

**Lab Manual- Setup and Manage Azure Sentinel**

**Prepared for**:

**Date:** 18th Nov 2021

**Prepared by:**

Document Name: Lab Manual **Document Number** AZLabn989

**Contributor:**

Contents

[*1.* Introduction 3](#_Toc100831850)

[2. Lab: Setup Azure Sentinel workspace 3](#_Toc100831851)

[2.1 Enable Microsoft Sentinel 3](#_Toc100831852)

[3.1 Connect to Active Directory 5](#_Toc100831853)

[2.2 Connect to Azure Activity 6](#_Toc100831854)

# Introduction

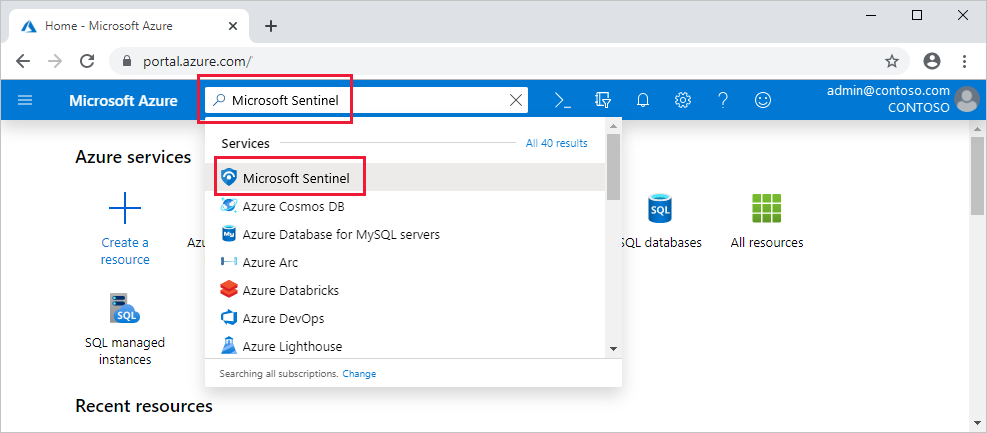
Microsoft Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Defender for Cloud Apps, security alerts from Microsoft Defender for Cloud, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Microsoft Sentinel

In this Lab , we will understand how to create an Azure sentinel workspace and connect with Data source

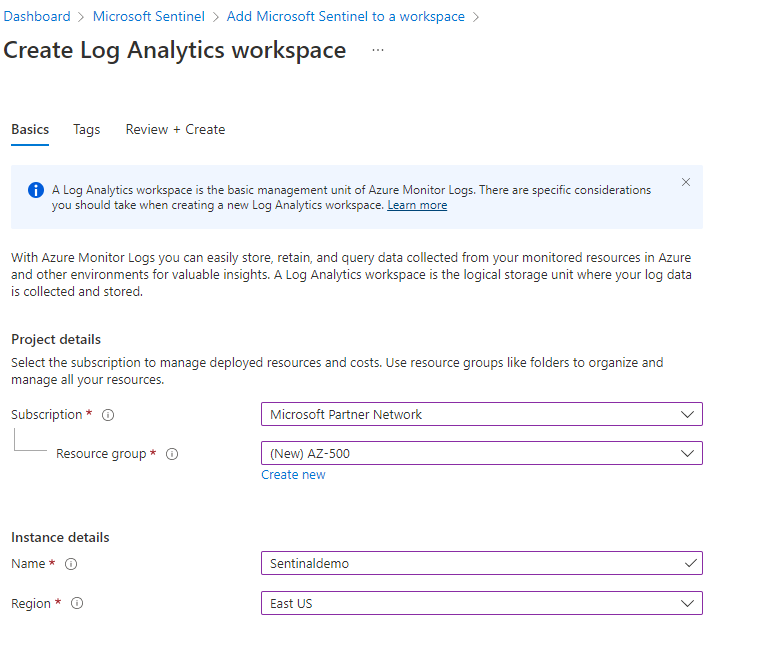
# Lab: Setup Azure Sentinel workspace

## Enable Microsoft Sentinel

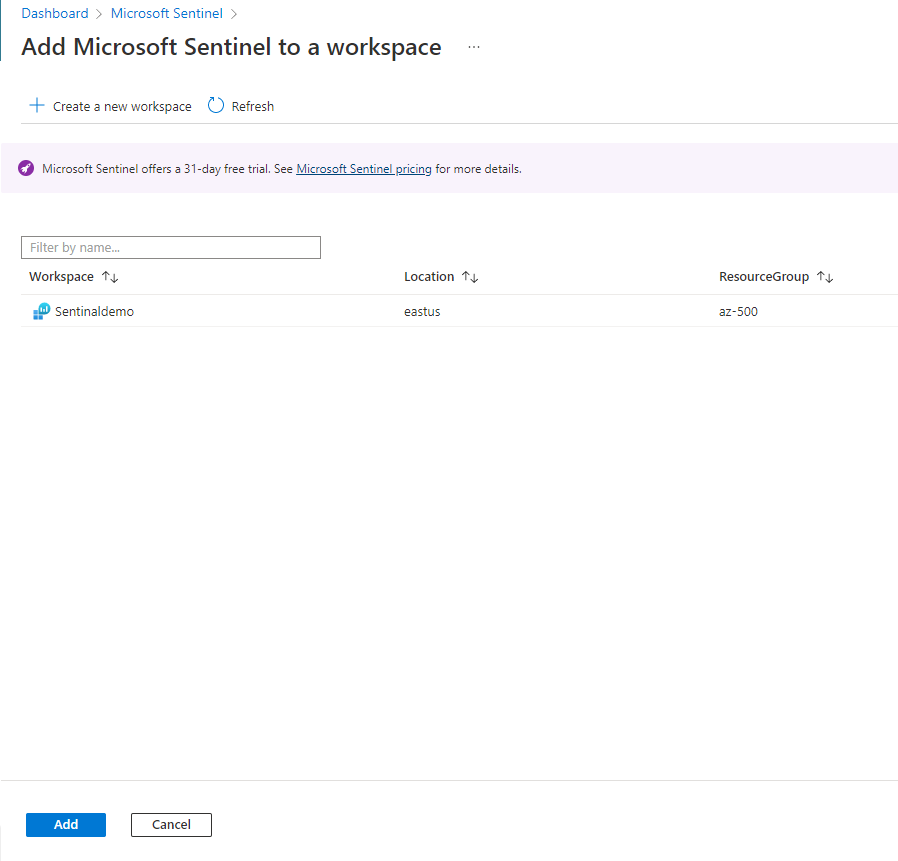
1. Sign in to the Azure portal. Make sure that the subscription in which Microsoft Sentinel is created is selected.
2. Search for and select **Microsoft Sentinel**.



