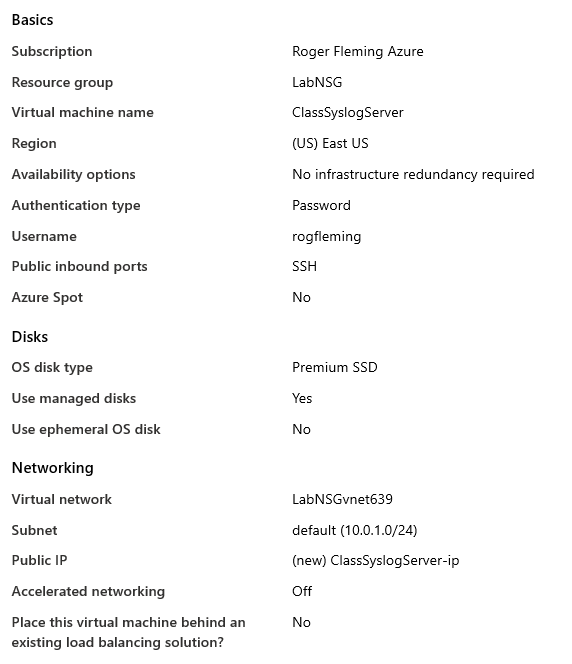
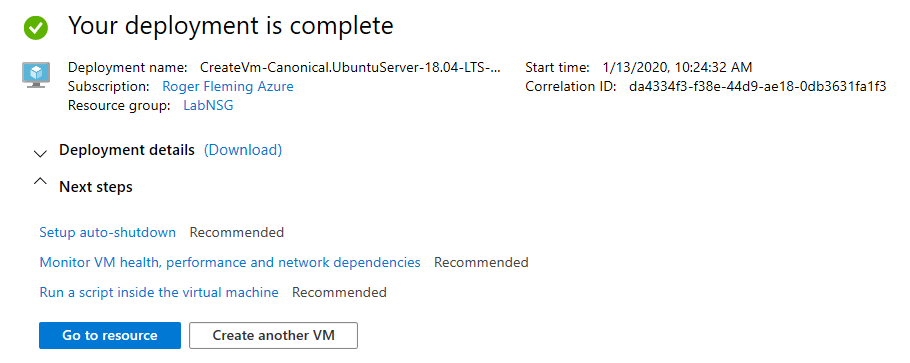
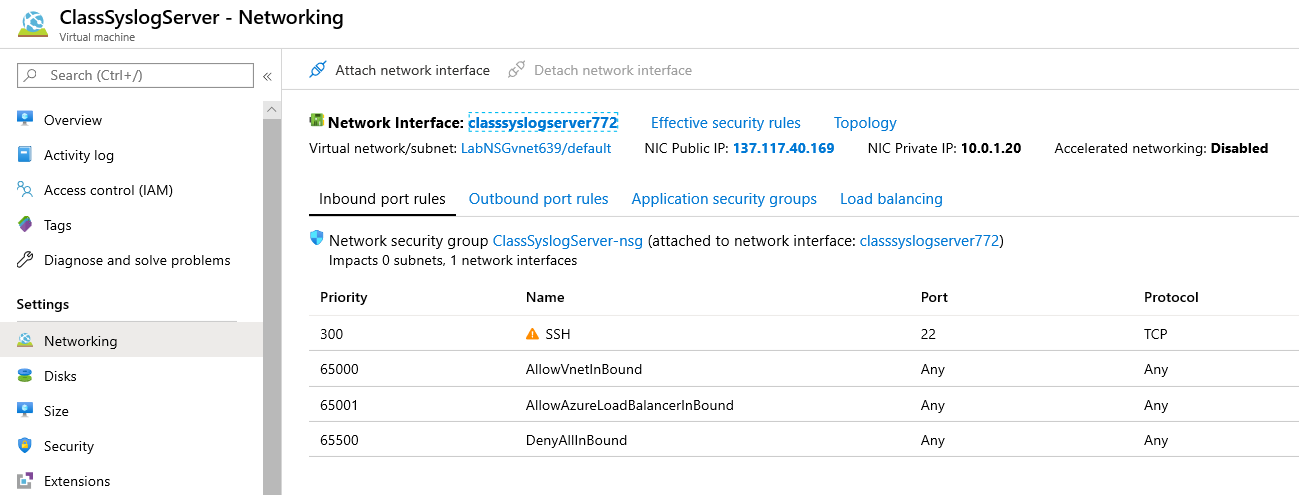
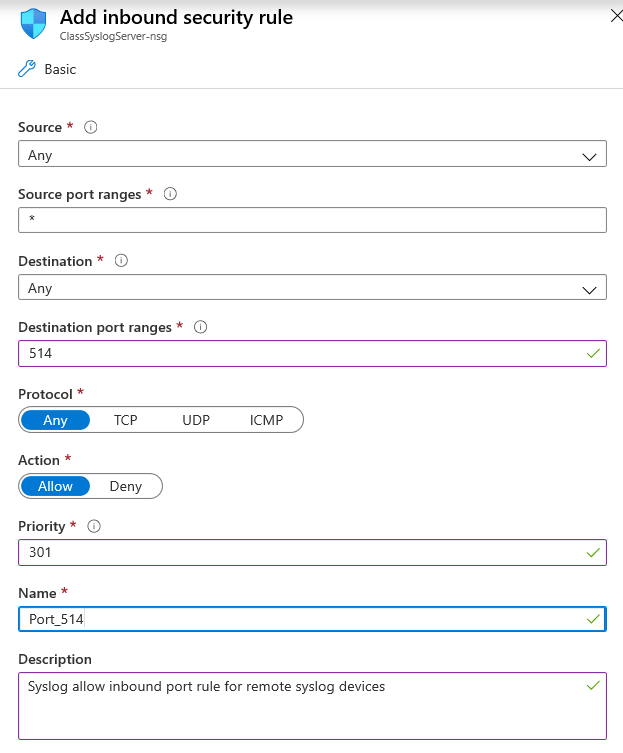
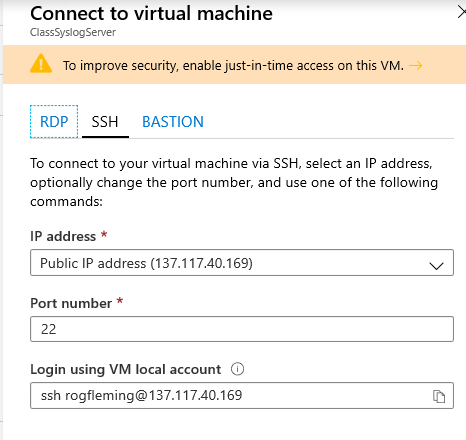
Lab: Setup and configure a Linux platform to forward Syslogs from 3rd party devices.

