

ESET Tech Center

Knowledgebase > ESET PROTECT On-prem > Connecting ESET PROTECT to Microsoft Sentinel

Connecting ESET PROTECT to Microsoft Sentinel

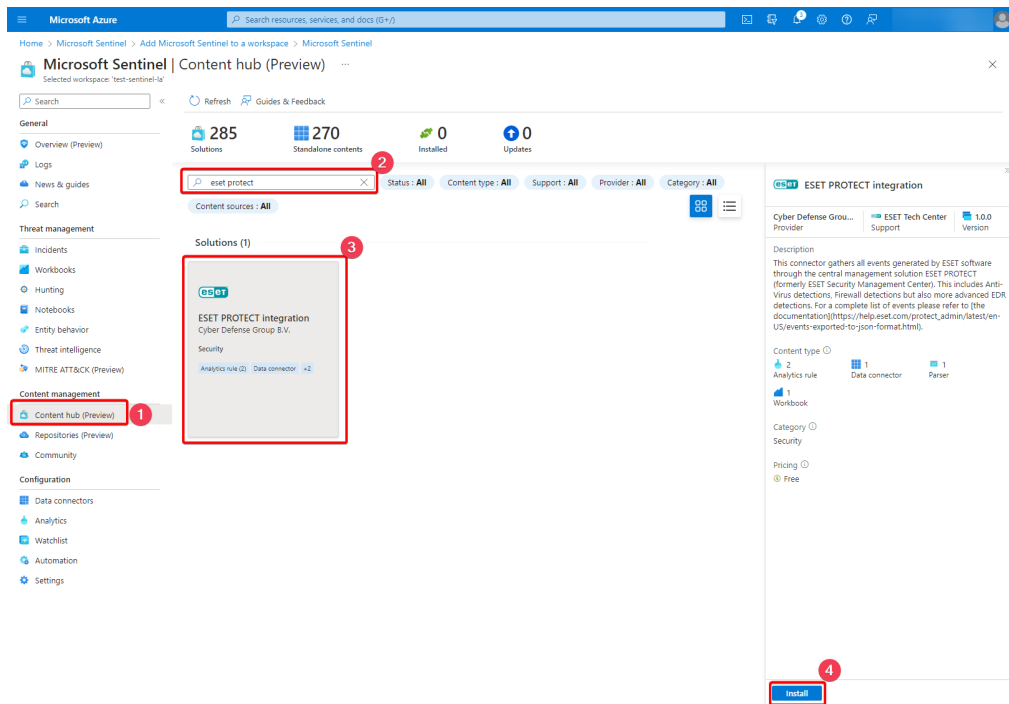
Mitchell | ESET Nederland - 2023-03-23 - Comments (0) - ESET PROTECT On-prem

Prerequisites:

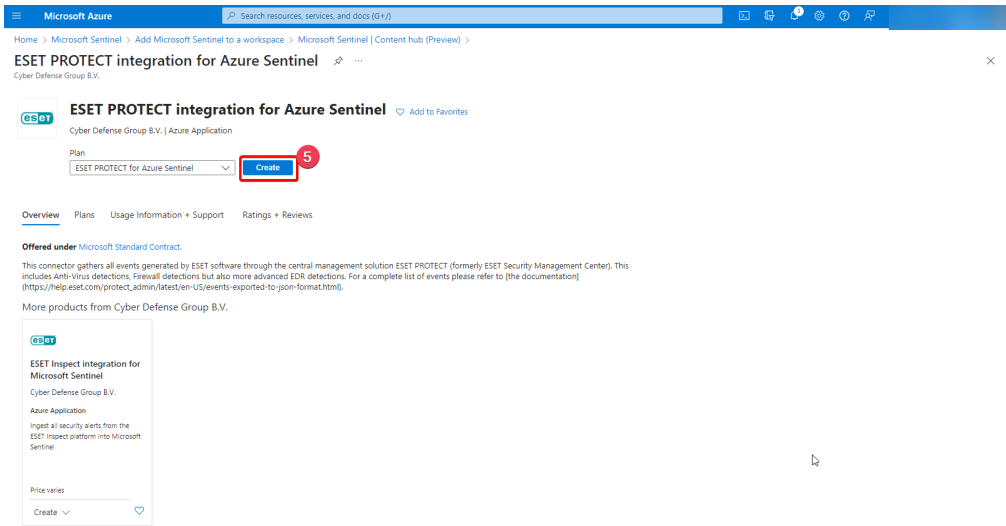
- ESET PROTECT installed
- Microsoft Sentinel
- A Linux server

