Contents

[Sentinel – Plural Sight 2](#_Toc165931246)

[Where Sentinel fits. 2](#_Toc165931247)

[Design Considerations of Sentinel 2](#_Toc165931248)

[Single tenant with single Microsoft Sentinel Workspace. 2](#_Toc165931249)

[Single tenant with regional Microsoft Sentinel Workspace. 3](#_Toc165931250)

[Multi-tenant 4](#_Toc165931251)

[Sentinel Roles 4](#_Toc165931252)

[Prerequisites before enabling Sentinel. 4](#_Toc165931253)

[Enabling Microsoft Sentinel 5](#_Toc165931254)

[Free trial of Sentinel. 5](#_Toc165931255)

[Pay-as-you-go vs commitment tiers. 6](#_Toc165931256)

[Commitment tiers of Log analytic workspace 6](#_Toc165931257)

[Dedicated cluster 6](#_Toc165931258)

[Log analytic workspace. 7](#_Toc165931259)

[Costs in Log analytic workspace 7](#_Toc165931260)

[Retention period of Sentinel and Log Analytic Workspace. 7](#_Toc165931261)

[Log Analytic Workspace 7](#_Toc165931262)

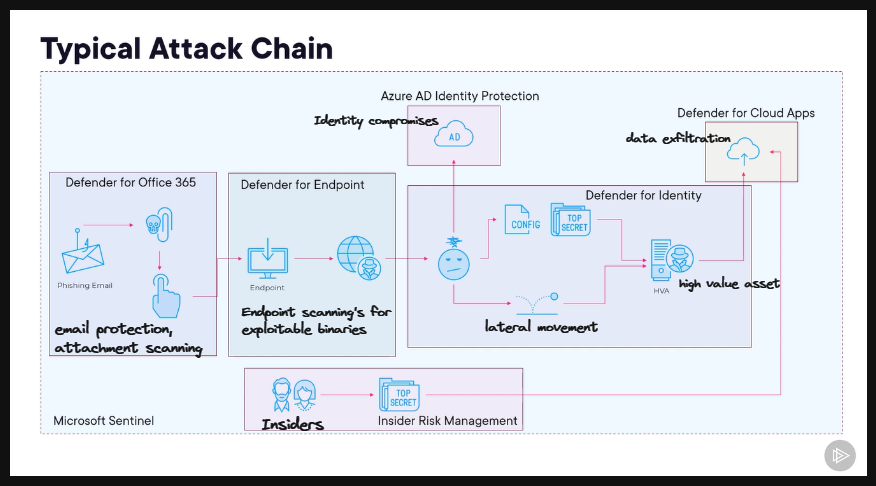
[Data Retention period on Log analytic workspace table Plans and Sentinel 8](#_Toc165931263)

[Data collection in Sentinel 9](#_Toc165931264)

[Syslog server and Syslog protocol 9](#_Toc165931265)