1. Create a Linux Azure Virtual Machine

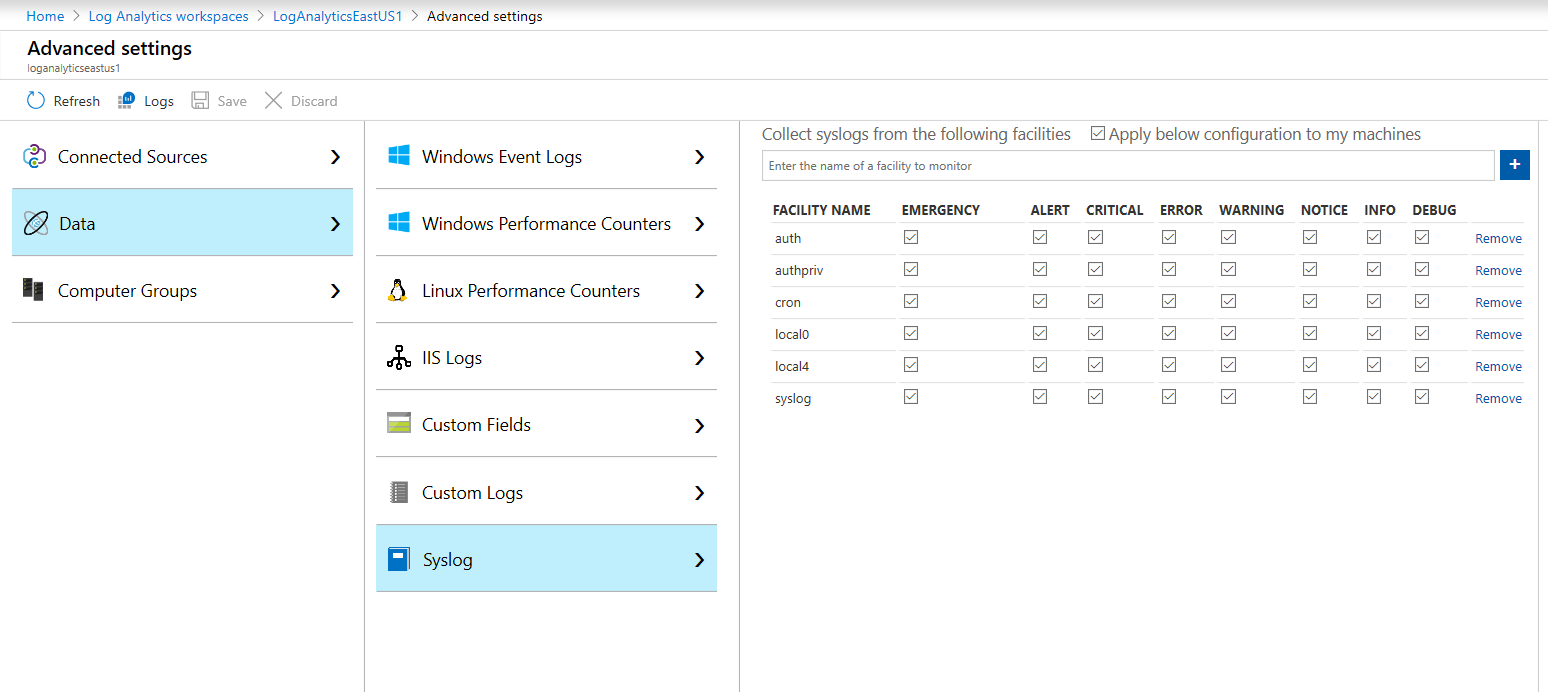


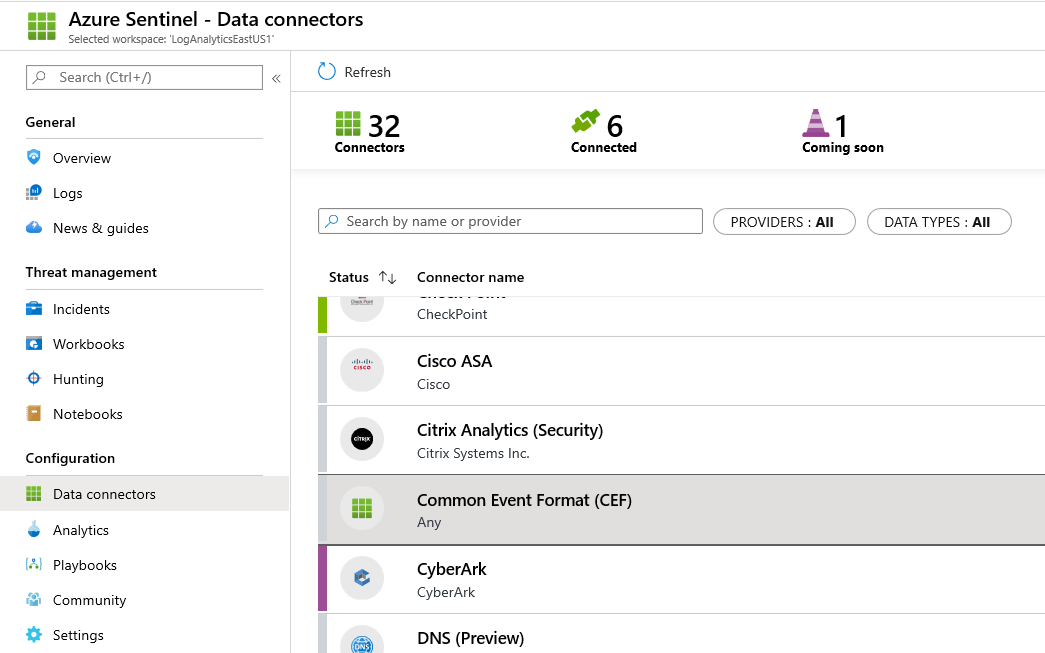