Deploy ESET PROTECT integration to Microsoft Sentinel

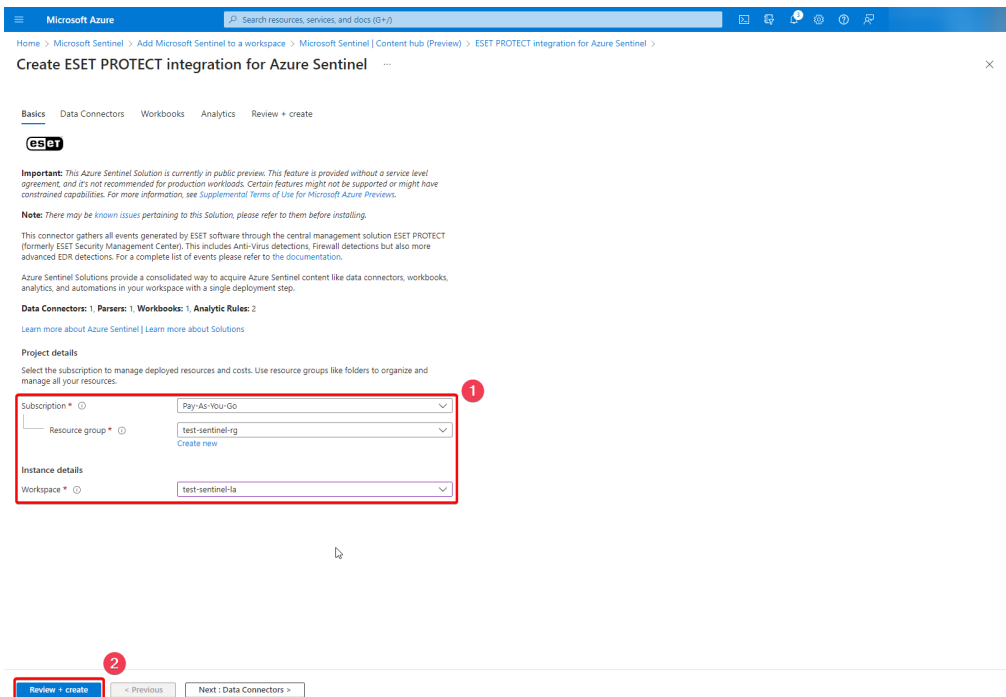
1. Navigate to Microsoft Sentinel > Content Hub
2. Search for ESET PROTECT
3. Select the ESET PROTECT integration by Cyber Defense Group B.V.
4. Click on “install”



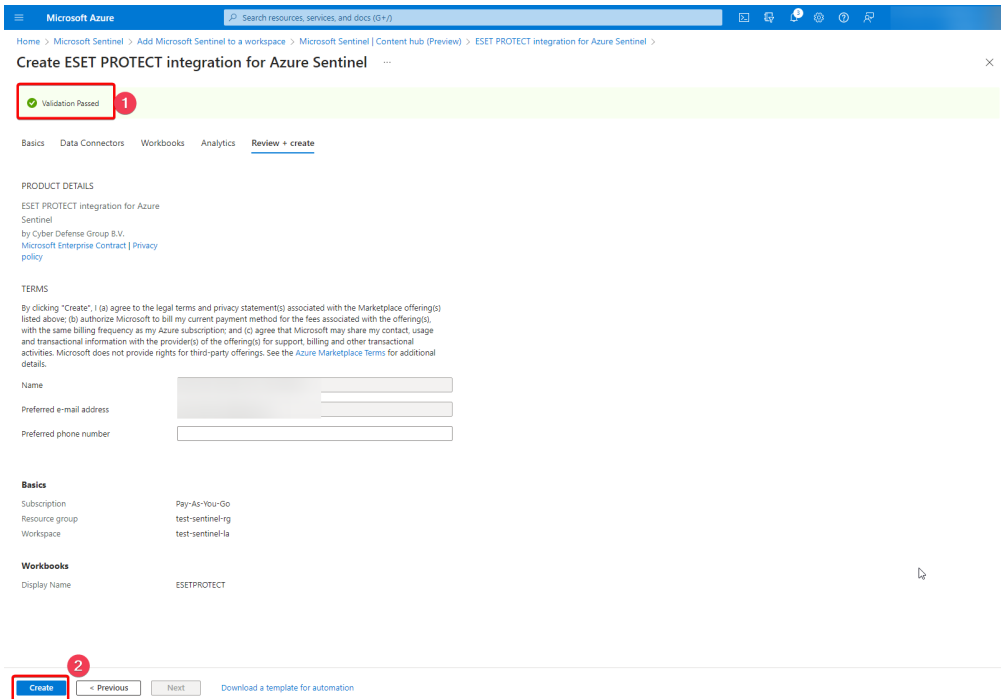
5. Click “create” in the next window:



6. Select the appropriate Log Analytics workspace to deploy the integration to and click “review + create”



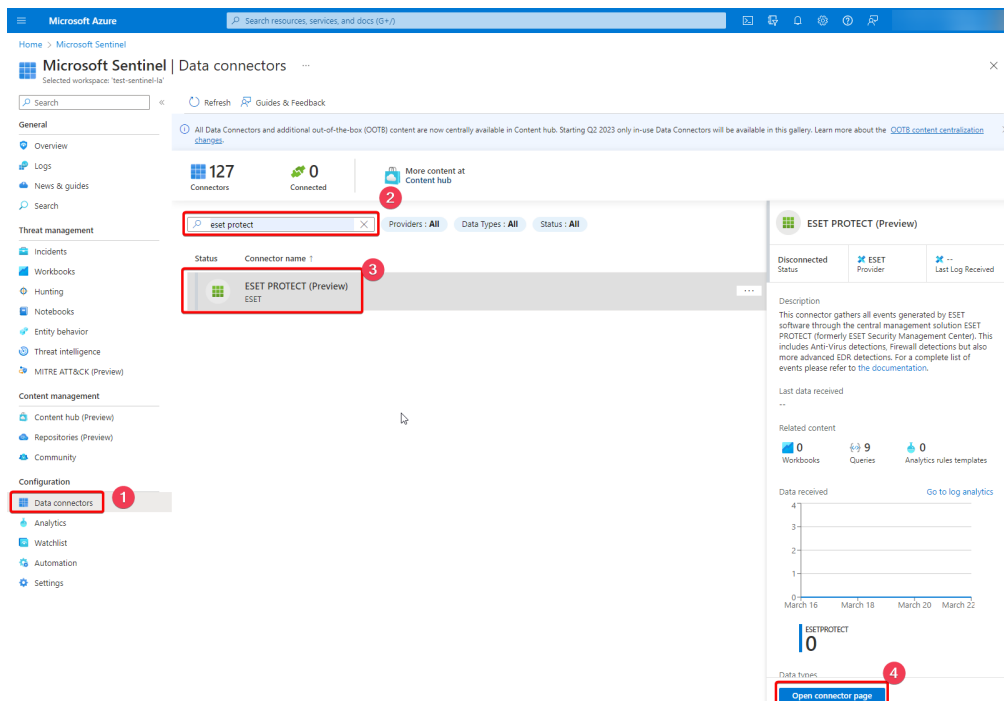
7. After the validation has passed, click “create” to start the deployment.



