Ingestion of Logs to sentinel Via Custom table

Ex: Vcenter, Miraki, JuniperIDP,ZPA,Apache Tomcat

**Steps:**

When vCenter is configured to forward logs to a Syslog server (like a Linux VM), and that server has AMA installed, you can collect those logs using the Syslog data source in a Data Collection Rule (DCR).

**At Vcenter Device >> allow Syslog IP over port 514 -- now logs coming to Syslog server**

Here logs will be at some path like

* Logs from vCenter typically go to **/var/log/syslog** or a custom file like **/var/log/vcenter.log**

**Now bcz, vCenter Logs May Not Use Standard Syslog Facilities, for Better Parsing and Normalization and For Syslog Format Limitations,**

**We can create a Custom table using Custom logs via AMA Data connector.**

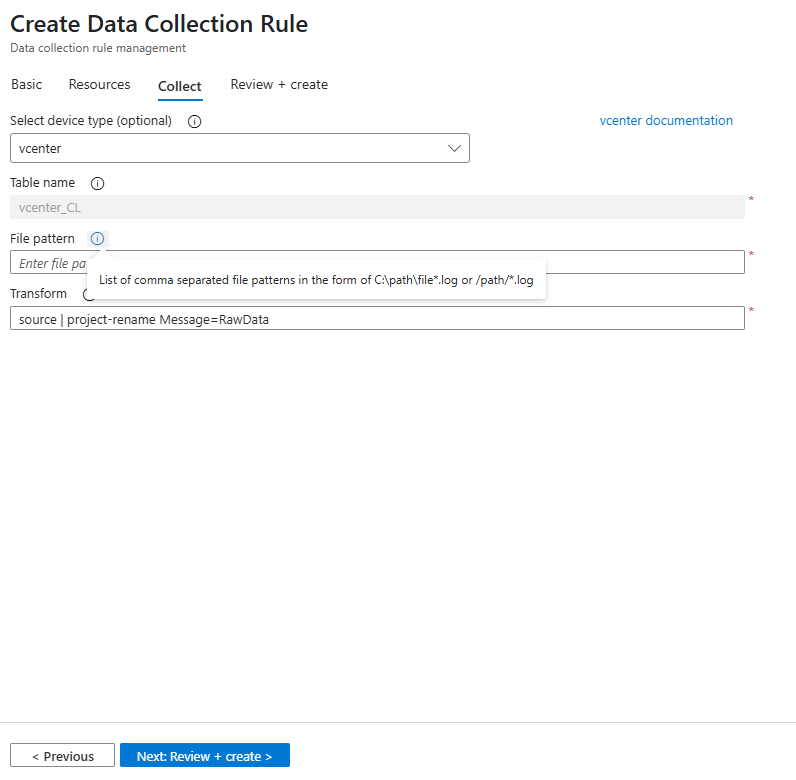
Here in the Data connector while creating DCR, fill below details

Select Device Type: Vcenter

Give Table Name as \_CL

File Path: The path of Syslog server where the venter logs stored like/var/log/vcenter.log

Create the DCR

****