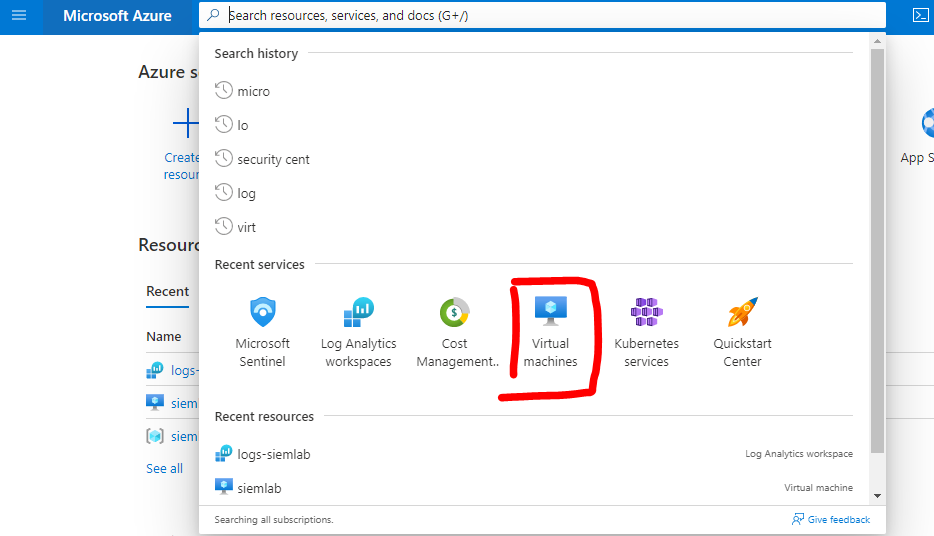
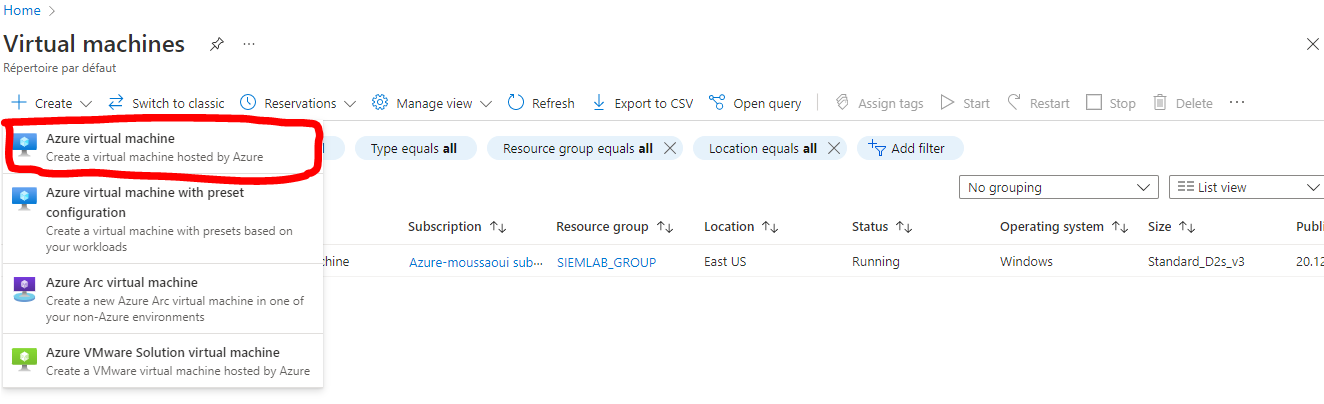