Configure ESET PROTECT to send events to Microsoft Sentinel

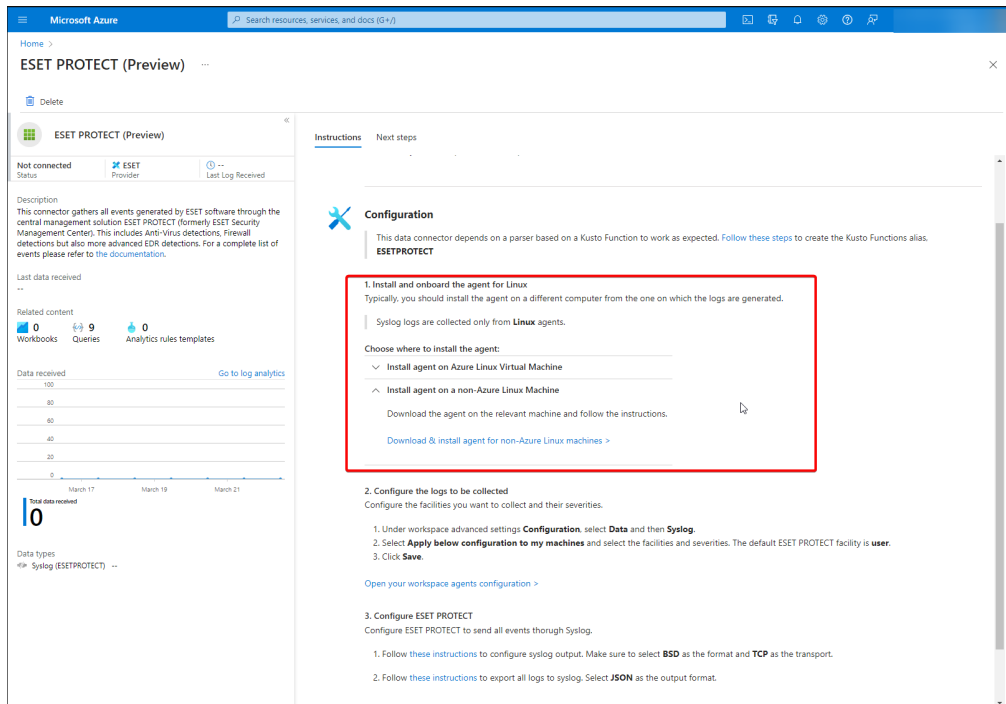
Install OMS-Agent

1. After deploying the solution you can find the "ESET PROTECT (Preview) Data Connector" in the Data connectors section:

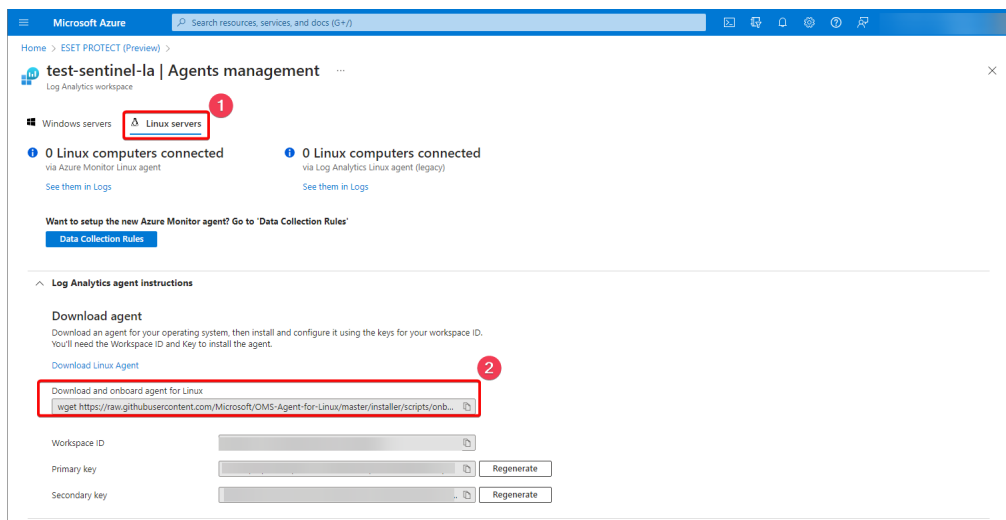


2. After opening the connector page, you will find the instructions to install the Log

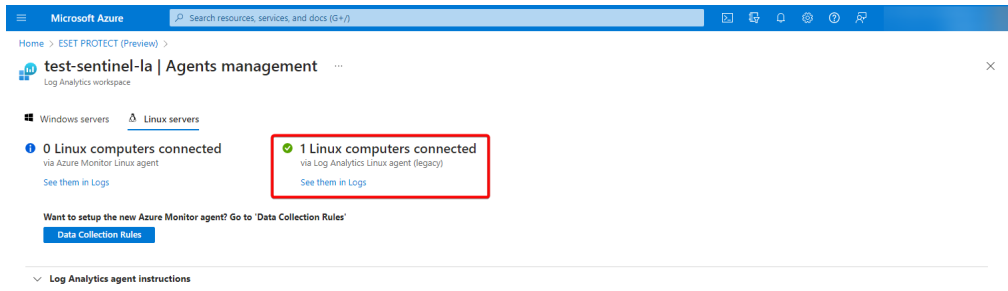
Analytics agent, because Syslog is only collected by the Linux agent, you will have to install the agent on a linux machine. (for example, the ESET PROTECT Server)