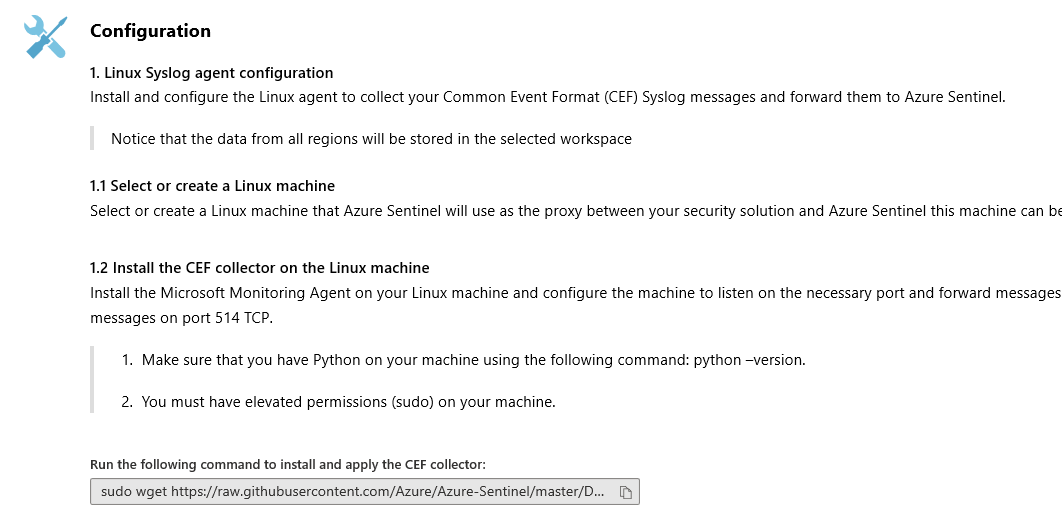
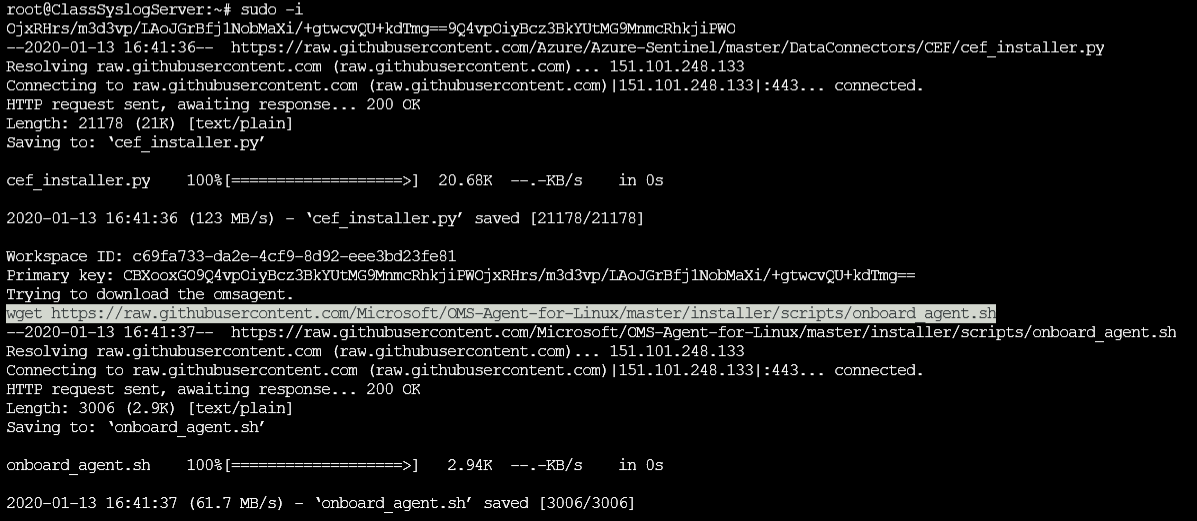
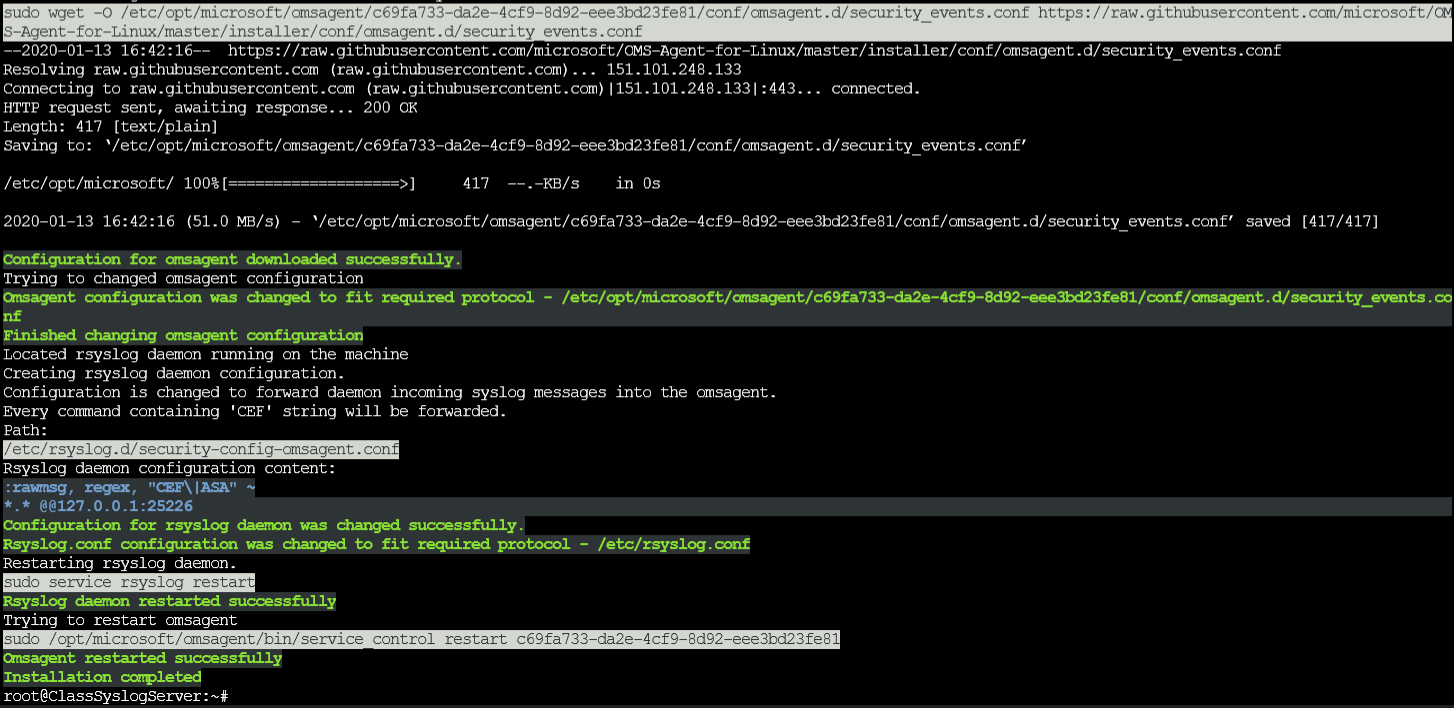


