

Integration of Azure KeyVault Logs to Datadog

- [Overview](#)
- [Problem](#)
- [Summary](#)
- [Solution](#)
- [Purpose](#)

Overview

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

Problem

When requesters ask for Integration of Azure KeyVault Logs to Datadog

Summary

Azure Key Vault is used to safeguard and manage cryptographic keys and secrets used by cloud applications and services. Use the Datadog Azure integration to collect metrics from Azure Key Vault.

Reference Document : Azure KeyVault Overview.

Solution

Purpose

- This document explains how to view/forward Azure KeyValult activity/logs to Datadog monitoring using Azure Event hub.

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:

1. The instructions below walk through a basic, initial setup using the Azure Portal.
2. All of these steps can also be performed with the **Terraform Components**, CLI, or PowerShell.
3. **Create** Event Hub Namespace:
4. In the **Azure portal**, navigate to the Event Hubs overview and click create
5. 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 *

Resource group *

[Create new](#)

Instance Details

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

Namespace name *

.servicebus.windows.net

Location *

i The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more.](#)

Pricing tier *

[Review + create](#)

[< Previous](#)

[Next: Networking >](#)

[Home](#) > [Event Hubs](#) >



Create Namespace

Event Hubs

[Basics](#) [Advanced](#) [Networking](#) [Tags](#) [Review + create](#)

Project Details

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

Subscription *

Resource group *

[Create new](#)

Instance Details

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

Namespace name *

.servicebus.windows.net

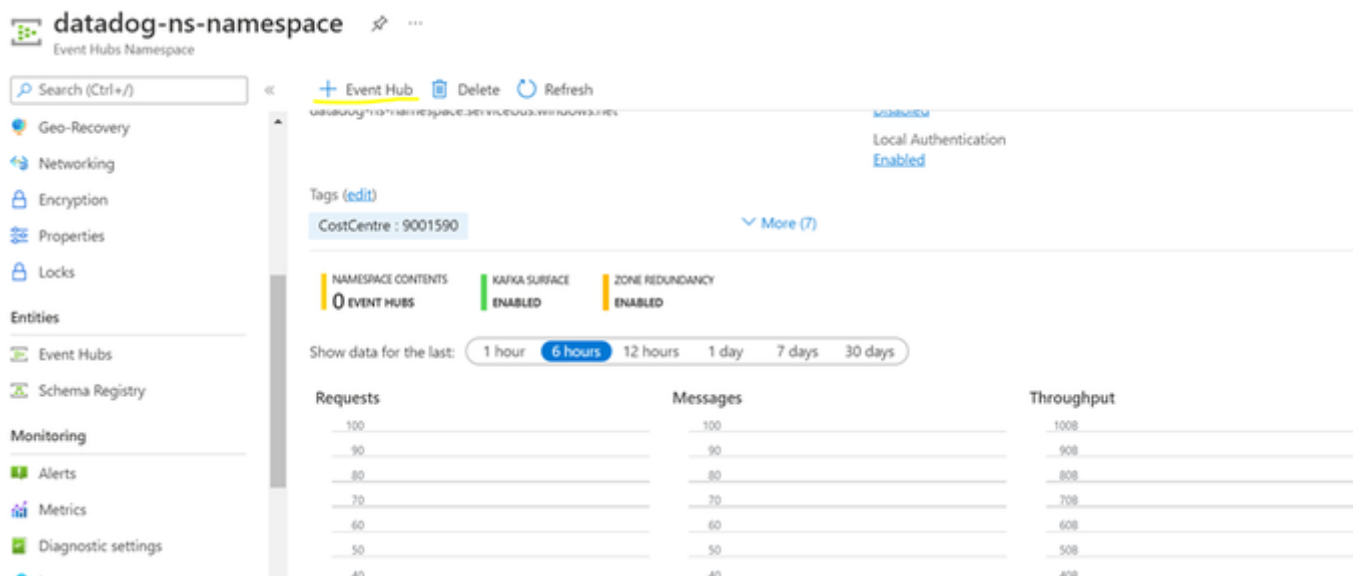
Location *

i The region selected supports Availability zones. Your namespace will have Availability Zones enabled. [Learn more.](#)

Pricing tier *

[Browse the available plans and their features](#)

1. Select your desired options for throughput units, pricing and networking. Click **Create**
2. **Add Event hub** to the Event Hub namespace:
3. In the Azure portal, navigate event hub namespace. Click + Event Hub
4. Select your desired options for name, partition-count, and message-retention. Click Create



Activity Logs:

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

[Home](#) > [Monitor](#) > [Diagnostic settings](#) >

Diagnostic setting

[Save](#) [Discard](#) [Delete](#) [Feedback](#)

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](#).

i 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:

1. In the Azure portal, navigate to the resource of the logs you want to send to Datadog.
2. Under the monitoring section of the resource blade, click Diagnostic settings.
3. Click Add diagnostic setting.
4. Under category details, select the categories of logs you want to send to Datadog.
5. Under destination details, select Stream to an event hub.
6. 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.
7. Set the shared access key. This key should be configured with send or manage access.
8. Click Save.

9. 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](#) >


Dagnostic setting ...

 Save  Discard  Delete  Feedback

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](#)

Dagnostic 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 *

Note:

- Upon successful configuration, you'll start to see your Azure platform logs appear in real time in Datadog's [Log Explorer](#).
- Datadog's log processing pipeline automatically parses metadata from your Azure platform logs and uses it to create log attributes, which you can use as tags to quickly filter, sort, and group your logs by key facets like service, action, user, subscription, and resource group. <Metrics Collected>