Table of Contents

[Sentinel – Plural Sight 2](#_Toc161853827)

[Design Considerations of Sentinel 2](#_Toc161853828)

[Single tenant with single Microsoft Sentinel Workspace. 2](#_Toc161853829)

[Single tenant with regional Microsoft Sentinel Workspace. 3](#_Toc161853830)

[Multi-tenant 3](#_Toc161853831)

[Sentinel Roles 4](#_Toc161853832)

[Prerequisites before enabling Sentinel. 4](#_Toc161853833)

[Log analytic workspace. 4](#_Toc161853834)

[Costs in Log analytic workspace 4](#_Toc161853835)

[Retention period of Sentinel and Log Analytic Workspace. 4](#_Toc161853836)

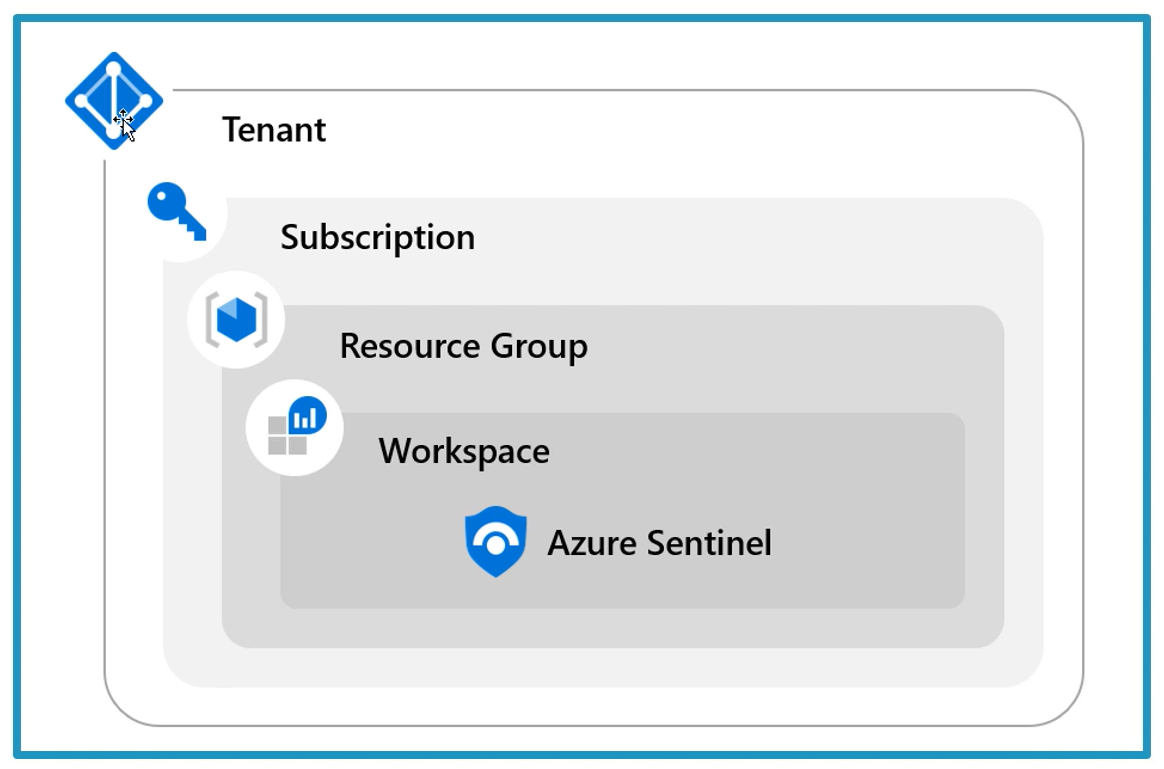
[Log Analytic Workspace 4](#_Toc161853837)

[Retention period on Log analytic workspace table Plans 5](#_Toc161853838)

# Sentinel – Plural Sight

## 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 |  |

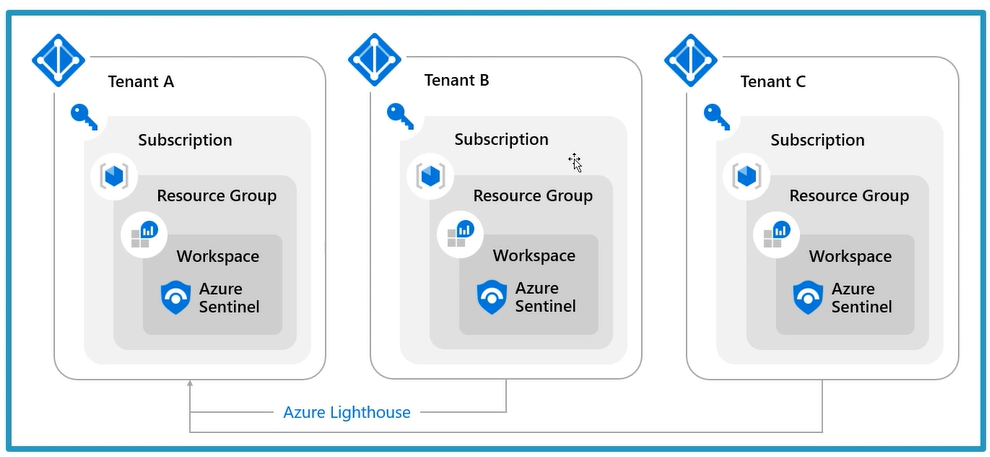
### Single tenant with regional Microsoft Sentinel Workspace.

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.

* 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.

## Log analytic workspace.

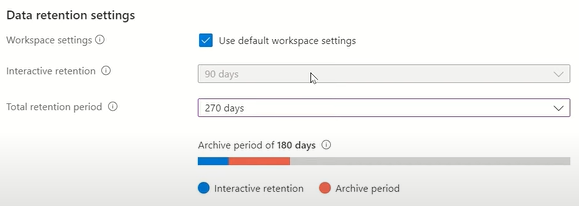
### Costs in Log analytic workspace

* 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 between 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.



### Retention period on Log analytic workspace table Plans

* For every table in the workspace fall under these ***two plans***.
  + Basic.
  + Analytic.
* Table with Basic plan.
  + **Archival period**: up to 7 years.
  + **Retention period**: 8 days and cannot be changed.
* Table with Analytics plan.
  + **Retention period**: between 30 days to 2 years.

## Syslog

* Syslog is natively supported by Linux devices. You can stream events to Sentinel using AMA agent.
* The agent is installed either **directly on the system** or on the dedicated Linux-based **log-forwarder**.
* The agent in Linux receives events from the Syslog daemon over UDP (Unix Domain Sockets).
* The AMA then transmits these events to the Microsoft Sentinel workspace.