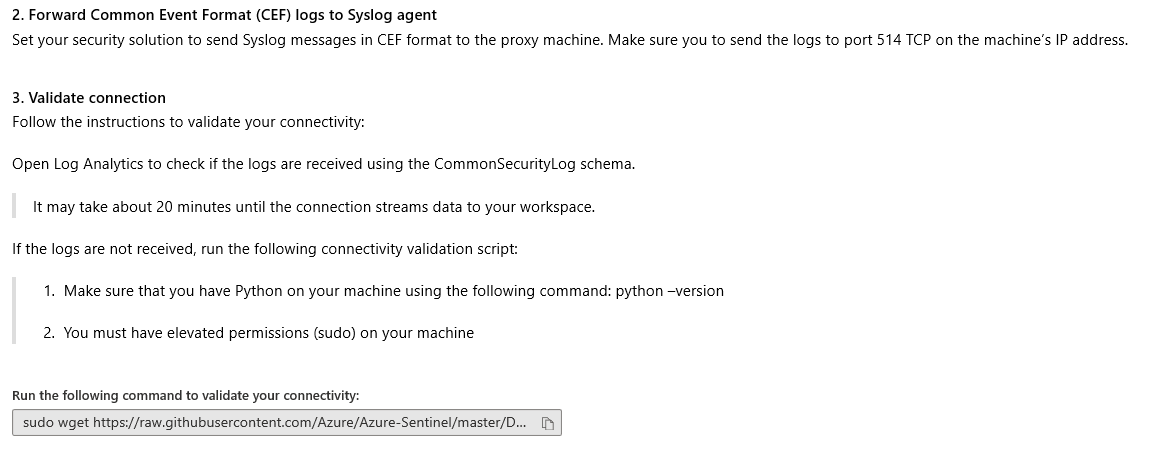
1. Enable tcp and udp port 514 for access to the virtual machine.  
   