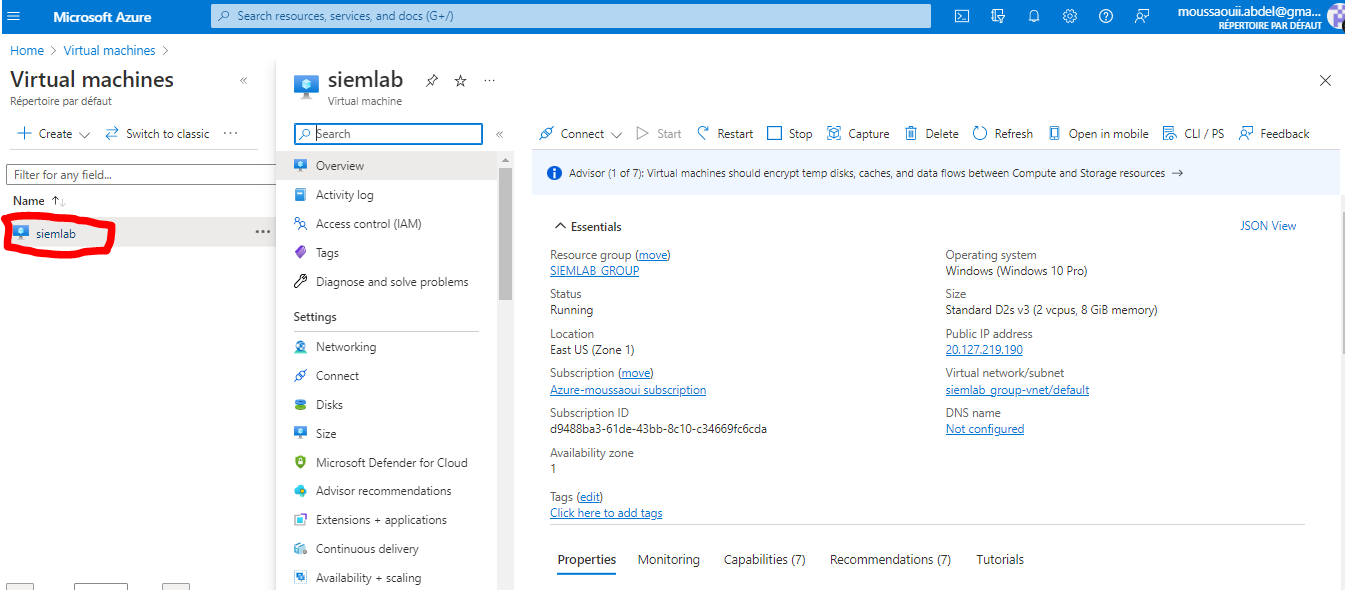
# SIEM LAB

