SUSE Security (formerly NeuVector)

Integrating SUSE Security with Microsoft Sentinel

Getting Started

SUSE Security (formerly NeuVector)
Microsoft Sentinel

Derek Reinhardt, Alliance Solutions Architect (SUSE)

Integrating SUSE Security with Microsoft Sentinel

Getting Started

Date: 2025-03-03

Summary

This guide provides a step-by-step process for integrating SUSE Security with Microsoft Sentinel, enabling a unified security approach. It covers resource creation through applying a base configuration. This integration allows for automated responses to threats and streamlines security operations.

Disclaimer

Documents published as part of the series SUSE Technical Reference Documentation have been contributed voluntarily by SUSE employees and third parties. They are meant to serve as examples of how particular actions can be performed. They have been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. SUSE cannot verify that actions described in these documents do what is claimed or whether actions described have unintended consequences. SUSE LLC, its affiliates, the authors, and the translators may not be held liable for possible errors or the consequences thereof.

Contents

1 Introduction

Security is becoming increasingly important for users and administrators alike. Unfortunately, many tools have unique interfaces or interactions that make getting an overview of the environment more difficult. This guide introduces a solution for unifying the security approach by integrating SUSE Security with Microsoft Sentinel. Integrating SUSE Security with Microsoft Sentinel provides a comprehensive overview of the environment. It also enables new ways to interact with security using Microsoft Security Copilot.

SUSE Security (https://www.suse.com/products/rancher/security/) ↗ (formerly NeuVector) is a fully open source, zero trust container security platform. SUSE Security offers enhanced runtime security, advanced threat detection, and expanded compliance features. It continuously scans throughout the container lifecycle. It can remove security roadblocks. Bake in security policies at the start to maximize developer agility.

Microsoft Sentinel (https://azure.microsoft.com/en-us/products/microsoft-sentinel) ↗ is a scalable, cloud-native security information and event management (SIEM) that delivers an intelligent and comprehensive solution for SIEM and security orchestration, automation, and response (SOAR). Microsoft Sentinel provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise.

By combining these two best-in-class offerings, you can receive alerts and automatic responses to security threats, including intrusions or other risks, for workloads running in Azure, whether VM or Kubernetes-based.

1.1 Scope

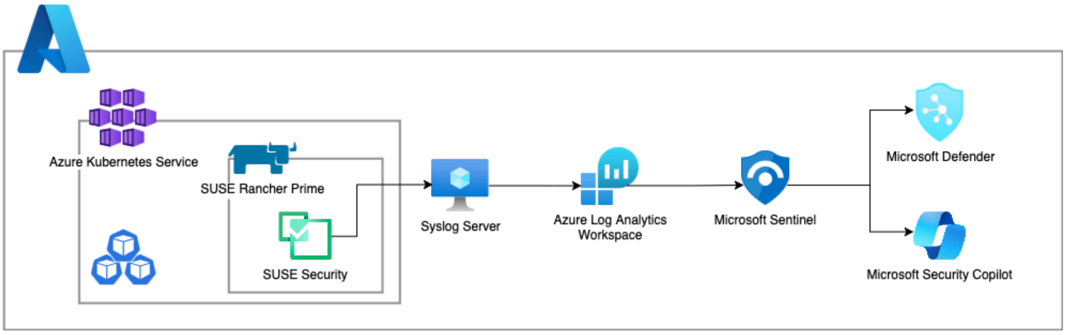
This guide will walk you through the process of deploying and configuring SUSE Security. It will also cover how to set up SUSE Security to export log data into Azure Log Analytics Workspace, which can be used in Microsoft Sentinel for monitoring across your entire Azure domain.

1.2 Audience

This guide is designed for System Administrators, SecOps, IT Operations, or anyone interested in creating a unified security view for an Azure environment, encompassing both VM and Kubernetes-based workloads.

2 Technical Overview

This guide demonstrates how to integrate SUSE Security with Microsoft Sentinel. This is accomplished by exporting data from SUSE Security into a Syslog server and then collecting it into an Azure Log Analytics Workspace. This data will then be used in Microsoft Sentinel. The following diagram provides a basic overview of the data flow.



2.1 Components and Tools

SUSE Rancher Prime

SUSE Rancher Prime is the unified cloud-native platform helping teams manage their Kubernetes from infrastructure to applications. 100% open source, SUSE Rancher streamlines cluster deployment, offering centralized authentication, access control and observability across your deployments anywhere.

SUSE Security

SUSE Security is the only fully open source, zero trust container security platform. SUSE Security offers enhanced runtime security, advanced threat detection, and expanded compliance features. Continuously scan throughout the container lifecycle. Remove security roadblocks. Bake in security policies at the start to maximize developer agility.

Azure Log Analytics Workspace

Log Analytics workspace is a data store into which you can collect any type of log data from all of your Azure and non-Azure resources and applications. Workspace configuration options let you manage all of your log data in one workspace to meet the operations, analysis, and auditing needs of different personas in your organization.

Microsoft Sentinel

Microsoft Sentinel is a scalable, cloud-native security information and event management (SIEM) that delivers an intelligent and comprehensive solution for SIEM and security orchestration, automation, and response (SOAR). Microsoft Sentinel provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise.

2.2 Process Overview

Getting started with integration SUSE Security and Microsoft Sentinel is fairly easy. The basic process:

1. Create an Azure Resource Group
2. Use SUSE Rancher Prime to deploy an Azure Kubernetes cluster
3. Create a VM to act as a Syslog server
4. Create an Azure Log Analytics Workspace to store log data
5. Configure the data from SUSE Security to flow into the Azure Log Analytics Workspace
6. Create alerts and actions in Microsoft Sentinel based on the data

3 Prerequisites

This guide aims to be comprehensive, but concise. To follow along, ensure you have the following:

- An active Azure subscription with permissions to deploy resources
- A registered instance of SUSE Rancher Prime Suite or higher

4 Procedure

4.1 Infrastructure

To create this integration, several resources need to be created in Azure. This includes an Azure Kubernetes (AKS) cluster where workloads will be running and a virtual machine (VM) to act as a Syslog server. An Azure Log Analytics Workspace and an instance of Microsoft Sentinel are needed for log data storage and processing. Additionally, one or more Security Compute Units (SCUs) are required to integrate Microsoft Sentinel further for use with Azure Security Copilot.

A separate Azure Resource Group is recommended to hold resources created throughout this guide. A new Resource Group can be created in the Azure Portal or through the Azure CLI. This guide will use the South Central US region in commands, however any region can be used.

```
az group create --name sentinel-demo --location southcentralus
```

The next step is to create an Azure Virtual Network. It will need two different subnets in the network. A larger one for the AKS resources and workloads and a much smaller one to hold the syslog server.

1. Create the Virtual Network

   ```
   az network vnet create -g sentinel-demo -n demo-vnet --address-prefix 10.10.0.0/22
   ```

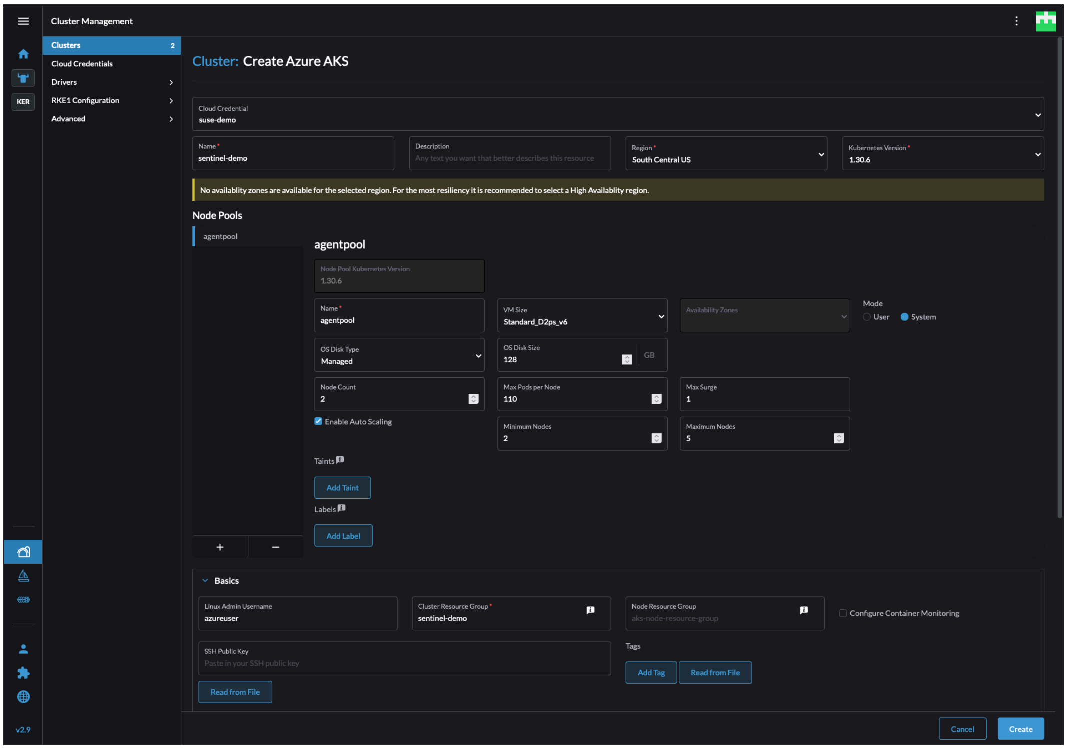
2. Create the larger subnet

   ```
   az network vnet subnet create -g sentinel-demo --vnet-name demo-vnet --name aks-
   subnet --address-prefixes "10.10.0.0/23"
   ```