2. Click the add inbound port rule button  
   
3. Click the Add button to save the rule
4. SSH or use Serial Console Connection to Login  
     
   
5. Change to Root user  
   rogfleming@ClassSyslogServer:~$ sudo -i

root@ClassSyslogServer:~#

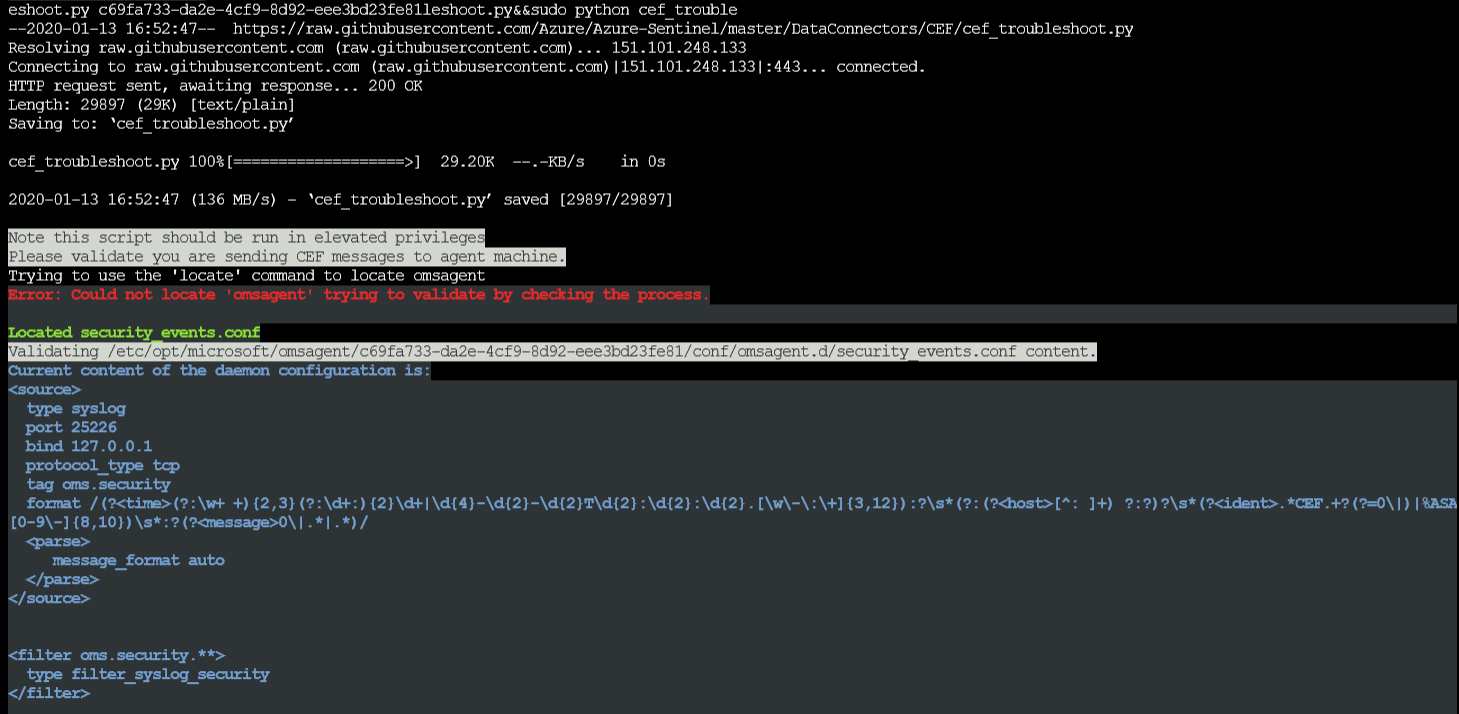
1. Create a new browser page and navigate to the Sentinel and enable Syslog and other Syslog facilities (Log Analytics Workspace – Advance settings – Data – Syslog)