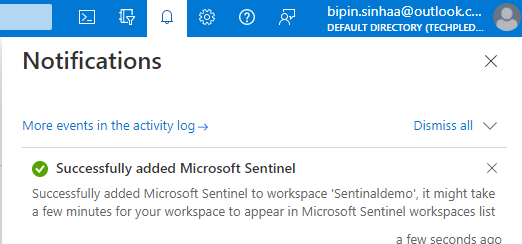
1. Select **Add**.
2. create a new one.



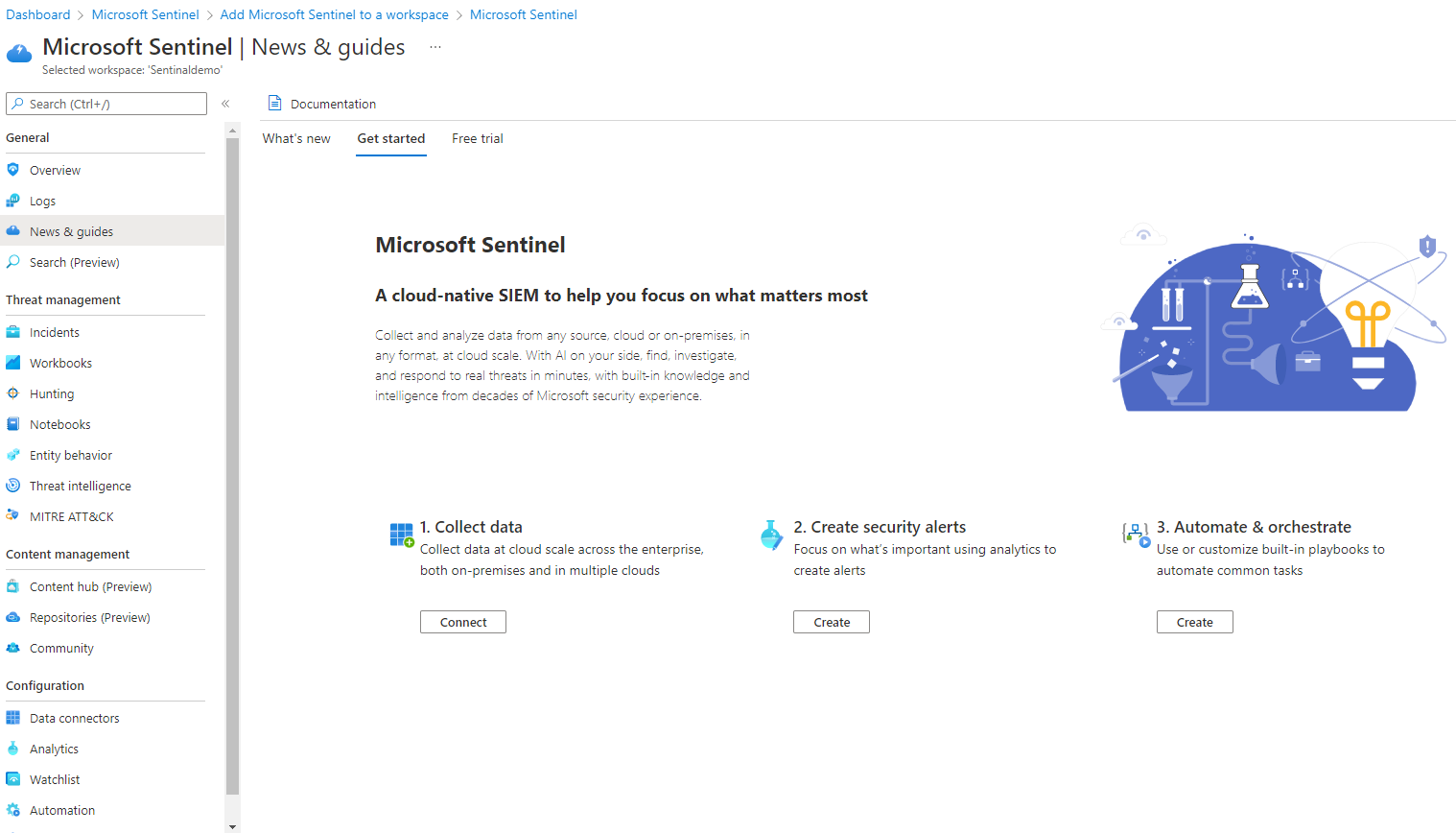
1. Click Review and Create
2. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade,



1. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade

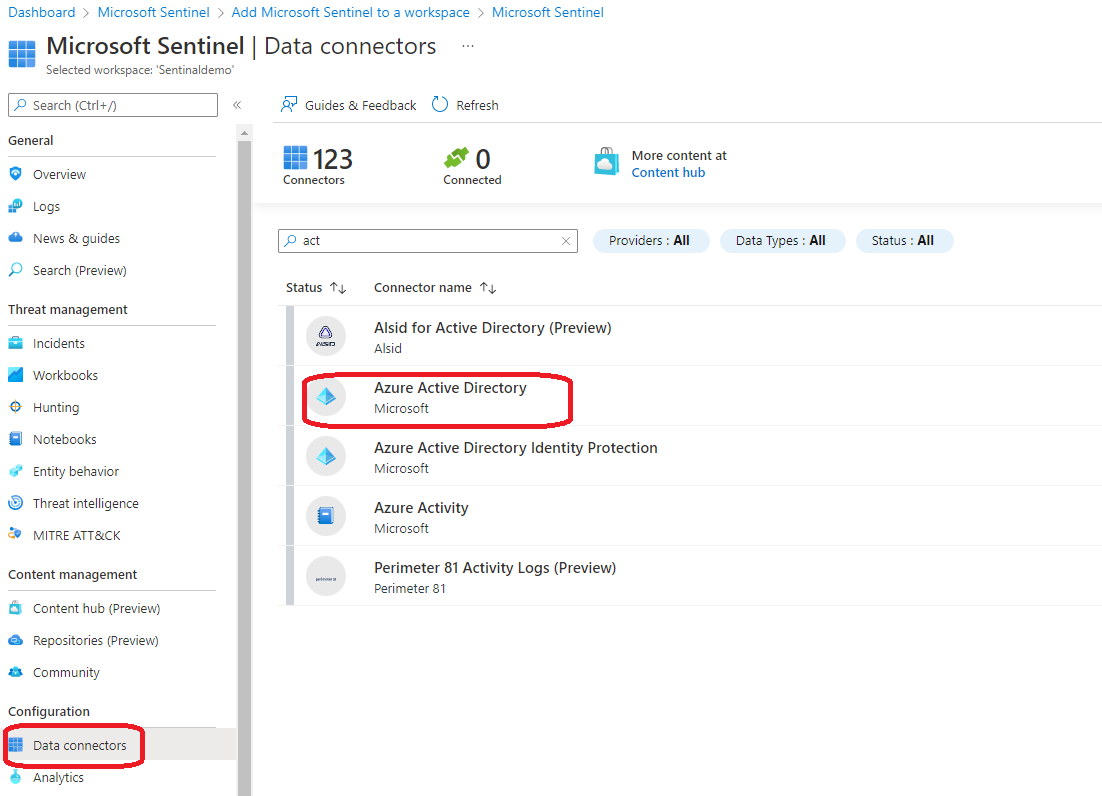


1. Once Created click add to On the **Add Microsoft Sentinel to a workspace** blade

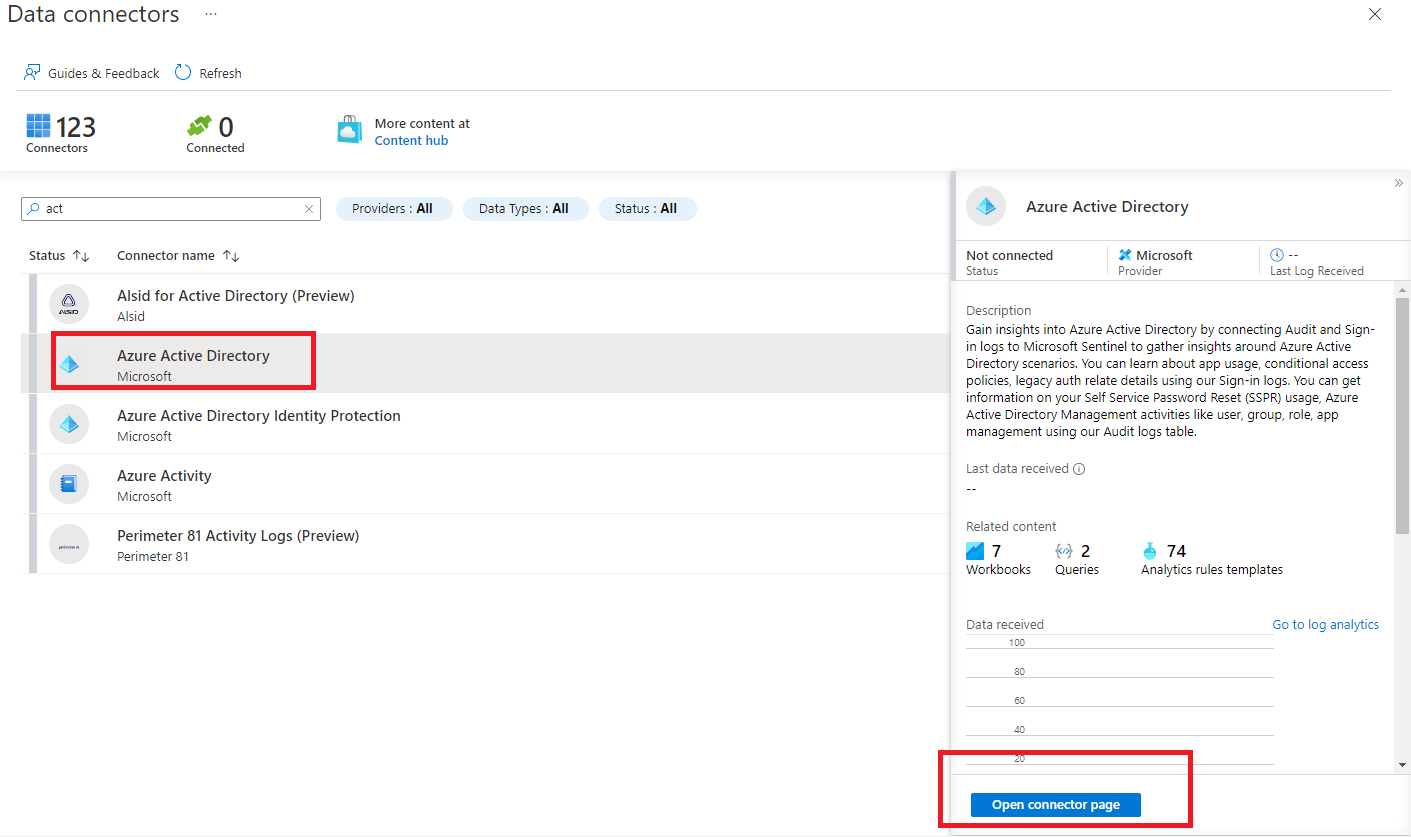