3. Create the smaller subnet

   ```
   az network vnet subnet create -g sentinel-demo --vnet-name demo-vnet --name syslog-
   subnet --address-prefixes "10.10.3.240/28"
   ```

With the network prepared, the next step is to create an AKS cluster. The easiest method is through SUSE Rancher Prime. From the Home page select *Create* above the cluster list, then select *Azure AKS*. Enter values for the requested fields and click *Create*. SUSE Rancher Prime will create the cluster inside of Azure and deploy the Rancher agent on the cluster to allow for management through the Rancher portal.



Cluster: Create Azure AKS

Cloud Credential: suse-demo

Name *: sentinel-demo

Description: Any text you want that better describes this resource

Region *: South Central US

Kubernetes Version *: 1.30.6

No availablity zones are available for the selected region. For the most resiliency it is recommended to select a High Availablity region.

Node Pools

agentpool

Node Pool Kubernetes Version: 1.30.6

Name *: agentpool

VM Size: Standard_D2ps_v6

Availability Zones

Mode: ○ User ● System

OS Disk Type: Managed

OS Disk Size: 128 GB

Node Count: 2

Max Pods per Node: 110

Max Surge: 1

☑ Enable Auto Scaling

Minimum Nodes: 2

Maximum Nodes: 5

Basics

Linux Admin Username: azureuser

Cluster Resource Group *: sentinel-demo

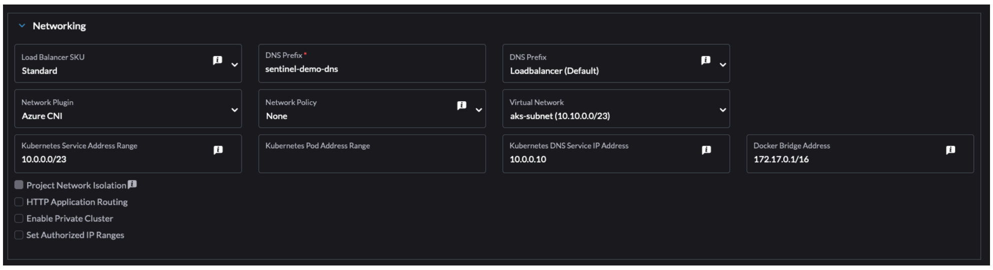
Node Resource Group: aks-node-resource-group

□ Configure Container Monitoring

SSH Public Key: Paste in your SSH public key

Note

This guide assumes Azure CNI networking is used. It is the recommended CNI from Azure for use with AKS clusters.



Networking

Load Balancer SKU: Standard

DNS Prefix *: sentinel-demo-dns

DNS Prefix: Loadbalancer (Default)

Network Plugin: Azure CNI

Network Policy: None

Virtual Network: aks-subnet (10.10.0.0/23)

Kubernetes Service Address Range: 10.0.0.0/23

Kubernetes Pod Address Range

Kubernetes DNS Service IP Address: 10.0.0.10

Docker Bridge Address: 172.17.0.1/16

□ Project Network Isolation

□ HTTP Application Routing

□ Enable Private Cluster

□ Set Authorized IP Ranges

Note

Existing clusters are supported, but must be imported into SUSE Rancher to deploy SUSE Security. See the SUSE Rancher documentation (https://ranchermanager.docs.rancher.com/how-to-guides/new-user-guides/kubernetes-clusters-in-rancher-setup/register-existing-clusters) ↗ for steps to import an existing cluster.

Important

If the network was not created as a part of this guide, then a small, separate network must be created to contain the Syslog server. The smallest network segment allowed by Microsoft Azure is /29.

```
az network vnet create -g sentinel-demo -n demo-vnet --address-prefix 172.16.0.0/29
 --subnet-name default --subnet-prefixes 172.16.0.0/29
```

This network must be peered with the network containing the AKS cluster to allow for the Syslog server to receive logs exported from SUSE Security.

```
# create demo-vnet to aks peering
az network vnet peering create --name syslog-to-aks-peer --vnet-name demo-vnet --
remote-vnet aks-vnet-xxxxx --resource-group sentinel-demo --allow-vnet-access --
allow-forwarded-traffic

# create aks to demo-vnet peering
az network vnet peering create --name aks-to-syslog-peer --vnet-name aks-vnet-xxxxx
 --remote-vnet demo-vnet --resource-group sentinel-demo --allow-vnet-access --
allow-forwarded-traffic
```

The next step is to create a virtual machine to act as the Syslog server. It will be placed in the smaller subnet previously created.

```
az vm create -n syslog-server -g sentinel-demo --image SUSE:sles-15-sp6:gen2:2024.11.13
 --vnet-name demo-vnet --subnet syslog-subnet --size Standard_B2s --generate-ssh-keys
```

Note

This command uses the pay-as-you-go version of SUSE Linux Enterprise Server. It can be substituted for the bring-your-own-license version as required.

The last piece of infrastructure to deploy is the Azure Log Analytics Workspace. This is used to store all of the log data sent to the Syslog server. It will be used as an intermediary between the Syslog server and Microsoft Sentinel where alerts and actions can be created.

```
az monitor log-analytics workspace create -g sentinel-demo -n demo-log-analytics
```

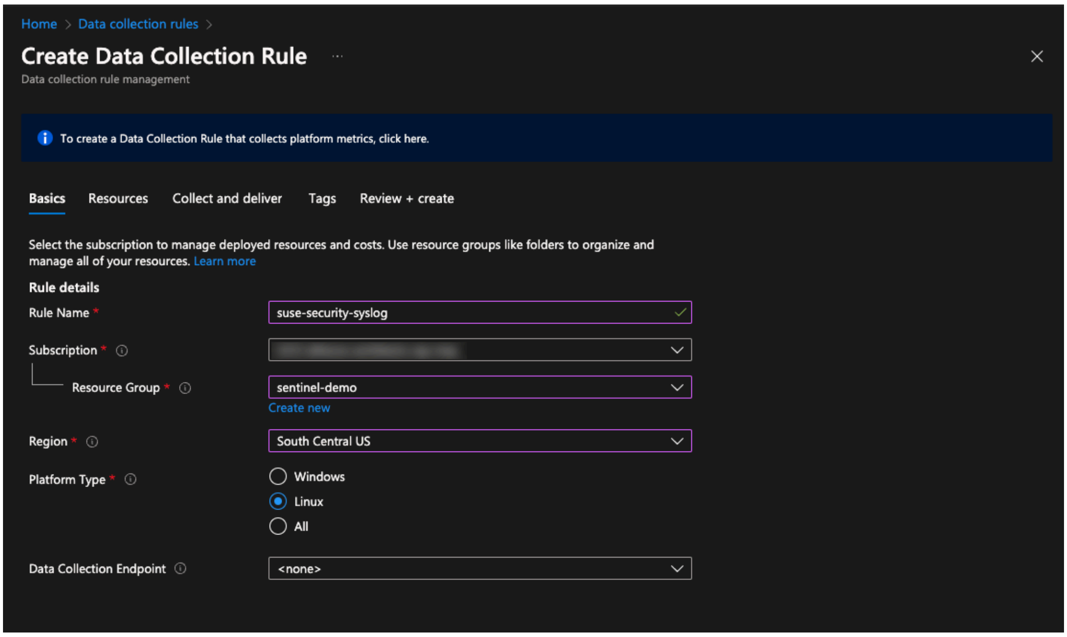
The environment is now deployed.

4.2 Configuration

This section will cover the configuration of SUSE Security and the data pipeline into Microsoft Sentinel.

4.2.1 Log Analytics Workspace

Create the necessary Data collection rule which will capture the syslog events from the VM and store them in the Log Analytics Workspace. In the Azure Portal search for `Data collection` rules in the top search box. This will bring up a list of existing rules. Click *Create* near the top to make a new one. In the template that appears give the rule a name such as `suse-security-syslog`. Then select the resource group created previously. Ensure that the region matches the region used for the other resources. Set the Platform Type to `Linux` and click *Next* at the bottom.