# Create VM:

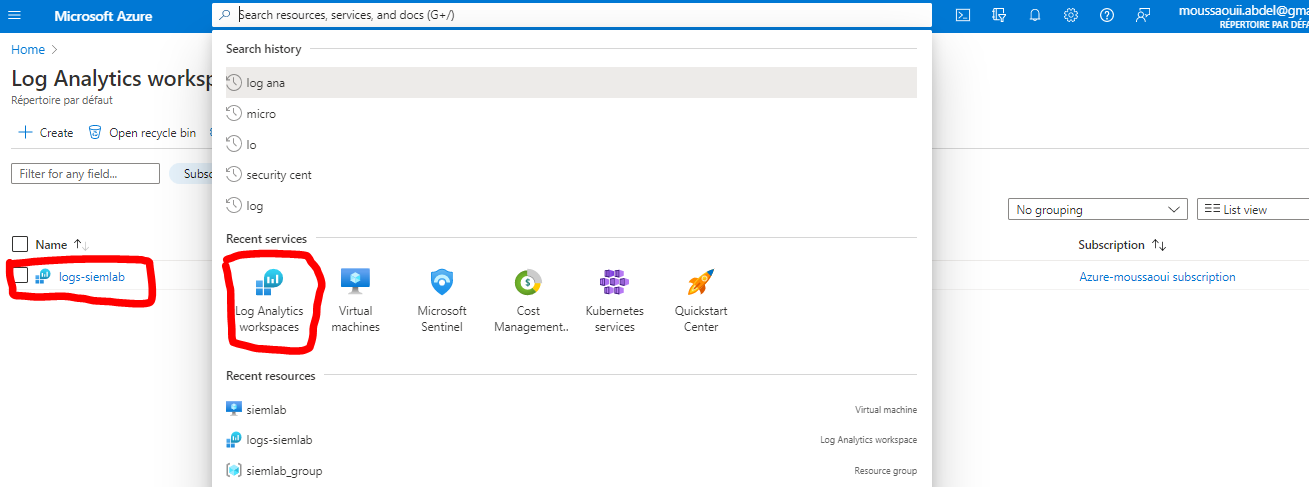


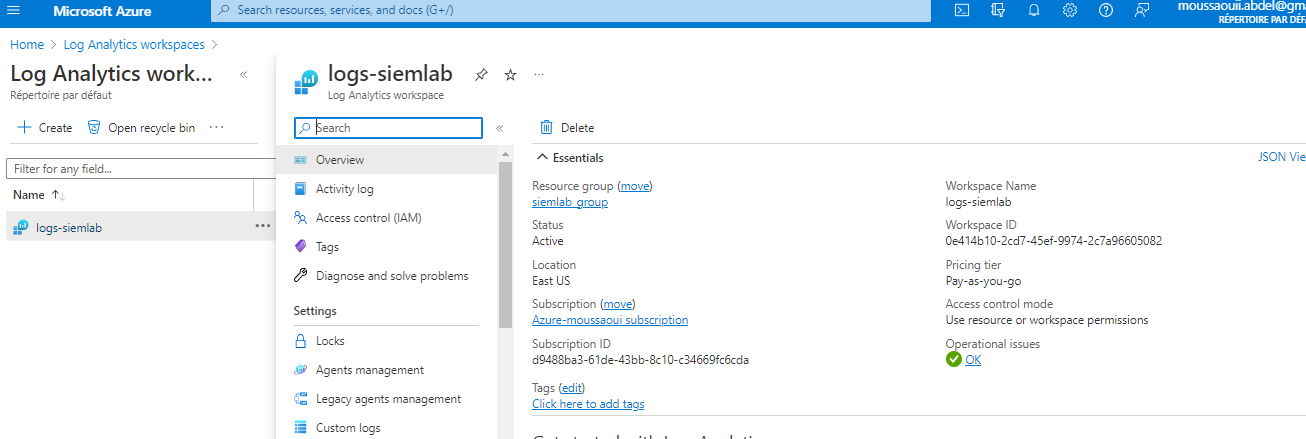


* Created machine

