# Integrating Azure resource Logs with Splunk

The document provides details on how to integrate Azure Resource logs with Splunk. This integration requires multiple steps such as follows:

* Create a Service principle for the WUIT.
* Create Event hub namespace & Event hub.
* Grant the necessary Event Hub permissions on the Service principle.
* Enable logging on each of the resources that you want to collect logs on.
* Ship the resource logs Event hub.
* Provide the necessary Event hub credentials to WUIT for Splunk integration.

## Step 1: Create a Service Principle

|  |  |
| --- | --- |
| * Open a ServiceNow request with WUIT to create a Service principal. * Follow the link: [WUSTL CSP Portal - WUSTL Portal (service-now.com)](https://wustl.service-now.com/sp?id=wu_csp_index) * Once in ServiceNow, search for **Service account, select** **“New Service Account”** |  |
| * After selecting the **“New Service Account”** option * For “**Request Account Type**” select “**Service Account**” and fill out the form as needed. * After filling out the form, before you checkout, ensure to enter “**CC0002751”** as your cost center number. * **P.S!** In the ticket, please request that they email you the **SecretID, TennantID** & **ClientID** of the Service Principle. |  |

## Step 2: Create Event Hub Namespace n azure

|  |  |
| --- | --- |
| * Log into azure and go to the Event hub Service and create an **Event Hub Namespace**. |  |
| * In the namespace creation window, ensure you select the **subscription** in which your resources are hosted in. * As namespaces are restricted to resources within the same subscription. * After selecting the subscription, fill in the other options as needed. * In the **advanced** window, always select the latest version i.e., **Version 1.2**. |  |
| * In the **networking window**, you can make it publicly or privately accessible. If you select private access, you will have to **create a private endpoint**. |  |
| * After the namespace is created, go to **Entities** -> **Event Hubs**. * Select the **+Event Hub** to create an Event hub. * The log will be shipped to the created event hub. |  |

## Step 3: Grant Service Principal Permissions.

|  |  |
| --- | --- |
| * Go to the created Event hub Namespace, then go to **Access Control (IAM)** * In the add **Role Assignment Window,** select the **“Azure Event Hubs Data Receiver” role and** select the appropriate service principle**.** |  |

## Step 4: Enable logging of Resources & ship logs to Event hub:

|  |  |
| --- | --- |
| * In azure, go to the resource, open the Monitoring **Window, select** **Diagnostic Settings** and select **add** **Diagnostic Settings** |  |
| * In the Diagnostic Setting window, select **Stream to an event hub.** * Next**,** enter the needed values for the **subscription, Event hub namespace, event hub.** * Next select the appropriate logs you would like to send. |  |

## Step 5: Ship logs to Splunk

|  |  |
| --- | --- |
| * Once you successfully ship logs to the appropriate Event hub, you will need to open a ServiceNow Data Onboarding request with WUIT. * Click on the following link to create a request: [Splunk Data Onboarding Request - WUSTL Portal (service-now.com)](https://wustl.service-now.com/sp?id=sc_cat_item&sys_id=2159b76e1b160250e32e11f72a4bcbe4) |  |
| * Once the request has been created you will need to provide the following details to the WUIT Splunk team | The provided info would look like this:  **Event Hub Namespace:** i2db-test000.servicebus.windows.net  **Client ID:** 50test00-test6-4188-944c-  **SecretID:**8GFRST~b9Rftx2CPlt5qu1L1DCFDqZz4J  **TenantID:** 4ccca3b5-71cd-4e6d-974b-4875581967 |