## Connect to Active Directory

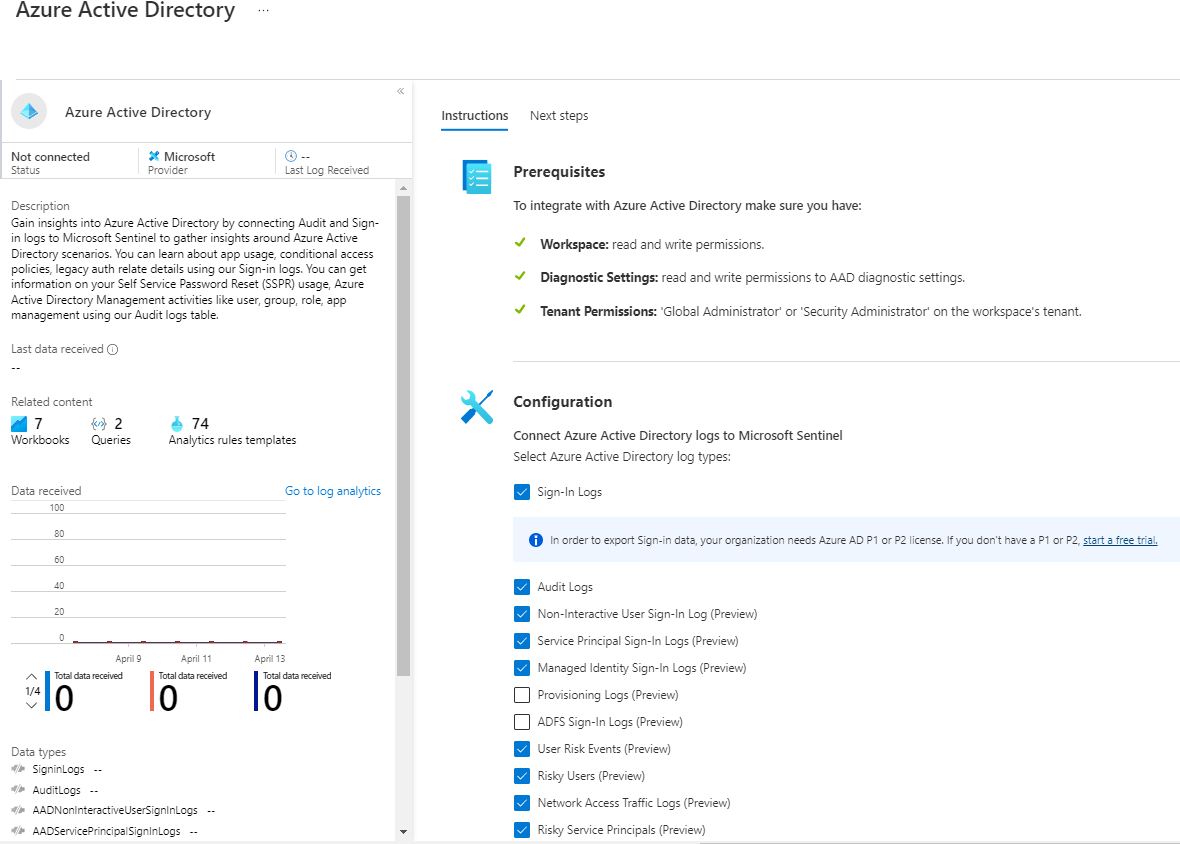
1. In Microsoft Sentinel, select **Data connectors** from the navigation menu.
2. From the data connectors gallery, select **Azure Active Directory**



