns-namespace

Event Hubs Namespace

Local Authentication Enabled

Tags (edit)

CostCentre : 9001590

NAMESPACE CONTENTS 0 EVENT HUBS

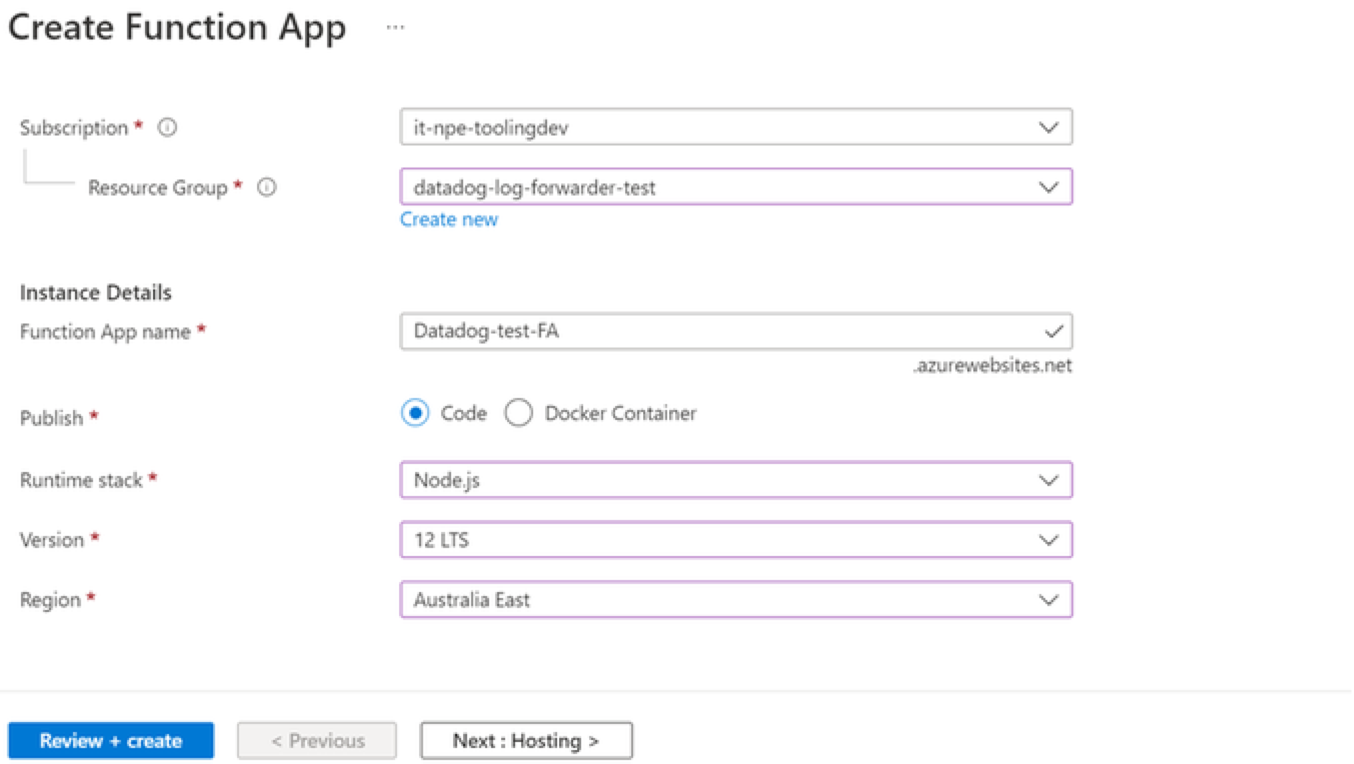
KAFKA SURFACE ENABLED

ZONE REDUNDANCY ENABLED

Show data for the last: 1 hour 6 hours 12 hours 1 day 7 days 30 days

Create Azure Function App:

- In the Azure portal, navigate to Function Apps and click Create.
- Select a subscription, resource group, region, and enter a name for your function.
- Select Publish to Code, Runtime stack to Node.js, and Version to 12 LTS.
- Click Next :hosting Select a storage account, operating system, and plan type
- Click Next: networking select your desired options
- Review and create the new function app



Create Function App ...

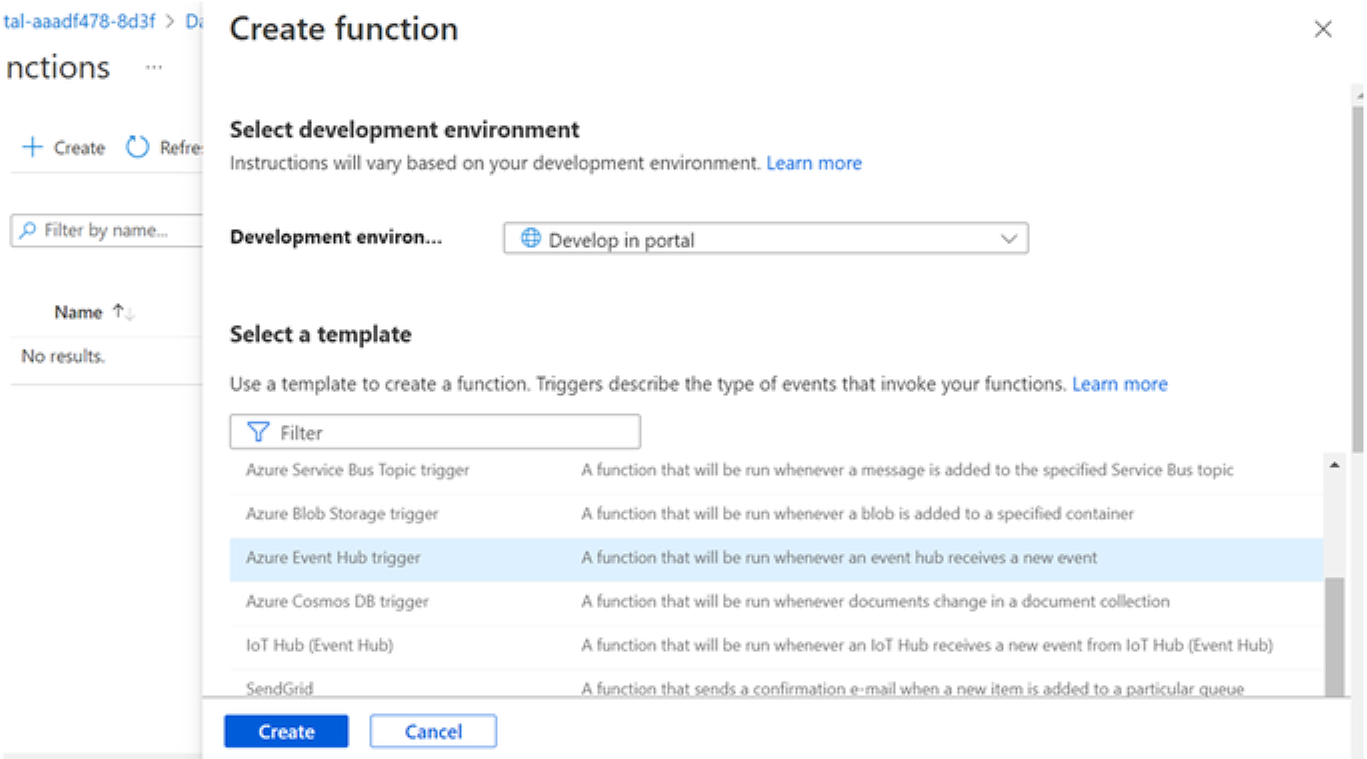
Subscription *	it-npe-toolingdev
Resource Group *	datadog-log-forwarder-test Create new