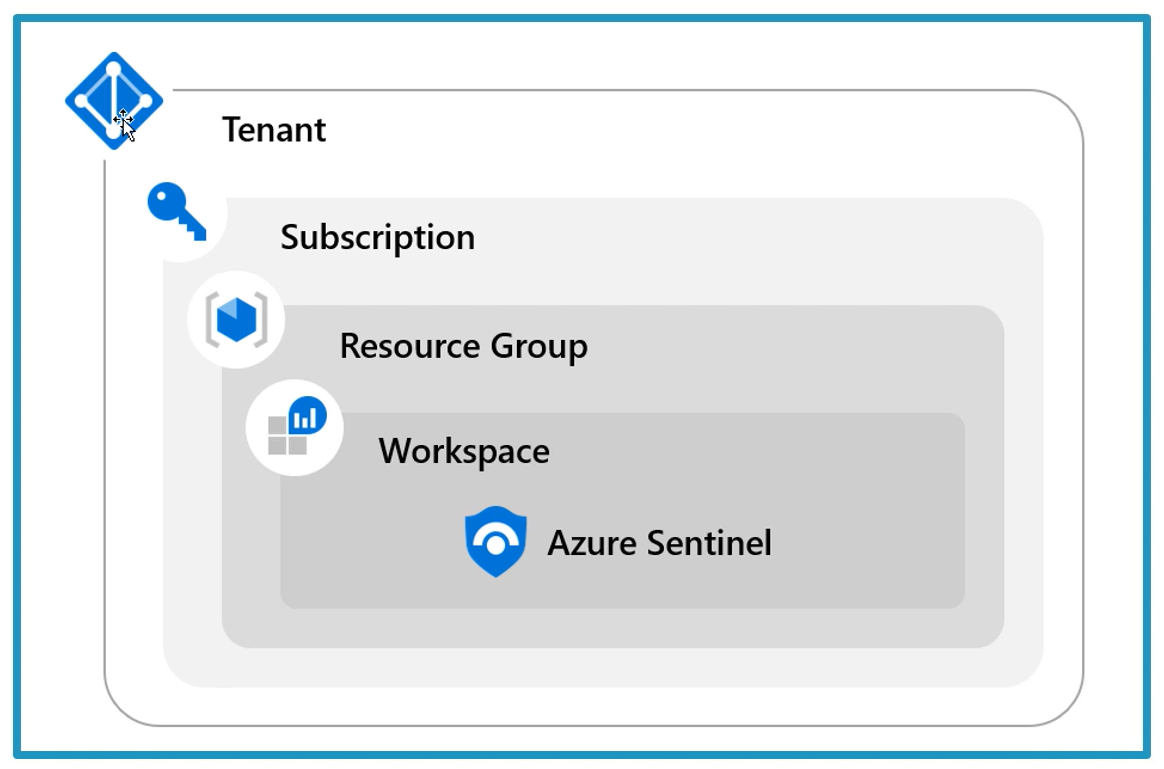
# Sentinel – Plural Sight

## Where Sentinel fits.



## Design Considerations of Sentinel

### Single tenant with single Microsoft Sentinel Workspace.



This workspace is the single repository of all the data and resources of all the regions of that tenant. Because the log data travels between regions and storing at another region, This causes two possible concerns.

* Incurring bandwidth cost
* Single workspace cannot be an option if there is any data governance requirements to store the data in a specific region.

|  |  |
| --- | --- |
| Pros | Cons |
| Central pane of glass | May not meet governance requirements |
| Consolidation logs | Can incur bandwidth cost between regions |
| Easier to query information |  |
| Log analytic RBAC to control access |  |
| Microsoft Sentinel RBAC |  |

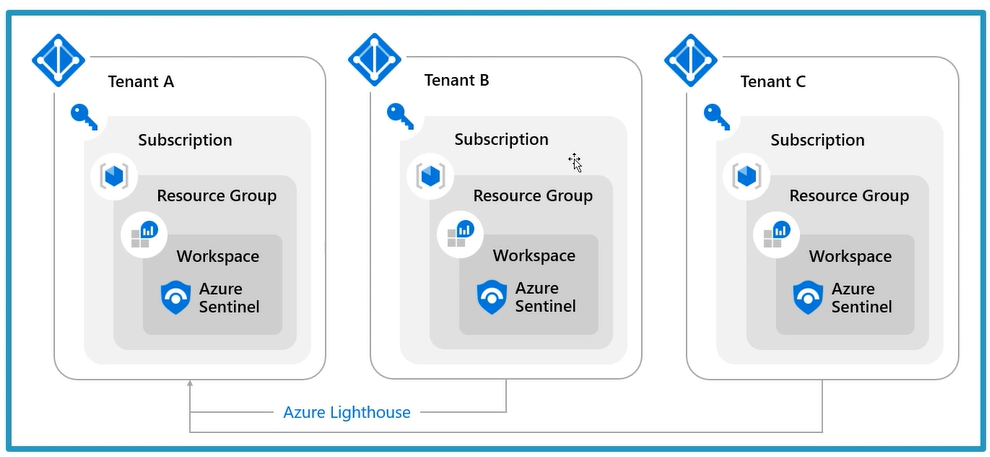
### Single tenant with regional Microsoft Sentinel Workspace.