3. Download & install the agent using the command provided:

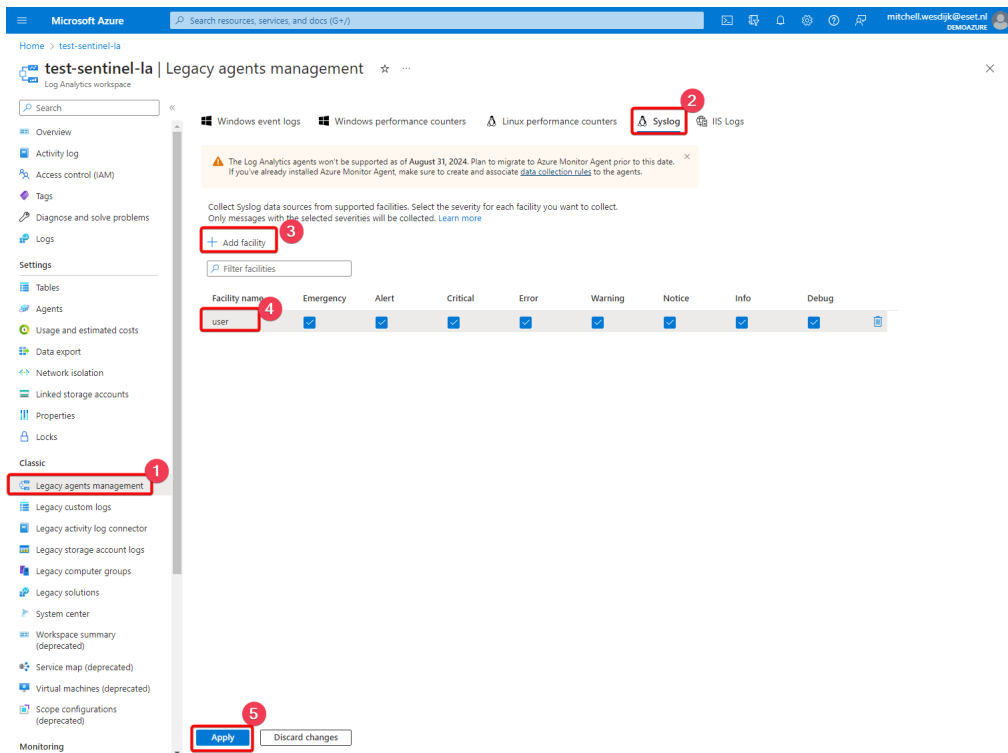


4. After installing the agent the Agents management overview should report that 1 Linux computer is connected:



Configure OMS-Agent to collect syslog data

1. Open the Log Analytics workspace
2. navigate to “Legacy Agent Management” > Syslog
3. Click on “add facility”
4. select the facility name “user”
5. save the changes by clicking “apply”



6. Note: If you installed the OMS-agent on a different computer, you will need to do some additional config because the OMS agent only listens on 127.0.0.1 by default.