1. Then select **Open connector page**.



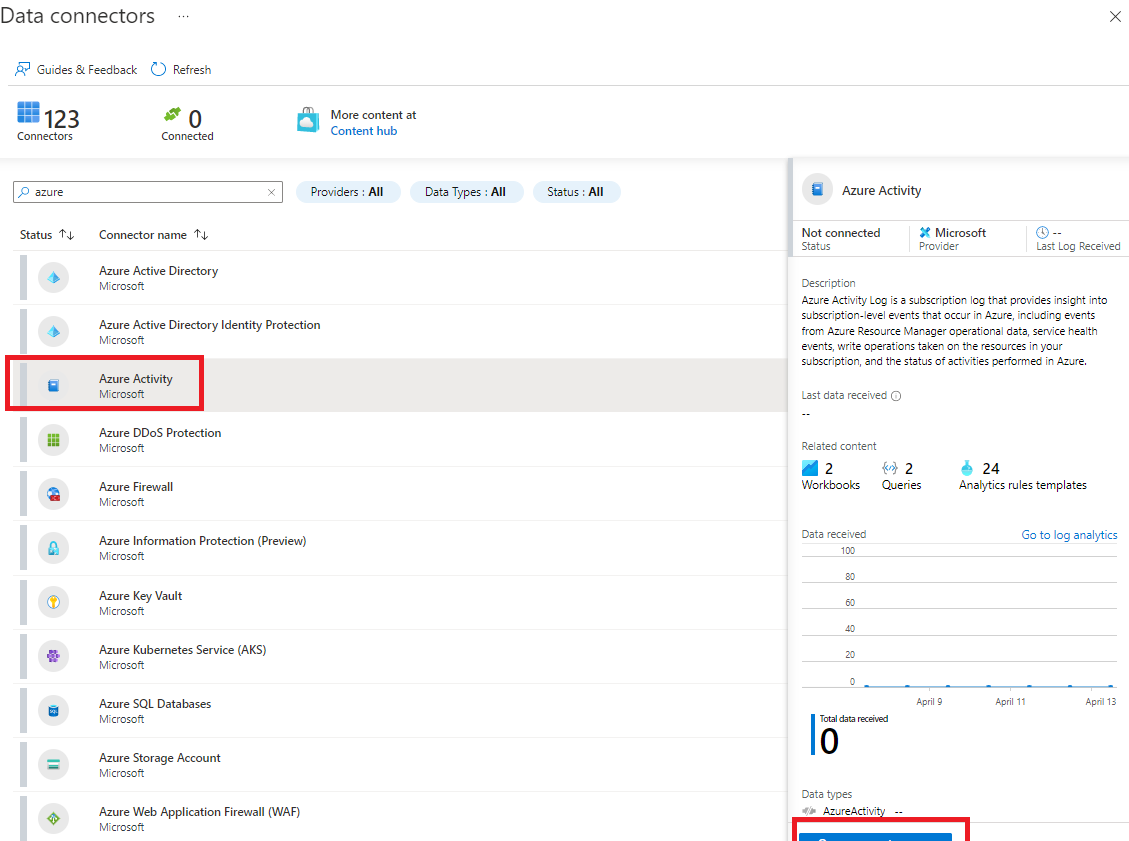
1. Mark the check boxes next to the log types you want to stream into Microsoft Sentinel (see below), and select **Connect**.



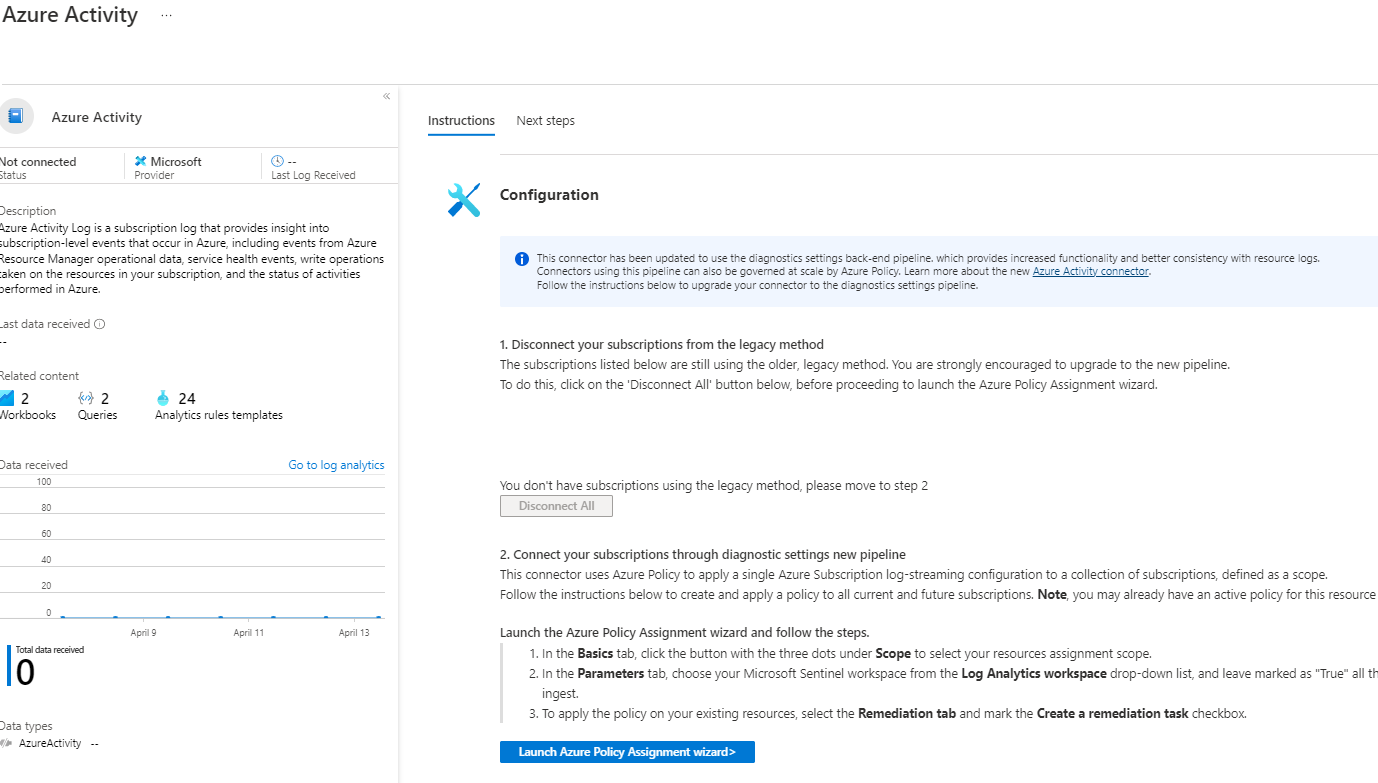
1. Mark the check boxes next to the log types you want to stream into Microsoft Sentinel (see below), and select **Apply Changes**