A screenshot of a computer

Description automatically generated

|  |  |
| --- | --- |
| Pros | Cons |
| No cross-region bandwidth costs | No central pane of glass |
| May be required to meet governance | Analytics, workbooks etc must be deployed multiple times |
| Granular data access control |  |
| Granular retention settings |  |
| Split billing |  |

### Multi-tenant



If you want to manage a workspace which is not in your tenant, you need to implement multi-tenant workspaces using Azure Lighthouse. Lighthouse helps you manage resources between multiple customers without having log in and out with different credentials.

## Sentinel Roles

* ***Sentinel Reader***– Can view incidents, workbooks other M Sentinel resources.
* ***Sentinel Responder*** – Can manage incidents (assign, dismiss etc).
* ***Sentinel Contributor*** – Can create and edit analytic rules and Sentinel resources.
* ***Sentinel Contributor + Logic App Contributor*** – Can create and run playbooks.

## Prerequisites before enabling Sentinel.

* Need an Entra ID license and tenant.
* An Azure Subscription.
* A Log-Analytic workspace.
* You need to have at least contributor role at subscription level to enable Sentinel.
* You need to have Contributor or reader role at resource group where workspace belongs to live.
* It is recommended to have a separate resource group for your Microsoft Sentinel and all the resources it uses like playbooks, workbooks, Log analytic workspace etc.

## Enabling Microsoft Sentinel

* You can enable Sentinel by creating a Log analytic workspace and using that workspace for sentinel for log ingestion. This will enable sentinel.
* Enable health and audit. This will check health and audit the resources used by the sentinel. It makes sure that the services are functioning as intended.
  + The first event generated by the selected resources will get injected in the sentinel workspace tables (*SentinelHealth, SentinelAudit*).

## Free trial of Sentinel.

* When you enable Sentinel on a workspace, 10 GB/day is free for 31 days. After that, usage beyond these limits will be charged as per the pricing tiers you choose.
* The free period is only up to 20 workspace limit per tenant.
* The total amount of data analysed by sentinel, and total amount of data injected to workspace will be considered in the billing.

## Pay-as-you-go vs commitment tiers.

* Commitment tiers give you discount on pay-as-you-go pricing which can save a lot of cost.
* Pay-as-you-go pricing is $5.22 per GB-ingested.
* Commitment tire for 100GB with 34% discount on per GB is $3.43 per GB.
* As the tier increases, discount will increase up to 55% on 50,000 GB per day.
* [comparison table](https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/#:~:text=10%5E9%20bytes).-,Commitment%20Tiers,-With%20Commitment%20tiers).

## Commitment tiers of Log analytic workspace

* Commitment tiers can be the effective way to save costs.
* Commitment tiers start from 100 GB per day. Beyond the limit of 100 GB will be billed.
* The commitment tiers will have **31 days** of commitment period from the time a commitment period is selected.
  + You can change to the higher commitment tiers during this period but not to lower tiers.
  + You cannot move back to pay-as-you-go until you cross the commitment period.
  + After the commitment period, workspace retains the commitment tiers, and we can change it to lower tiers or else move back to pay-as-you-go.
* Billing is done per workspace on daily bases. If the workspace is a part of cluster, billing is done on the cluster.

## Dedicated cluster

* Is a collection of workspaces in a single managed Azure Data Explorer cluster.
* They must have a commitment tier of at least 100 GB/day.
* There is no pay-as-you-go option for clusters.
* Custer commitment is 31 days. During this period, tier cannot be reduces but can be increased.
* Data ingestion billing for those workspaces is done at the cluster level using the configured commitment tier level.
* There are two modes of billing when you create a cluster.
  + Cluster (default).
    - Billing for data ingestion is done at cluster level.
    - The total ingested data of all the workspaces are aggregated to calculate the daily bill for the cluster.
  + Workspaces.
    - Commitment tier costs are distributed among the workspaces within the cluster.
    - If total ingestion volume for the day is above the commitment tire, each workspace pays a fraction of the commitment tier based on its portion of the ingested data.
* The cluster billing starts when it is created regardless of workspaces are associated with the cluster.
* Workspaces associated to a cluster no longer have their own pricing tier.
* Workspaces can be unlinked from a cluster at any time.
* If a cluster is deleted, billing for the cluster will stop even if the cluster is within its 31-day commitment period.

## Log analytic workspace.

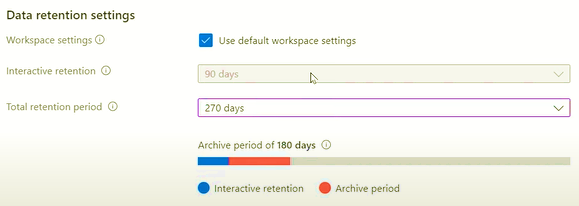
### Costs in Log analytic workspace

* There is no cost to create a workspace. You are only charged for the data you ingest.
* You are charged based on the retention period you choose.
* Region selection for log analytic workspace can help you save egress cost.
  + If your resources and workspace are deployed in a same region, it can help you save egress cost.
* Daily Cap will limit the ingestion of data till the threshold you set. After that, data collection will stop for that day.
  + You can configure it in ***Usage and estimated costs > Daily Cap.***
  + Whenever daily cap limit is reached, a warning is shown on portal.
  + As well as an event is generated in ***operations table*** of log analytic workspace.
  + There is a ***reset time*** which will resume the data collection. You cannot change the reset time. For every workspace, the reset time is different.

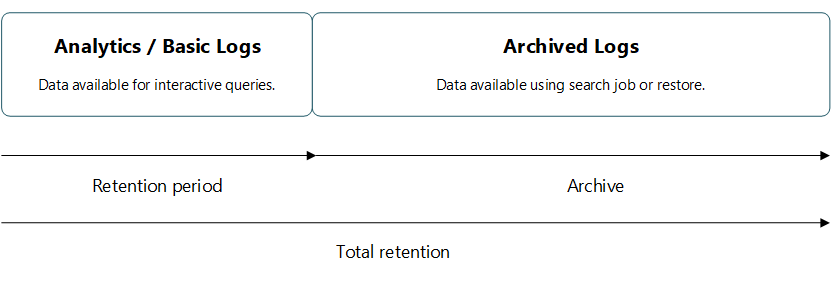
## Retention period of Sentinel and Log Analytic Workspace.

### Log Analytic Workspace

* ***Total retention period =*** ***interactive retention period*** + ***Archival retention period.***
* **Interactive retention period:** This is the period of 4 days to 2 years. This is the period where you can retain data for interactive queries.
* **Archive retention period:** This is the period up to 12 Years. This period is for the data to be accessible less frequently.
  + The Archival data can be retrieved only via *search jobs* or *restore*.
* Both interactive and Archival period can be customized for each table.
* The default data retention period is 30 days. You can configure it in ***Usage and estimated costs > data retention.***
* The data retention period is configured at workspace level, this configured value is then inherited by all the interactive retention period of individual tables of that workspace.
* You can change the retention period of individual tables by clicking on three dots > manage table, which will not inherit the default value of workspace data retention. You can also see options to choose archival period.
* You can now change the total amount of retention period by choosing the archival period which will add on interactive retention period.