1. change the bind address in the following file/etc/opt/microsoft/omsagent/conf/omsagent.d/syslog.conf

```
/etc/opt/microsoft/omsagent/conf/omsagent.d/syslog.conf
<source>
  type syslog
  port 25224
  bind 0.0.0.0
  protocol_type udp
  tag oms.syslog
</source>

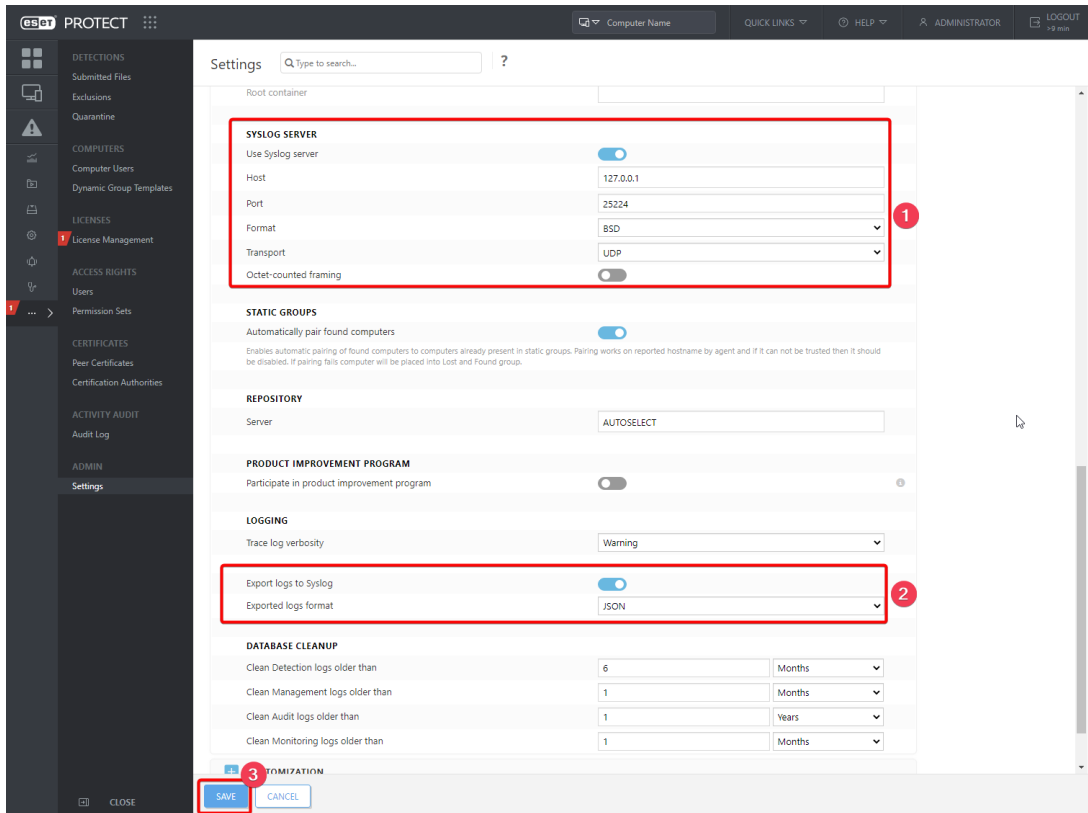
<filter oms.syslog.**>
  type filter_syslog
</filter>
```

2. restart the agent

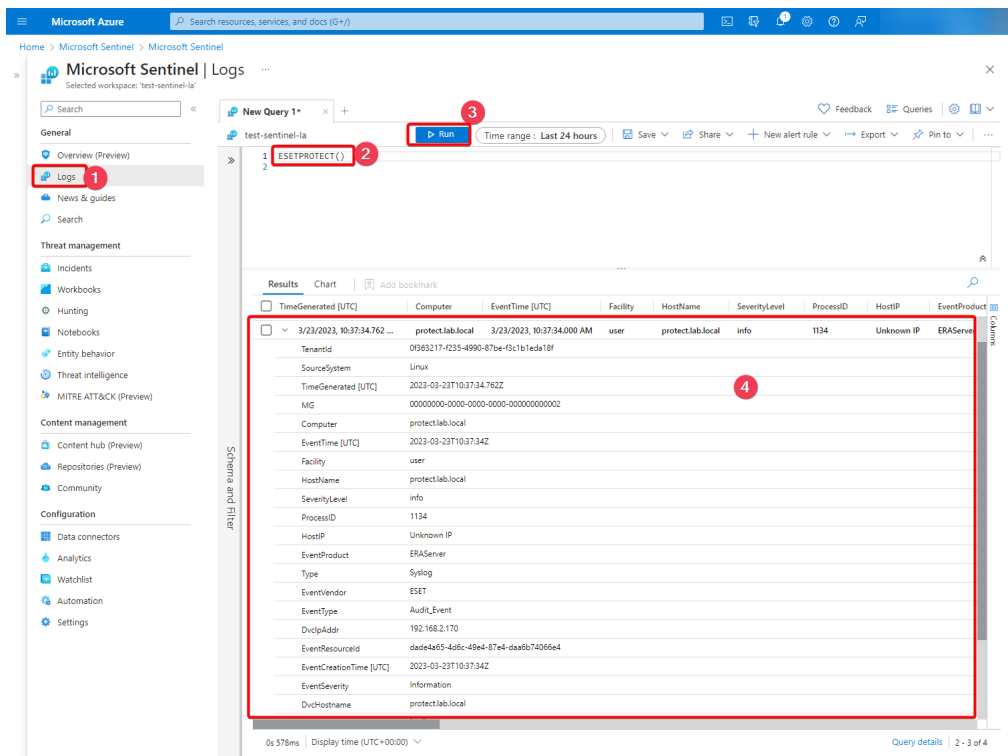
```
/opt/microsoft/omsagent/bin/service_control restart
```

Configure ESET PROTECT to export syslog data to the OMS Agent.