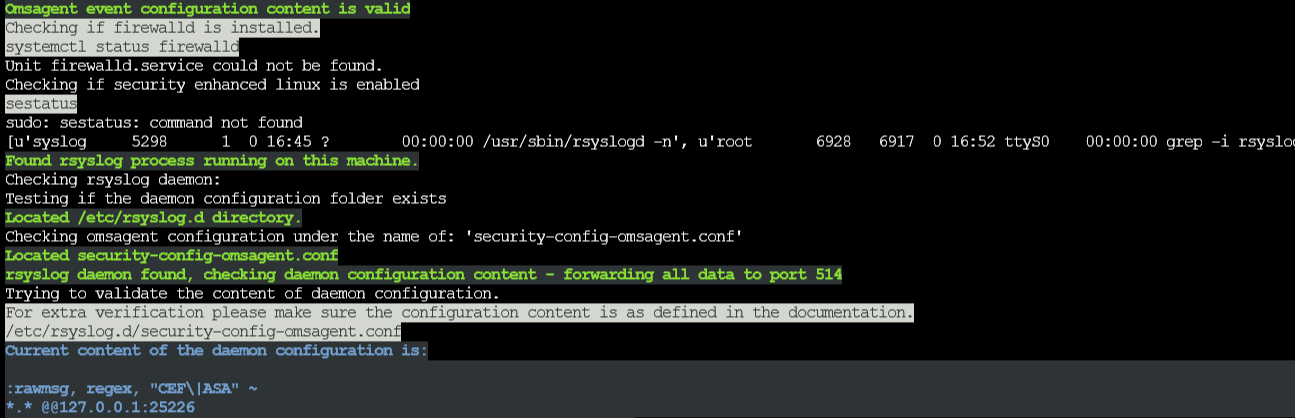


1. Open the CEF Connector in Sentinel Data Connector page  
     
   
2. Click the Open Connector Page button  
     
   
3. Click the copy/Paste icon to copy the Python script to the clipboard
4. Paste in the Virtual Machine cli the python OMSAgent Install script command  
     
   
5. Wait until the Python script completes  
     
    
6. Now that the installation is complete, we need to confirm that everything is working as expected.
7. We need to run the Python Troubleshooting script to create Mock log events for us to query in Sentinel.

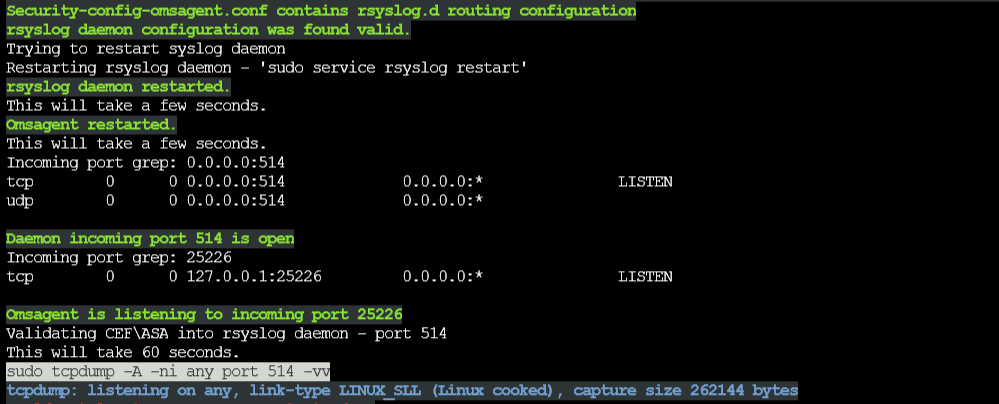


1. Copy and paste the Python command from the copy/paste icon and paste it in the cli of the virtual machine.

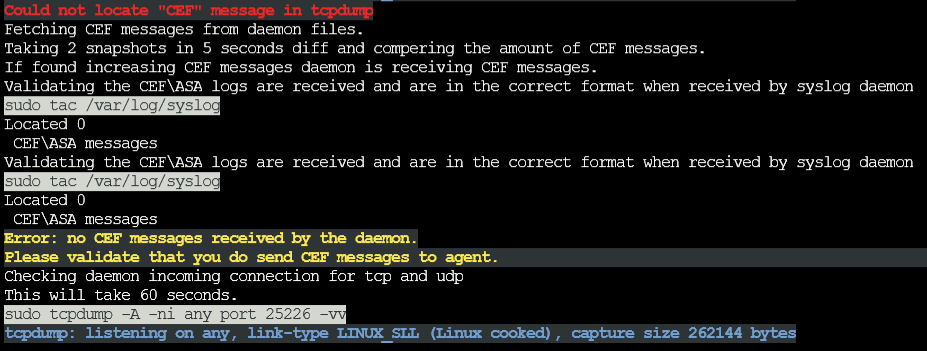
  
This confirm the regexp expression has been installed on the agent to parse CEF message on local4