## Connect to Azure Activity

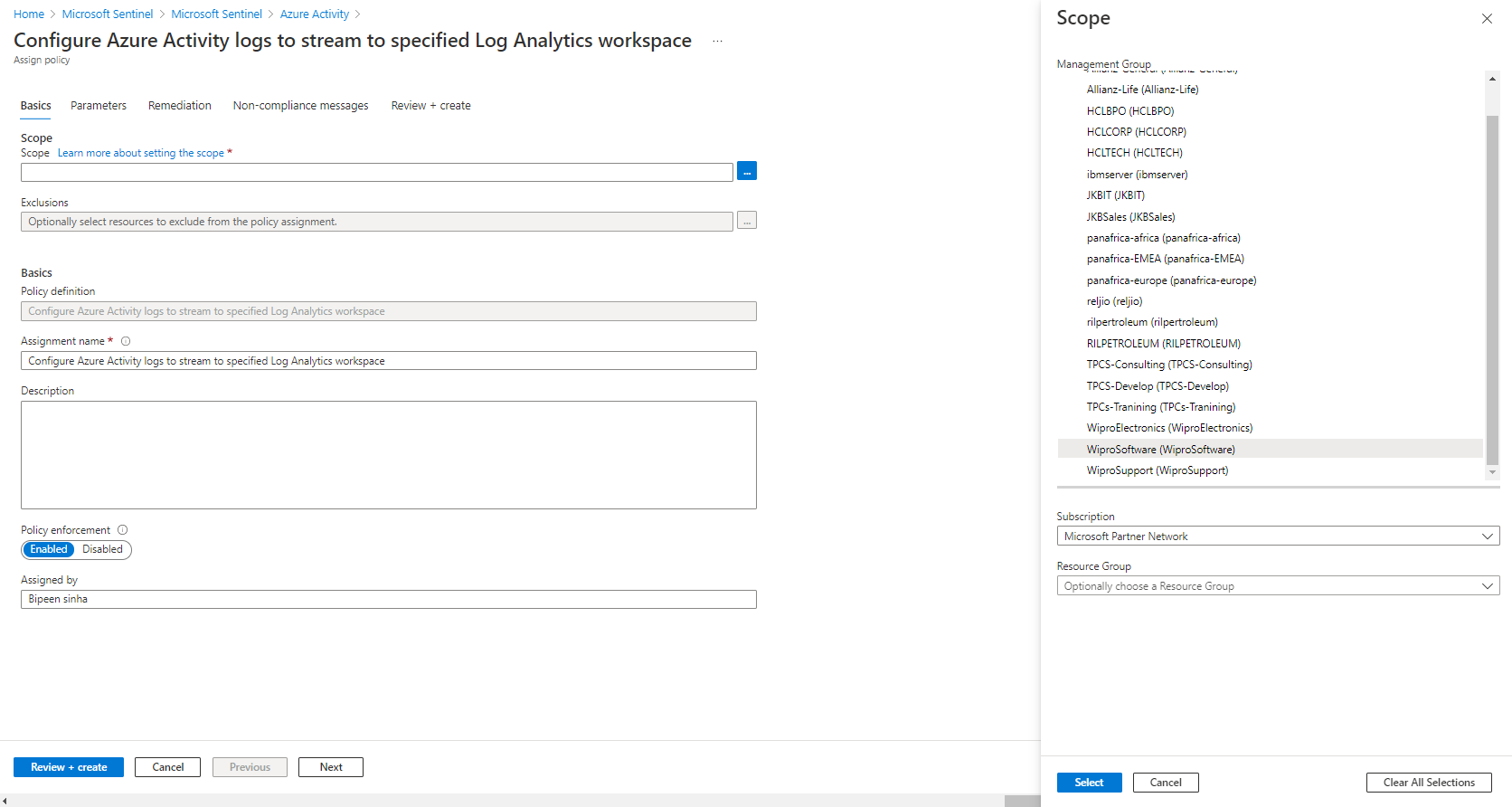
1. On the **Microsoft Sentinel | Data connectors** blade, review the list of available connectors, type **Azure** into the search bar and select the entry representing the **Azure Activity** connector

.