7. Login to ESET PROTECT
8. Navigate to more > Admin > Settings
9. Configure the syslog settings based on the screenshot below:



1. All ESET PROTECT event data should now be sent to Sentinel, you can generate some audit events by logging out and back in to ESET PROTECT for example. confirm that the events reached Sentinel by running the following query:

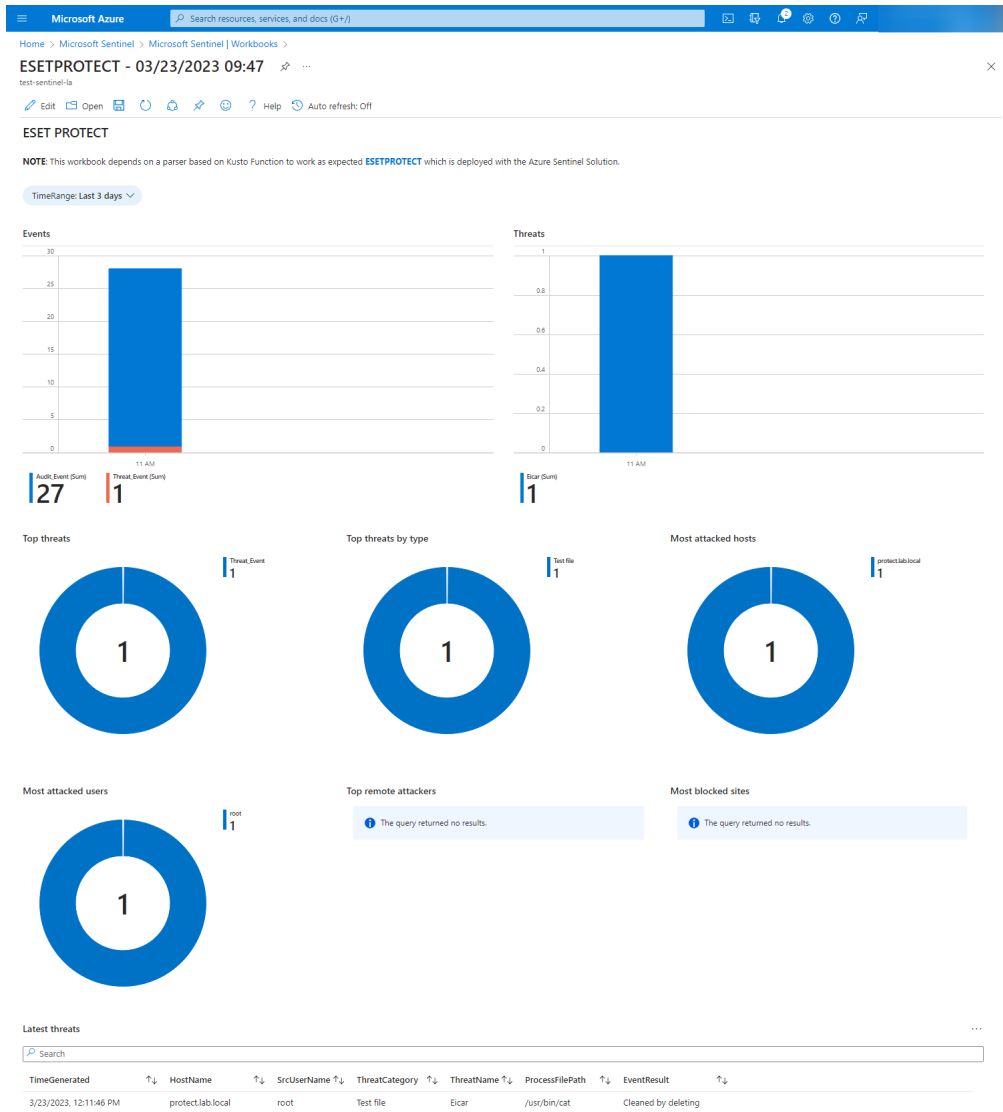


2. Alternatively you can open the workbook that was created after deploying the

solution:

The screenshot shows the Microsoft Sentinel Workbooks interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The main header displays 'Microsoft Sentinel | Workbooks' and 'Selected workspace: test-sentinel-lq'. Below the header, there are statistics: 1 Saved workbook, 142 Templates, and 0 Updates. A 'My workbooks' section is highlighted with a red box and a '2' in a red circle. Below this, a table lists workbooks with columns for 'Workbook name' and 'Content source'. A specific workbook, 'ESETPROTECT - 03/23/2023 09:47', is highlighted with a red box and a '3' in a red circle. The 'Content source' for this workbook is 'Custom'. On the left sidebar, the 'Workbooks' menu item is highlighted with a red box and a '1' in a red circle. On the right, a details panel for the selected workbook shows 'Connected Status' and 'Description: Customer defined workbook'. At the bottom right, a 'View saved workbook' button is highlighted with a red box and a '4' in a red circle, next to a 'Delete' button.

Workbook name	Content source
ESETPROTECT - 03/23/2023 09:47	Custom



Enable analytics rules to create incidents from ESET detections

1. Navigate to Microsoft Sentinel > Configuration > Analytics
2. Select the 2 ESET analytic rules
3. Click "Enable"

The screenshot shows the Microsoft Sentinel Analytics interface. On the left sidebar, the 'Data connectors' section is expanded, and 'Analytics' is highlighted with a red box and a '1' callout. In the main content area, a table of active rules is displayed. The second rule, 'Threats detected by...', is selected with a blue checkmark and a red box and a '2' callout. Above the table, the 'Enable' button is highlighted with a red box and a '3' callout. A callout box on the right side of the screen contains the text: '2 analytics rules selected. Select one of the action buttons from the top command bar.'

Severity	Name	Rule type	Status	Tactics	Technique
<input type="checkbox"/>	Low	Website blocked b...	Scheduled	Disabled	Execution
<input checked="" type="checkbox"/>	Low	Threats detected b...	Scheduled	Disabled	Execution
<input type="checkbox"/>	High	Advanced Multista...	Fusion	Enabled	+8

4. Triggering threat detections will now create an incident:

The screenshot shows the Microsoft Sentinel Incidents interface. On the left sidebar, the 'Incidents' section is highlighted with a red box and a '1' callout. In the main content area, a table of incidents is displayed. The first incident, 'Threats detected by...', is highlighted with a red box and a '2' callout. A callout box on the right side of the screen contains the text: 'View full details' with a red box and a '3' callout.

Severity	Incident ID	Title	Alerts	Product names	Cr
Low	1	Threats detected by...	1	Microsoft Sentinel	09

Microsoft Azure Search resources, services, and docs (G+)

Home > Incident ... Incident ID: 1

Refresh Delete incident Tasks (Preview)

Switch to the new, improved incident page (currently in preview) Try the new experience

Threats detected by ESET

Incident ID: 1

Unassigned Owner New Status Low Severity

Description
Escalates threats detected by ESET.

Alert product names
Microsoft Sentinel

Evidence
1 Events 1 Alerts 0 Bookmarks

Last update time: 03/23/23, 12:17 PM
Creation time: 03/23/23, 12:17 PM

Entities (3)
protect 192.168.2.170 3395836CE81F2B7...
View full details >

Tactics and techniques
Execution (0)

Incident workbook
Incident Overview

Analytics rule
Threats detected by ESET

Tags
+

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insigh...

Investigate Actions

Timeline Similar incidents (Preview) Alerts Bookmarks Entities Comments

Search Timeline content: All Severity: All Tactics: All

Mar 23 12:11 PM Threats detected by ESET
Low | Detected by Microsoft Sentinel | Tactics: Execution

Threats detected by ESET

Description
Escalates threats detected by ESET.

Severity: Low Status: New

Events
Link to LA Product name: Microsoft Sentinel

Entities (3)
protect 192.168.2.170 3395836CE81F2B73...

Tactics and techniques
Execution (0)

System alert ID: 1dddbefb6-8628-e1c3-7b16... Rule name: Threats detected by ESET

Last update time: 03/23/23, 12:17 PM Updates: 0

Start time: 03/23/23, 12:11 PM End time: 03/23/23, 12:11 PM

Alert link: --