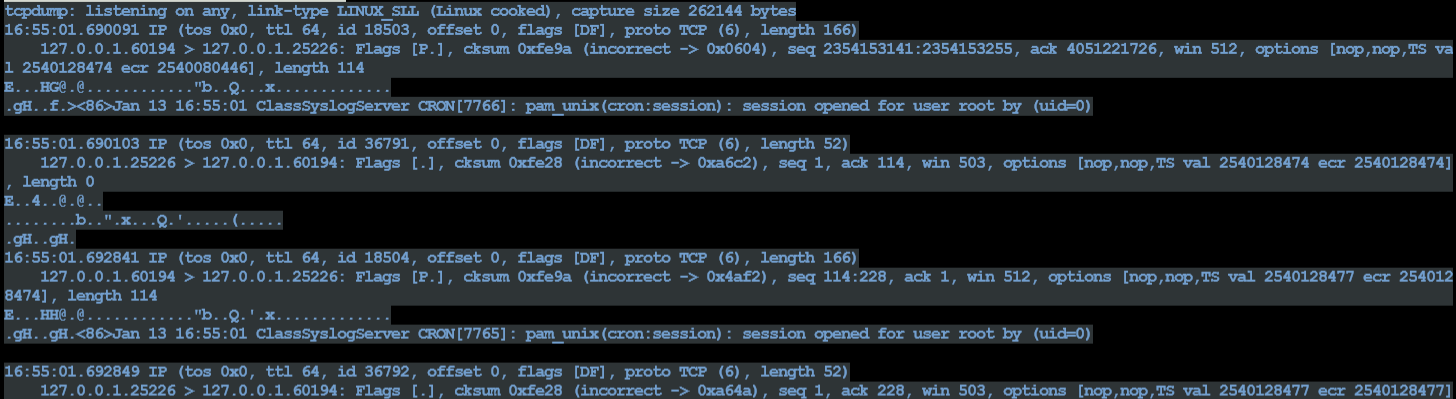
This confirms that the Syslog filter for ASA/CEF has been created



This validates that syslog server is listening and the OMSAgent is also up and running

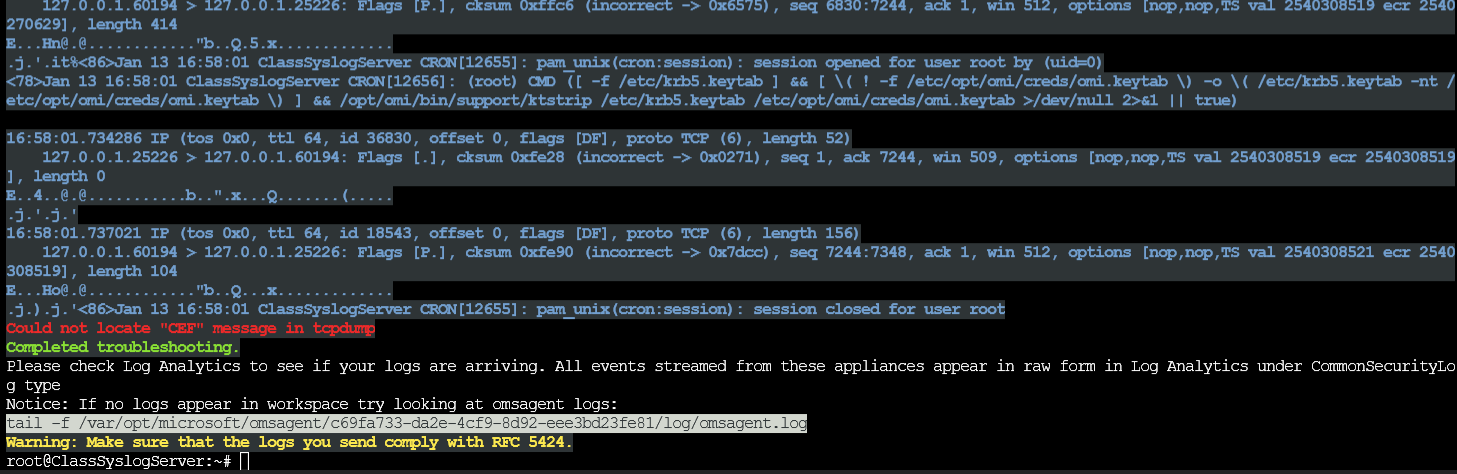


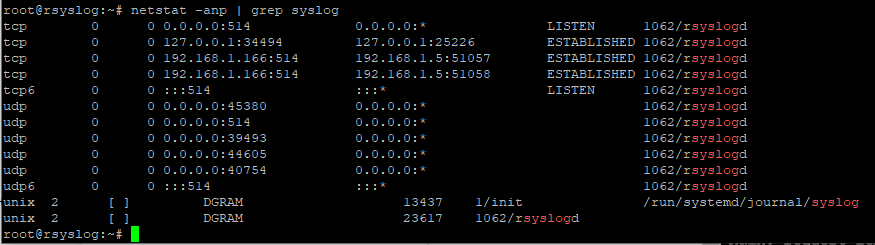
This means no logs from the external devices is being received by the syslog server



These are normal syslog host syslog logs, these are not the ones we are looking for