Create Data Collection Rule

Data collection rule management

To create a Data Collection Rule that collects platform metrics, click here.

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. Learn more

Rule details

Rule Name * suse-security-syslog

Subscription * [redacted]

Resource Group * sentinel-demo

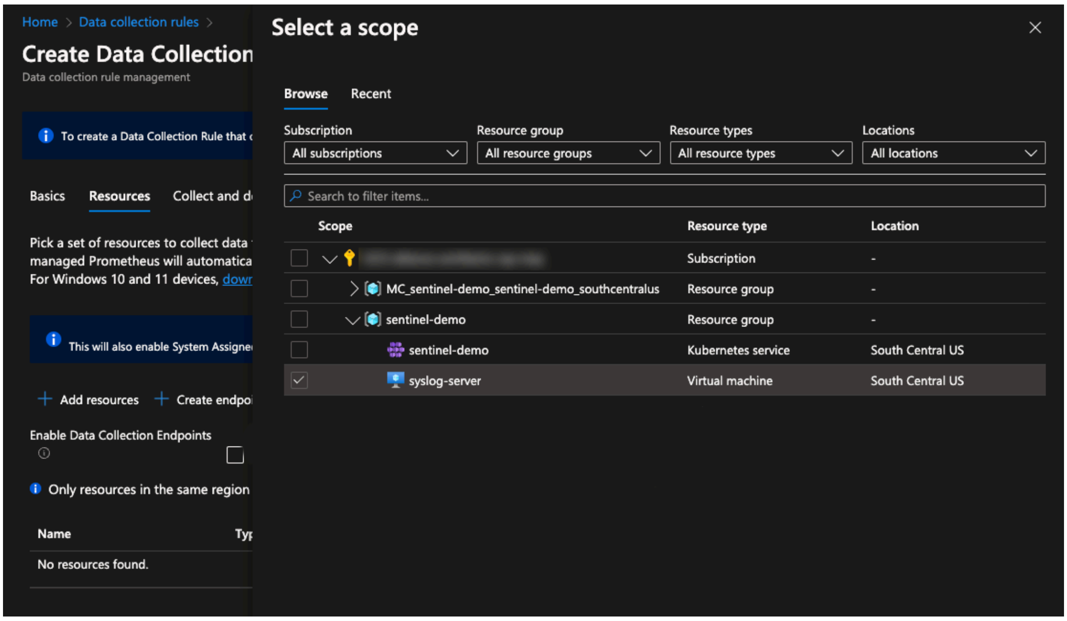
Create new

Region * South Central US

Platform Type * ○ Windows ● Linux ○ All

Data Collection Endpoint <none>

The next tab, `Resources`, allows for the selection of the systems or data producers to collect from and add into the Log Analytics Workspace. Click *Add resources*. This will open a sidebar for selecting the scope. Use the tabs to navigate to the correct resource groups. Select the syslog-server VM previously created. Then click *Apply*. This will add the server to the resources page. Click *Next* at the bottom to continue.



Home > Data collection rules >

Create Data Collection

Data collection rule management

To create a Data Collection Rule that c

Basics | Resources | Collect and d

Pick a set of resources to collect data
managed Prometheus will automatica
For Windows 10 and 11 devices, dowr

This will also enable System Assigne

+ Add resources + Create endpo

Enable Data Collection Endpoints ☐

Only resources in the same region

Name	Typ
No resources found.	

Select a scope

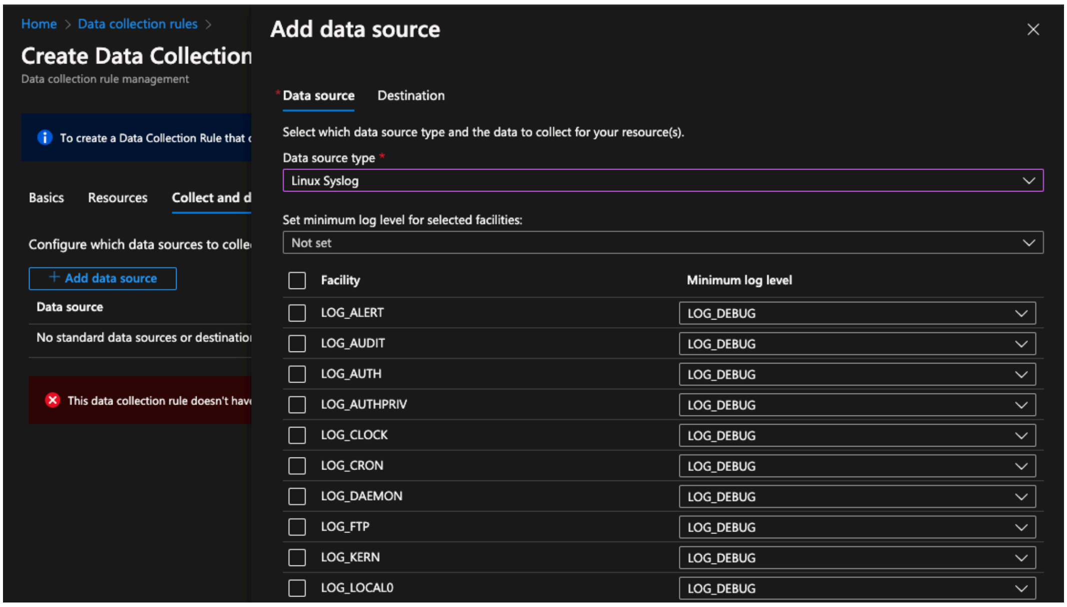
Browse | Recent

Subscription: All subscriptions
Resource group: All resource groups
Resource types: All resource types
Locations: All locations

Search to filter items...

	Scope	Resource type	Location
☐	[redacted]	Subscription	-
☐	MC_sentinel-demo_sentinel-demo_southcentralus	Resource group	-
☐	sentinel-demo	Resource group	-
☐	sentinel-demo	Kubernetes service	South Central US
☑	syslog-server	Virtual machine	South Central US

The next tab determines how Azure will attempt to collect data from the resources specified. Click *Add data source* to open another sidebar. In the first tab of the sidebar, change the Data source type to `Linux Syslog`. Then click *Next* at the bottom.



Home > Data collection rules >

Create Data Collection

Data collection rule management

To create a Data Collection Rule that c

Basics | Resources | Collect and d

Configure which data sources to colle

+ Add data source

Data source
No standard data sources or destinatio

This data collection rule doesn't hav

Add data source

Data source | Destination

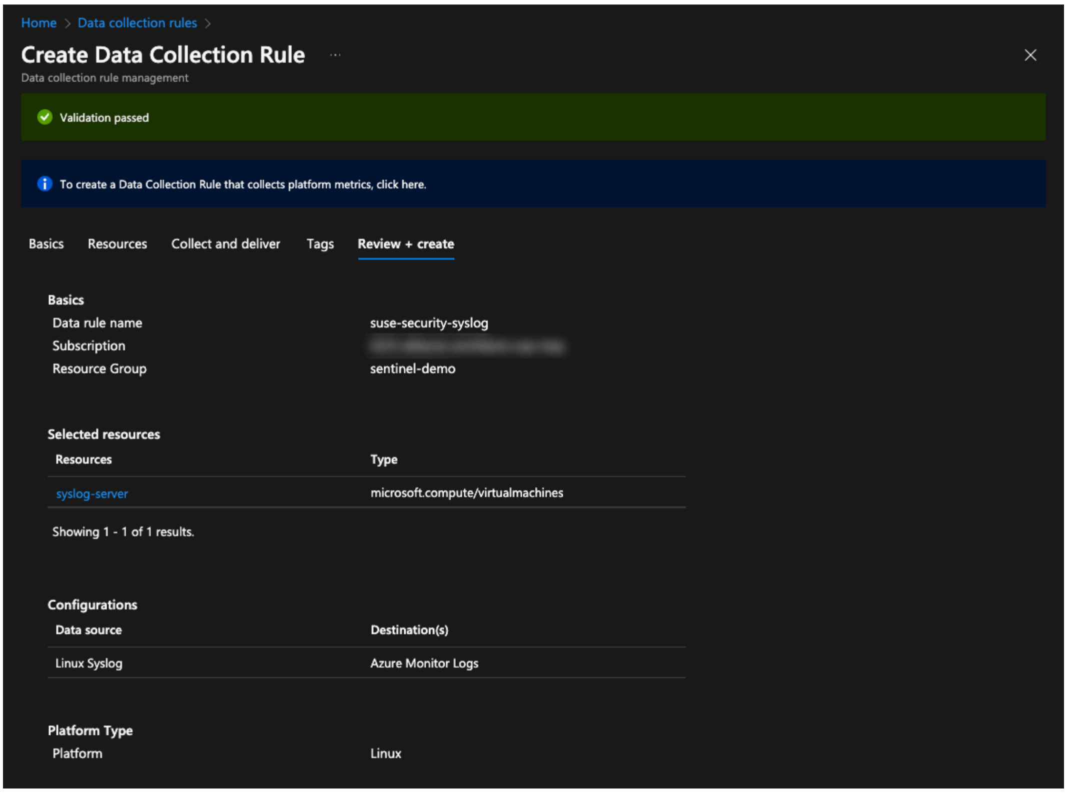
Select which data source type and the data to collect for your resource(s).