### Data Retention period on Log analytic workspace table Plans and Sentinel



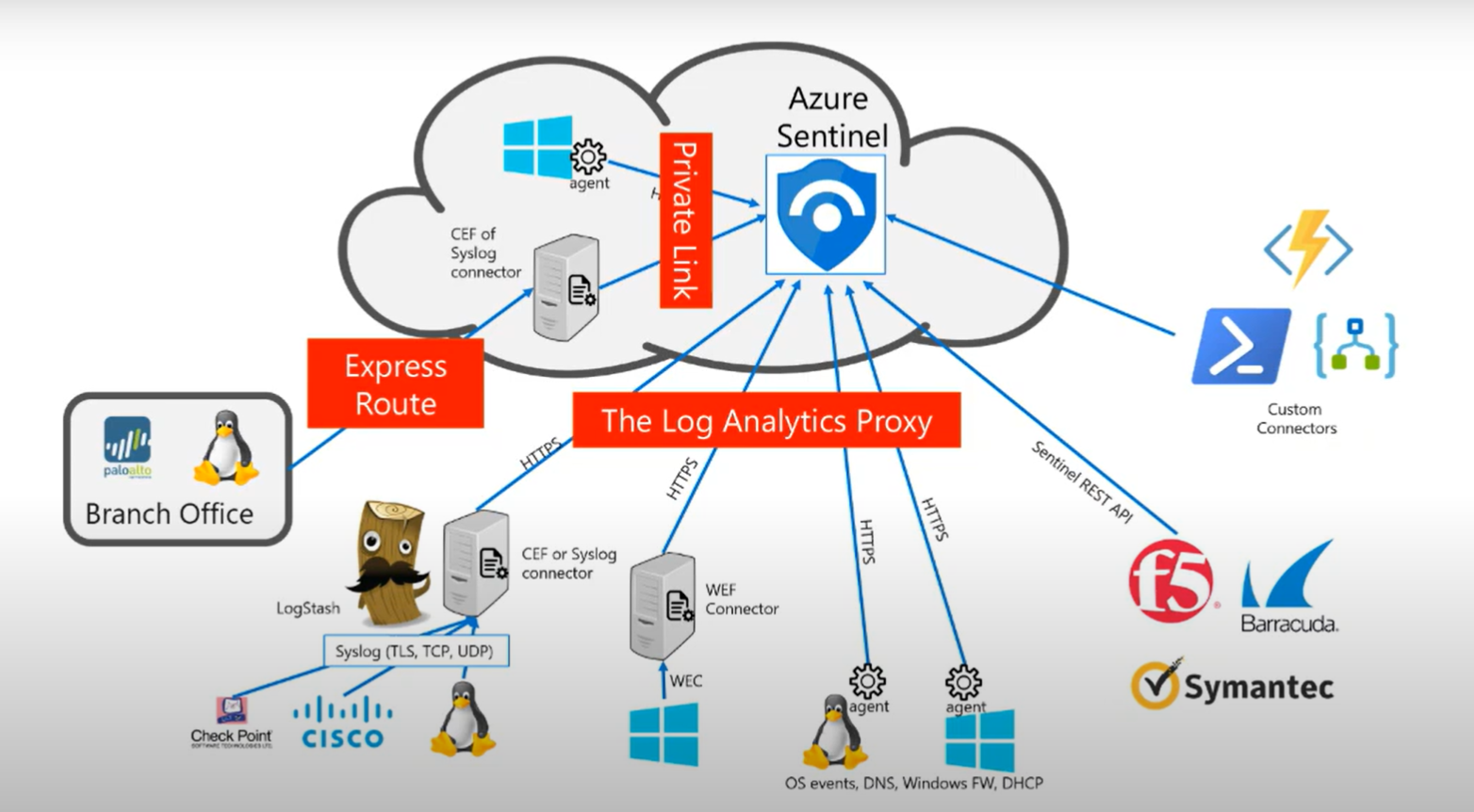
* For every table in the workspace fall under these ***two plans***.
  + ***Basic.***
  + ***Analytic.***
* Table with Basic plan.
  + **Retention period**: 8 days and cannot be changed.
  + **Archival period**: up to 12 years.
* Table with Analytics plan.
  + **Retention period**: between 30 days to 2 years.
  + **Archival period**: up to 12 years.

| **Category** | **Analytics** | **Basic** |
| --- | --- | --- |
| Ingestion | Regular ingestion cost. | Reduced ingestion cost. |
| Log queries | Full query capabilities No extra cost. | [Basic query capabilities](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/basic-logs-query#limitations). Pay-per-use. |
| Retention | Configure retention from 30 days to two years. | Retention fixed at eight days. When you change an existing table's plan to Basic logs, [Azure archives data](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive) that's more than eight days old but still within the table's original retention period. |
| Alerts | Supported. | Not supported. |

* The default retention period for Sentinel is 90 days. You can decrease it to 30 days or increase it up to 90 days.
* If you want to increase beyond it, you can use tools like
  + Sentinel Archive,
  + data explorer,
  + storage Account.

## Data collection in Sentinel

Sentinel is a cloud native tool which needs to be feed with logs and events to co-relate and analyse them to create incidents on which we can do investigations and remediate them. Logs are collected by sentinel by installing log analytic agent on Windows and Linux servers.



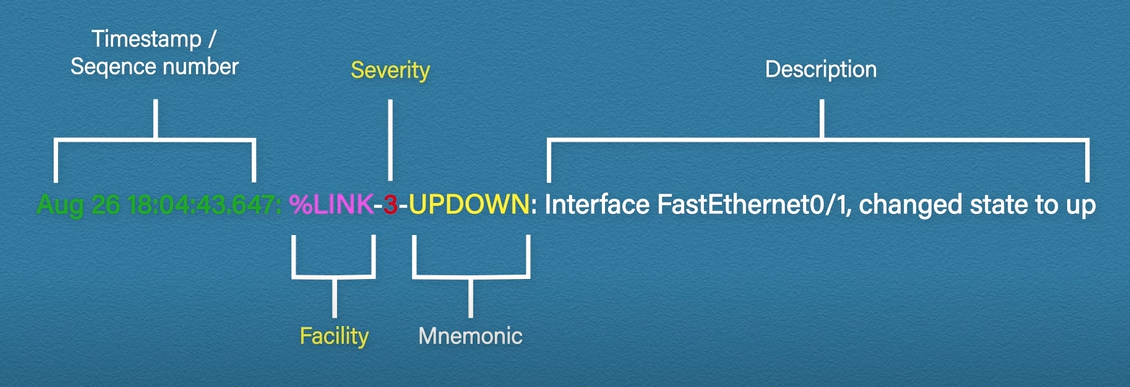
### Syslog server and Syslog protocol

Syslog is an industry standard protocol for message logging. Logs are important for troubleshooting problems. It is easy to manage the logs when we have less number of network devices. If we have many resources, it is an overhead to manage all the logs generated by all the devices in the network.

It is when syslog server comes into play. Using syslog server allows to centrally manage our log information. All the logs from the devices are sent to this centralized place. ***The log messages are sent on UDP port 514 to syslog server***. From here he can manage, search, and archive all the log information.

Cisco devices by default store the log information inside RAM. Once the device is rebooted, the log information will be deleted. Not all devices store info inside RAM, many devices store inside disk if available, but network devices use RAM to storage log information. Syslog servers can be helpful for data retention and archiving that information safely.

