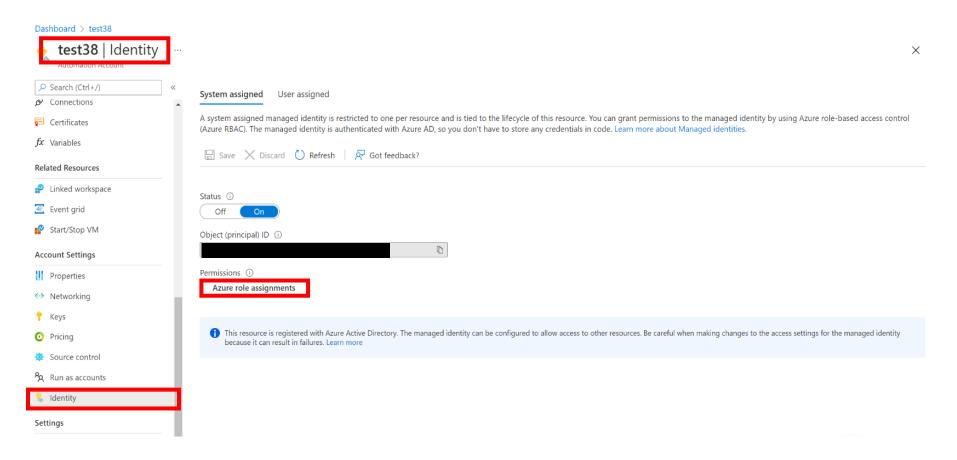
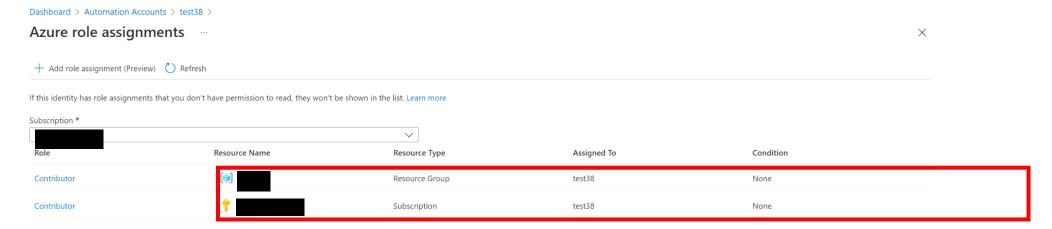
Guidance to detect Anomalous activity

Step 1: Check resources that had exposure

a) Go to your Automation account in <u>Azure Portal</u>. Navigate to the Identity tab under "Account Settings". Take note of the Id of your automation account on top left corner (The Id in the example below is 'test 38'). Then click on the "Azure role assignments".

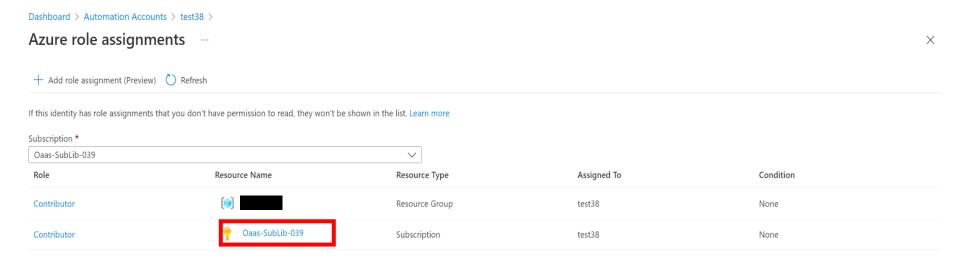


b) The page will list all Azure resources that are linked to Managed identities.

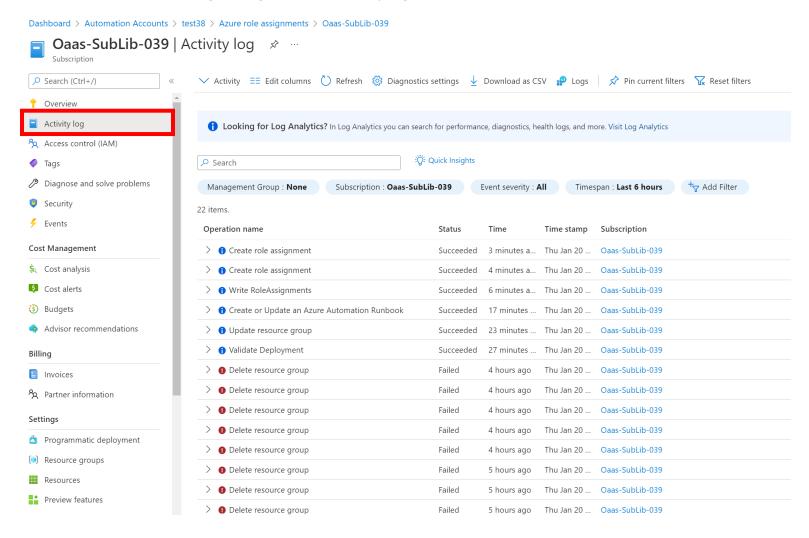


Step 2: Scan Logs for anomalous activity

a) For the previous step (Step 1b), click on the resource to be redirected to the portal page of that resource



b) On the resource portal page, navigate to the "Activity logs"



- c) Set "Timespan" from December 1, 2021, to December 10, 2021, and scan for any anomalous activity. Possible actions include (not an exhaustive list): Resetting of a password on a VM, change access level from "Contributor" to higher privileges, Starting and Stopping of a VM. Such an event will be logged by the Automation Id (Collected in Step 1a) in the column "Event initiated by"
- d) Repeat steps 2a to 2c for every resource discovered in step 1b.