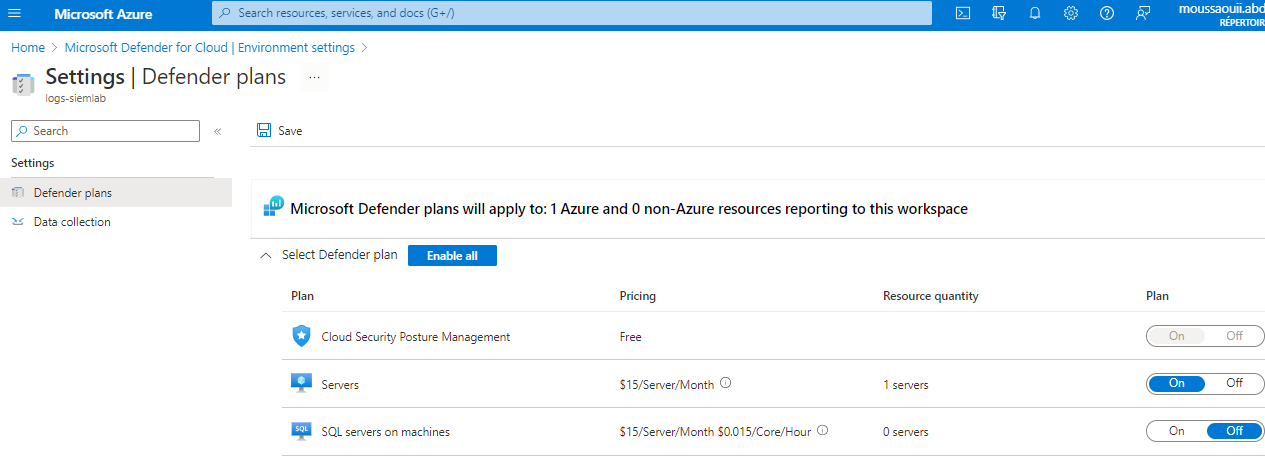


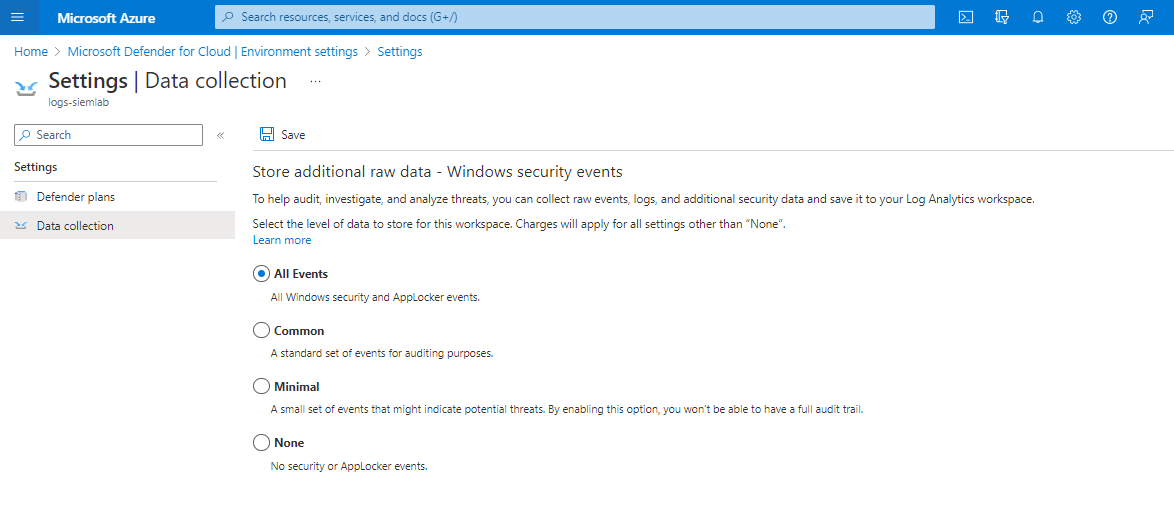
# Create log analytics:



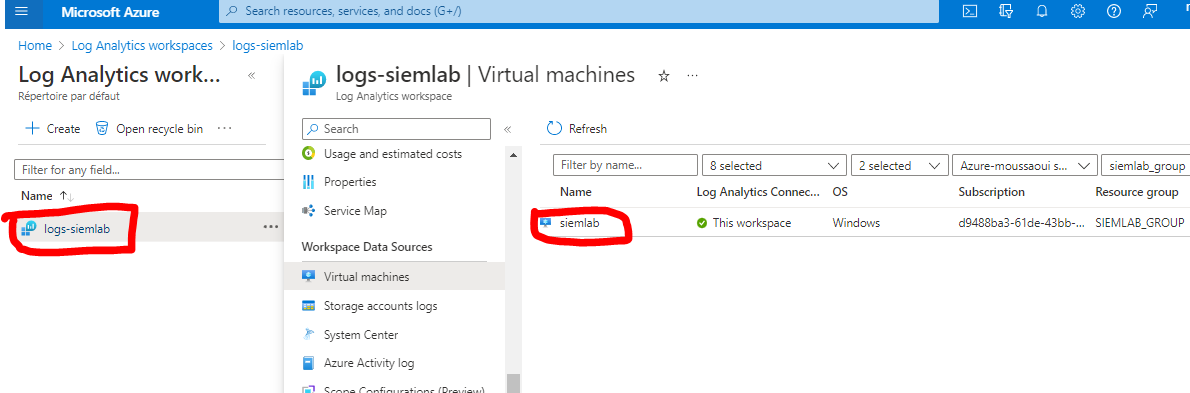


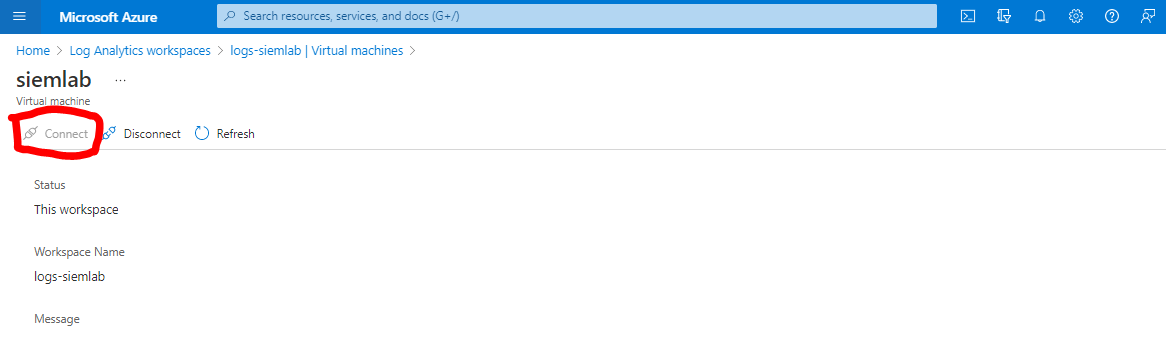
# Enable gathering logs from VM to log analytics:



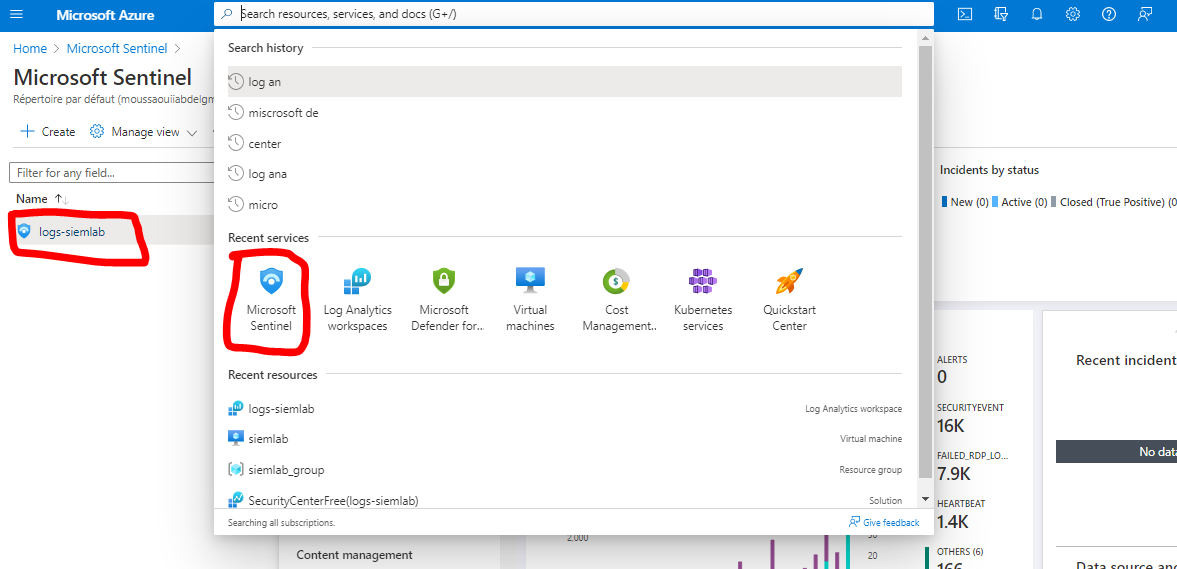


***Connect Log analytics to VM***

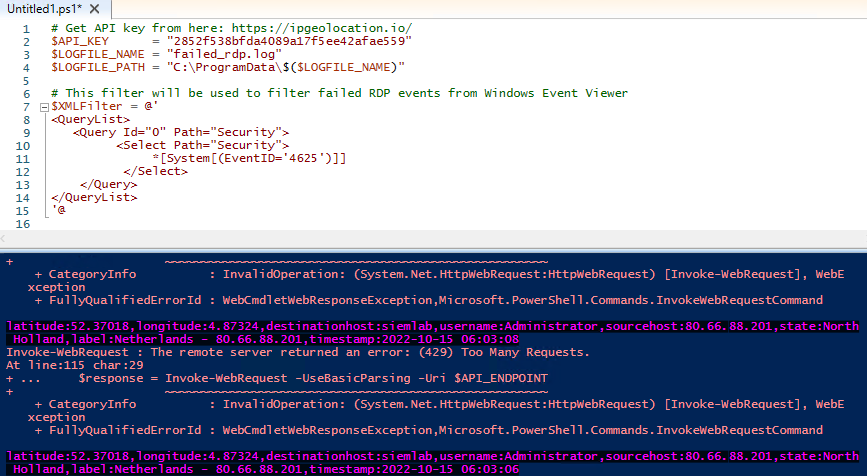




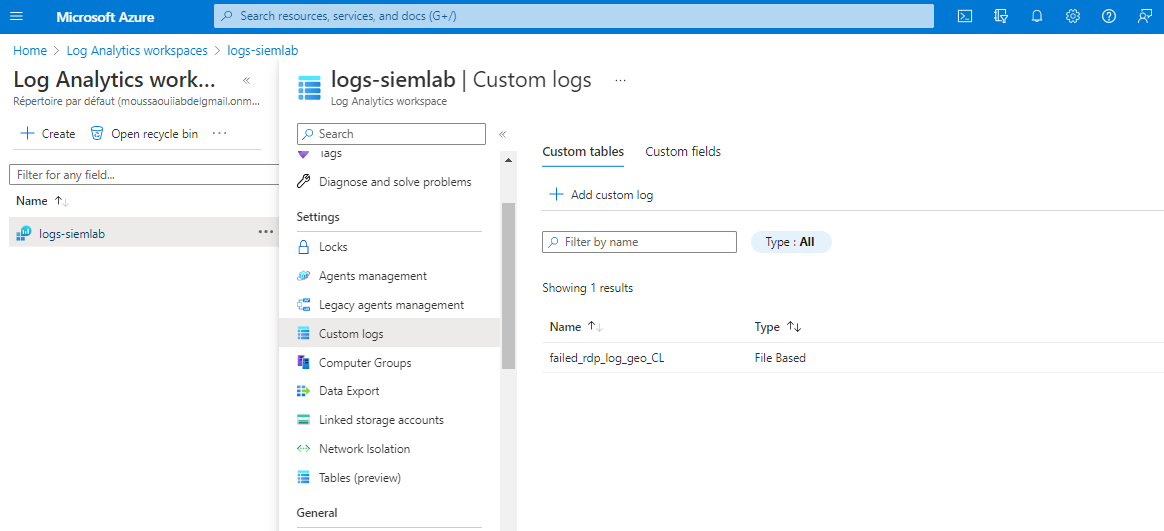
***Set up SIEM(Microsoft Sentinel) and connect it with log analytics***