Instance Details

Function App name *	Datadog-test-FA ✓ .azurewebsites.net
Publish *	● Code ○ Docker Container
Runtime stack *	Node.js
Version *	12 LTS
Region *	Australia East

Add Function to Azure Function App:

- In the Azure portal, navigate to function app
- Select Functions from the functions menu and click Add.
- Select Azure Event Hub trigger from the templates menu and click New.
- Select Event hub namespace and Event Hub for Event Hub connection and click OK.
- Click Create Function



Create function

Select development environment

Instructions will vary based on your development environment. Learn more

Development environ... Develop in portal

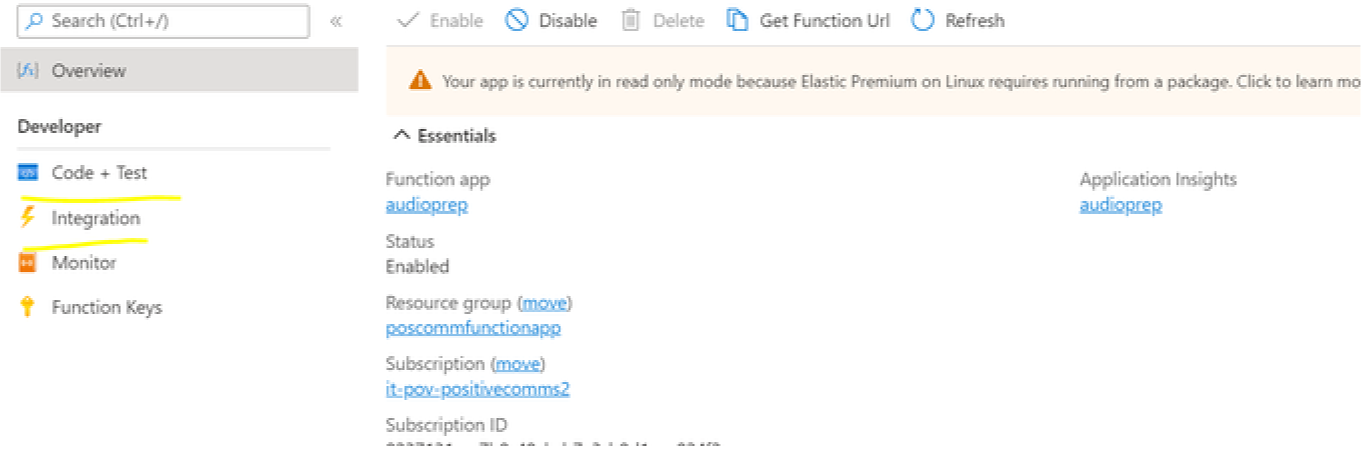
Select a template

Use a template to create a function. Triggers describe the type of events that invoke your functions. Learn more

Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue

Point Event Hub trigger to Datadog:

- Select Event Hub trigger from the functions view.
- Click on Code + Test under the developer side menu.
- Add the Datadog-Azure Function code to your index.js file.
- Add DD API key by creating a DD_API_KEY environment variable under the configuration tab of function app or copy it into the function code by replacing <DATADOG_API_KEY> on line 22.



Your app is currently in read only mode because Elastic Premium on Linux requires running from a package. Click to learn mo