Data source type *: Linux Syslog

Set minimum log level for selected facilities: Not set

☐ Facility	Minimum log level
☐ LOG_ALERT	LOG_DEBUG
☐ LOG_AUDIT	LOG_DEBUG
☐ LOG_AUTH	LOG_DEBUG
☐ LOG_AUTHPRIV	LOG_DEBUG
☐ LOG_CLOCK	LOG_DEBUG
☐ LOG_CRON	LOG_DEBUG
☐ LOG_DAEMON	LOG_DEBUG
☐ LOG_FTP	LOG_DEBUG
☐ LOG_KERN	LOG_DEBUG
☐ LOG_LOCAL0	LOG_DEBUG

In the second tab, `Destination`, click *Add destination*. This will add a new entry to the list. For this entry change **Destination Type** to `Azure Monitor Logs`. Also change **Destination Details** to `demo-log-analytics` which is the name of the Log Analytics Workspace previously created. Click *Add data source* at the bottom, then *Review + Create*. This will show the rule being created and allow for verification that everything is correct. When ready, click *Create*.



Create Data Collection Rule

Data collection rule management

✓ Validation passed

To create a Data Collection Rule that collects platform metrics, click here.

Basics

Data rule name	suse-security-syslog
Subscription	[redacted]
Resource Group	sentinel-demo

Selected resources

Resources	Type
syslog-server	microsoft.compute/virtualmachines

Showing 1 - 1 of 1 results.

Configurations

Data source	Destination(s)
Linux Syslog	Azure Monitor Logs

Platform Type

Platform	Linux

When the deployment is complete, Log Analytics is ready to receive data from the Syslog server.

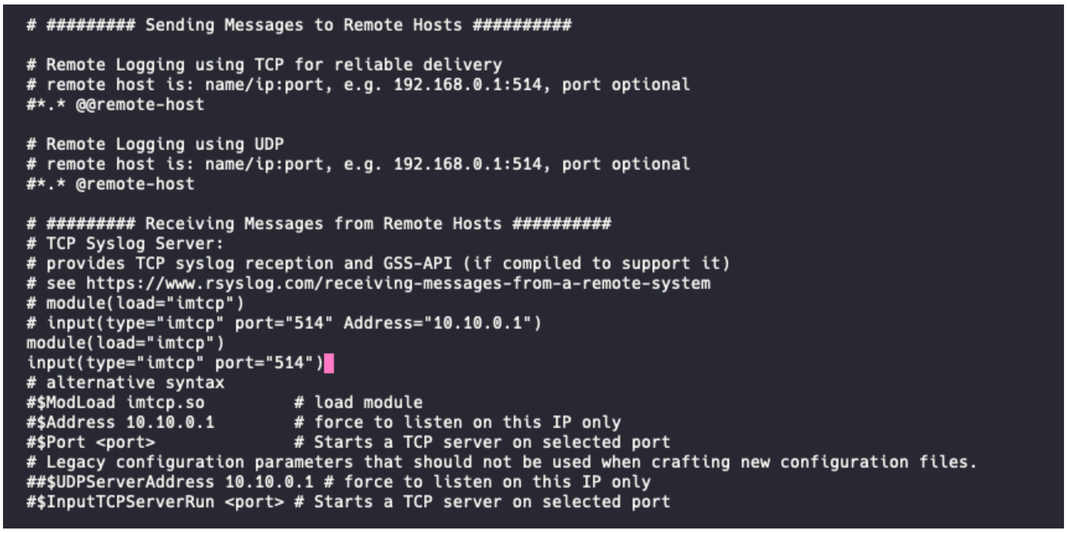
4.2.2 Syslog Server

The syslog server is used as an intermediary between the SUSE Security platform and Azure Log Analytics Workspaces. SUSE Security can export data to a syslog server, but Log Analytics Workspaces cannot act as that server. To allow the VM to act as this server, the Rsyslog service must be configured to allow for remote connections. To accomplish this, connect via SSH to the syslog-server VM created using the SSH key created during the VM creation process previously. They will be stored locally to where the command was run.

After connecting to the system, edit the file `/etc/rsyslog.d/remote.conf` and add the following two lines.

```
module(load="imtcp")
input(type="imtcp" port="514")
```

Save the file and restart the Rsyslog daemon, `sudo systemctl restart rsyslog`.



```
# ######### Sending Messages to Remote Hosts ##########

# Remote Logging using TCP for reliable delivery
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host

# Remote Logging using UDP
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @remote-host

# ######### Receiving Messages from Remote Hosts ##########
# TCP Syslog Server:
# provides TCP syslog reception and GSS-API (if compiled to support it)
# see https://www.rsyslog.com/receiving-messages-from-a-remote-system
# module(load="imtcp")
# input(type="imtcp" port="514" Address="10.10.0.1")
module(load="imtcp")
input(type="imtcp" port="514")
# alternative syntax
#$ModLoad imtcp.so          # load module
#$Address 10.10.0.1         # force to listen on this IP only
#$Port <port>               # Starts a TCP server on selected port
# Legacy configuration parameters that should not be used when crafting new configuration files.
##$UDPServerAddress 10.10.0.1 # force to listen on this IP only
#$InputTCPServerRun <port> # Starts a TCP server on selected port
```

The Syslog server is now ready to receive data from SUSE Security.

4.2.3 SUSE Security

To install SUSE Security log in to the Web UI for SUSE Rancher Prime and select the AKS cluster created at the start.

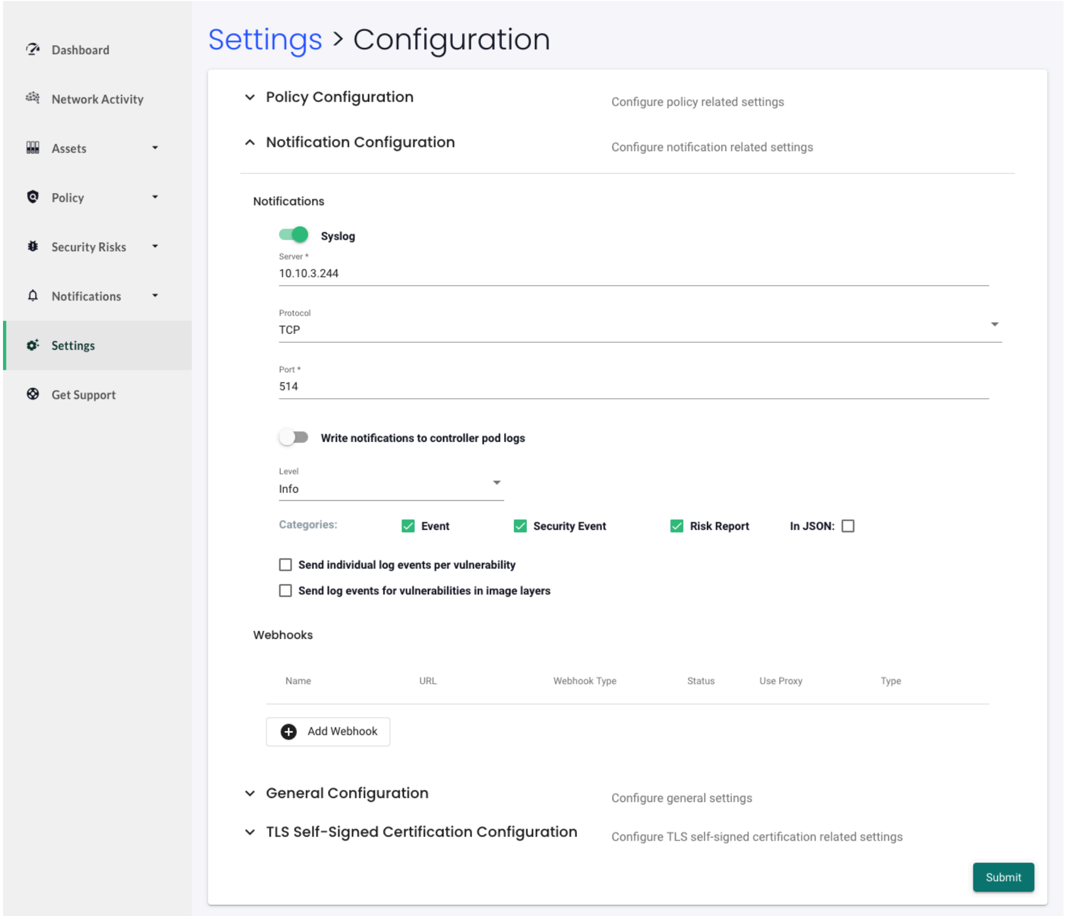
Tip

For existing cluster, they must be imported into SUSE Rancher Prime to install SUSE Security. Refer to the SUSE Rancher documentation (https://ranchermanager.docs.rancher.com/how-to-guides/new-user-guides/kubernetes-clusters-in-rancher-setup/register-existing-clusters) ↗ for guidance.