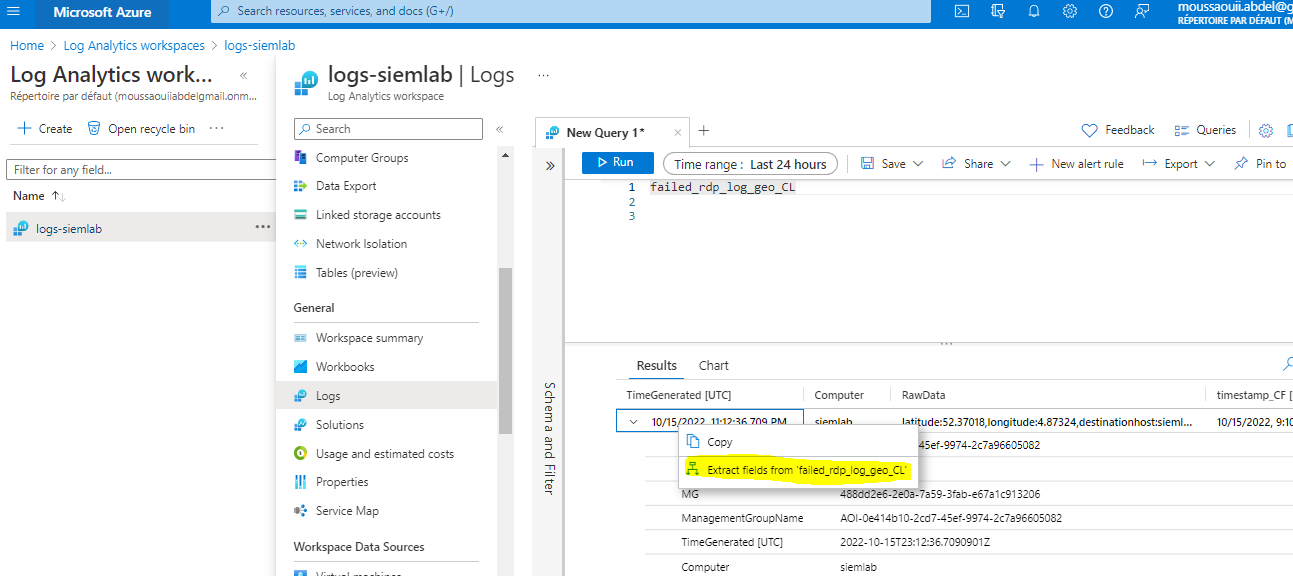
***Gather geodata for faild rdp login***