#### Syslog message format



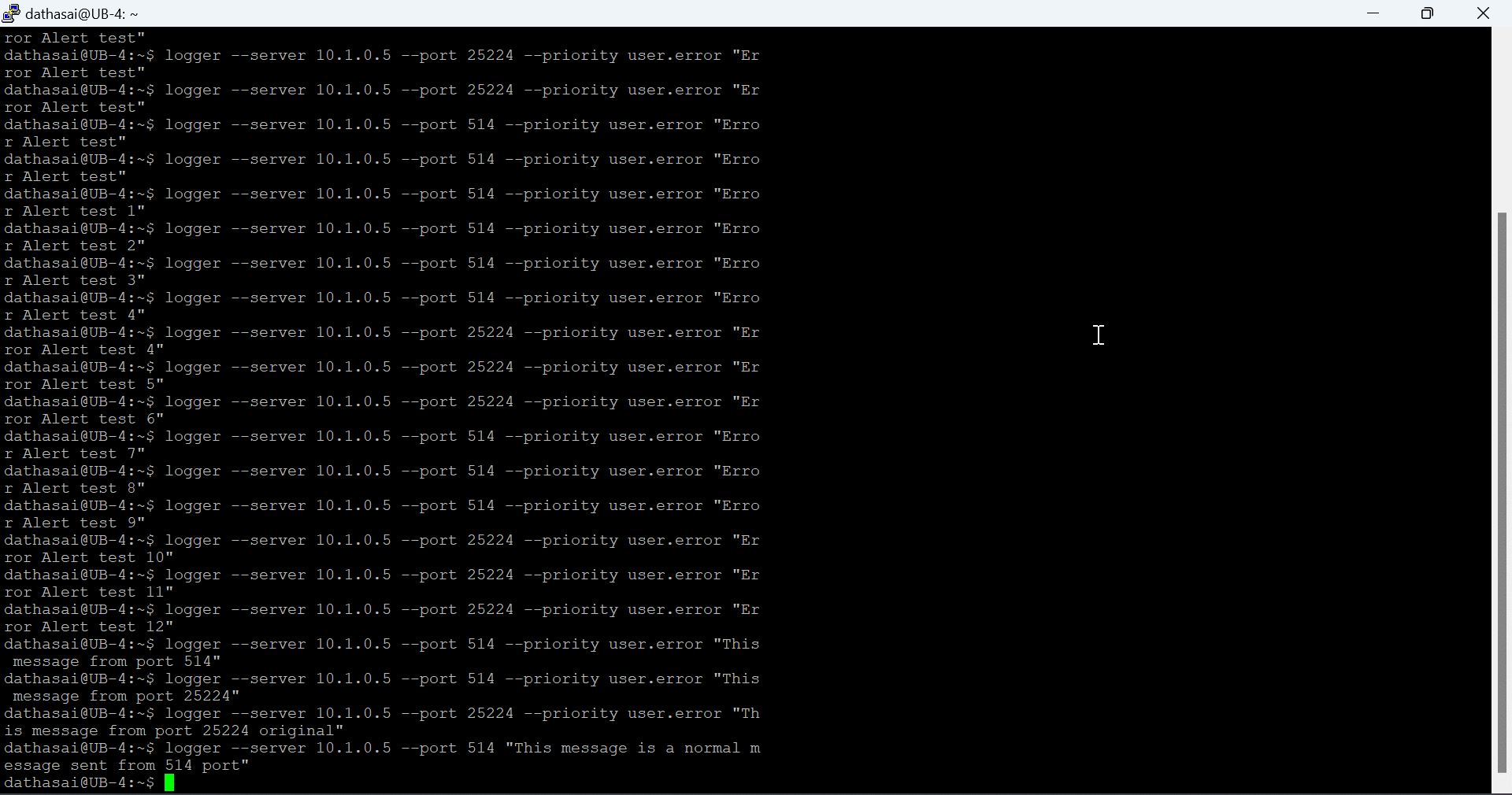
|  |  |  |
| --- | --- | --- |
| CODE | SEVERITY | DESCRIPTION |
| 0 | Emergency | System is unusable |
| 1 | Alert | Action must be taken immediately |
| 2 | Critical | Critical conditions |
| 3 | Error | Error conditions |
| 4 | Warning | Warning conditions |
| 5 | Notice | Normal but significant conditions |
| 6 | Informational | Informational messages |
| 7 | Debug | Debug-level messages |

You can send logs based on the severity of the code for not clogged up with messages.