In the left sidebar after connecting to the cluster, select *Apps* and then *Charts*. This will list all available applications in the **SUSE Application Collection**. Find **SUSE Security** in the list and follow the instructions to install it into the cluster. After installation there will be a new item in the left sidebar, *Security*. Select this to connect to the SUSE Security interface.

INFO: This guide will not go over the myriad of configurations and optimizations that can be made in SUSE Security to increase overall security and compliance in an environment. Refer to the SUSE Security documentation (https://open-docs.neuvector.com/) ↗ or contact a SUSE representative for any questions.

In the sidebar select *Settings* and then the box labeled *Configuration*. Under the Notification Configuration turn on the Syslog toggle to enable export. Enter the local IP address for the syslog-server VM above, and change the Protocol from `UDP` to `TCP`. Then click *Submit*. SUSE Security will now write all events into the Syslog server, which in turn, will submit them to the Log Analytics Workspace.



Settings > Configuration

Policy Configuration — Configure policy related settings

Notification Configuration — Configure notification related settings

Notifications

● Syslog

Server *
10.10.3.244

Protocol
TCP

Port *
514

○ Write notifications to controller pod logs

Level
Info

Categories: ☑ Event ☑ Security Event ☑ Risk Report In JSON: □

□ Send individual log events per vulnerability

□ Send log events for vulnerabilities in image layers

Webhooks

Name	URL	Webhook Type	Status	Use Proxy	Type

General Configuration — Configure general settings

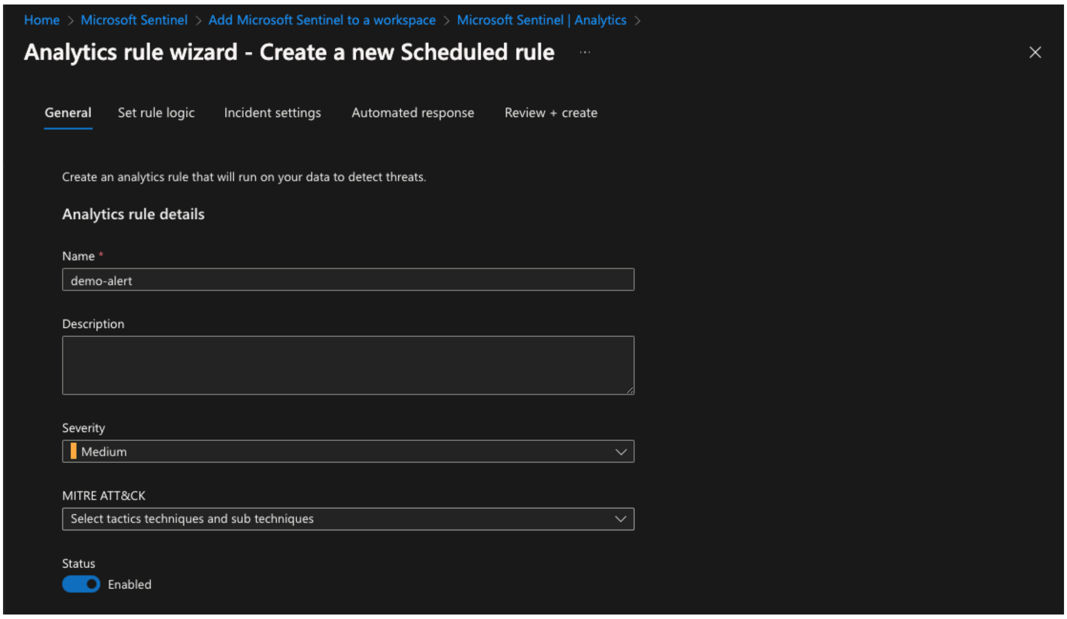
TLS Self-Signed Certification Configuration — Configure TLS self-signed certification related settings

4.2.4 Microsoft Sentinel

With the data pipeline in place it is now possible to configure Microsoft Sentinel to use data from SUSE Security. In the Azure Portal search for `Microsoft Sentinel` in the top bar. Click *Create* to add Microsoft Sentinel to the existing Log Analytics Workspace. Select the workspace created previously, then click *Add* at the bottom of the page. This will deploy Microsoft Sentinel and configure it to use the data from the Log Analytics Workspace.

After it has deployed, in the left sidebar select *Analytics*. This section allows for custom queries to search the log data and either flag them or take action according to query definition. For this guide, the rule defined will not take any action, but will raise an incident for review. Consult the Microsoft Sentinel documentation (https://learn.microsoft.com/en-us/azure/sentinel/) ↗ or contact an Azure representative to learn more about Microsoft Sentinel.

Click *Create* near the top, then select *Scheduled Query rule*. In the template popup give the rule a descriptive name. The Severity drop-down selection is used to define the level of any incidents created by the rule. These can be used to take additional actions based on the severity level. When ready select *Next* at the bottom.


Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Analytics >
Analytics rule wizard - Create a new Scheduled rule
General
Set rule logic
Incident settings
Automated response
Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *: demo-alert

Description:

Severity: Medium

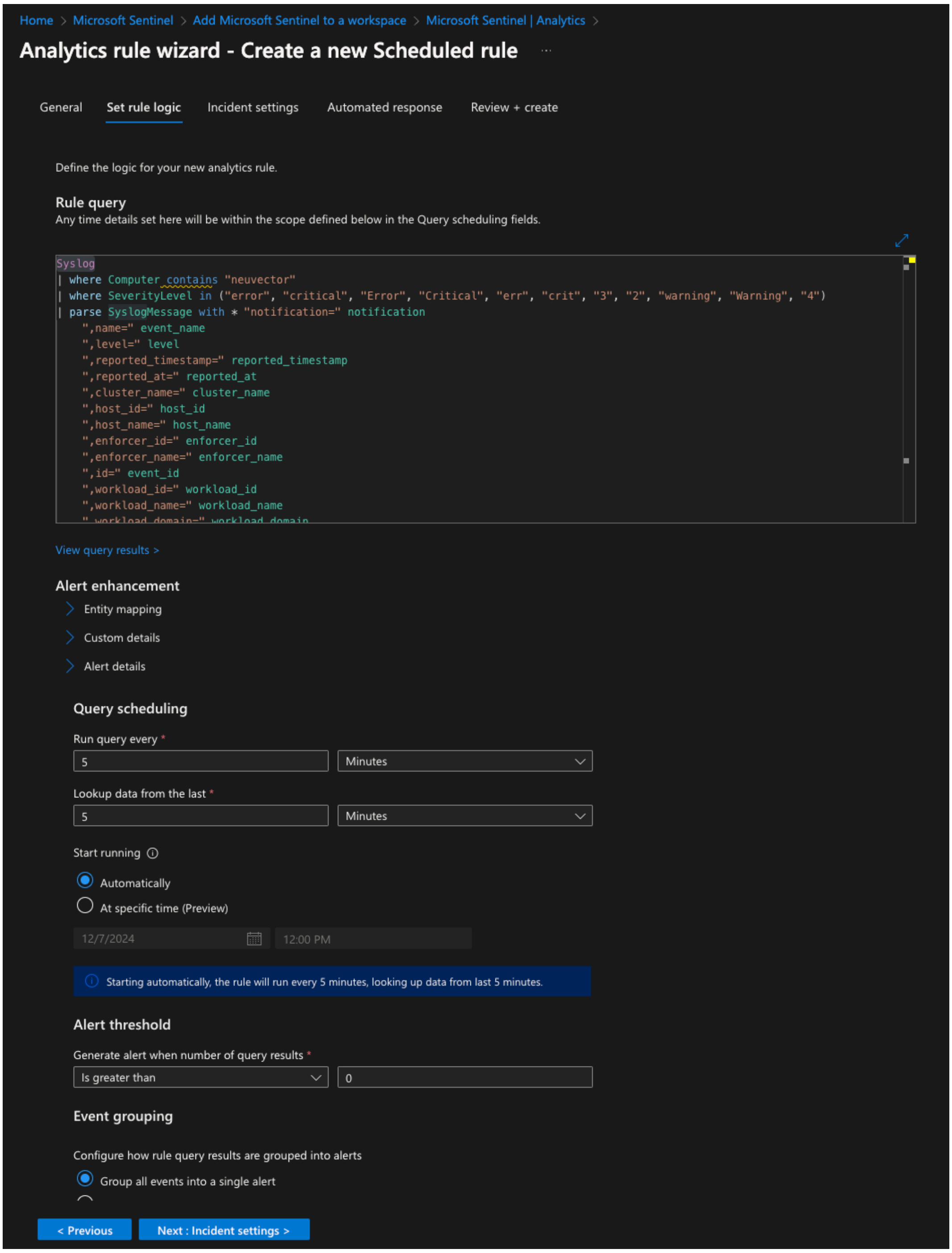
MITRE ATT&CK: Select tactics techniques and sub techniques