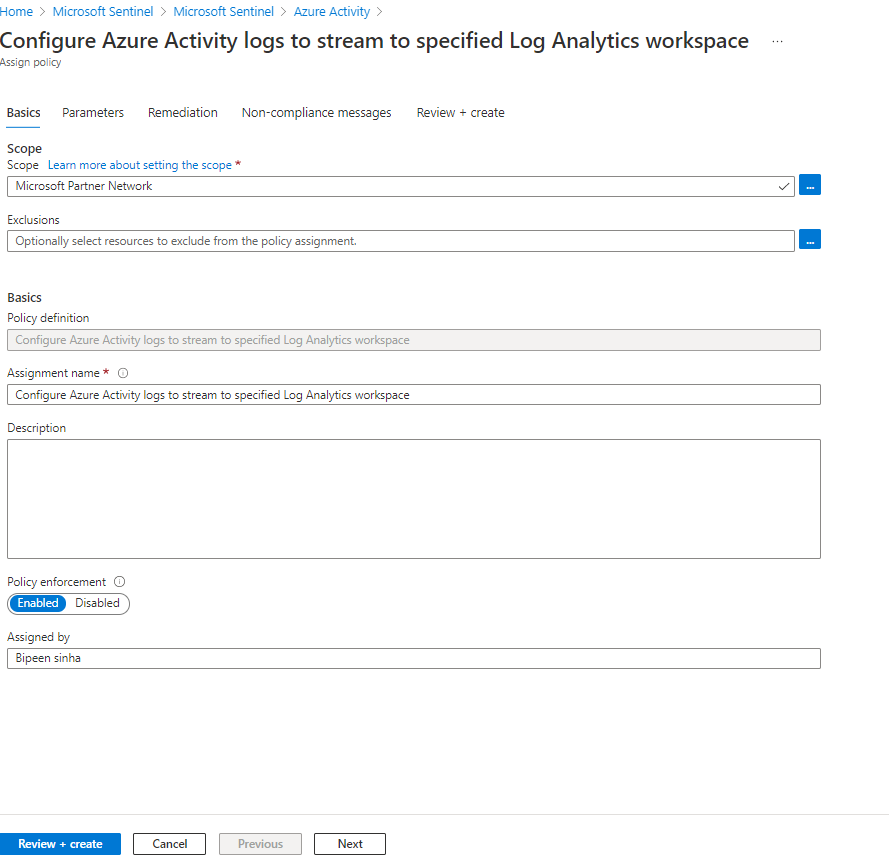
1. Then select **Open connector page**.
2. On the **Azure Activity** blade the **Instructions** tab should be selected, note the **Prerequisites** and scroll down to the **Configuration**. Take note of the information describing the connector update. Your Azure Pass subscription never used the legacy connection method so you can skip step 1 (the **Disconnect All** button will be grayed out) and proceed to step 2.
3. In step 2 **Connect your subscriptions through diagnostic settings new pipeline**, review the "Launch the Azure Policy Assignment wizard and follow the steps" instructions then click **Launch the Azure Policy Assignment wizard>**.



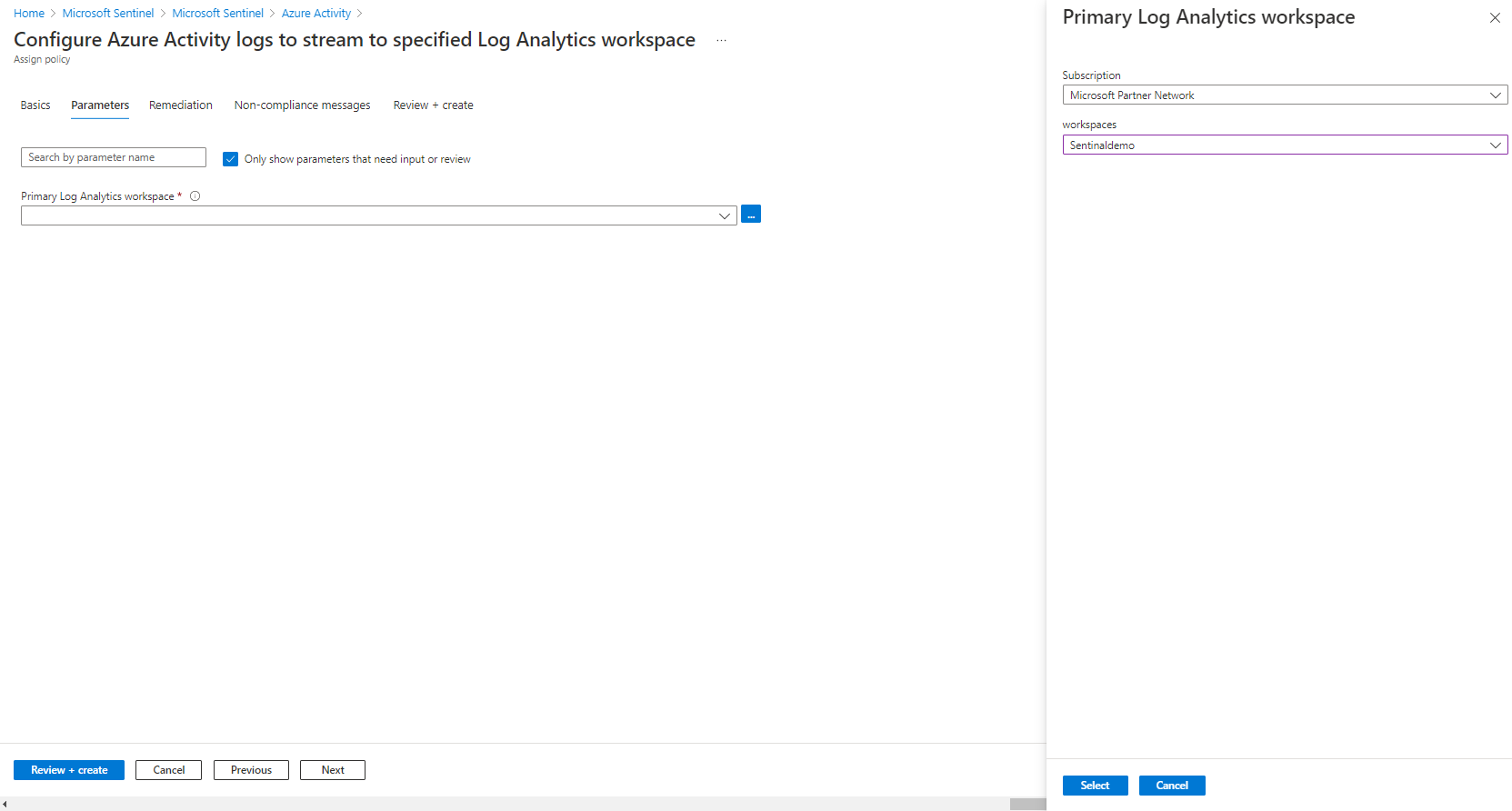
1. On the **Configure Azure Activity logs to stream to specified Log Analytics workspace** (Assign Policy page) **Basics** tab, click the **Scope elipsis (...)** button. In the **Scope** page choose your Azure Pass subscription from the drop-down subscription list and click the **Select** button at the bottom of the page.