Function app
audioprep

Application Insights
audioprep

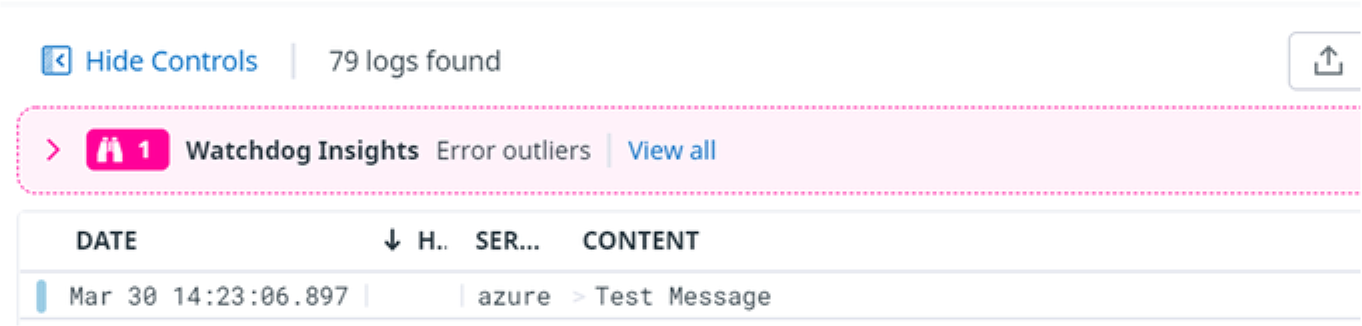
Status
Enabled

Resource group (move)
poscommfunctionapp

Subscription (move)
it-pov-positivecomms2

Subscription ID

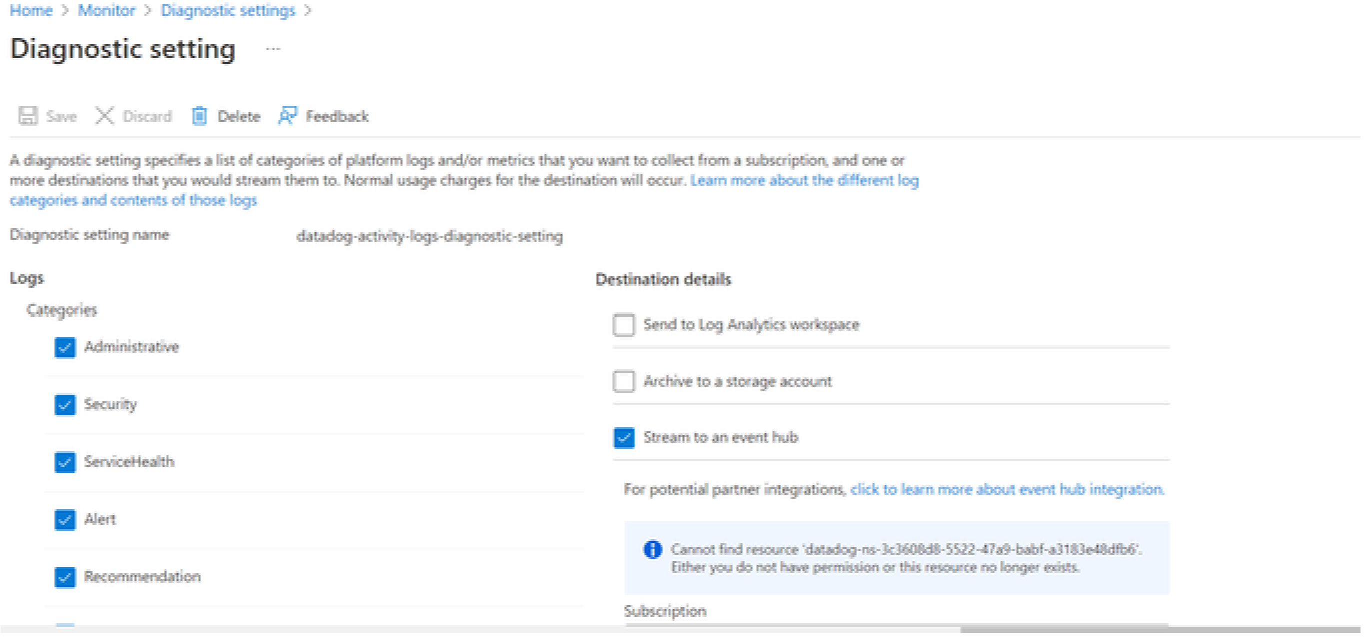
- Click on Integration then Azure Event Hubs under trigger and check the following settings: a. Event Parameter Name is set to event Hub Messages. b. Event Hub Cardinality is set to Many. c. Event Hub Data Type is left empty.
- Click Save.
- Verify your setup is correct by running the function and then checking the Datadog log explorer for the test message.



```
DATE                    H..  SER...  CONTENT
Mar 30 14:23:06.897          azure   Test Message
```

Activity Logs:

- In the Azure portal, navigate to the Activity Log.
- Click on Diagnostic Settings.
- Click Add diagnostic setting.
- Under category details, select the categories of logs want to send to Datadog.
- Under destination details, select Stream to an event hub.
- Set the Event Hub namespace and name.
- Set the shared access key. This key should be configured with send or manage access.
- Click Save.
- Verify your setup is correct by checking the Datadog log explorer for logs from this resource.



Diagnostic setting ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a subscription, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name datadog-activity-logs-diagnostic-setting

Logs

Categories

- ☑ Administrative
- ☑ Security
- ☑ ServiceHealth
- ☑ Alert
- ☑ Recommendation

Destination details

- ☐ Send to Log Analytics workspace
- ☐ Archive to a storage account
- ☑ Stream to an event hub