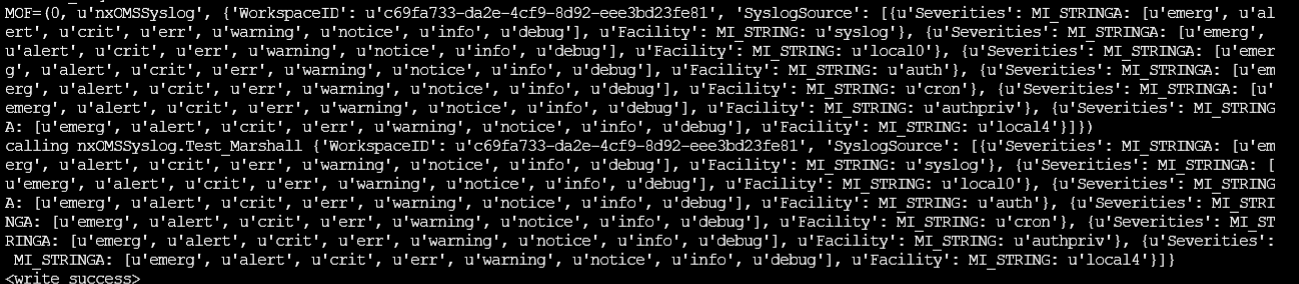
  
The Python script sent MOCK logs to Azure for testing

1. What do we need to check to confirm that everything is working correctly?  
   a. Is the syslog server started and connected to the OMSAgent  
     
   

b. Is the OMSAgent filer file present and populated  
  


c. Does the OMSAgent have the solution to collect syslogs? Run the following command which will cause the OMSAgent to fetch a update from the LAW

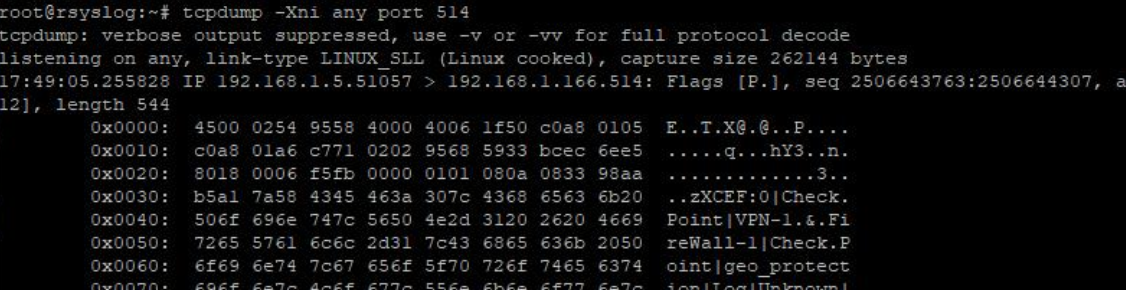
sudo su omsagent -c 'python /opt/microsoft/omsconfig/Scripts/PerformRequiredConfigurationChecks.py'



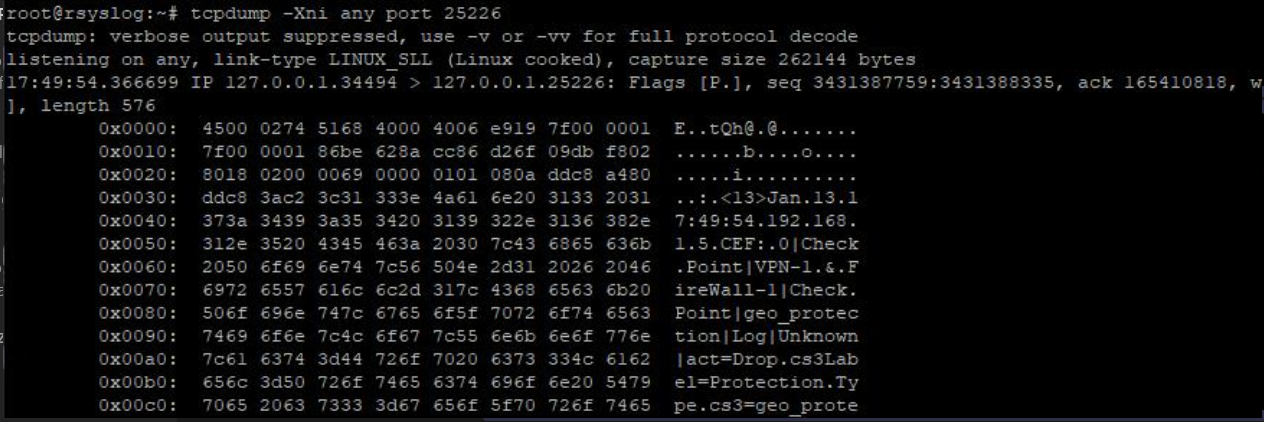
Examine the output and look for keywords Syslog, Info0, and info4

1. Tcpdump can provide details

root@ClassSyslogServer:/etc/rsyslog.d# tcpdump -Xni any port 514



root@ClassSyslogServer:/etc/rsyslog.d# tcpdump -Xni any port 25226



1. Open the Log Analytics Workspace and query CommonSecurityLog

