

CEF ASA Syslog DSR Template

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

example of DSR

```

{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "dataCollectionRules_CEF_Rule_name": {
      "defaultValue": "CEF_Rule",
      "type": "String"
    },
    "workspaces_SecureScoreData_ropcp3iyqhmwm_externalid": {
      "defaultValue": "/subscriptions/0a177a01-8b95-42cd-963a-a363c0e1e52b/resourceGroups/LabNSG/provide",
      "type": "String"
    }
  },
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Insights/dataCollectionRules",
      "apiVersion": "2021-04-01",
      "name": "[parameters('dataCollectionRules_CEF_Rule_name')]",
      "location": "centralus",
      "kind": "Linux",
      "properties": {
        "dataSources": {
          "syslog": [
            {
              "streams": [
                "Microsoft-CommonSecurityLog",
                "Microsoft-CiscoAsa"
              ],
              "facilityNames": [
                "local0"
              ],
              "logLevels": [
                "Info"
              ],
              "name": "sysLogsDataSource-1688419672"
            }
          ]
        },
        "destinations": {
          "logAnalytics": [
            {
              "workspaceResourceId": "[parameters('workspaces_SecureScoreData_ropcp3iyqhmwm_exte",
              "name": "la--1908599500"
            }
          ]
        },
        "dataFlows": [
          {
            "streams": [
              "Microsoft-CommonSecurityLog",
              "Microsoft-CiscoAsa"
            ],
            "destinations": [
              "la--1908599500"
            ]
          }
        ]
      }
    }
  ]
}

```