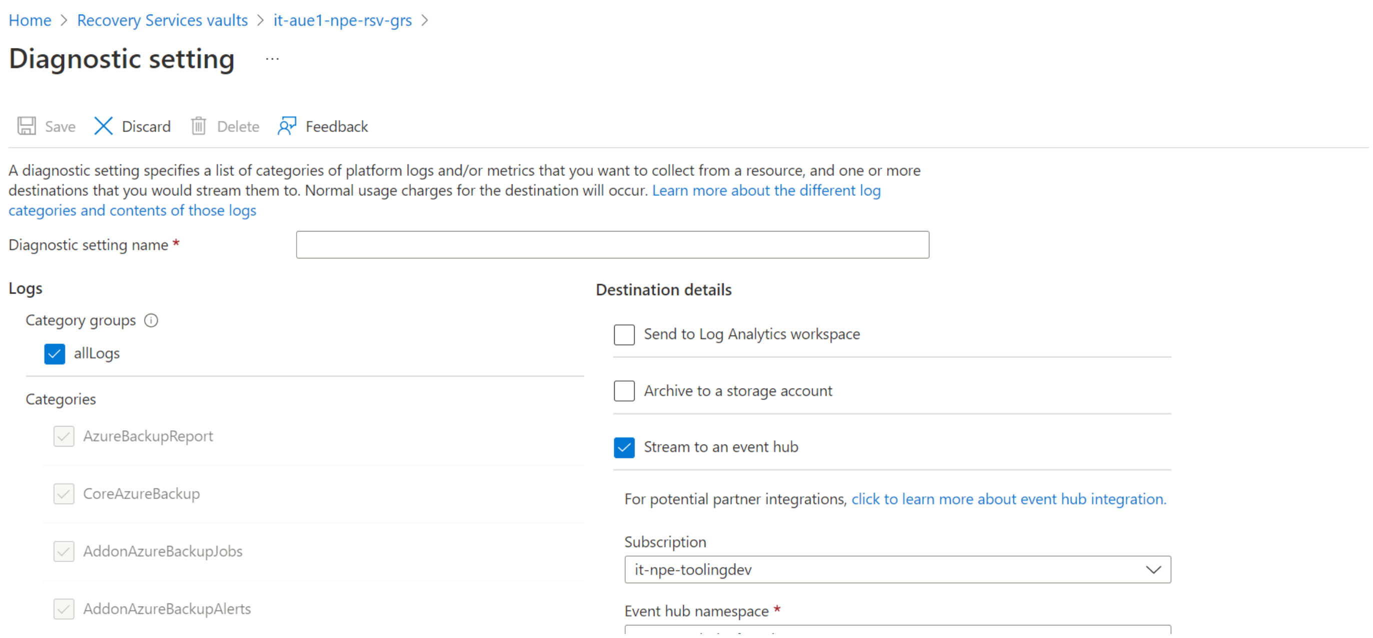
For potential partner integrations, click to learn more about event hub integration.

Cannot find resource 'datadog-ns-3c3608d8-5522-47a9-babf-a3183e48dfb6'. Either you do not have permission or this resource no longer exists.

Subscription

Resource Logs:

- In the Azure portal, navigate to the resource of the logs you want to send to Datadog.
- Under the monitoring section of the resource blade, click Diagnostic settings.
- Click Add diagnostic setting.
- Under category details, select the categories of logs you want to send to Datadog.
- Under destination details, select Stream to an event hub.
- Set the Event Hub namespace and name. These should match the Event Hub namespace and name that you used to create your Event Hub trigger.
- Set the shared access key. This key should be configured with send or manage access.
- Click Save.
- Verify your setup is correct by checking the Datadog log explorer for logs from this resource



Home > Recovery Services vaults > it-aue1-npe-rsv-grs >

Diagnostic setting ...

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name *

Logs

Category groups ⓘ

☑ allLogs

Categories

☑ AzureBackupReport

☑ CoreAzureBackup

☑ AddonAzureBackupJobs

☑ AddonAzureBackupAlerts

Destination details

□ Send to Log Analytics workspace

□ Archive to a storage account

☑ Stream to an event hub

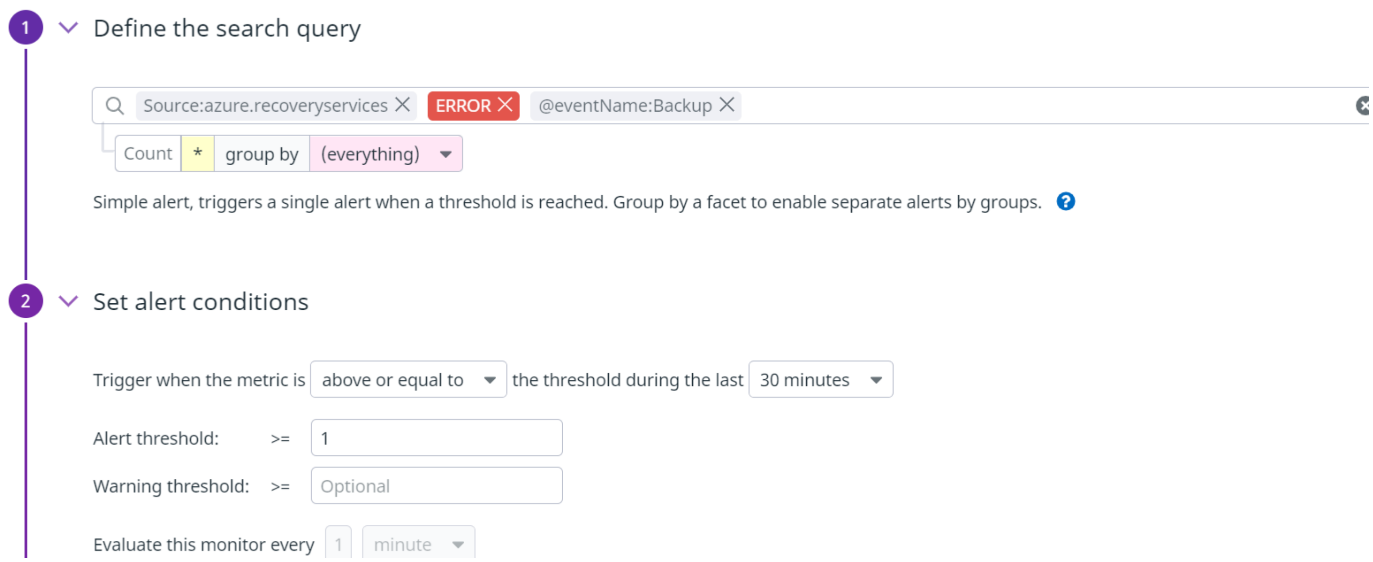
For potential partner integrations, click to learn more about event hub integration.

Subscription: it-npe-toolingdev

Event hub namespace *

Creating DD monitor alerts for AZURE RSV backup failures:

- In the Datadog portal, navigate to the monitor - click new monitor
- Add search query details and conditions and team to notify and message



1 Define the search query

Source:azure.recoveryservices ERROR @eventName:Backup

Count * group by (everything)

Simple alert, triggers a single alert when a threshold is reached. Group by a facet to enable separate alerts by groups.