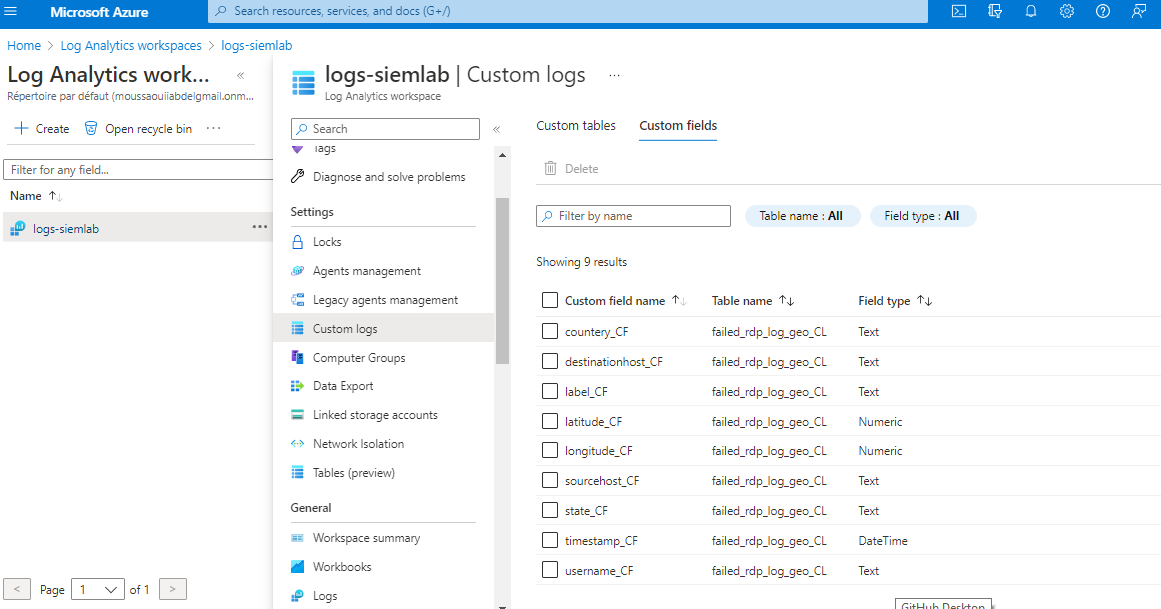


***Create customized log***

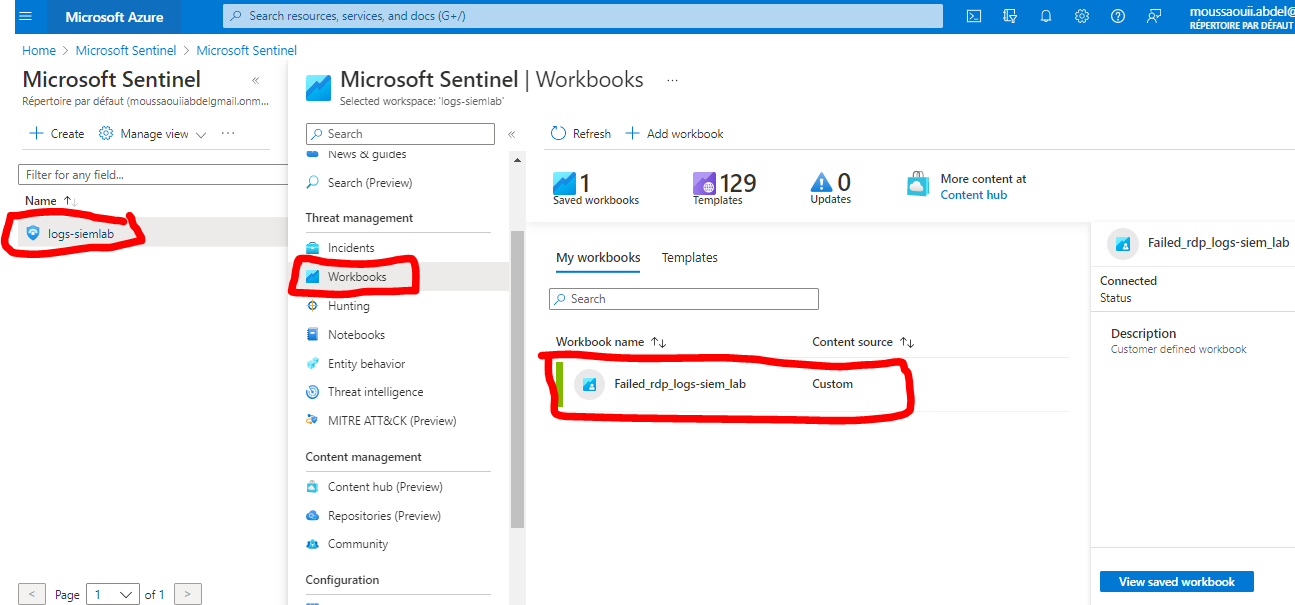


***Create custom fields***





***Set up map in sentinel***



* Used query

failed\_rdp\_log\_geo\_CL | summarize event\_count=count () by sourcehost\_CF,latitude\_CF,longitude\_CF,

countery\_CF, label\_CF, destinationhost\_CF | where destinationhost\_CF != "samplehost"

| where sourcehost\_CF != ""

Result