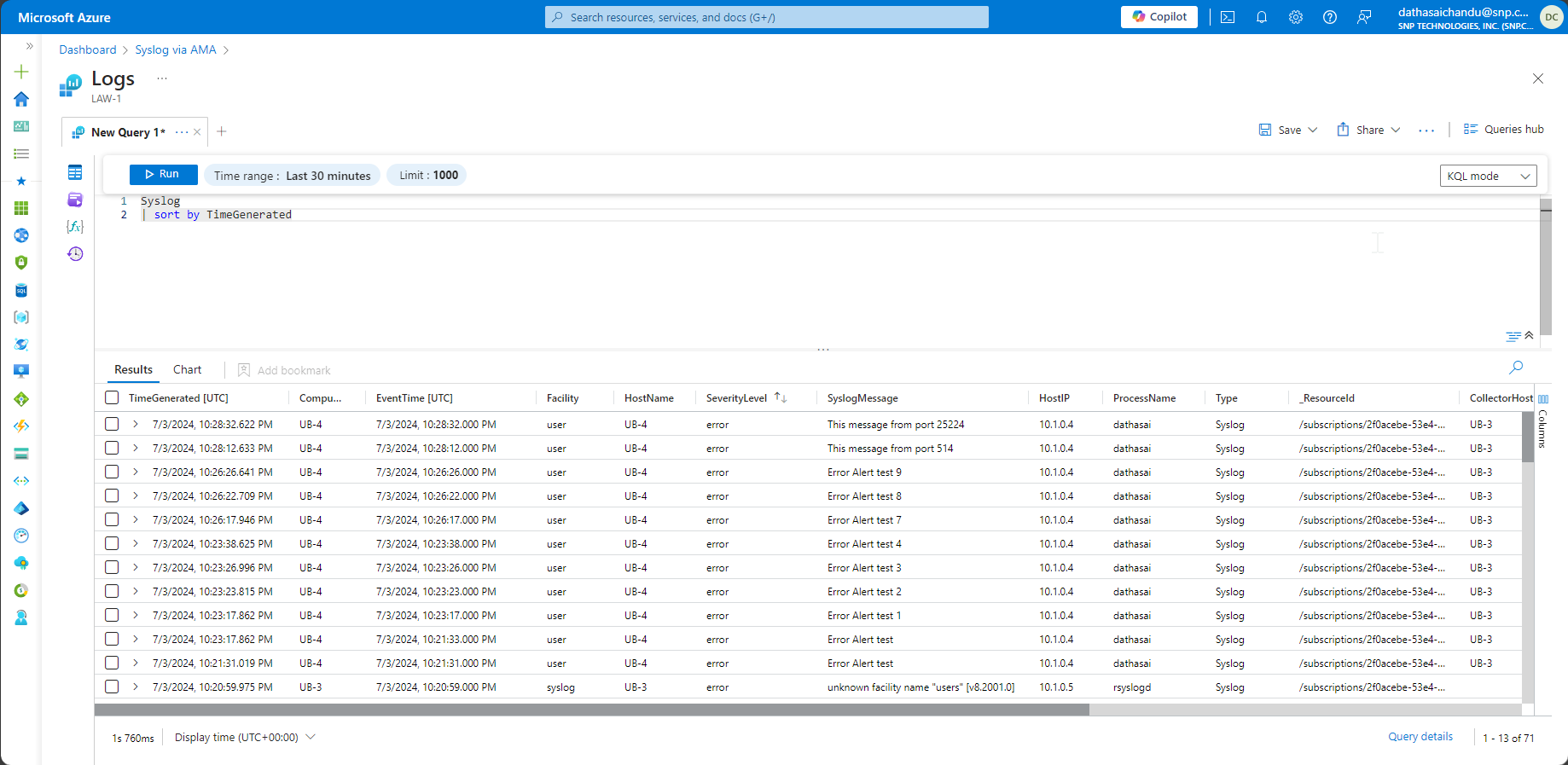
### Lab on Syslog forwarder

**Scripts**

* Installing rsyslog
  + *sudo apt install rsyslog*
* Installing net-tools to use netstat -ano which is used to check the status of ports.
  + *sudo apt install net-tools*
  + *sudo netstat -ano*
* Installing tcpdump to listen the packet capturing through ports.
  + *sudo tcpdump -i etf0 port 514*
  + etf0 is the ethernet name. can be found by the *ifconfig* command.
* Configuration file of rsyslog
  + *sudo nano /etc/rsyslog.conf*
* Restart the rsyslog service when ever you change the rules or rsyslog configuration file.
  + *service rsyslog restart*
* rsyslog logs are default stored location.
  + *cd /var/log/syslog*
  + *tail -5 syslog*
* Logs are sent from VM-1 to VM-2.
  + *Logger –server* VM-2\_ip\_address *–port 514 “message”.*
  + *Logger –server* VM-2\_ip\_address *–port 514 –priority user.error “message”.*



* Install OMS or AMA agent in the VM to export the rsyslog logs to sentinel.



* The logs are sent to the workspace which are further monitored from Sentinel.