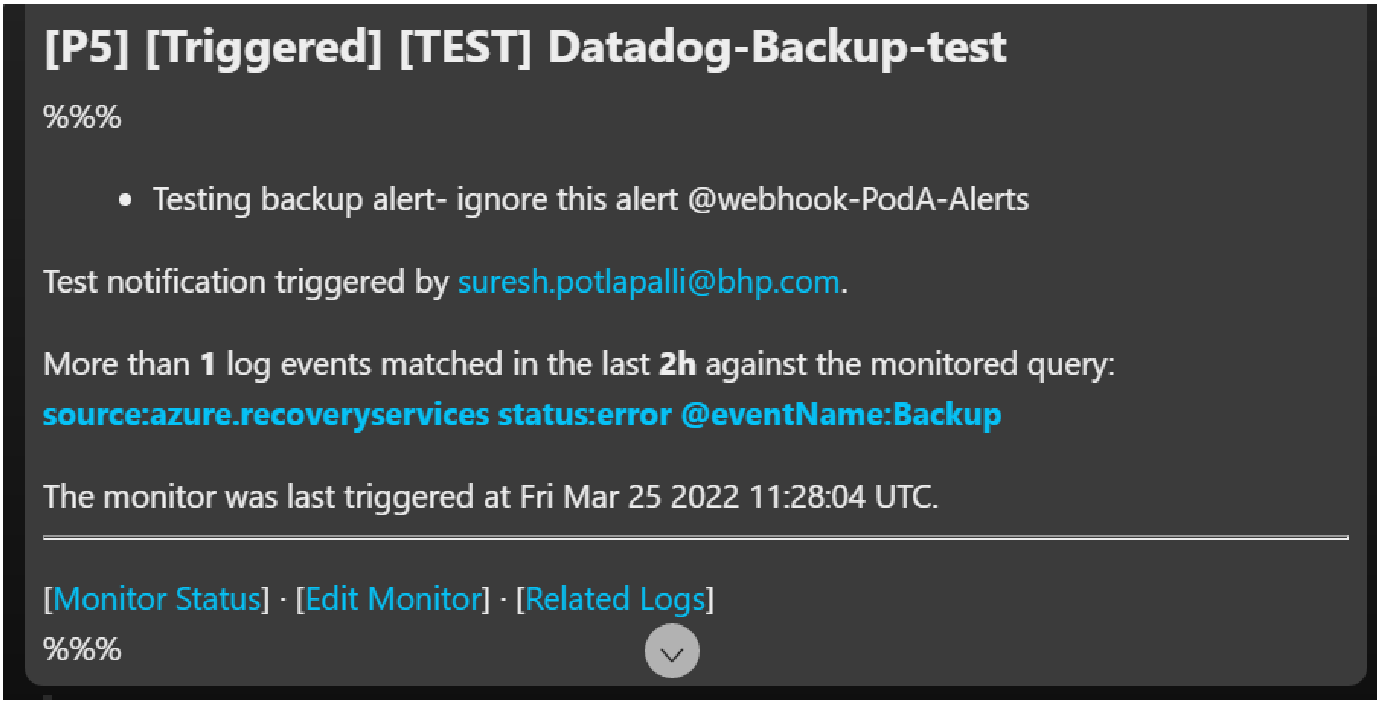
2 Set alert conditions

Trigger when the metric is above or equal to the threshold during the last 30 minutes

Alert threshold: >= 1

Warning threshold: >= Optional

Evaluate this monitor every 1 minute



[P5] [Triggered] [TEST] Datadog-Backup-test

%%%

- Testing backup alert- ignore this alert @webhook-PodA-Alerts

Test notification triggered by suresh.potlapalli@bhp.com.

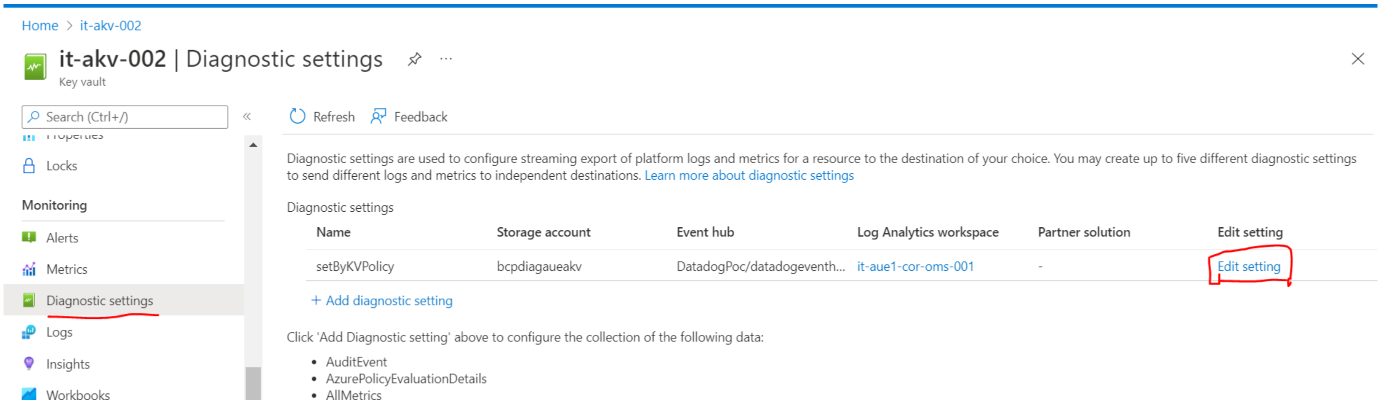
More than **1** log events matched in the last **2h** against the monitored query: **source:azure.recoveryservices status:error @eventName:Backup**

The monitor was last triggered at Fri Mar 25 2022 11:28:04 UTC.