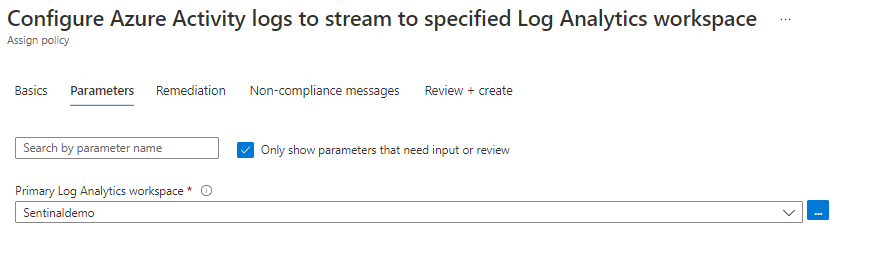
1. Click Next



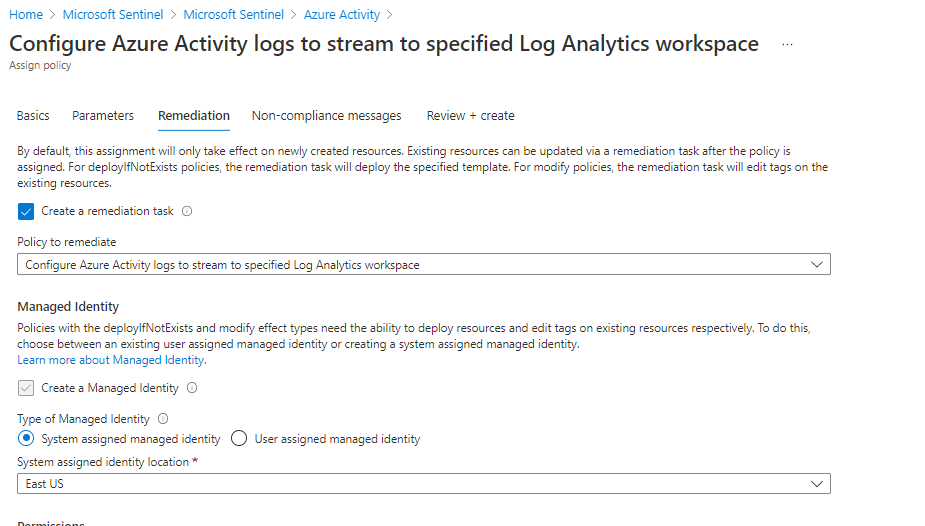
1. Click Next
2. Click the **Next** button at the bottom of the **Basics** tab to proceed to the **Parameters** tab. On the **Parameters** tab click the **Primary Log Analytics workspace elipsis (...)** button. In the **Primary Log Analytics workspace** page, make sure your Azure pass subscription is selected and use the **workspaces** drop-down to select the Log Analytics workspace you are using for Sentinel.



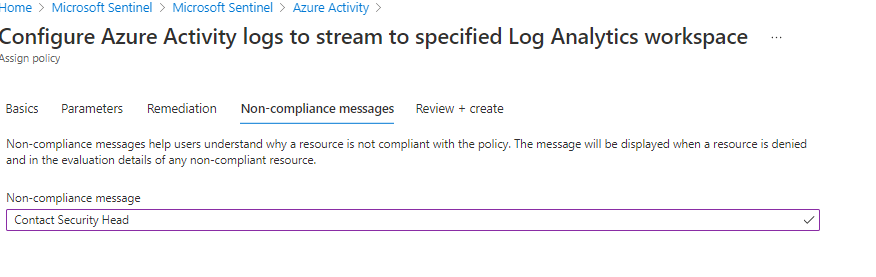
1. When done click the **Select** button at the bottom of the page and click **Next**



1. Click the **Next** button at the bottom of the **Parameters** tab to proceed to the **Remediation** tab. On the **Remediation** tab select the **Create a remediation task** checkbox. This will enable the "Configure Azure Activity logs to stream to specified Log Analytics workspace" in the **Policy to remediate** drop-down. In the **System assigned identity location** drop-down, select the region (East US for example) you selected earlier for your Log Analytics workspace.

c

1. Click the **Next** button at the bottom of the **Remediation** tab to proceed to the **Non-compliance message** tab. Enter a Non-compliance message if you wish (this is optional) and click the **Review + Create** button at the bottom of the **Non-compliance message** tab.



1. Click the **Create** button. You should observe three succeeded status messages: **Creating policy assignment succeeded, Role Assignments creation succeeded, and Remediation task creation succeeded**.
2. Verify that the **Azure Activity** pane displays the **Data received** graph (you might have to refresh the browser page).

**Note**: It may take over 15 minutes before the Status shows "Connected" and the graph displays Data received.