Status: Enabled

The **Set rule logic** tab is where queries are defined to filter all of the log data stored in the Log Analytics Workspace. For now, here is an example query that will select any entry that is logged as either a Warning, Error, or Critical. When it has selected those entries, it will filter out unnecessary columns.

```
Syslog
| where Computer contains "neuvector"
| where SeverityLevel in ("error", "critical", "Error", "Critical", "err", "crit", "3",
 "2", "warning", "Warning", "4")
| parse SyslogMessage with * "notification=" notification
    ",name=" event_name
    ",level=" level
    ",reported_timestamp=" reported_timestamp
    ",reported_at=" reported_at
    ",cluster_name=" cluster_name
    ",host_id=" host_id
    ",host_name=" host_name
    ",enforcer_id=" enforcer_id
    ",enforcer_name=" enforcer_name
    ",id=" event_id
    ",workload_id=" workload_id
    ",workload_name=" workload_name
    ",workload_domain=" workload_domain
    ",workload_image=" workload_image
    ",workload_service=" workload_service
    ",proc_name=" proc_name
    ",proc_path=" proc_path
    ",proc_cmd=" proc_cmd
    ",proc_effective_user=" proc_effective_user
    ",proc_parent_name=" proc_parent_name
    ",proc_parent_path=" proc_parent_path
    ",action=" action
    ",group=" group
    ",rule_id=" rule_id
    ",aggregation_from=" aggregation_from
    ",count=" count
    ",message=" message
| extend
    AlertSeverity = case(
        SeverityLevel in ("critical", "Critical", "crit", "2"), "Critical",
        SeverityLevel in ("error", "Error", "err", "3"), "High",
        SeverityLevel in ("warning", "Warning", "warn", "4"), "Warning",
        "Unknown"
    )
| project
    TimeGenerated,
    Computer,
    AlertSeverity,
    event_name,
    level,
    cluster_name,
    workload_name,
    workload_domain,
    workload_service,
    workload_image,
    proc_name,
    proc_path,
    proc_cmd,
    proc_effective_user,
    proc_parent_name,
    proc_parent_path,
    action,
    message,
    SyslogMessage
```

Copy this into the text box at the top of the tab. Clicking *View query results* will run the query against data currently in the Log Analytics Workspace and present the results in a table. This is useful in refining a query to include only the information needed. It is also possible to adjust how frequently this query is run. The minimum time is every five minutes. When ready, click *Next* at the bottom of the page.



Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Analytics >
General
Set rule logic
Incident settings
Automated response
Review + create