[Monitor Status] · [Edit Monitor] · [Related Logs]

%%%

Azure key vault activity logs to Datadog:



Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

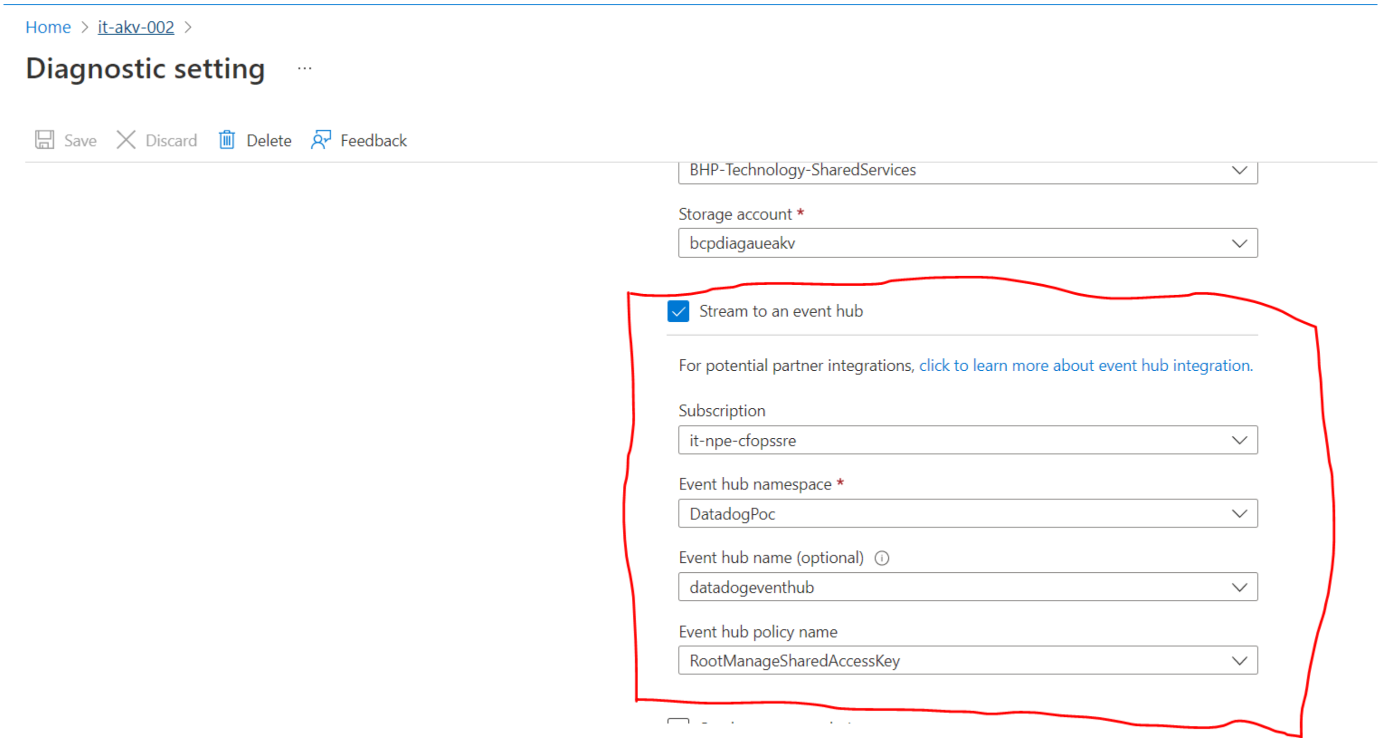
Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
setByKVPolicy	bcpdiagaueakv	DatadogPoc/datadogeventh...	it-aue1-cor-oms-001	-	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AuditEvent
- AzurePolicyEvaluationDetails
- AllMetrics

Select the Event hub which was created in above step



Home > it-akv-002 >

Diagnostic setting ...

BHP-Technology-SharedServices

Storage account *
bcpdiagaueakv

☑ Stream to an event hub

For potential partner integrations, click to learn more about event hub integration.

Subscription
it-npe-cfopssre

Event hub namespace *
DatadogPoc

Event hub name (optional)
datadogeventhub

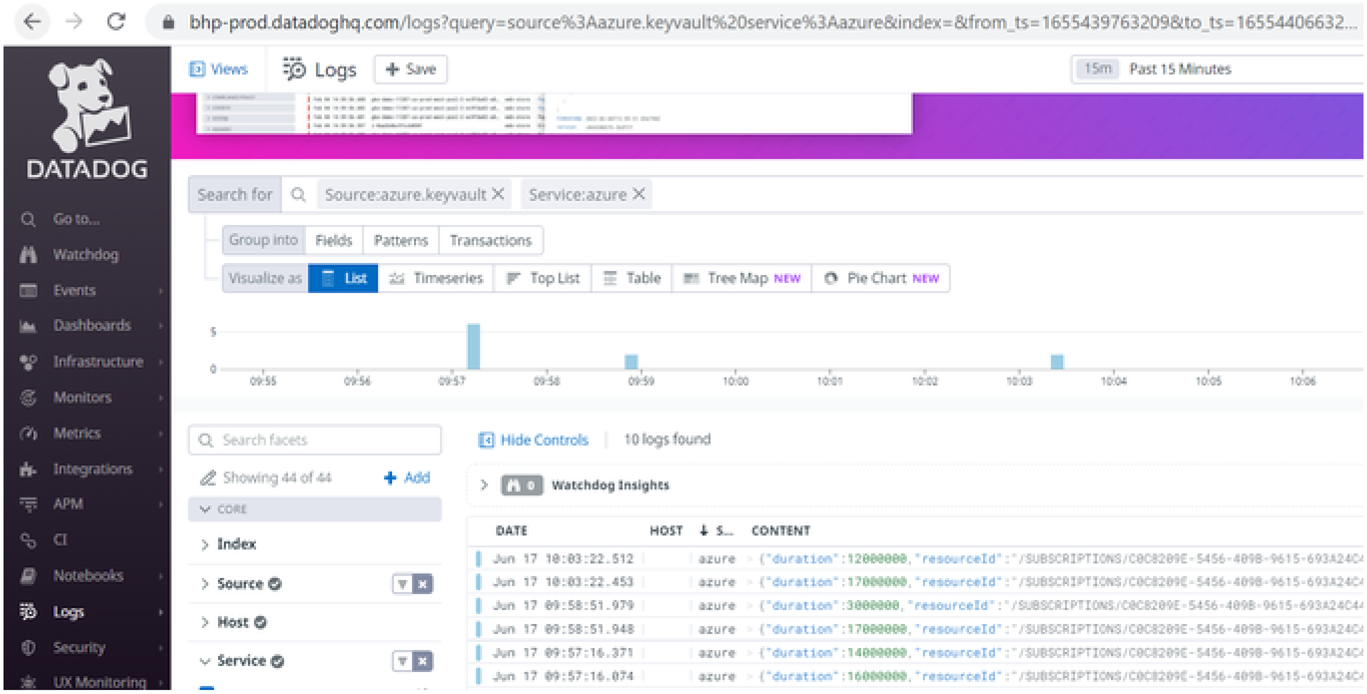
Event hub policy name
RootManageSharedAccessKey

