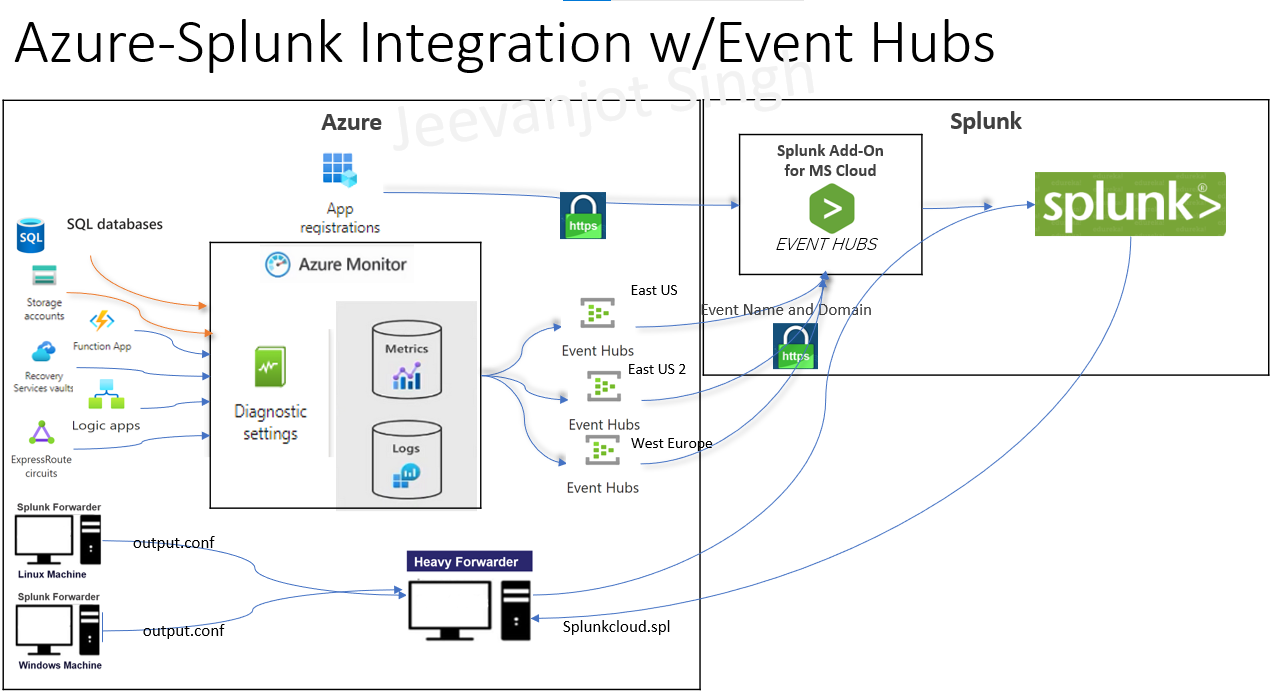
**Azure – Splunk Integration: A Streamlined Monitoring Solution**

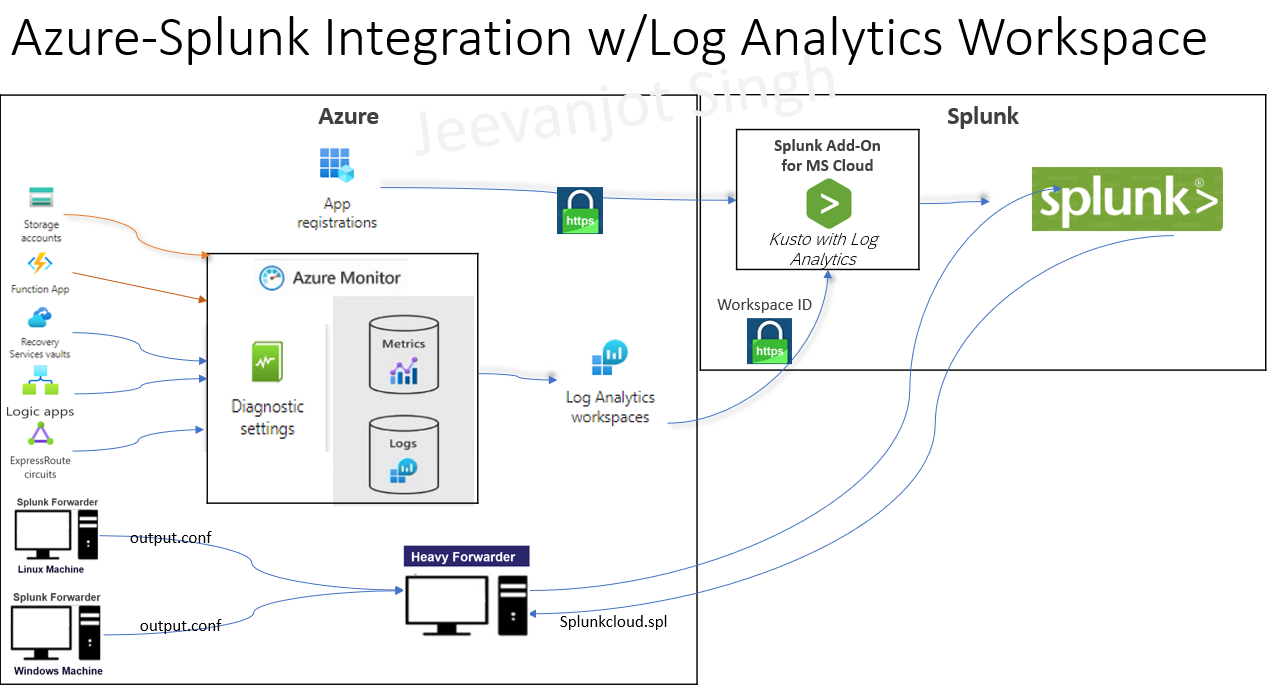
**Use Case:** Integrating Splunk cloud with Azure using Event Hubs/Log Analytics Workspace- a centralized platform to glean valuable insights and optimize your cloud environment.