Analytics rule wizard - Create a new Scheduled rule

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
Syslog
| where Computer contains "neuvector"
| where SeverityLevel in ("error", "critical", "Error", "Critical", "err", "crit", "3", "2", "warning", "Warning", "4")
| parse SyslogMessage with * "notification=" notification
    ",name=" event_name
    ",level=" level
    ",reported_timestamp=" reported_timestamp
    ",reported_at=" reported_at
    ",cluster_name=" cluster_name
    ",host_id=" host_id
    ",host_name=" host_name
    ",enforcer_id=" enforcer_id
    ",enforcer_name=" enforcer_name
    ",id=" event_id
    ",workload_id=" workload_id
    ",workload_name=" workload_name
    ",workload_domain=" workload_domain
```

Alert enhancement

Query scheduling

Run query every *: 5 Minutes

Lookup data from the last *: 5 Minutes

Start running

● Automatically

○ At specific time (Preview)

12/7/2024 12:00 PM

Starting automatically, the rule will run every 5 minutes, looking up data from last 5 minutes.

Alert threshold

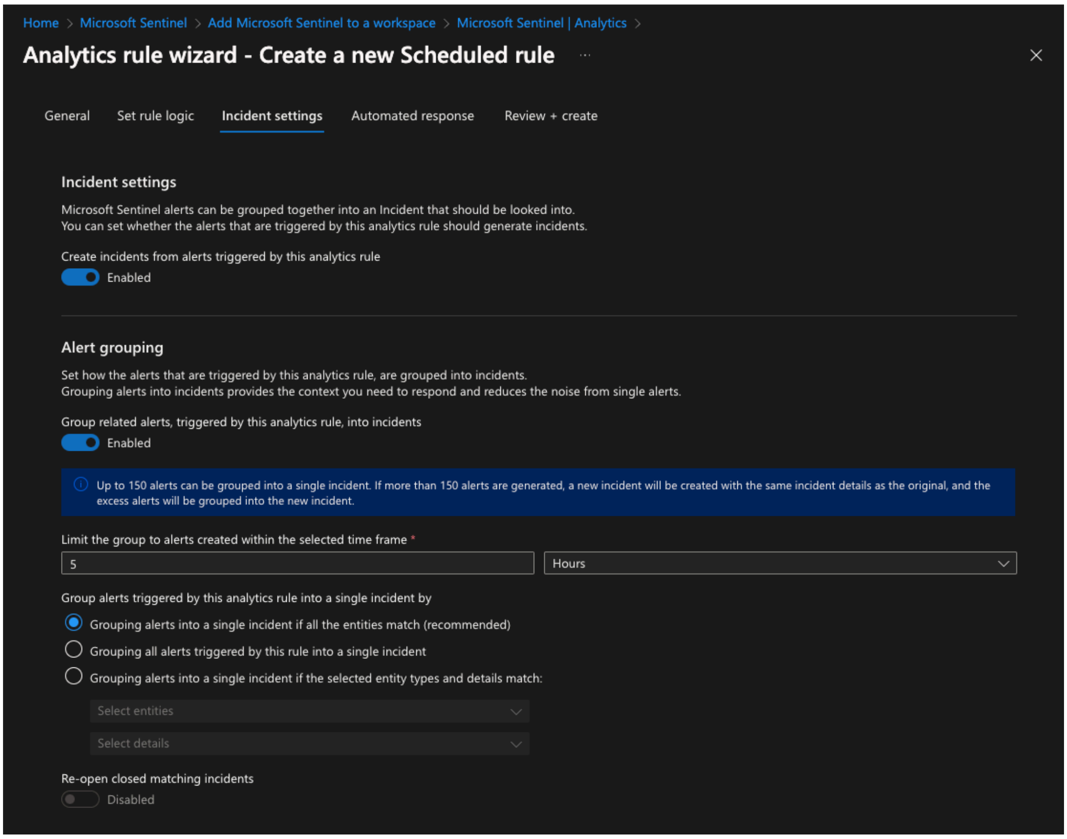
Generate alert when number of query results *: Is greater than 0

Event grouping

Configure how rule query results are grouped into alerts

● Group all events into a single alert

On the next tab, **Incident settings**, enable the toggle `Group related alerts, triggered by this analytics rule, into incidents`. This will help reduce the number of incidents received if the same issue triggers multiple times inside of SUSE Security. Click through the rest of the tabs, and click *Save* on the Review + Create tab.


Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Analytics >
General
Set rule logic
Incident settings
Automated response
Review + create

Analytics rule wizard - Create a new Scheduled rule

Incident settings

Microsoft Sentinel alerts can be grouped together into an Incident that should be looked into.
You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule
Enabled

Alert grouping

Set how the alerts that are triggered by this analytics rule, are grouped into incidents.
Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents
Enabled

Up to 150 alerts can be grouped into a single incident. If more than 150 alerts are generated, a new incident will be created with the same incident details as the original, and the excess alerts will be grouped into the new incident.

Limit the group to alerts created within the selected time frame *
5 | Hours

Group alerts triggered by this analytics rule into a single incident by
● Grouping alerts into a single incident if all the entities match (recommended)
○ Grouping all alerts triggered by this rule into a single incident
○ Grouping alerts into a single incident if the selected entity types and details match:
Select entities
Select details

Re-open closed matching incidents
Disabled

This completes the configuration. The environment will now send all logs and alerts raised by SUSE Security into Microsoft Sentinel for additional processing. By integrating with other Microsoft Azure services like Microsoft Defender and Microsoft Security Copilot, administrators gain a unified interface. This interface allows them to monitor, query, and actively manage the security of their environment.

5 Next Steps

While this is a great step in unifying security visibility, there is one additional step that can be taken to extend that data and make it more interactive. This can be completed by adding Microsoft Sentinel as a data source in Microsoft Security Copilot.

5.1 Microsoft Security Copilot

Microsoft Security Copilot will allow for interacting with data through a traditional chat interface. Security Copilot requires Security compute units (SCUs) to be provisioned in the Azure subscription. This can be done by searching for `Microsoft Security Copilot compute ca-`

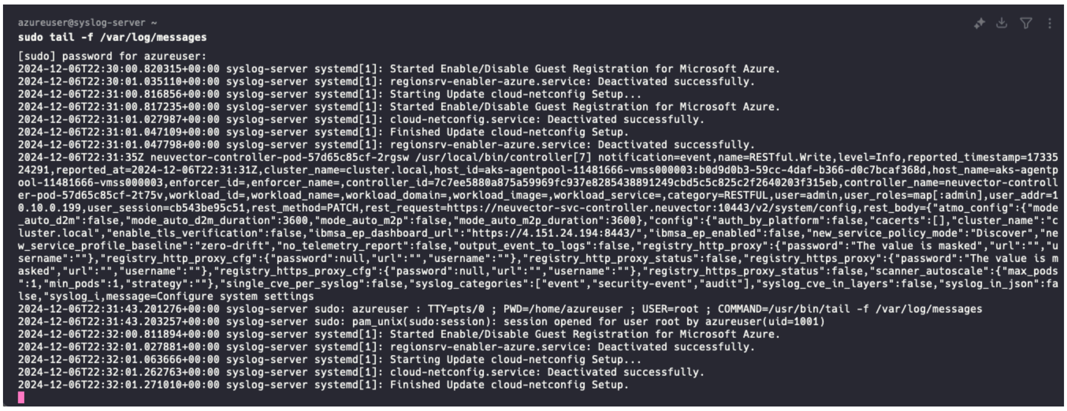
pacities in the Azure Portal. It is recommended to provision two to three SCUs for testing. These can be scaled up and down as required to assist in cost control. After the provisioning is complete, follow Microsoft's guide for connecting Microsoft Sentinel as a data source for Security Copilot (https://learn.microsoft.com/en-us/azure/sentinel/sentinel-security-copilot) ↗. The guide will also show how to use the data from Microsoft Sentinel inside of Microsoft Defender. This combination will allow for questions to be asked to Microsoft Security Copilot about cluster state, open CVEs, or other incidents raised by SUSE Security without combing through all log files manually.

6 Troubleshooting

If the system is not sending data as expected, it is recommended to check the following locations.

6.1 Syslog Server

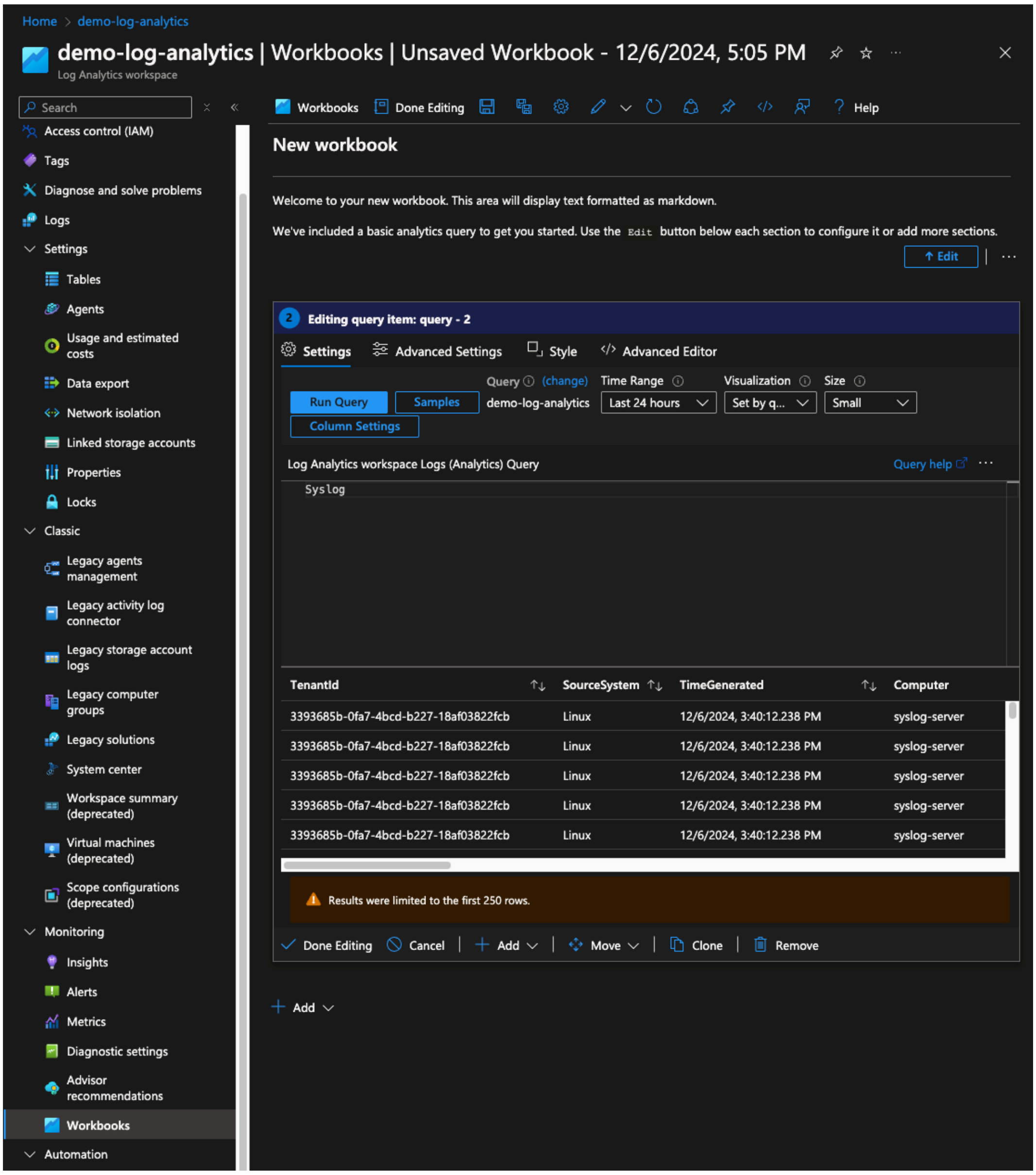
To confirm that data is flowing as expected from SUSE Security into the Syslog server connect to the VM using SSH. After connecting, execute the command `sudo tail -f /var/log/messages`. This will present a real-time flow of syslog entries. If there are entries with "controller-pod" or "aks-agentpool" then data is correctly flowing from SUSE Security into the Syslog server.



```
azureuser@syslog-server ~
sudo tail -f /var/log/messages
[sudo] password for azureuser:
2024-12-06T22:30:00.820315+00:00 syslog-server systemd[1]: Started Enable/Disable Guest Registration for Microsoft Azure.
2024-12-06T22:30:01.035110+00:00 syslog-server systemd[1]: regionsrv-enabler-azure.service: Deactivated successfully.
2024-12-06T22:31:00.816856+00:00 syslog-server systemd[1]: Starting Update cloud-netconfig Setup...
2024-12-06T22:31:00.817235+00:00 syslog-server systemd[1]: Started Enable/Disable Guest Registration for Microsoft Azure.
2024-12-06T22:31:01.027987+00:00 syslog-server systemd[1]: cloud-netconfig.service: Deactivated successfully.
2024-12-06T22:31:01.047109+00:00 syslog-server systemd[1]: Finished Update cloud-netconfig Setup.
2024-12-06T22:31:01.047798+00:00 syslog-server systemd[1]: regionsrv-enabler-azure.service: Deactivated successfully.
2024-12-06T22:31:35Z neuvector-controller-pod-57d65c85cf-2rgsw /usr/local/bin/controller[7] notification=event,name=RESTful.Write,level=Info,reported_timestamp=17335
24291,reported_at=2024-12-06T22:31:31Z,cluster_name=cluster.local,host_id=aks-agentpool-11481666-vmss000003:b0d9d0b3-59cc-4daf-b366-d0c7bcaf368d,host_name=aks-agentp
ool-11481666-vmss000003,enforcer_id=,enforcer_name=,controller_id=7c7ee5880a875a59969fc937e8285438891249cbd5c5c825c2f2640203f315eb,controller_name=neuvector-controll
er-pod-57d65c85cf-2t75v,workload_id=,workload_name=,workload_domain=,workload_image=,workload_service=,category=RESTFUL,user=admin,user_roles=map[:admin],user_addr=1
0.10.0.199,user_session=cb543be95c51,rest_method=PATCH,rest_request=https://neuvector-svc-controller.neuvector:10443/v2/system/config,rest_body={"atmo_config":{"mode
_auto_d2m":false,"mode_auto_d2m_duration":3600,"mode_auto_m2p":false,"mode_auto_m2p_duration":3600},"config":{"auth_by_platform":false,"cacerts":[],"cluster_name":"c
luster.local","enable_tls_verification":false,"ibmsa_ep_dashboard_url":"https://4.151.24.194:8443/","ibmsa_ep_enabled":false,"new_service_policy_mode":"Discover","ne
w_service_profile_baseline":"zero-drift","no_telemetry_report":false,"output_event_to_logs":false,"registry_http_proxy":{"password":"The value is masked","url":"","u
sername":""},"registry_http_proxy_cfg":{"password":null,"url":"","username":""},"registry_http_proxy_status":false,"registry_https_proxy":{"password":"The value is m
asked","url":"","username":""},"registry_https_proxy_cfg":{"password":null,"url":"","username":""},"registry_https_proxy_status":false,"scanner_autoscale":{"max_pods
":1,"min_pods":1,"strategy":""},"single_cve_per_syslog":false,"syslog_categories":["event","security-event","audit"],"syslog_cve_in_layers":false,"syslog_in_json":fa
lse,"syslog_i,message=Configure system settings
2024-12-06T22:31:43.201276+00:00 syslog-server sudo: azureuser : TTY=pts/0 ; PWD=/home/azureuser ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/messages
2024-12-06T22:31:43.203257+00:00 syslog-server sudo: pam_unix(sudo:session): session opened for user root by azureuser(uid=1001)
2024-12-06T22:32:00.811894+00:00 syslog-server systemd[1]: Started Enable/Disable Guest Registration for Microsoft Azure.
2024-12-06T22:32:01.027881+00:00 syslog-server systemd[1]: regionsrv-enabler-azure.service: Deactivated successfully.
2024-12-06T22:32:01.063666+00:00 syslog-server systemd[1]: Starting Update cloud-netconfig Setup...
2024-12-06T22:32:01.262763+00:00 syslog-server systemd[1]: cloud-netconfig.service: Deactivated successfully.
2024-12-06T22:32:01.271010+00:00 syslog-server systemd[1]: Finished Update cloud-netconfig Setup.
```

6.2 Azure Log Analytics Workspace

To confirm that Azure Log Analytics Workspace is ingesting the data from the syslog-server navigate to **Workbooks** in the Log Analytics Workspace page of the Azure Portal. Select *Default Template*, then change the text in the query to `Syslog` and click *Run Query*. The results should populate with data and allow for scrolling to verify that log data is coming in from the syslog-server VM as expected.



New workbook

Welcome to your new workbook. This area will display text formatted as markdown.

We've included a basic analytics query to get you started. Use the `Edit` button below each section to configure it or add more sections.

Query demo-log-analytics

Time Range Last 24 hours

Visualization Set by q...

Size Small

Log Analytics workspace Logs (Analytics) Query

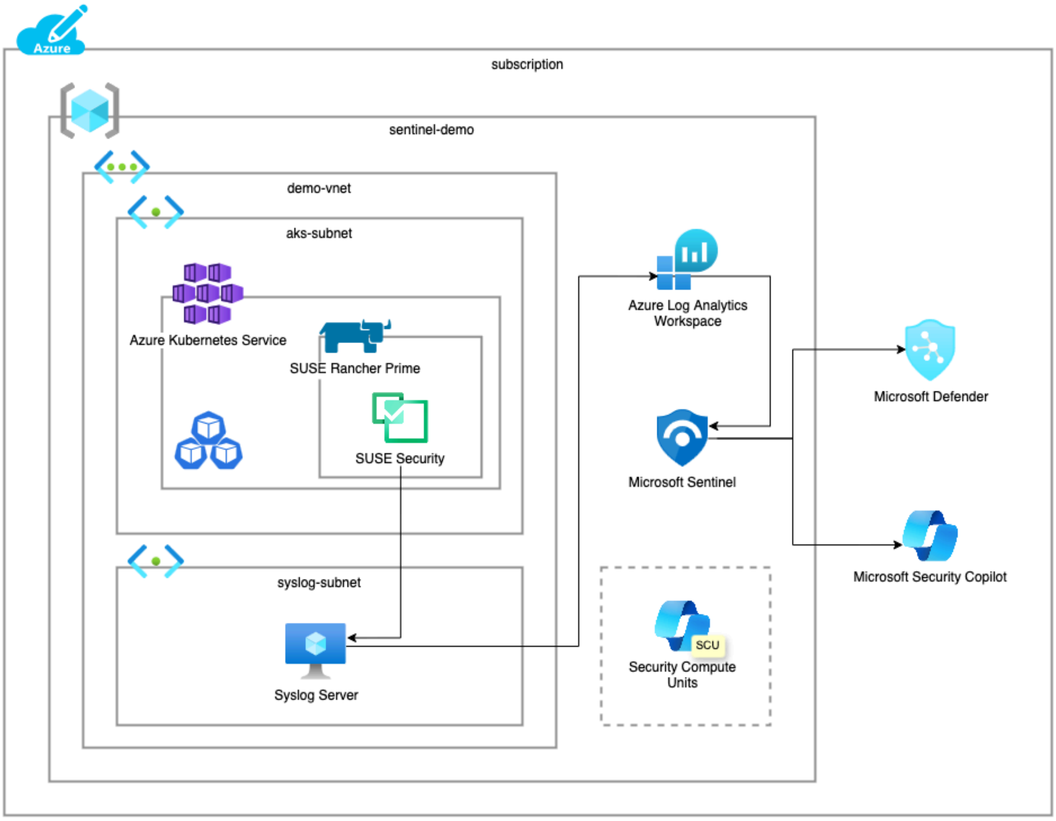
```
Syslog
```

TenantId	SourceSystem	TimeGenerated	Computer
3393685b-0fa7-4bcd-b227-18af03822fcb	Linux	12/6/2024, 3:40:12.238 PM	syslog-server
3393685b-0fa7-4bcd-b227-18af03822fcb	Linux	12/6/2024, 3:40:12.238 PM	syslog-server
3393685b-0fa7-4bcd-b227-18af03822fcb	Linux	12/6/2024, 3:40:12.238 PM	syslog-server
3393685b-0fa7-4bcd-b227-18af03822fcb	Linux	12/6/2024, 3:40:12.238 PM	syslog-server
3393685b-0fa7-4bcd-b227-18af03822fcb	Linux	12/6/2024, 3:40:12.238 PM	syslog-server

⚠ Results were limited to the first 250 rows.

7 Summary

This guide has shown how to take the data produced by SUSE Security and integrate it into Microsoft Sentinel to create a unified threat interface for an environment. This is accomplished by exporting the data from SUSE Security into an Azure Log Analytics Workspace which can be queried by Microsoft Sentinel and by Microsoft Defender and Microsoft Security Copilot.



The preceding network diagram illustrates this integration within a typical Azure environment. As shown, SUSE Security, deployed within an Azure Kubernetes cluster, forwards security logs to a dedicated Syslog server. This server then transmits the data to the Log Analytics Workspace, where it becomes accessible to Microsoft Sentinel and other security tools for analysis and response.

By centralizing security data in this manner, organizations can gain a comprehensive view of their security posture, enabling faster threat detection and response. This unified approach streamlines security operations and strengthens defenses against increasingly sophisticated cyberattacks.

Modern environments generate vast amounts of log data, which can be overwhelming. Tools that simplify the parsing and analysis of this data are crucial for maintaining awareness and flexibility in security efforts. This ultimately contributes to the safety of our systems, environments, and customers.

To learn more about integrating SUSE Security with Microsoft Sentinel, explore the detailed documentation available for SUSE Security (https://open-docs.neuvector.com) ↗ and Microsoft Sentinel (https://learn.microsoft.com/azure/sentinel) ↗. For personalized assistance, contact your SUSE or Microsoft representative to discuss your specific needs and security objectives.

8 Legal notice

Documents published as part of the series SUSE Technical Reference Documentation have been contributed voluntarily by SUSE employees and third parties. They are meant to serve as examples of how particular actions can be performed. They have been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. SUSE cannot verify that actions described in these documents do what is claimed or whether actions described have unintended consequences. SUSE LLC, its affiliates, the authors, and the translators may not be held liable for possible errors or the consequences thereof.

9 GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document’s license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all

Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
   Permission is granted to copy, distribute and/or modify this document
   under the terms of the GNU Free Documentation License, Version 1.2
   or any later version published by the Free Software Foundation;
   with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
   A copy of the license is included in the section entitled “GNU
   Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “ with… Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
   Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.