Validate the Keyvault logs in Datadog Console:

search with the below filters under log explorer in Datadog Console

source: Azure.keyvault

service: Azure



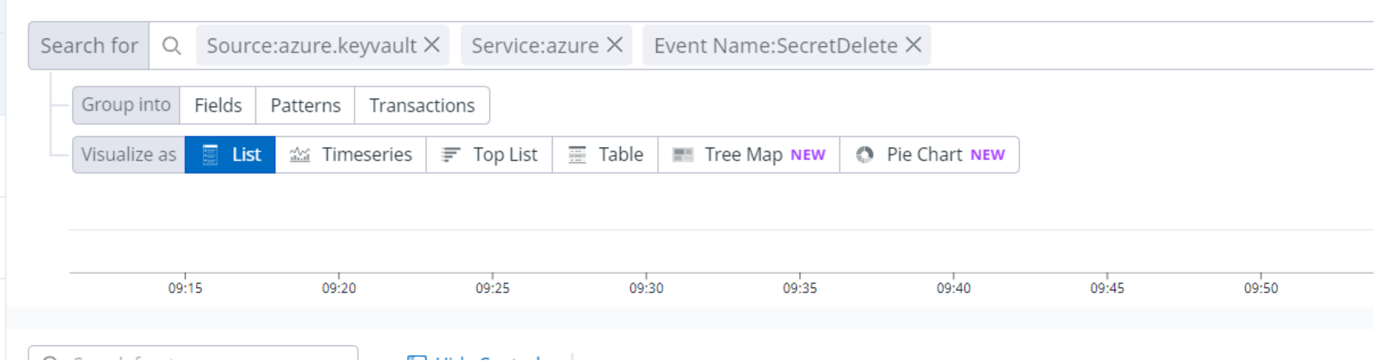
bhp-prod.datadoghq.com/logs?query=source%3Aazure.keyvault%20service%3Aazure&index=&from_ts=1655439763209&to_ts=16554406632...

Search for Source:azure.keyvault Service:azure

10 logs found

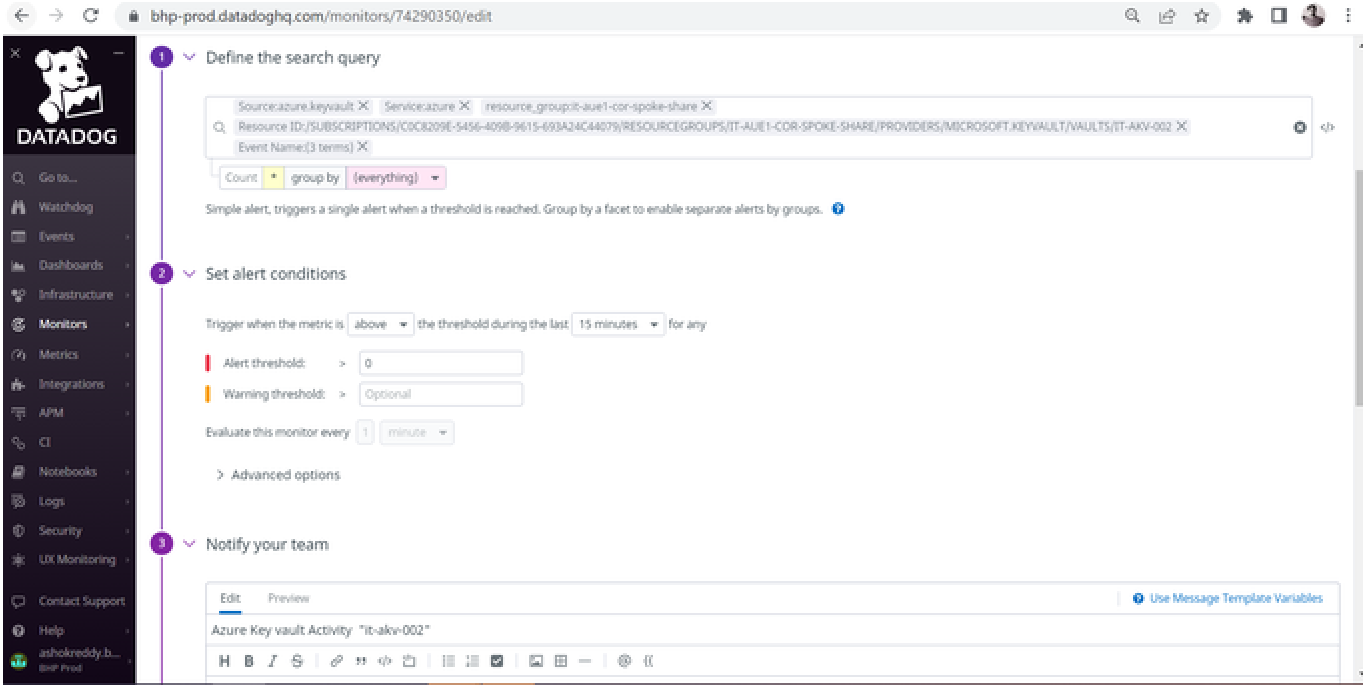
```
DATE                  HOST   S...   CONTENT
Jun 17 10:03:22.512          azure  {"duration":12000000,"resourceId":"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C4
Jun 17 10:03:22.453          azure  {"duration":17000000,"resourceId":"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C4
Jun 17 09:58:51.979          azure  {"duration":3000000,"resourceId":"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C4
Jun 17 09:58:51.948          azure  {"duration":17000000,"resourceId":"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C4
Jun 17 09:57:16.371          azure  {"duration":14000000,"resourceId":"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C4
Jun 17 09:57:16.074          azure  {"duration":16000000,"resourceId":"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C4
```

search query example to track the delete operation on key vault



Search for Source:azure.keyvault Service:azure Event Name:SecretDelete

Monitor Setup for Key vault Activity:



bhp-prod.datadoghq.com/monitors/74290350/edit

1 Define the search query

Source:azure.keyvault Service:azure resource_group:it-aue1-cor-spoke-share Resource ID:/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C44079/RESOURCEGROUPS/IT-AUE1-COR-SPOKE-SHARE/PROVIDERS/MICROSOFT.KEYVAULT/VAULTS/IT-AKV-002 Event Name:(3 terms)

Count * group by (everything)

Simple alert, triggers a single alert when a threshold is reached. Group by a facet to enable separate alerts by groups.

2 Set alert conditions

Trigger when the metric is above the threshold during the last 15 minutes for any

Alert threshold: > 0

Warning threshold: > Optional

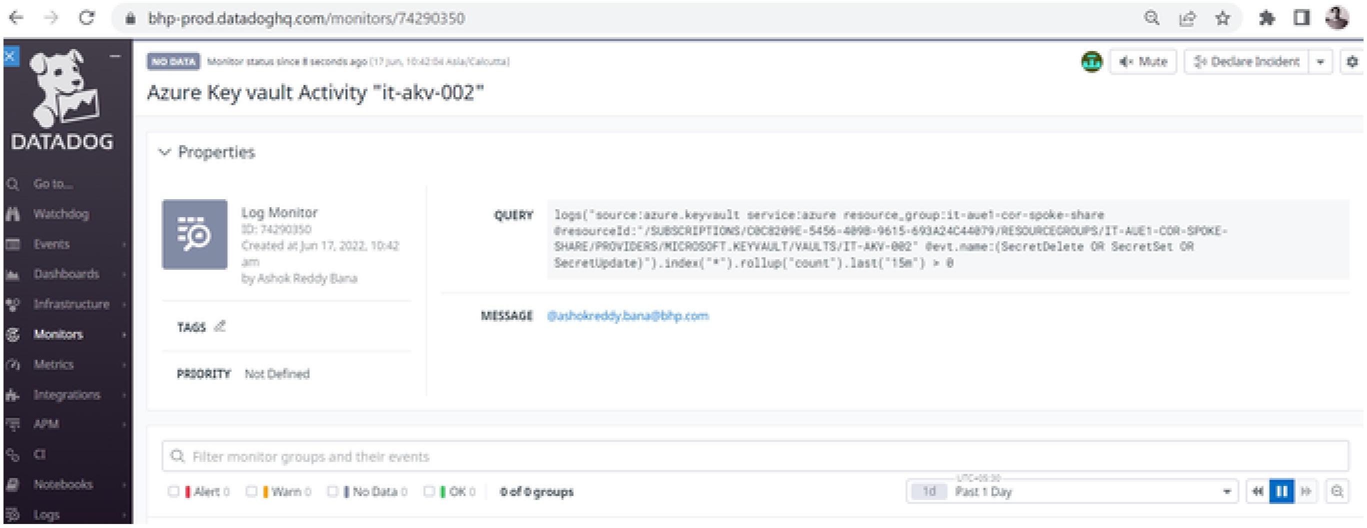
Evaluate this monitor every 1 minute

Advanced options

3 Notify your team

Azure Key vault Activity "it-akv-002"

Search query: `logs("source:azure.keyvault service:azure resource_group:it-aue1-cor-spoke-share @resourceId:"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C44079/RESOURCEGROUPS/IT-AUE1-COR-SPOKE-SHARE/PROVIDERS/MICROSOFT.KEYVAULT/VAULTS/IT-AKV-002" @evt.name:(SecretDelete OR SecretSet OR SecretUpdate)").index("*").rollup("count").last("15m") > 0`



bhp-prod.datadoghq.com/monitors/74290350

NO DATA Monitor status since 8 seconds ago (17 Jun, 10:42:04 Asia/Calcutta)

Azure Key vault Activity "it-akv-002"

Properties

Log Monitor
ID: 74290350
Created at Jun 17, 2022, 10:42 am
by Ashok Reddy Bana

TAGS

PRIORITY Not Defined

QUERY

```
logs("source:azure.keyvault service:azure resource_group:it-aue1-cor-spoke-share
@resourceId:"/SUBSCRIPTIONS/C0C8209E-5456-409B-9615-693A24C44079/RESOURCEGROUPS/IT-AUE1-COR-SPOKE-
SHARE/PROVIDERS/MICROSOFT.KEYVAULT/VAULTS/IT-AKV-002" @evt.name:(SecretDelete OR SecretSet OR
SecretUpdate)").index("*").rollup("count").last("15m") > 0
```

MESSAGE @ashokreddy.bana@bhp.com

Reference Document :

https://docs.datadoghq.com/integrations/azure/?tab=manualinstallation#log-collection ,https://docs.datadoghq.com/logs/explorer/

Cost:

Cost of this solution depends largely on the number of executions for Function App.

TC = Memory Size X Execution Time x Executions/Mo.

https://azure.microsoft.com/en-au/pricing/details/functions/