**Why Splunk over Azure's Native Monitoring?**

Splunk is a powerhouse for real-time data ingestion, transformation, and analysis. Even though Azure offers built-in monitoring tools but Splunk empowers to:

* **Unify Data from Diverse Sources:** Consolidate logs and metrics from your entire Azure infrastructure, including VMs, databases, web apps, and more, into a single, searchable platform.
* **Unlock Hidden Insights:** Splunk's intuitive search and analytics capabilities allow you to unearth valuable trends, identify anomalies, and troubleshoot issues with unprecedented ease.
* **Flexible Data Ingestion:** Splunk seamlessly integrates with a wider range of data sources beyond Azure.
* **Advanced Analytics:** Splunk's powerful search language and visualization tools provide deeper insights into your data.

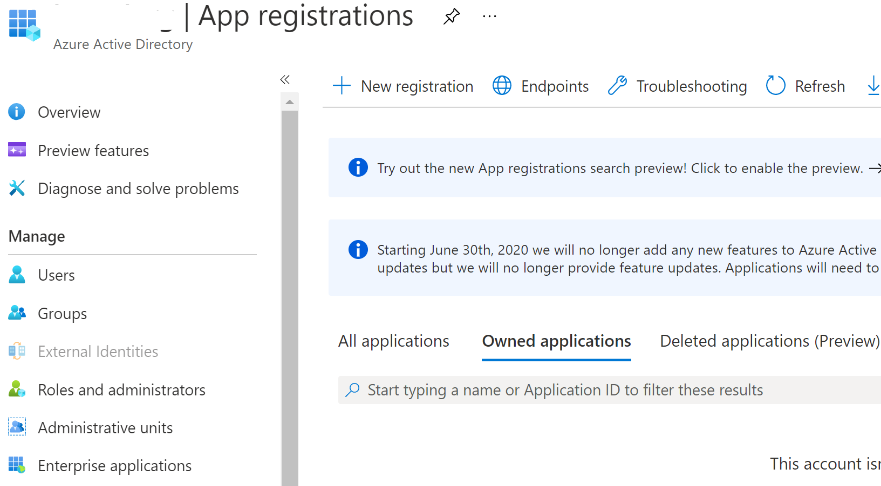
****

****

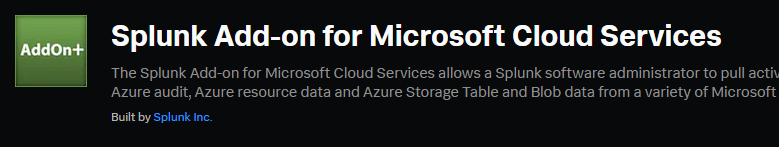
**Delving to integrating:**

Here's a high-level overview:

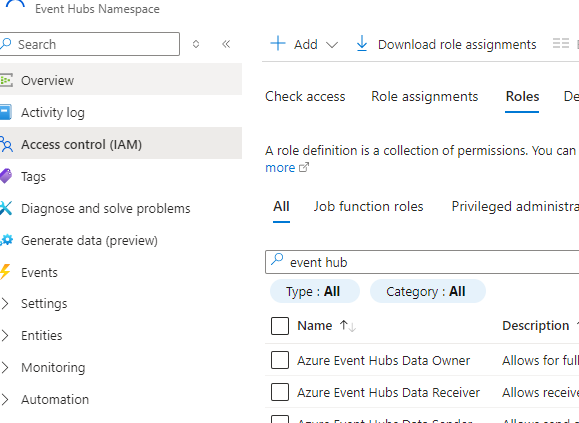
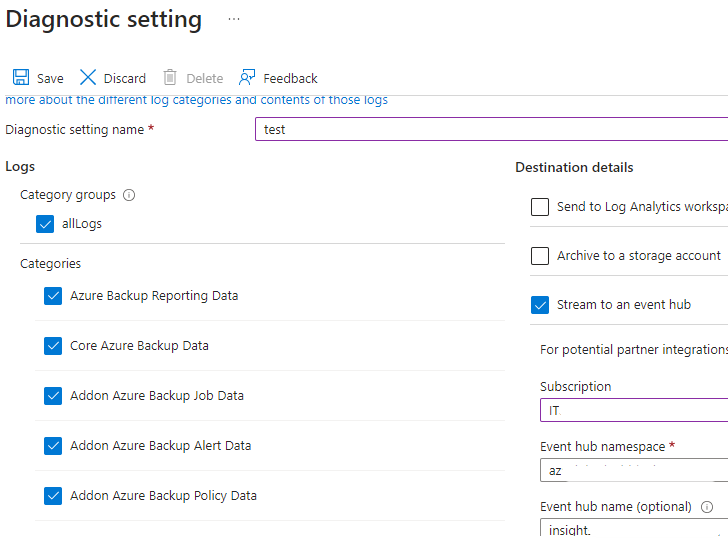
1. **App Registration Service:** Azure Active Directory (AAD) plays a crucial role in access management for Azure resources. The App Registration service within AAD allows you to create service principals, which are essentially identities used by applications (like Splunk) to access Azure resources securely



1. **Splunk Add-on for Microsoft Cloud Services:** Configure this add-on within Splunk to establish a robust connection with your Azure environment.

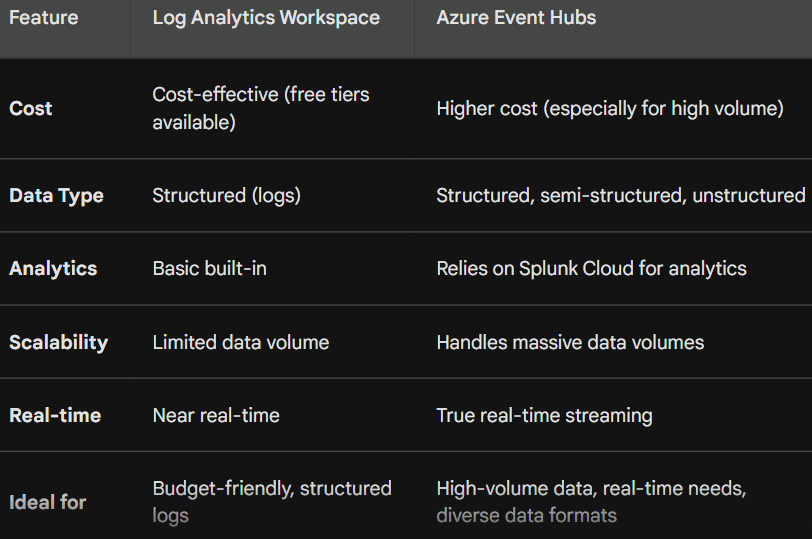


Once the connection is established: -

1. **Configure data collection for various Azure services**:
   * + **VMs (Linux/Windows):** For comprehensive log collection from your Azure VMs, you'll need to install Splunk Forwarders on each VM. These lightweight agents act as data shippers. Once installed and configured, it will communicate with a Splunk Heavy Forwarder, which can acts as a central consolidation point for log data collected from multiple Splunk Forwarders.
     + **Other Azure Services**: Identify the Azure services you want to collect data from (say Azure SQL/MI, Web Apps, ExpressRoute, RSV etc.) you can leverage Azure Monitor diagnostic settings to navigate appropriate logs and metrics to Log Analytics Workspace or Event Hubs with appropriate role assignment.

Once you've chosen the metrics to collect in Azure portal then configure the streaming service destination according to your organizational needs.

PFA summarized comparison of these services:



Select the suitable add-on in Splunk and configure with correct Host name of the streaming service.

Open your Splunk portal to validate the logs (it may take some time for data ingestion across platform).

PFA sample logs to be monitored:

