

Malware Detection within Object Storage

Author: Matthew Battagel, Supervisor: Theodoros Spyridopoulos

Acknowledgments -

I would like to extend my sincere gratitude to my supervisor Theo, my colleague Harry, parents, and Lo for their unwavering support and encouragement during my project. Their combined expertise and guidance provided were critical in the shaping and execution of the project. I am truly thankful to all of them for their contributions.

Abstract

Lorem Ipsum

Contents

1	Introduction	3
1.1	Overview	3
1.2	Motivation	3
1.3	Project Aims	4
2	Background	4
2.1	Signature Detection	4
2.2	Malware Detection with ClamAV	5
2.3	Microservices	5
2.4	Amazon S3 Malware Detection	5
3	Specification	5
3.1	Functional Requirements	6
3.2	Non-Functional Requirements	7
3.3	Constraints	7
4	Architecture	7
4.1	Candidate Design 1 - Post-Write	8
4.2	Candidate Design 2 - Upload Queue	9
4.3	Candidate Design 3 - Write Interception	10
4.4	Candidate Design 4 - Per Node	11
4.5	Selected Candidate Design	11
5	Implementation	12
5.1	Service Selection and Creation	12
5.2	Aegis Module Design and Creation	15
5.3	External Package Integration	18
5.4	Aegis' Internal Workflow	21
5.5	Testing	27
5.6	Kubernetes Deployment	28
6	Results and Evaluation	31
6.1	Solution Workflow	31
6.2	Benefits of Metric Collection	32
6.3	Performance Evaluation	32
6.4	Comparing Functional Requirements	32
6.5	Comparing Non-Functional Requirements	32
6.6	Testing Evaluation	32
6.7	Project Aims Evaluation	33
7	Product Issues / Future work	33
7.1	33
8	Conclusions	33
8.1	33

9	Reflection on Learning	33
9.1	33
10	Appendix	33

1. Introduction

1.1. Overview

The exponential growth of data generation has made data storage an increasingly important aspect for both individuals and organizations alike (John and David, 2012). Object storage has emerged as a promising solution due to its ability to store vast amounts of unstructured data in a cost-effective and scalable manner (Ot, 2022). Unlike traditional storage techniques, object storage abstracts the lower-level functions inside of the data store (M. *et al.*, 2005). Functions such as, space management and access control are handled on an per object basis, allowing for greater flexibility and security (M. *et al.*, 2005).

One of the most widely used object storage platforms is Amazon S3, which provides a highly scalable and reliable solution for storing data (Vlad *et al.*, 2018). However, an open-source alternative called MinIO has emerged as a promising contender, providing similar features to Amazon S3 while giving customers greater control over their data (MinIO, 2023b). MinIO is written in Go and is available for free under the Apache License 3.0 or, for commercial and enterprise purposes, at a reduced cost compared to Amazon S3 (MinIO, 2023c). MinIO offers a wide range of features, including high performance, data replication, encryption and erasure coding (MinIO, 2023b). Most importantly, MinIO is designed to scale out horizontally to ensure that it can handle the demands of large-scale applications.

With MinIO, scalability is made simple by allowing multiple types of hardware platforms to work together in separate nodes each with their own compute and storage within a microservice architecture (MinIO, 2023b). This is extremely attractive for customers who want to utilise their existing hardware without being tied down to a specific provider. This also applies for customers looking to migrate their data from Amazon S3 to cheaper solution without compromising on the high performance, reliability and scalability of the S3 platform.

While MinIO is a great alternative to Amazon S3, it does not offer any form of integrated malware detection. This could deter potential customers from choosing MinIO as a viable platform to migrate to from Amazon S3 or leave existing users data vulnerable to malware attacks. This project aims to address this issue by integrating a malware detection system into MinIO without negatively impacting the scalability or performance such that MinIO is still an effective alternative to Amazon S3.

1.2. Motivation

Due to the high amount of unstructured data expected to be both written and read to the object store, and the increasing amount of malware being produced (Ormandy, 2011), there are increased risk of encountering malicious files. Therefore malware detection within object storage is crucial in modern cloud storage scenarios. Most popular off-the-shelf object storage platforms, such

as AWS, already have integrated third-party antivirus software, such as ClamAV and Sophos (Srinivasan *et al.*, 2022), to mitigate security risks. MinIO on the other hand is vulnerable to malware attacks as it currently does not have any native antivirus integration (MinIO, 2023b). This forces customers who require complete virus protection to either not use MinIO or to use potentially costly third-party software. As antivirus scanning is inherently resource intensive, if the software is integrated incorrectly, it could reduce the ability for the storage solution to scale horizontally. The purpose of this project is to implement malware detection within MinIO while being mindful to not impact the scalability or performance of the platform.

1.3. Project Aims

The primary objective of this project is to integrate malware detection into MinIO without compromising the platform's scalability or performance. The solution must be able to detect malware within files uploaded to MinIO and deal with them accordingly. The solution must also be production-ready and offer all the required features for a customer to use it in a real-world scenario, including; the ability to configure the solution, both metric collection and audit logging for monitoring, and the ability for it to scale to meet the users demand.

From a personal standpoint, this project serves as an opportunity to enhance my knowledge of the Go programming language and the MinIO platform. Additionally, it aims to expand my experience in designing and implementing production-ready solutions within a microservice environment. Lastly, this project seeks to develop my proficiency in managing time, scope, and resources for large-scale projects.

2. Background

2.1. Signature Detection

Signature-Detection is a method used to detect malware within files. A signature is a string that represents a malicious file (Liao *et al.*, 2013). These signatures come in multiple forms, including MD5 hashes to represent whole-files (Aslan *et al.*, 2020), byte sequences which can be matched internally or regex patterns, often written in YARA (Nitin *et al.*, 2019), to allow for more fuzzy matching. If malware were to have a different signature than the one present in the virus database, fuzzy matchers like YARA could be used to compare more abstract properties of the file using a set of rule (Nitin *et al.*, 2019). These rules are reverse engineered from known malware to include common indicators of compromise (IOC) like text or hex strings (Naik *et al.*, 2020).

However, signature detection is not foolproof. It is ineffective against unknown malware or significantly modified variants of existing malware (Liao *et al.*, 2013). This requires frequent updates to the signature database to ensure that knowledge of new malware is kept up to date. In addition, YARA rules can be generated automatically but are often not as effective as manually generated ones (Nitin *et al.*, 2019).

2.2. Malware Detection with ClamAV

ClamAV uses the latest signature-based detection techniques to scan files located on the disk (Kil *et al.*, 2011). It is the most popular open-source antivirus software and has already been optimised to use less memory and to speed up signature matching (Kil *et al.*, 2011). ClamAV pulls its signatures from an online database which contains two types of signatures, MD5 whole-file signatures and multi-part patterns (Po-ching *et al.*, 2006). ClamAV uses both of these signatures in its detection process, firstly prioritising the single sequence signatures and if no match then using the multi-part patterns (Po-ching *et al.*, 2006). ClamAV has frequent updates to its signature database to negate the disadvantages of signature detection (ClamAV, 2023a).

2.3. Microservices

Microservices are a software development technique that structures an application as a collection of loosely coupled services with high cohesion. This allows for each service to be independently deployable into logical business functions providing a high level of scalability and flexibility (Nuha *et al.*, 2016). Cloud-native applications are often built using a microservice to take advantage of scaling for variable demand (Nuha *et al.*, 2016). Developing a microservice architecture also comes with challenges that should be addressed, such as service discovery, load balancing, and inter-service communication (Nuha *et al.*, 2016).

2.4. Amazon S3 Malware Detection

As MinIO's largest competitor, this project draws a lot of inspiration from Amazon S3's integrated malware detection blog page (Srinivasan *et al.*, 2022). The blog explains Amazon's current approach for managing malware detection within their service. Amazon S3 uses a combination of ClamAV and Sophos as their third-party scanning engines due to their out-of-the-box nature (Srinivasan *et al.*, 2022). Amazon then gives you the option to use either of these engines or both. The blog goes on to describe the three main interaction mechanisms that Amazon S3 uses to flag files for scanning. Firstly, an API endpoint would be provided to handle all uploads. This forms a queue of uploads which are then scanned before entering the bucket. Next, event-driven scanning is used to keep track of all regular file uploads. The antivirus will then scan each file after they have been written to the bucket. Finally, retro-driven scanning is used to scan all existing files within the bucket. The user then has the flexibility to define what types of files should be scanned including defining time windows. This blog has given some useful methodologies of how to keep track of both incoming and previously scanned files. Creating a system that can match these methods is important for offering a matching level of scalability and security within MinIO.

3. Specification

The purpose of the project specification is to guide the project towards achieving the goals outlined in the previous section. The specification is divided into three main categories; functional requirements, non-functional requirements, and constraints.

The MoSCoW method is employed to prioritize the projects requirements. It is a prioritization technique utilized in business analysis and software development to establish a shared understanding among stakeholders regarding the significance assigned to the delivery of each requirement (Gita *et al.*, "2018"). The acronym stands for:

- Must have: Critical for the project's success and must be included in the final solution.
- Should have: Important but not absolutely necessary for the project's success. They should be included if possible, but the project can proceed without them.
- Could have: Desirable but not essential. They can be included if time and resources permit but can be left out without impacting the project's success.
- Won't have: Not necessary for the current project and will not be included. They may be considered for future development.

3.1. Functional Requirements

Functional requirements are provided in the table 1. The requirement is given with a MoSCoW priority and a description to justify the priority.

Requirement	Description	Priority
Provide a way of detecting the latest uploads to the object store	Key part of automating scans	Must
Record the results of the malware detection within the object store	Some feedback from the scan must be provided to the user.	Must
Provide the ability to measure various metrics	Metric collection is very attractive for satisfying production-ready status.	Must
Scale alongside MinIO to ensure that it does not bottleneck the object store at high loads	To handle maximum throughput, the solution should scale alongside MinIO to ensure it is production-ready.	Must
Provision for future expansion and ongoing maintenance	Having the ability to build on-top of the project will increase the attractiveness to users looking to migrate from AWS	Must
Have a high level of customisability to allow for different use cases	Gives flexibility to the user but is not a requirement for proof of concept	Should
Allow for efficient and transparent debugging in the event of failure	Creating a robust product mitigates the priority of debugging.	Should
Add more complex metrics - Histogram, Gauges, etc	Additional metrics are more beneficial in a production environment but unnecessary for size of project scope.	Should
Provide the choice of multiple antivirus engines	not necessary for the proof of concept as it requires too much time.	Could
Provide a warning when under "delete" cleanup policy	not necessary for the proof-of-concept as it requires too much time.	Could
Automatically event queue to bucket notifications	Can be completed manually with instructions instead. Removes customisability from the user if done automatically.	Could
Supply the MinIO policies the solution will use e.g. "put" and "get".	MinIO denies by default and therefore operations could fail when MinIO is not run with admin permissions.	Could
Prevent the downloading of files if flagged as infected	Is covered by cleanup policies. Would also require GUI changes.	Wont
Protection from "inside man" attacks	The system will be maintained by an admin. The admin could attempt to compromise the system. Protection against this is significantly harder without reducing extensibility.	Wont
Provide multiple types of scanners e.g. hash or server based AV scanner	These would have different workloads and requirements. Not achievable in project scope.	Wont

Table 1: Functional Requirements

3.2. Non-Functional Requirements

Requirement	Description	Priority
Speed	The solution must be able to keep up with the rate of uploads made to MinIO. This can be measured by comparing the time difference between uploading an object to MinIO and the object being scanned and tagged	Must
Availability	Over a long period of time, the solution must be able to handle all requests. This can be measured by comparing the number of requests made to the number of requests completed over a large time frame	Must
Reliability	100% of the files uploaded to MinIO must go through the scanning process. The recorded metrics can be used to compare MinIO uploads with the number of objects scanned. It is worth noting that checking the clean and infected results add to the total sum of scanned objects	Must
Capacity	The solution should be able to handle the maximum number of simultaneous requests that MinIO can handle. This can be measured by monitoring the amount of cache used by the solution under load	Should
Usability	Future additions, maintenance, and debugging should be as simple as possible. This requirement is more subjective and therefore an explanation of how this has been achieved will be discussed in the implementation section. Prolonged use of the solution should be enabled by recording dependency versions.	Should
Security	The solution could implement the best practices for security, including data protection and secure communication between components. This is less of a priority as sensitive information is kept within the Kubernetes deployment and all external interaction is handled by MinIO's internal authentication.	Could
Privacy	The solution is not directly responsible for following privacy laws and regulations, such as the DPA (Government, 2018).	Wont

Table 2: Non-Functional Requirements

3.3. Constraints

The primary constraint for this project is the strict 12-week timeline, which significantly restricts the project scope. To overcome this constraint, careful prioritization of features and efficient time management for their implementation is crucial.

Another constraint is the requirement that all external software used must be open source, available for commercial use under a license, or require a fee. This ensures the project's legal viability if the solution is to be employed commercially.

Lastly, my personal knowledge and experience pose constraints on the project. The learning curve for new technologies may extend the average time needed to achieve milestones. Moreover, potential errors could result in unforeseen delays. As a result, when selecting technologies, factors such as ease of use, documentation, and community support should be considered to minimize the impact of these constraints.

4. Architecture

Choosing the correct architecture for the project is critical for ensuring that the solution is scalable, performant and maintainable. Given the specification above, various potential architectures

can be created and evaluated based my own thoughts and from reading the background material. The best candidate design will then be chosen based on which candidate design satisfies the most requirement with as little compromises as possible. Thought will also be given to which architecture fits within the constraints of the project.

Project Naming

Due to the defined functionality of the solution, an suitable name can be chosen. “Aegis” is the name of the shield that Zeus used to protect himself in Greek mythology and is also a noun synonymous with protection (Wikipedia)). This is appropriate given that the solution is designed to protect the MinIO object store from malware. Aegis will be used synonymously with the solution throughout the rest of the report.

4.1. Candidate Design 1 - Post-Write

The first candidate design makes use of the performance benefits of MinIO by allowing puts to be initially written to the bucket without being scanned. The design then uses a event queue compatible with MinIO to keep track of all the files that have been uploaded. The queue is then used to trigger a scan of the file once an antivirus is available. The candidate design is shown in figure 1.

This design has many benefits over other potential implementations. Firstly, it uses the storage provided by MinIO to store all incoming files without having to manage a separate storage solution. This removes a lot of complexity from the solution by not having to account for a number of failure conditions that could occur with a high availability, production ready storage solution. For example, the solution would not be responsible for handling partial writes, loss of data, or data corruption. Removing this responsibility allows the solution to focus on the core functionality of the project, the scanning of files, which is essential for keeping the project within the time constraints.

Secondly, the design also makes use of the integrated event queue provided by MinIO. This again removes responsibility from the solution by differing the scalability and reliability requirements to the event queue and MinIO.

Lastly, having Aegis dispatch the files to a scalable number of antivirus scanners allows the solution to scale to meet the demands of the system. This meets a key requirement as the solution is expected to have the capacity for a large number of operations. This method does require the use of a load balancer to effectively distribute the load across the available antivirus scanners.

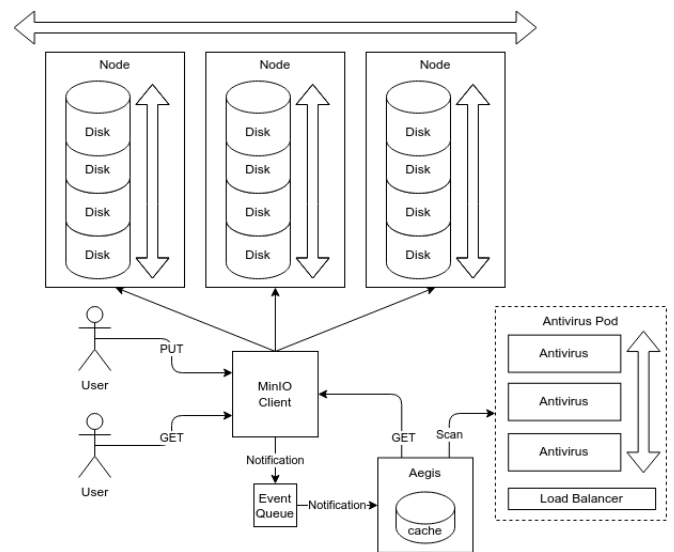


Figure 1: Post-Write Architecture

The candidate design also has a number of drawbacks. Firstly, the design still requires a small amount of cache to temporarily store the object when it is being dispatched to the antivirus. Provisioning of this cache has to be large enough to handle the largest file possible to be uploaded to the object store. In reality, this cache would be provisioned even larger to allow for the temporary storage of multiple objects while multiple scans are being performed asynchronously. In addition, the cache needs to be large enough to ensure that the system does not become overwhelmed by the number of objects being scanned as the system scales. This is a minor issue as store capacity is cheap and the provisioning of the cache easy to scale up. Additionally, a higher priority can be given to scaling up and out antivirus scanners to ensure that the smallest number of files are being cached, while being scanned, at any point.

The second drawback is that, for each event, Aegis makes a get request for the object to be scanned. This effectively doubles the number of requests made to the object store. This also means that Aegis must have the ability to get any file expected to be scanned and therefore must have access to the whole storage network. The impact of this drawback is mitigated as the solution is expected to be deployed on the same network as the object store which should reduce the latency of each request made by Aegis. However, this still leaves MinIO to handle twice as many requests with the performance loss being noticed mainly on more distributed storage topologies.

Thirdly, the candidate design only allows for a single Aegis instance to dispatch all incoming objects to available scanners. This is a potential bottleneck for the system as this instance could become overwhelmed by the number of requests it is receiving. This is a minor issue as the dispatching of objects to scanners is not as performance intensive as other areas of the solution, such as the actual scanning, and therefore it is not expected to be a major bottleneck.

Lastly, any object uploaded to the store will have a certain period of time where it remains unchecked. In this time, the user could potentially download an unscanned object or the object could cause harm to the store before it is detected. Although the handling of infected objects is out of scope, in an actual implementation of the solution, the user could be made unable to download unscanned objects until they have been scanned.

4.2. Candidate Design 2 - Upload Queue

This candidate design created a wrapper around MinIO that the user interacts with instead of MinIO. This means that all puts go through Aegis before being uploaded to the object store. The candidate design is shown in figure 2.

The main benefit of this design is that the user interacts only with Aegis when uploading files. This means that all incoming files can be stored within a temporary storage before ever entering the object store. This offers the best protection against malicious files as the user cannot ever download an unscanned or infected file as it is never uploaded to the object store. Infected files can then either be deleted or moved to a separate quarantine store for analysis.

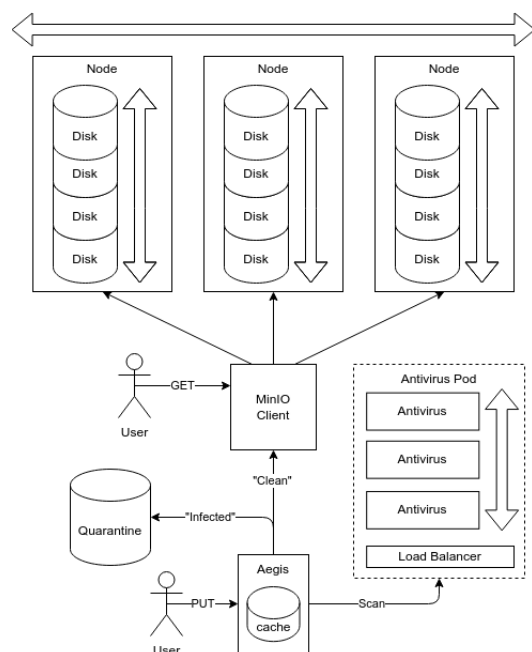


Figure 2: Upload Queue Architecture

This candidate design's main advantage also comes with a major drawback. This design requires Aegis to handle the full throughput of all the puts to the system. Aegis then has the full responsibility of being available to all puts and, in a failure scenario, to handle the recovery of the system. Additionally, the cache provisioned must be large enough to handle the largest files at maximum throughput with extra room for unexpected delays. This negatively affects the scope of the project by requiring the solution to prioritise features that are already covered by MinIO.

Because MinIO is dependent on Aegis to handle the puts, MinIO must wait to be passed incoming objects sequentially after Aegis has finished processing the previous object. This removes the potential for aggregate performance where

4.3. Candidate Design 3 - Write Interception

Candidate Design three is very similar to the second candidate design, however, instead of wrapping outside the MinIO service, it intercepts the writes from the client before objects are written to the object store. With this interception, Aegis can scan the object and decide whether to allow the object to be written to the store or to quarantine the object. The candidate design is shown in figure 3.

This candidate design has similar benefits as the second candidate design. It offers the most protection against malicious files by never allowing either un-scanned or infected objects to be stored in the object store. However, it also has similar drawbacks. This is because Aegis is still in sequence with MinIO meaning that for optimal throughput, Aegis would need to match the performance of MinIO.

Similar to the upload queue candidate design, this design also requires Aegis to have a large cache to handle the largest files at maximum throughput. This cache must also be large enough to handle the number of objects being put by MinIO into the store. This issue cannot be mitigated without the risk of compromising performance at increased loads.

However, this design does have an advantage over the second candidate design as there is less responsibility placed on Aegis to be as failure tolerant.

MinIO is still directly responsible for accepting objects into the store and therefore is still

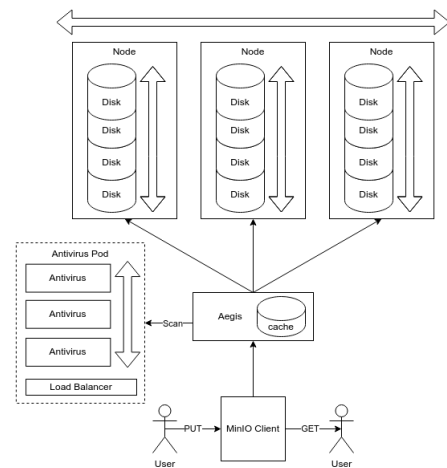


Figure 3: Write Interception Architecture

responsible for the recovery of the system in a failure scenario. This allows the scope to focus on more related features to malware scanning.

4.4. Candidate Design 4 - Per Node

The final candidate design distributes Aegis onto each node in the object store. This means that each node has a local instance of Aegis that is responsible for scanning objects before they are written to the store. The candidate design is shown in figure 4.

This candidate design makes use of the distributed nature of MinIO to match the demand when scaling out the system. As more nodes are added, more Aegis instances are added to handle the increased scanning demand. This removes the need for having a cache repository as Aegis already has access to the files that need scanning. By removing this single point of failure, in theory, the system only relies on the antivirus pod to be able to scale out on its own.

Independent scaling of the antivirus pod allow for efficient usage of available hardware. A simple load based auto-scaler can be used to scale the number of pods based on the current load. This allows for the system to flexible scale with the demand of the system and to reduce usage of valuable resources, such as power. There is also the opportunity to use intelligent scaling techniques to predict the load on the system and prematurely scale the system to meet the demand. For example, to scale the number of pods depending on the time of day or the day of the week.

The major drawback of this candidate design is that it relies on the ability to scan whole files by only using data on a single node. In actual implementations, MinIO makes use of erasure coding to add increased redundancy to the store (MinIO Erasure Coding, 2023). Erasure coding splits objects into multiple parts known as blocks, and then calculates corresponding parity blocks. These data and parity blocks are then distributed among all nodes in the system allowing for on-the-fly data recovery even with the loss of multiple drives or nodes . This means that the Aegis instance on each node only has access to the part available on their node and therefore will not be able to reconstruct the whole file for scanning. This makes this candidate design unsuitable for MinIO as it erasure coding is one of its key features.

4.5. Selected Candidate Design

Given the above evaluations of each candidate design, design one best meets the requirements and constraints of the project. It makes the most use of the existing features that MinIO provides in order to handle failure scenarios and to scale out. This also means that this design has less

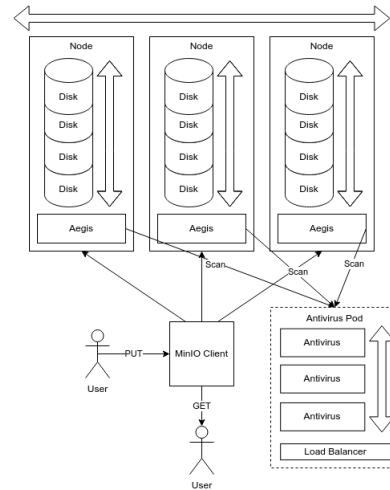


Figure 4: Antivirus per Node Architecture

critical responsibility and will better fit the scope constraints allowing for more time to be spent on supplementary features, such as testing, logging, and metric collection. Because of this, the produced solution will be closer to production-ready than the other candidate designs.

This candidate design keeps the user in control by giving them the ability to store unscanned files / known malware without wasting resources on a scan. Protection can be added per bucket therefore a user could have a known malware bucket and a clean bucket within the same object store. This allows for the system to be more flexible and to be able to handle more use cases. Candidate Designs two and three would not be as able to handle this use case as they both scan all objects before they are written to the store.

The size of the cache required is smaller than all other candidate designs as it only needs to store the objects actively being scanned. This is in opposition to upload queue and write interception candidate designs as they have to be prepared to handle the full demand placed on the store. This makes candidate design one the most lightweight of all the candidate designs which should lead to a smaller resource footprint.

In the event of an error or high demand, a backlog of requests would be stored on the event queue enabling system to recover from a failure scenario without losing any scan requests. This is in contrast to the other candidate designs where the incoming requests are directly handled by Aegis and in the event of a failure or high demand, the requests would be lost. This is an example of event driven architecture (EDA), the asynchronous processing of events, being used to improve the reliability of the system (Zhelev and Rozeva, 2019).

5. Implementation

5.1. Service Selection and Creation

Throughout the implementation, the development of the solution followed a waterfall approach. The project's progress was determined by milestones outlined in the project plan Gantt chart, which can be found in the appendix at figure 10. As this is a solo project with a limited timeline, the waterfall methodology is a better fit than an agile methodology as agile caters more to larger team with longer timelines where the requirements are less concrete.

Before beginning to implement the solution, it was necessary to research, create, configure, and understand each external service that would be used. Up to this point, the types of services needed were identified, but the specific services to be used had not been determined. This section will describe the process of selecting each service and then initially configuring them to form a bare-bones proof of concept.

Object Store - MinIO

The object store is the only service that did not require further research or comparison as it is already the subject of this project. However, creating and configuring a local instance of MinIO for development was necessary. MinIO itself is available from various sources, including Docker, Homebrew, and the MinIO website. Homebrew, a MacOS package manager, was chosen as it is the easiest to install and update. The MinIO documentation was then used to create a local instance of MinIO accessible through the web client at <http://localhost:9000>. This allowed for

the creation of buckets, uploading objects to the store, and familiarization with MinIO's features. An image of the MinIO console is available in the appendix at figure 11.

MinIO has integrated the ability to send notifications to event queues depending on the operation performed on the store. This makes it quick and easy to set up a locally running instance of an event queue to read messages sent by MinIO. MinIO offers wide support for many different event queues, such as Kafka, Webhook, Redis, PostgreSQL, and many more.

Event Queue

Any event queue is needed to store the incoming events produced from MinIO whenever a put event is triggered. The event queue must be able to handle a high throughput of events and be able to scale out to meet the demand of the system (Zhelev and Rozeva, 2019).

Kafka is a popular and well-supported event queue that is used in many different industries (Zhelev and Rozeva, 2019). It offers many features that make it a good choice for this project, such as high-throughput, low latency, and open-source. Kafka is also available from both Docker and Homebrew, making it easy to install and run locally. Most modern event queues offer similar high throughput and low latency, but Kafka is lighter in resource usage than other queues, such as RabbitMQ (Levy, 2022). This is beneficial as it will be easier to implement and not overuse resources when it has a simple use case.

Kafka has a dependency on Zookeeper, which is a distributed coordination service (Zhelev and Rozeva, 2019). Zookeeper must be installed as a separate service but is available from the same sources as Kafka. Kafka can be run in Kafka Raft mode (KRaft), which will eventually replace Zookeeper, but as of writing KRaft has not been fully adopted yet (M, 2022).

With Kafka and Zookeeper set up, the Kafka command line interface (CLI) was used to start the service and create a topic. The MinIO documentation was then used to configure MinIO to send all put notifications to the Kafka topic. The Kafka CLI was used to read messages from the topic and see the messages sent by MinIO. This demonstrated that the event queue is working and that MinIO is sending messages to it whenever a put operation is performed. An example Kafka message is available in the appendix in listing 1.

Antivirus

The antivirus chosen needed to meet a list of requirements for it to be suitable for use in this project. Firstly, it must be able to scale with the solution in order to keep up with the demand placed on the system. Secondly, it must have a CLI that the program can interact with in order to scan files. Finally, it must be free or as inexpensive as possible to make it viable for commercial use. This narrows down the available options to a few contenders.

Sophos is a popular antivirus that is used by many businesses and is available for free for personal use. However, has some major downsides. It is both paid for commercial use and uses more naive signature detection techniques as stated in (Ormandy, 2011). This makes it less suitable for this project.

ClamAV, on the other hand, is completely free and open-source. It comes with a scalable and multi-threaded daemon that can be accessed via CLI for high-performance and on-demand file scanning (ClamAV, 2023a). It is capable of scanning many different file types, including archives and mail files. Built-in is freshclam, a tool for automatically updating the virus database

definitions. The virus database itself is also open-source and is updated regularly by the open source community. Although ClamAV is not the fastest or most accurate antivirus, it offers a good starting point to building a solution with multiple antivirus engines for higher accuracy as stated in (Omer, 2017). ClamAV has a docker image and is available from Homebrew.

ClamAV was chosen for this project because it is entirely free for commercial use, open-source, and has a CLI that can be used to scan files. It is also very well documented and has a large community of users who regularly update and maintain the virus database.

ClamAV comes with a daemon, clamd, that can be run in the background and can be accessed via a CLI using clamdscan, the clamd client. A configuration file is needed to point clamdscan to the IP address that the daemon is running. In this case, it is running locally on port 3310. Performing the clamdscan command and providing a file will scan the file and return the result. An example of this is available in the appendix in listing 2.

Aegis will be designed so that it can be easily extended to support multiple antivirus engines aggregated together for higher accuracy (Omer, 2017). Initially, only ClamAV will be implemented.

Metric Collection

As the project is expected to be as production-ready as possible, a system for collecting metrics is needed. This will allow the system to monitor its activity for easier maintenance, debugging and to aid in the evaluation section of this report. A few different options are available for metric collection, such as Prometheus, InfluxDB, and Graphite with Prometheus being the best option as it is open-source and the most popular metric server. It uses a pull model which periodically scrapes metrics from a specified address and endpoint. Prometheus then aggregates the results from the scrape and stores them in a time-series database (Prometheus, 2023). This database can be queried through Prometheus or exposed to another graphing service, such as Grafana.

Prometheus also has the ability to gather metrics short-term processes via a push gateway which pushes metrics on completion instead of waiting for the scrape period. However, this is not needed for this project as centralised metric collectors will be used to continually aggregate and expose metrics. Prometheus is available for download from Homebrew as well as a Docker image available.

Prometheus is currently unusable as it is not being sent any metrics to collect. However, the Prometheus server can still be launched, and the web interface can be accessed on port 9090 (Prometheus, 2023). In the meantime, a configuration file can be created, defining the address and endpoint expected to be exposing metrics to, in this case, address `localhost:2112` and `/metrics`.

Audit Log Store

Production-ready software should have a method to store logs for auditing and analysis purposes. A central database can be used due to the relatively low amount of data needing to be written and stored. The audit log's purpose is to store information about the scans performed by the system, such as the time and result of the scan, as well as the antivirus used. In the case that the scan returns an infected result, the type of malware found should be recorded. This allows the system to review previous scans, which can aid in debugging and maintenance.

PostgreSQL is an open-source object-relational database management system compliant with SQL standard queries (Drake and Worsley, 2002). Since the use case is simple, SQL queries can be used to perform all actions needed when recording audit logs shown in the PostgreSQL guide (Momjian, 2001). PostgreSQL is also available from both Docker and Homebrew.

At this stage, PostgreSQL is not yet storing any data. However, the PostgreSQL server can be launched, and the database accessed via the PostgreSQL shell prompt (psql). A database and a user for the database can be created. The database can then be exposed to port 5432 on the localhost, making it ready for Aegis to use.

Data Visualisation

The final dependency that needs to be configured is a data visualisation tool. This will not directly be implemented into the microservice but instead will be connected to Prometheus to display the metrics collected. Grafana is a popular open-source data visualisation tool that allows you to visualise and query the metrics produced (Sharma, 2022). Grafana enables the creation of dashboards that can display multiple relevant metrics in a single view.

Data visualisation will be an important part of this project for both the evaluation section and for the system's ongoing maintenance.

5.2. Aegis Module Design and Creation

Now all of the dependencies have been downloaded, initialised and configured, the Aegis Go module can be created. A module is a collection of packages

The most common language to use for microservice based projects is GoLang. Go is a compiled language that is statically typed and high concurrency support. This makes it a perfect fit for this project to ensure that the system is as performant as possible. MinIO is also written in Go should allow for easier integration. Go has certain standards and guidelines for clean architecture that should be followed to ensure high usability and efficiency.

Go introduces some specific language that are commonly used during the project. A list of common terms and their definitions are available in table 3.

Go Specific Term	Definition
Go keyword	Launches a function as a goroutine, which is a lightweight thread managed by the Go runtime, enabling concurrent execution.
Select	Waits on multiple communication operations, typically used with channels, to handle different cases depending on which operation is ready.
Switch	Multi-way branching statement that allows conditional execution of code blocks based on the evaluation of an expression or comparisons.
Goroutine	Lightweight thread managed by Go runtime, allowing concurrent execution of functions without the overhead of managing traditional threads.
Channel	Communication mechanism between goroutines, allowing them to synchronize and share data, providing a way to safely pass data between them.
Struct	Composite data type for creating custom structures composed of different fields, useful for grouping related data together.
Package	Collection of related Go source files organized under a specific namespace, allowing code organization, reuse, and dependency management.
Module	Collection of related Go packages, providing versioning and dependency management, simplifying the process of building and sharing Go code.
Capitalised first letters	All functions, variables and types that are intended to be exported outside of a package must be capitalised.
Defer	Defers the execution of a function until the surrounding function returns.

Table 3: Go Specific Terms and Their Definitions

Project Structure

In Go you should separate the code into different packages, where each package represents a distinct function of the system. This allows for easier maintenance and debugging in the future. These packages are then grouped into different directories depending on their intended scope and function. There are three main directories that are used in GoLang projects, `cmd`, `pkg` and `internal`. The `cmd` directory is used to store the `main.go` file which manages the workflow and is the entry point of the program. The `pkg` directory is used to store all of the packages that are intended to be used by external applications, in this case our other services. The `internal` directory is used to store all of the packages that are intended to be used by the application itself. This is where the packages in the `pkg` directory will be consumed to perform the Aegis' core actions as follows:

- Listen for PUT events on the event queue
- Read the message from the event queue and extract the bucket and object path
- GET the object from the object store and store in cache
- Initiate a scan on the object using the antivirus software
- Collect the result of the scan and add tags to the object
- Collect metrics throughout the process
- Store the result of the scan in the audit log
- Expose metrics to Prometheus

From these requirements, the internal design of Aegis can be planned. We can visualise this plan using various UML diagrams such as, class, sequence and flow diagrams. Class diagrams are useful for understanding the relationships between different classes - in this case packages - and what attributes and methods they require (Doaa *et al.*, 2022). It is worth noting that Go itself does not have classes but instead uses structs which can be used to achieve the same effect. Sequence diagrams are also valuable for understanding the timeline of the system during the execution of a workflow (Yang, 2009). Flow diagrams are useful for visualising the flow of

processes and decisions during a workflow. This class diagram is shown in the appendix at figure 12 along side with a both the sequence and flow diagram at figures 13 and 14 respectively.

From this diagram a file structure can be created inline with Go standards. Go comes with a CLI tool used to initialise a new go module, which is a collection of packages that are intended to be used together. This tool will create a go mod file which is used to define the module and its dependencies. This tool will also create a go sum file which is used to store the hashes of the dependencies to ensure that the same version is used across all environments. Now go commands can be used to install go dependencies and then download them to a local vendor folder for use in building. Building the project is also done with the go CLI. All binaries are stored within the build folder. The initial project structure is shown by the figure 5.

Version Control

Considering the size of this project, version control is necessary to ensure maintainability and the availability of a backup. Git, in combination with GitHub, was chosen for version control due to its widespread use, familiarity, and cost-free nature. The Git CLI was used to initialize a new repository within the root directory of the Go module. Additionally, a .gitignore file was created to prevent unnecessary files from being tracked by Git, such as, the vendor or build folder.

To maintain usability, commits to the remote GitHub repository will be made after each significant change to the project, accompanied by relevant commit messages. This approach facilitates easier tracking of changes for debugging and maintenance purposes.

Structured Logging

Structured logging is a method of logging that allows for easier parsing of the log messages by adding structure to the message (Jayathilake, 2012). This is done by adding key value pairs containing relevant information to the log message. This enables for easier filtering and searching of the logs. This is especially useful when using a log aggregation tool such as, Splunk or LogRhythm (Jayathilake, 2012).

Go has many external modules that can handle this type of logging including Zap by Uber. Zap is a very fast and efficient logging library that can be configured to change the level of logging output, such as for info or debug useful for production or development respectively

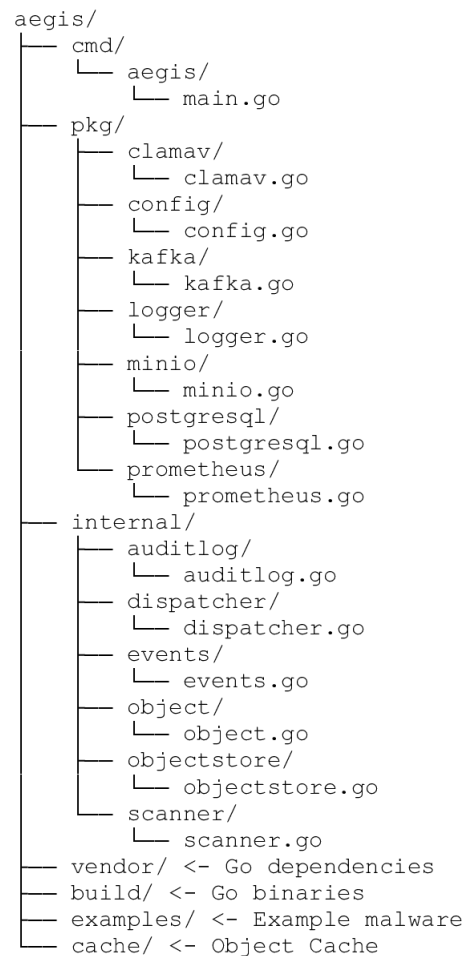


Figure 5: Aegis' Initial File Structure

(Uber, 2023). Zap also has the ability to change between structured and unstructured logging depending on the use case. Structured logging comes with the drawback of being less human readable than unstructured logging and therefore Zap offers the ability to change between the two (Uber, 2023).

As Zap is an external module, it must be added as a dependency and all code contained in the pkg folder. A package called logger is created to encapsulate all logging functionality. This package contains two go files, one for interacting with the Zap and one for defining the structure of the log commands inside of an interface. In Go, it is idiomatic to keep the interface as close to the implementation as possible. Keeping the interface in the same package as the implementation allows for easier mocking of the package when testing. This package goes against this by containing the interface within the repository because multiple packages will need to use the same interface when interacting with them. This reduces code duplication as we don't have to define the interface in each package that uses it, which in this case would be every package.

Configuration

As Aegis is a microservice, it is important that it is configurable to allow for easy deployment to different environments. This is done by using a configuration file in tandem with Viper, a Go module that can read in the configuration file (spf13, 2023).

This configuration file contains all of the values that are likely to change between environments. This includes values such as the endpoints, ports and credentials of external services, logging options and database names. This configuration file will be a dotenv file which is a key value store of environment variables. This is beneficial as Viper has the ability automatically override the config file with environment variables if the same key is found. This allows for easier configuration of the application when it is built locally or deployed in a Kubernetes cluster. This gives the user the ability to tailor the deployment to their needs or existing implementation.

Much like the logger package, the configuration package contains two go files. A repository file that defines the interface and a config file that contains the Viper configuration.

Adding both the configuration and structured logging as the first packages reduces the need for refactoring in the future. No hard coded values are needed for initial development as all values can be stored in the configuration file from the start.

Makefile

A Makefile is a file that contains a set of instructions that can be run from the command line (GNU, 2023). These instructions are used to automate processes such as building, testing and deploying. Through the project, longer workflows will be automated and put into the Makefile to reduce the amount of time spent on running commands. Makefiles also simplify the usage of program by users by encapsulating complex commands into an explicit action the user can understand. Makefile commands can also be used by the Dockerfile when building the application in a container.

5.3. External Package Integration

With the dependency services still running, the next step is to integrate them into the Aegis application using Go. This is done by creating a new package for each of the services within

the pkg folder. Each package will contain a go file for each of the services that will later be consumed by Aegis' internal workflow.

One significant advantage of separating external services from internal implementation is that it allows for a higher level of abstraction from the services used. This abstraction provides flexibility in the use of multiple external services that fulfill the same purpose, such as multiple antivirus scanners. The creation of external packages allows for the use of a single internal implementation for all of these services. This reduces the need for extensive changes in the future, making the application more maintainable and scalable.

MinIO

The initial external service to be incorporated is MinIO. The MinIO package manages interactions with the MinIO service. For this project, the required operations include getting, putting, and removing objects, as well as getting and putting tags. MinIO provides a Go Software Development Kit (SDK) that already supports these operations in Go (MinIO, 2023a). The SDK simplifies the complexities of making requests and offers straightforward methods for operations such as putting and getting, as well as accessing type definitions like tags.

Once the MinIO SDK is imported, a new MinIO client object is generated to communicate with the MinIO service. The `CreateMinio` function accepts essential connection parameters, such as a context, an endpoint, access and secret keys, and an SSL usage flag, and initializes the MinIO client using the `minio.New` function. This client object is then incorporated into a custom `Minio` struct, along with a logger. Various methods are implemented for the `Minio` struct to execute different object storage operations:

- `GetObject`: Retrieves an object from a specified bucket and returns its data as a byte slice.
- `PutObject`: Takes in a byte stream and uploads it to a specified bucket with a specified object name.
- `RemoveObject`: Removes a specified object from a specified bucket.
- `GetObjectTagging`: Fetches the tags associated with an object and returns them as a map of key-value pairs.
- `PutObjectTagging`: Replaces the existing tags of an object with a new set of tags provided as a map of key-value pairs.
- `AddObjectTagging`: Adds new tags to an object by first fetching the existing tags, updating them with the new key-value pairs, and then setting the updated tags back to the object. Necessary for not overriding existing object tags that may exist.

All of these methods take in a context which is used in the shutdown process to close the connection to the MinIO service. This context is passed in during the creation of the `MinIO` struct so that all methods have access.

Kafka

The next external service to be integrated is Kafka. The Kafka package will handle the interactions with the Kafka service. For this project, the operations needed are to consume messages from a specified topic. Kafka provides a Go library, *kafka-go*, which simplifies the consumption of messages in a Go application (Segmentio, 2022).

The package imports necessary dependencies and creates a custom `KafkaConsumer` struct, which embeds a `kafka.Reader` object and a logger. The `CreateKafkaConsumer` function initializes a new `KafkaConsumer` instance by taking connection parameters such as the list of brokers, the topic to be consumed, a group ID, and a maximum number of bytes per message.

- `ReadMessage`: Uses the Kafka library to halt until a message is received from the specified topic. It then decodes it using the `decodeMessage` function, and returns the bucket name and object key.
- `decodeMessage`: Decodes a Kafka message by unmarshalling its JSON payload and extracting the bucket name and object key. If the message event is `s3:ObjectCreated:PutTagging`, it returns empty strings, as this event does not require processing.

During the shutdown process, the `ReadMessage` function is halted by closing the context passed in. This closes the connection to the Kafka service and therefore stops the reading of any new Kafka messages, leaving unprocessed messages in the event queue.

ClamAV

ClamAV is another external service to be integrated into the project. The primary operation needed for this project is scanning a file and returning the scan results. The ClamAV daemon can be interacted with through the command-line interface (CLI) using the `clamscan` command (ClamAV, 2023b).

Initially, a `ClamAVScanner` struct is created, embedding a logger. The `CreateClamAV` function initializes a new `ClamAVScanner` instance. Methods for the `ClamAVScanner` struct are implemented to perform various file scanning operations:

- `ScanFile`: Accepts a file path as an argument and scans the file using the built-in Go `exec` library to run the `clamscan` command with the `--config` flag set to use a custom configuration file located at `clamav.conf`. The `exec` library enables the execution of external commands, providing the ability to interact with the ClamAV antivirus daemon. A process attribute is added, which starts the process in a different process group than the main execution. This approach aids in achieving a graceful shutdown later on, as calling a system interrupt terminates the entire process group (McKusick *et al.*, 2014). As a result, `ScanFile` can continue executing after the shutdown, ensuring that no scans are interrupted. The method returns false if the file is clean, true if infected, and the type of malware detected. If any errors occur during the execution, it returns true (infected) along with an error message, ensuring that the worst-case scenario is assumed when it comes to security.
- `findVirusType`: Takes the output from the `clamscan` command, extracts the virus type using regular expressions, and returns it as a string.
- `GetName`: Returns the name of the antivirus engine, in this case, "clamav". The name must be accessed through a method, as ClamAV will implement an interface that does not have access to any attributes.

This package can now implement the `Antivirus` interface given in the internal scanner package and be used as an antivirus engines. More external antivirus services can be created in the same way, as long as they implement the `Antivirus` interface, if they are needed in the future.

Prometheus

The Prometheus package is in charge of creating and managing an HTTP server that exports metrics from Aegis. It does this by providing a plaintext response containing the metrics in the Prometheus exposition format. The exposed endpoint is then used by the Prometheus server to collect metrics from Aegis.

- `CreatePrometheusServer`: Initializes a new Prometheus exporter by setting up a new HTTP server with the specified endpoint and path. The Prometheus handler, provided by the `promhttp.Handler()` function from the Prometheus Go client library, is linked to the given path, which serves the plaintext. Read and write timeouts for the HTTP server are established using constants since these values are not expected to be configurable.
- `Start`: Initiates the Prometheus server by calling the `ListenAndServe()` method on the HTTP server. An example of the generated plaintext output can be found in the appendix at listing 3.
- `Stop`: Handles the graceful shutdown of the Prometheus server by invoking the `Shutdown` method to close the HTTP server.

PostgreSQL

The package imports necessary dependencies and creates a custom `PostgresqlDB` struct, which embeds a `pgxpool.Pool` object and a logger. The `CreatePostgresqlDB` function initializes a new `PostgresqlDB` instance by taking connection parameters such as the user, password, endpoint, and database name. It also returns a `CloseFunc` function to close the connection when needed.

- `CreatePostgresqlDB`: Is responsible for establishing a connection to the PostgreSQL database and returning a `PostgresqlDB` instance. The function takes in connection parameters such as the user, password, endpoint and database name. Additionally, it returns a `CloseFunc` function to facilitate a graceful shutdown of the connection pool when necessary. Instead of connecting straight to the database, the function uses a connection pool to manage connections. This allows multiple concurrent clients to perform operations on the database without having to wait for other clients to finish their transactions. In this case, when multiple files are being scanned at the same time and the results are being saved to the database, the connection pool ensures that a database connection is always available.
- `CreateTable`: Uses the connection pool to create a new table with the specified name if it does not exist. The table schema includes columns for ID, ObjectKey, BucketName, Result, Antivirus, Timestamp, and VirusType. The SQL query used to execute this operation is available in the appendix at listing 4.
- `Insert`: Uses the connection pool to insert a record into the specified table with values for ObjectKey, BucketName, Result, Antivirus, Timestamp, and VirusType. The SQL query used to insert is available in the appendix at listing 5.

The PostgreSQL instance is provided with a context to close the connection to the database when the application is shutting down.

5.4. Aegis' Internal Workflow

Metrics and Collectors

The internal metrics collection comprises two primary components: the metric manager and various metric collectors specific to each package. The metric manager is responsible for managing interactions with Prometheus, which includes executing the `Start` and `Stop` methods for handling the starting and graceful shutdown of Prometheus respectively.

Each package contains a metric collector in a file named `metrics.go`. These collectors define the available metrics that can be collected and exported by the respective packages. The `promauto` library facilitates the creation of a global registry when the metric manager is initialized. This registry is accessed by all metric collectors to record the metrics they collect and is also utilized by the Prometheus exporter for publishing these metrics.

Object

The object package presents the `Object` struct as the internal representation of an object within the object store. It includes all methods and attributes related to an object, such as the object key (the path of the object within a bucket) and bucket name. Operations involving an object are performed within the object instance itself.

Since the object represents a concrete entity, there is no need for an interface when using it. This design choice allows the object to have attributes that can be accessed directly, without the need for getter functions.

The `CreateObject` function enables the creation of a new `Object` instance, given a specified object key and bucket name.

The `SetCachePath` method defines the cache path for an object by concatenating the cache path, bucket name, and object key, separated by slashes. This method is called when an update to the cache path is needed.

The `SaveByteStreamToFile` method stores an object's byte stream in a file. First, it checks if the path attribute is empty since, by default, no path is provided. It returns an error if this is the case, as other types of scanners may not always require this information to perform a scan. Next, it ensures that the file's parent directory exists, creating it if necessary. Lastly, the method writes the byte stream to the file using Go's built-in IO writer.

The `RemoveFileFromCache` method is responsible for deleting an object file from the cache. It tries to remove the file specified by the object's path attribute. If the removal is unsuccessful, it logs an error message and returns the error.

Events Manager

The events package includes the event manager, which is responsible for reading messages from the event queue and forwarding scan requests to the scanner. The `Kafka` interface provides methods for reading messages from the Kafka queue and closing the connection. The `EventManager` struct consists of four fields: a `logger`, a `kafka` instance for interacting with Kafka, a `scanChan` channel to forward scan requests and an `eventsCollector` for gathering metrics.

The `CreateEventManager` function creates a new `EventManager` instance, accepting the necessary arguments. The `Start` method of the `EventManager` takes in a context and

then enters a loop that uses a switch statement to first check if the context has been canceled. If it has, it closes the `scanChan` channel, closes the Kafka connection and returns. Otherwise, it invokes the `ReadMessage` method of the `kafka` instance to read a message from the Kafka queue. Upon confirming that there is no error and the message is not nil, it increments the `eventsCollector` counter and creates a new `object.Object` instance with the received bucket name and object key. It then forwards the object to the `scanChan` channel for scanning.

Since the event manager runs within a goroutine, if an error occurs, it sends the error to the provided `errChan` channel.

Object Store

In the object store package, several structs and interfaces are defined to handle object storage operations. The `Minio` interface contains the abstract object store operations, such as; get, put and remove objects, as well as get and put object tags. These are also reflected by the `ObjectStoreCollector` in the form of metric counters that track the number of each operation performed.

Once the object store is created by the `CreateObjectStore` function, it can be used by the rest of the application to perform object storage operations. In addition to the standard object storage operations, two more operations are added to the object store: `MoveObject` and `AddObjectTagging`. These both combine multiple standard operations into one as follows:

- `MoveObject`: Retrieves an object from the source bucket, puts it into the destination bucket, and removes it from the source bucket.
- `AddObjectTagging`: Retrieves the object tags from the source bucket, adds the new tags to the existing ones, and puts the combined object tags onto the object.

Object Scanner

The scanner package provides the functionality for multiple workflows when it comes to scanning an object. In this instance, an object scanner refers to process of downloading the object from the object store, performing a scan with its antivirus engines, and then passing the result to the cleaner which will execute the cleanup policy. Having the ability to use multiple types of scanners allows for flexibility in the system as in the future, the workflow for scanning an object might change. For example, if one of the antivirus engines could require the hash of the file. In this case, another scanner called `HashScanner` could be created to handle this alternate workflow. For this project, the `ObjectScanner` will be the only type of scanner implemented.

The `CreateObjectScanner` function creates a new `ObjectScanner` instance with the following arguments:

- `logger`: A logger instance for logging messages.
- `objectStore`: An object store instance for downloading objects.
- `antiviruses`: An array of antivirus instances for scanning objects.
- `cleaner`: A cleaner instance for cleaning up objects.
- `auditLogger`: An audit logger instance for logging scan results.
- `scanCollector`: A scan collector instance for collecting metrics.
- Various configuration values, such as, `removeAfterScan`, `datetimeFormat`, and `cachePath`.

All instances passed to the `CreateObjectScanner` function are interfaced to both allow for future mocking and to allow for other abstract implementations of the interfaces. Namely, the `Antivirus` interface is implemented by the external antivirus engines.

The `ScanObject` method handles the workflow for downloading and scanning an object. It takes in an `object.Object` instance, which it fetches from the object store, and an `errChan` for returning errors. It then sets the object cache path by calling `SetCachePath` on the object. With this set, the scanner can perform a `GetObject` on the object store to retrieve the byte stream of the object and call `SaveByteStreamToCache` with the byte stream to save it to the cache.

The scanner can now perform a scan on the object by calling `Scan`, with the cache location, on every antivirus engine. If any of the antivirus engines detect the object as infected, then using the assume the worst mentality, the file is deemed infected. The object is then passed to the cleaner to execute the cleanup policy. During this execution various metrics are being collected by the `scanCollector` about the scan, such as, the number of clean or infected files, total files scanned and total errors encountered. In addition, audit logs are also generated by the `auditLogger` for each scan by each antivirus recording the object key, bucket name, antivirus name, scan result, timestamp and if infected, the virus type.

After performing the scan and dealing with the results, if the `removeAfterScan` flag is set to true, the object is removed from the cache after scanning.

The `ObjectScanner` is will be run within a goroutine, if an error is encountered during the scan, it will be sent to the provided `errChan`.

Cleanup Policies

As mentioned in the previous section, the `ObjectScanner` passes the object to the cleaner to execute the cleanup policy. The cleaner package defines how to react given a clean or infected result from the antivirus engines. Multiple policies are available in the `config.env` file to give the user flexibility in how they want to deal with infected objects. These policies include:

- **Tag:** Adds a tag to the object in the object store based on the scan result.
- **Remove:** Removes the object from the object store if it is deemed infected
- **Quarantine:** Moves the object to a quarantine bucket if it is deemed infected.

In `CreateCleaner` function, a new `Cleaner` instance is created with a logger, object store, metrics and audit loggers, and various configuration parameters such as the cleanup policy and quarantine bucket.

The `Cleanup` method is called by the `ObjectScanner` where it passes the object after it has been scanned. This method uses a switch statement, shown in figure 6, to determine which policy to implement and executes the appropriate cleanup method. If no policy is specified, the switch statement has a default case of logging that it will do nothing, in the case that the user only wants the audit logs. However, when a cleanup policy is given, the corresponding cleanup method is called. Each of these use the object store and object store to perform the cleanup.


```

switch c.cleanupPolicy {
case "tag":
    err = c.TagInfected(object, result, scanTime)
case "remove":
    err = c.RemoveInfected(object, result, scanTime)
case "quarantine":
    err = c.QuarantineInfected(object, result, scanTime)
default:
    c.logger.Warnln("No cleanup policy found")
}

```

Figure 6: Cleanup policy switch statement

Dispatcher

The `dispatcher` package is responsible for managing the scanning of objects using multiple scanners concurrently. It defines a `Scanner` interface with a single method, `ScanObject`, that will be implemented by one of the available scanners. The `Dispatcher` struct contains three fields: a logger for logging messages, a `scanChan` channel for receiving object scan requests, with a `scanners` slice to hold the available scanners.

The `CreateDispatcher` initialises a new `Dispatcher` instance with the required fields. The `Start` method enters into a loop where it ranges over the `scanChan` channel. If the channel is empty, the loop will block until a new object is sent through the channel. If the channel has an object, the dispatcher will spawn a new goroutine to handle the scan. However, if the channel is closed, the loop will continue to process the remaining objects in the channel and then exit (Go by Example, 2022b). This is because when channels are closed, no more values can be sent to them, but the values that have already been sent can still be received (Go by Example, 2022a). This is shown in the provided dispatcher loop code in figure 7.

```

func (d *Dispatcher) Start(errChan chan error, done chan struct{}) {
    var wg sync.WaitGroup

    for request := range d.scanChan {
        for _, scanner := range d.scanners {
            wg.Add(1)
            go func(req *object.Object, sc Scanner) {
                defer wg.Done()
                sc.ScanObject(req, errChan)
            }(request, scanner)
        }
    }
    wg.Wait()
    done <- struct{}{} //Send empty done message
}

```

Figure 7: Dispatcher loop

When the program receives a termination signal, there should be no loss of information about

incoming scan requests. This is a security risk as it could lead to objects not being scanned. To prevent this, the dispatcher uses a `sync.WaitGroup` to wait for all goroutines to finish before exiting the program. This is done by calling `wg.Add(1)` before starting a new anonymous goroutine to increment an active goroutine counter, and using `defer wg.Done()` when the goroutine has finished to decrement the counter. The `wg.Wait()` call will block until the counter is zero, meaning all goroutines will have finished processing (Go by Example, 2022c). This ensures that all scans that are currently being processed since `scanChan` was closed will be completed before the program exits.

Main

The main package orchestrates the top-level workflow that Aegis executes throughout its operation. The entry point of the program is the `main` function, which performs one task - calling the `run` function and exiting the program based on its return value. This design choice enhances extensibility and testability since alternate workflows can be implemented while maintaining a single entry point. Furthermore, the `run` function can be tested without running the entire program (Ryer, 2020). The `run` function serves as an abstraction from `main`, as it encompasses Aegis' main workflow.

The `run` function is divided into three distinct sections: Initialization and configuration, the main loop, and cleanup. The initialization and configuration section is responsible for initializing all the components Aegis requires and configuring them with the values provided by the configuration package.

- The configuration is loaded from `config.env`, and the logger is created. An initial context is also created and passed to everything that requires it, apart from the event system.
- The metric manager and various metric collectors are created, with the metric manager taking in the Prometheus exporter.
- The audit logger is implemented by the PostgreSQL database.
- The object store is implemented by the Minio client.
- The event system is implemented by the Kafka consumer with the `scanChan` passed in as well.
- The scanning workflow is created. This includes creating the antivirus engines, in this case ClamAV, creating the cleaner with the configured policy and passing both of them to the scanners, namely the object scanner. The scanners are then passed to the dispatcher alongside the `scanChan`.

The main loop is the continuous execution of the goroutines that handle Aegis' asynchronous operations. These are the event manager, dispatcher, and metric manager. The goroutines are started using the `go` keyword, which spawns new goroutines to execute the functions in a separate thread. An additional context is created and passed into the `Start` method of the `EventManager`. Multiple channels are then created to handle errors, shutdown command, and the shutdown complete with `errChan`, `shutdownChan` and `done` respectively. The `Start` methods of the `EventManager`, `dispatcher` and `metricManager` are called to begin the main workflow of the program. An error channel (`errChan`) is created to handle errors generated by the event manager and metric manager goroutines.

Finally, the shutdown section ensures a smooth termination when the program receives an interrupt signal or encounters errors from the goroutines. The shutdown sequence is vital as it allows Aegis to maintain the progress of processed objects when receiving messages, enabling it to resume scanning objects from where it left off upon restart. The shutdown sequence unfolds as follows:

When an interrupt signal or an error from any goroutine is received, Aegis starts its graceful shutdown sequence. A `select` statement is used to wait for a message from either the `errChan` or `shutdownChan` channels. If any of these channels receive a message, a message or error is logged, and the shutdown sequence begins by canceling the context passed to the event manager. This action halts the event manager from consuming messages from the Kafka consumer and subsequently closes the `scanChan` channel. As a result, incoming notifications remain in the Kafka queue and can be consumed by Aegis upon restart leading to no scans lost.

The code then waits for the `done` channel to send a message, signaling that the goroutines have completed processing the remaining objects in the `scanChan` channel. Once this process is finished, the program stops the Prometheus metric exporter and exits with a status code of 0, indicating a successful operation. To better indicate the graceful shutdown process, a sequence diagram is available in the appendix at figure 15.

5.5. Testing

Unit Tests

Unit testing is an essential aspect of software development that focuses on testing individual units or components of a software application. The objective of unit testing is to ensure that each component functions correctly in isolation, thus improving the overall quality and reliability of the software.

In this project, unit tests were developed for each internal package, ensuring that the core functionality of each package was thoroughly tested. Unit tests were created using the built-in `testing` library. This package allows for the easy creation and execution of test cases, as well as the measurement of code coverage.

To facilitate the process of unit testing and ensure that the focus remains on the functionality of the components under test, the mocking technique was employed using the Mockery framework. This approach allows for the isolation of individual components by replacing dependencies with mock implementations.

Mocking

Mocking is a technique employed in unit testing to replace dependencies that packages rely on for their functionality. This allows for the testing of individual packages in isolation, minimizing the impact of potential errors from external sources and ensuring that tests focus solely on the functionality of the component being tested.

A mocking framework called Mockery is utilized for this purpose. Mockery is a tool that generates mocks implementing each interface within a package (Miguel, 2021). It offers the ability to override methods, enabling the mock to return a predetermined output for specific inputs. This capability can also be extended to accommodate any input of a specific type.

To generate the mocks, mockery has a configuration file in which defines where the mock files are created. I opted to create the mocks in the same package as the interface to avoid any import conflicts. Creation of the mocks can be done by the corresponding makefile command.

Code Coverage

The command `go test` is used to run tests, which outputs the results of all unit tests and the code coverage for the package. Code coverage is computed as the ratio of the number of lines of code executed to the total number of lines of code in the package, as illustrated in equation 1. Code coverage serves as a valuable metric for assessing the thoroughness of package testing.

$$\text{Code Coverage Percentage} = \frac{\text{Number of lines of code executed}}{\text{Total Number of lines of code in an application}} \times 100 \quad (1)$$

By combining unit tests and mocking techniques, thorough testing of each component's functionality was possible. Unit tests were continually updated and refined throughout the development process, contributing to the overall quality and reliability of the solution.

5.6. Kubernetes Deployment

To turn the solution into a microservice, a process is required to turn Aegis into a self-contained business unit. This process is called containerisation and is achieved by packaging the application and its dependencies into a container. Next, a deployment can be created

deployment to a Kubernetes cluster is required.

Docker

Docker is a platform for developing, shipping, and running applications in containers (Docker, 2022). Containers are lightweight, portable, and provide a consistent environment for applications, simplifying deployment and scaling. Docker allows developers to build and package applications and their dependencies into containers that can run on any system with Docker installed. These smaller, self-contained business units can be networked together to form a microservice architecture.

Kubernetes

Kubernetes (K8s) is an open-source container orchestration system for automating deployment, scaling, and management of containerised applications (Kubernetes, 2023). It groups containers into logical units called "pods" and manages their lifecycle, networking, and storage. Kubernetes enables the scaling of applications using multiple decentralised nodes controlled by internal and horizontal load balancers. Kubernetes supplies a CLI tool called `kubectl` for interacting and managing Kubernetes clusters.

K3d

K3d is a lightweight Kubernetes distribution designed for local development and testing (K3d, 2023). It runs Kubernetes clusters inside of Docker containers, making it easy to create, delete, and manage clusters using the provided CLI. K3d provides a convenient way to test Kubernetes deployments and configurations before deploying them to a production environment. K3d uses a configuration file called `k3d.yaml` to define the cluster's configuration, including creating a registry for storing Docker images, exposing ports, and mounting volumes (?).

Registries are used to store Docker images that will be available for Kubernetes to use. In this case, I create a local registry using K3d which I can then later upload the Aegis Docker image to using the k3d CLI.

Aegis Containerisation

For the Aegis solution to be deployed on Kubernetes, it needs to be containerised using Docker. A Dockerfile is used to describe the steps required to build the Docker image (Docker, 2023) (Baresi *et al.*, 2022). It contains 2 major sections. Firstly, for building the Aegis application, it defines the base docker image, in this case `golang:1.19`, and the instructions to compile the application. These instructions include copying the source code to the container along with any configuration files, such as the `config.env` and `clamd.conf` and building the application using the `makefile` command.

The second stage is for the execution of the program. This stage downloads the `clamscan` dependency, copies over the config files and the binary from the previous stage and then runs the application. This separation is beneficial because after the binary is build, the source code can be deleted which reduces the size of the image, therefore saving resource demand. Once the Docker image is built, it can be uploaded to the local container registry, ready for use by Kubernetes.

Helm

Helm is a package manager for Kubernetes that simplifies the deployment and management of applications on a Kubernetes cluster (Helm, 2023). It uses "charts" as templates for Kubernetes resources allowing for easy configuration, versioning, and sharing of applications. Helm charts define the application's networking, services, and dependencies, making it easy to deploy and maintain applications in a Kubernetes environment.

Helm can be used to streamline the installation and management of all the dependencies required for the solution. This approach saves time compared to manually installing and configuring each dependency, as described in the "Service Selection and Creation" section. Each of these dependencies has its own Helm chart, which can be found using the online Helm chart repository Artifact Hub (Artifact Hub, 2022). Artifact Hub stores the Helm charts that can be installed and managed using Helm, along with documentation on how to configure them.

Service Configuration

Using this documentation, environment variables can be configured for each deployment. Within the Helm chart, a `values.yaml` file holds the default values for these variables, which will be passed into several template files. These template files are used in Kubernetes to generate the appropriate configuration settings for each deployment. By customising the `values.yaml` file, you can tailor the deployments to suit the specific requirements of your environment. As

we have already allowed the overriding of variables in Aegis by using environment variables, this means that configuring the solution to work within Kubernetes is an easy task. In figure 8, you can see how these environment variables are overridden for Aegis and all other services.

```
env:
  MINIO_ENDPOINT: aegis-minio.default.svc.cluster.local:9000
  KAFKA_BROKERS: "aegis-kafka.default.svc.cluster.local:9092"
  PROMETHEUS_ENDPOINT: 0.0.0.0:2112
  PROMETHEUS_PATH: /metrics
  POSTGRESQL_ENDPOINT: aegis-postgresql.default.svc.cluster.local:5432

minio:
  auth:
    rootUser: minioadmin
    rootPassword: minioadmin

postgresql:
  auth:
    enablePostgresUser: true
    postgresPassword: postgres
    database: aegis_antivirus

kafka:
  auth:
    clientProtocol: plaintext
  provisioning:
    topics:
      - minio-put-events

clamav:
  service:
    milter:
      enabled: false
```

Figure 8: Overriding Environment Variables

Internal Communication

In Kubernetes, service endpoints are represented by DNS names that are automatically generated upon service creation. These DNS names resolve to the corresponding service's ClusterIP and remain stable throughout the service's lifecycle. To enable communication between services, these DNS names can be used as cluster internal addresses instead of the localhost address.

Utilizing DNS names instead of ClusterIPs offers several advantages, including the abstraction of the ClusterIP. This abstraction allows Kubernetes to change the ClusterIP without requiring any reconfiguration of the deployment to locate the updated IP. In the `env:` field of figure 8 you can see how the new addresses are used to configure the services to communicate with each other.

Exposing Services

ClusterIP services are only accessible within the node, so to access the services outside of the cluster, say to upload files to MinIO, a different type of service must be used (Martínez, 2022).

NodePort services expose the service on a static port on each node. NodePort has ports available in the range 30000-32767. NodePort can be used with all TCP or UDP traffic and therefore fits the purposes of all three services that need to be exposed; the MinIO console, Prometheus metric server and PostgreSQL audit log database. The main drawback with NodePort is that each node must be accessed separately, which is not ideal for a multi-node production environment. However, this is less of an issue as the solution is only being deployed on a single node.

The alternative to NodePort is LoadBalancer, which uses ClusterIP and NodePort services in combination to access all nodes in the cluster. As this is a single node cluster, there is no need to create a load balancer between them, so NodePort is sufficient. This can be changed in the Helm chart if need in the future.

In the appendix is an output logs displaying all services, pods and cronjobs from the command `kubectl get all` available in the figure 8.

Connecting Prometheus Metrics

The Prometheus deployment must be configured to know where to scrape metrics from. This can be done by adding annotations to the deployment, which can be seen in figure 9. These annotations tell the Prometheus deployment to scrape metrics from the Aegis service on the port 2112.

```
podAnnotations:
  prometheus.io/scrape: "true"
  prometheus.io/path: /metrics
  prometheus.io/port: "2112"
```

Figure 9: Adding Annotation for Prometheus

6. Results and Evaluation

Virus Database Updates

The Helm chart deployment of ClamAV

6.1. Solution Workflow

The solution is now ready for deployment. Provided below is the workflow of a standard deployment of the solution.

- 1) Ensure all dependencies are installed.
- 2) Launch the cluster with `make create-cluster`.
- 3) Connect to the MinIO web console at `localhost:9000`. You can perform all standard actions here, such as creating buckets and uploading files.
- 4) Add the event queue configuration to MinIO. Pictured in figure 16. You will need to restart the MinIO server for the change to update.

- 5) Configure a bucket to send put events to the event queue. Pictured in the appendix at figure 17.
- 6) Upload a file to the bucket. This will trigger Aegis to download and scan the file. The logs can be viewed in the appendix at figure 6.
- 7) Depending on the cleanup policy, Aegis will perform the appropriate cleanup action which can be seen on the web console.
- 8) In addition, you can connect to the Prometheus web console at `localhost:9090`. You can view the metrics collected by Prometheus here. Example is available in the appendix at figure 18. To use the metrics you can also connect Grafana to the same address.
- 9) Connect to the PostgreSQL database at `localhost:5432` using the `psql --localhost` command. You can view an example of the audit log in the appendix at figure 7.

6.2. Benefits of Metric Collection

Because of the metrics collection we implemented earlier, getting values such as files scanned and total infected files already present. Using the exposed Prometheus, Grafana can be used to visualise these metrics. These graphs can help us evaluate the performance of the solution.

6.3. Performance Evaluation

6.4. Comparing Functional Requirements

6.5. Comparing Non-Functional Requirements

6.6. Testing Evaluation

In Aegis, every internal package is accompanied by a set of unit tests. These tests can be executed using the Go CLI, and their coverage varies across different packages. The overall test coverage for Aegis is a good indicator of the effectiveness of the tests in place. This also supports the reliability of the solution as errors should be caught before deployment.

The current test coverage for Aegis is 85%. Supplied in the appendix in the output from performing the tests at figure ??.

For future development, achieving 100% coverage over all packages is a worth while goal, especially to claim production-ready status. This will ensure that every piece of code is thoroughly tested, improving the overall robustness and reliability of the system. One way to achieve this is through test-driven development (TDD), a software development methodology that involves writing tests before implementing the actual code. By adopting TDD, testing becomes the priority, and each package's level of quality and encapsulation will be constantly assessed, therefore catching more errors before deployment.

6.7. Project Aims Evaluation

Given the analysis of the functional and non-functional requirements...

7. Product Issues / Future work

7.1.

8. Conclusions

8.1.

9. Reflection on Learning

9.1.

10. Appendix

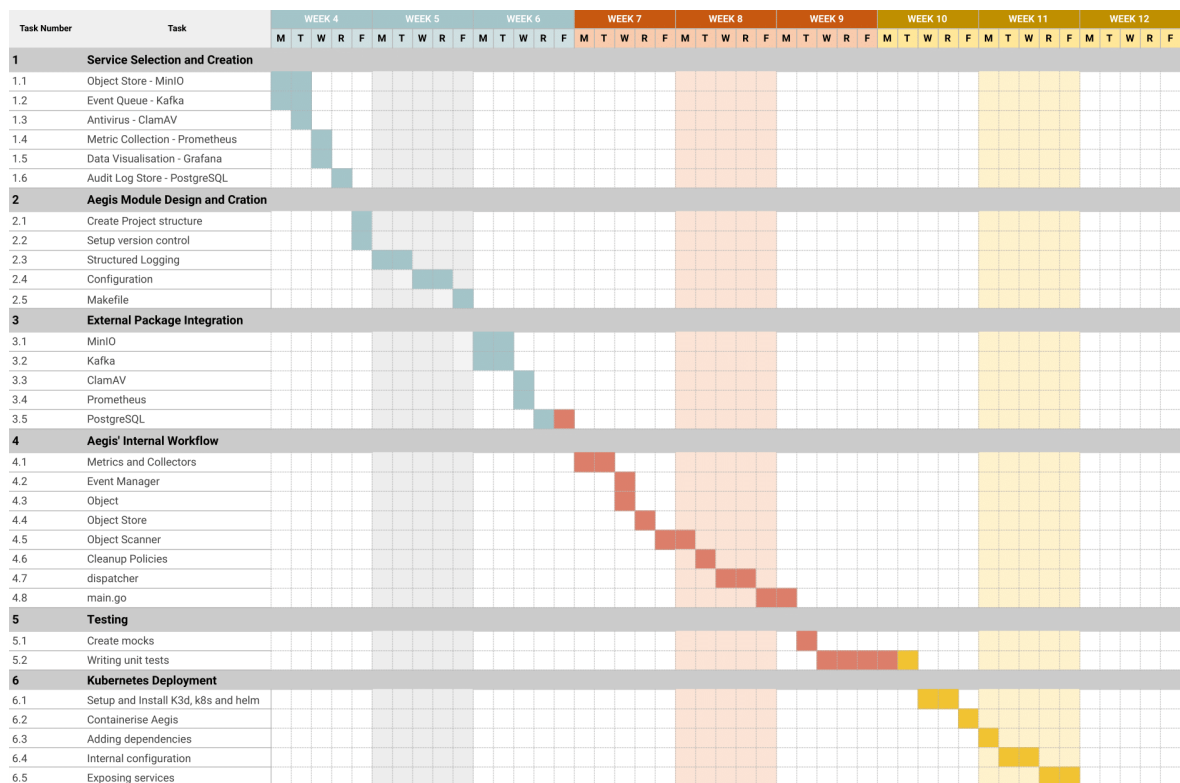


Figure 10: Timeline of Aegis' Development

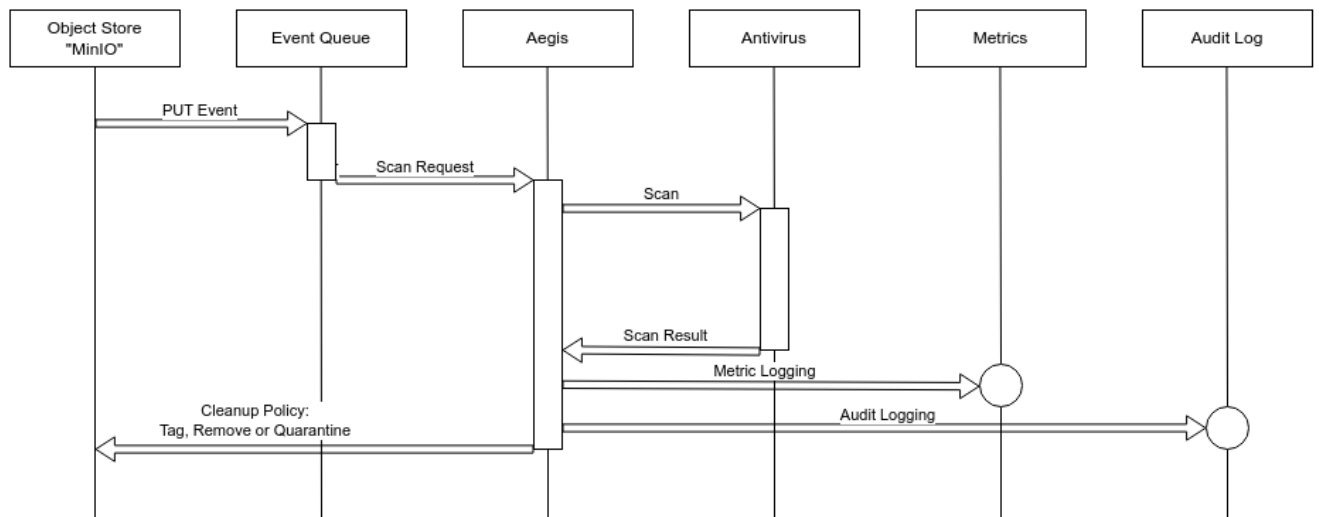


Figure 13: Aegis General Sequence Diagram

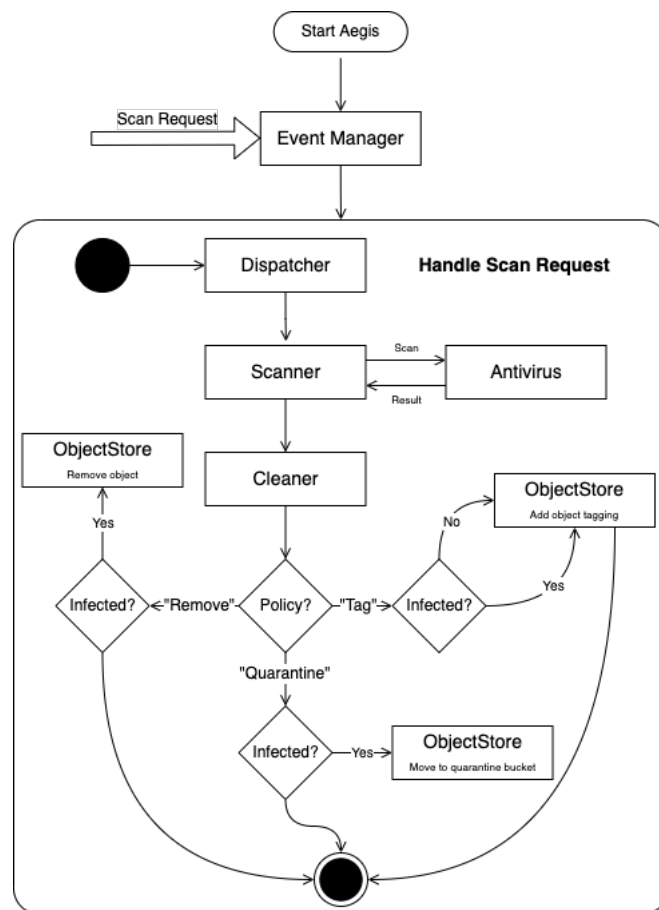


Figure 14: Aegis Scan Request Flow Diagram

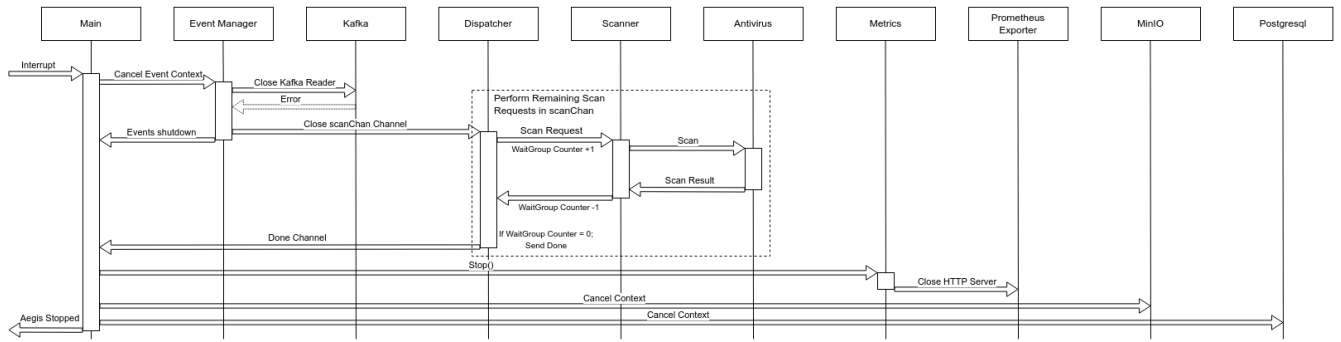


Figure 15: Aegis Shutdown Sequence Diagram

Listing 1: Example Kafka Notification

```

1 {
2   "eventName": "s3:ObjectCreated:Put",
3   "key": "test-bucket/gantt.png",
4   "Records": [
5     {
6       "eventVersion": "2.0",
7       "eventSource": "minio:s3",
8       "awsRegion": "",
9       "eventTime": "2023-03-24T12:23:27.844Z",
10      "eventName": "s3:ObjectCreated:Put",
11      "userIdentity": {
12        "principalId": "minioadmin"
13      },
14      "requestParameters": {
15        "principalId": "minioadmin",
16        "region": "",
17        "sourceIPAddress": "127.0.0.1"
18      },
19      "responseElements": {
20        "content-length": "0",
21        "x-amz-id-2": "e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855",
22        "x-amz-request-id": "174F5A6C715ECB50",
23        "x-minio-deployment-id": "439d9d33-3cca-42ae-b778-d703cbf9bbf7",
24        "x-minio-origin-endpoint": "http://192.168.1.138:9000"
25      },
26      "s3": {
27        "s3SchemaVersion": "1.0",
28        "configurationId": "Config",
29        "bucket": {
30          "name": "test-bucket",
31          "ownerIdentity": {
32            "principalId": "minioadmin"
33          },
34          "arn": "arn:aws:s3:::test-bucket"
35        },
36        "object": {
37          "key": "gantt.png",
38          "size": 92704,

```

```

39         "eTag": "22c4ae87e652bce0865536964cb8bb8d",
40         "contentType": "image/png",
41         "userMetadata": {
42             "content-type": "image/png"
43         },
44         "sequencer": "174F5A6C71C977E8"
45     }
46 },
47     "source": {
48         "host": "127.0.0.1",
49         "port": "",
50         "userAgent": "MinIO (darwin; arm64) minio-go/v7.0.49 MinIO Console /(dev)"
51     }
52 }
53 ]
54 }

```

Listing 2: Example Kafka Notification

/Users/username/test.jpg: OK

```

----- SCAN SUMMARY -----
Infected files: 0
Time: 0.332 sec (0 m 0 s)
Start Date: 2023:03:27 11:53:15
End Date: 2023:03:27 11:53:16

```

Listing 3: Example Exposed Metrics

```

# HELP aegis_kafka_total_messages Kafka total messages received
# TYPE aegis_kafka_total_messages counter
aegis_kafka_total_messages 0
# HELP aegis_objectstore_get_objects Object Store total get objects
# TYPE aegis_objectstore_get_objects counter
aegis_objectstore_get_objects 0
# HELP aegis_objectstore_get_objects_tagging Object Store total get objects tagging
# TYPE aegis_objectstore_get_objects_tagging counter
aegis_objectstore_get_objects_tagging 0
# HELP aegis_objectstore_put_objects_tagging Object Store total put objects tagging
# TYPE aegis_objectstore_put_objects_tagging counter
aegis_objectstore_put_objects_tagging 0
# HELP aegis_scanner_clean_files Total of clean files scanned by Aegis
# TYPE aegis_scanner_clean_files counter
aegis_scanner_clean_files 0
# HELP aegis_scanner_errors Total number of errors encountered during scans by Aegis
# TYPE aegis_scanner_errors counter
aegis_scanner_errors 0
# HELP aegis_scanner_infected_files Total of infected files scanned by Aegis
# TYPE aegis_scanner_infected_files counter
aegis_scanner_infected_files 0
# HELP aegis_scanner_time Time taken to perform a scan
# TYPE aegis_scanner_time histogram
aegis_scanner_time_bucket{le="0"} 0
aegis_scanner_time_bucket{le="125"} 0

```

```
aegis_scanner_time_bucket{le="250"} 0
aegis_scanner_time_bucket{le="500"} 0
aegis_scanner_time_bucket{le="1000"} 0
aegis_scanner_time_bucket{le="2000"} 0
aegis_scanner_time_bucket{le="4000"} 0
aegis_scanner_time_bucket{le="8000"} 0
aegis_scanner_time_bucket{le="16000"} 0
aegis_scanner_time_bucket{le="+Inf"} 0
aegis_scanner_time_sum 0
aegis_scanner_time_count 0
# HELP aegis_scanner_total_scans Total number of scans performed by Aegis
# TYPE aegis_scanner_total_scans counter
aegis_scanner_total_scans 0
# HELP go_gc_duration_seconds A summary of the pause duration of garbage collection cycles
# TYPE go_gc_duration_seconds summary
go_gc_duration_seconds{quantile="0"} 0
go_gc_duration_seconds{quantile="0.25"} 0
go_gc_duration_seconds{quantile="0.5"} 0
go_gc_duration_seconds{quantile="0.75"} 0
go_gc_duration_seconds{quantile="1"} 0
go_gc_duration_seconds_sum 0
go_gc_duration_seconds_count 0
# HELP go_goroutines Number of goroutines that currently exist.
# TYPE go_goroutines gauge
go_goroutines 17
# HELP go_info Information about the Go environment.
# TYPE go_info gauge
go_info{version="go1.19.4"} 1
# HELP go_memstats_alloc_bytes Number of bytes allocated and still in use.
# TYPE go_memstats_alloc_bytes gauge
go_memstats_alloc_bytes 1.363496e+06
# HELP go_memstats_alloc_bytes_total Total number of bytes allocated, even if freed.
# TYPE go_memstats_alloc_bytes_total counter
go_memstats_alloc_bytes_total 1.363496e+06
# HELP go_memstats_buck_hash_sys_bytes Number of bytes used by the profiling bucket hash
# TYPE go_memstats_buck_hash_sys_bytes gauge
go_memstats_buck_hash_sys_bytes 4941
# HELP go_memstats_frees_total Total number of frees.
# TYPE go_memstats_frees_total counter
go_memstats_frees_total 2757
# HELP go_memstats_gc_sys_bytes Number of bytes used for garbage collection system metadata
# TYPE go_memstats_gc_sys_bytes gauge
go_memstats_gc_sys_bytes 3.745832e+06
# HELP go_memstats_heap_alloc_bytes Number of heap bytes allocated and still in use.
# TYPE go_memstats_heap_alloc_bytes gauge
go_memstats_heap_alloc_bytes 1.363496e+06
# HELP go_memstats_heap_idle_bytes Number of heap bytes waiting to be used.
# TYPE go_memstats_heap_idle_bytes gauge
go_memstats_heap_idle_bytes 3.678208e+06
# HELP go_memstats_heap_inuse_bytes Number of heap bytes that are in use.
# TYPE go_memstats_heap_inuse_bytes gauge
go_memstats_heap_inuse_bytes 3.8912e+06
# HELP go_memstats_heap_objects Number of allocated objects.
```

```
# TYPE go_memstats_heap_objects gauge
go_memstats_heap_objects 16646
# HELP go_memstats_heap_released_bytes Number of heap bytes released to OS.
# TYPE go_memstats_heap_released_bytes gauge
go_memstats_heap_released_bytes 3.678208e+06
# HELP go_memstats_heap_sys_bytes Number of heap bytes obtained from system.
# TYPE go_memstats_heap_sys_bytes gauge
go_memstats_heap_sys_bytes 7.569408e+06
# HELP go_memstats_last_gc_time_seconds Number of seconds since 1970 of last garbage collection.
# TYPE go_memstats_last_gc_time_seconds gauge
go_memstats_last_gc_time_seconds 0
# HELP go_memstats_lookups_total Total number of pointer lookups.
# TYPE go_memstats_lookups_total counter
go_memstats_lookups_total 0
# HELP go_memstats_mallocs_total Total number of mallocs.
# TYPE go_memstats_mallocs_total counter
go_memstats_mallocs_total 19403
# HELP go_memstats_mcache_inuse_bytes Number of bytes in use by mcache structures.
# TYPE go_memstats_mcache_inuse_bytes gauge
go_memstats_mcache_inuse_bytes 12000
# HELP go_memstats_mcache_sys_bytes Number of bytes used for mcache structures obtained from system.
# TYPE go_memstats_mcache_sys_bytes gauge
go_memstats_mcache_sys_bytes 15600
# HELP go_memstats_mspan_inuse_bytes Number of bytes in use by mspan structures.
# TYPE go_memstats_mspan_inuse_bytes gauge
go_memstats_mspan_inuse_bytes 95184
# HELP go_memstats_mspan_sys_bytes Number of bytes used for mspan structures obtained from system.
# TYPE go_memstats_mspan_sys_bytes gauge
go_memstats_mspan_sys_bytes 97632
# HELP go_memstats_next_gc_bytes Number of heap bytes when next garbage collection will take place.
# TYPE go_memstats_next_gc_bytes gauge
go_memstats_next_gc_bytes 4.194304e+06
# HELP go_memstats_other_sys_bytes Number of bytes used for other system allocations.
# TYPE go_memstats_other_sys_bytes gauge
go_memstats_other_sys_bytes 1.300043e+06
# HELP go_memstats_stack_inuse_bytes Number of bytes in use by the stack allocator.
# TYPE go_memstats_stack_inuse_bytes gauge
go_memstats_stack_inuse_bytes 819200
# HELP go_memstats_stack_sys_bytes Number of bytes obtained from system for stack allocation.
# TYPE go_memstats_stack_sys_bytes gauge
go_memstats_stack_sys_bytes 819200
# HELP go_memstats_sys_bytes Number of bytes obtained from system.
# TYPE go_memstats_sys_bytes gauge
go_memstats_sys_bytes 1.3552656e+07
# HELP go_threads Number of OS threads created.
# TYPE go_threads gauge
go_threads 12
# HELP promhttp_metric_handler_requests_in_flight Current number of scrapes being served.
# TYPE promhttp_metric_handler_requests_in_flight gauge
promhttp_metric_handler_requests_in_flight 1
# HELP promhttp_metric_handler_requests_total Total number of scrapes by HTTP status code.
# TYPE promhttp_metric_handler_requests_total counter
promhttp_metric_handler_requests_total{code="200"} 0
```

```
promhttp_metric_handler_requests_total{code="500"} 0
promhttp_metric_handler_requests_total{code="503"} 0
```

Listing 4: Create Table SQL Query

```
CREATE TABLE IF NOT EXISTS %s (  
    ID SERIAL PRIMARY KEY,  
    ObjectKey TEXT NOT NULL,  
    BucketName TEXT NOT NULL,  
    Result TEXT NOT NULL,  
    Antivirus TEXT NOT NULL,  
    Timestamp TIMESTAMP NOT NULL,  
    VirusType TEXT  
);
```

Listing 5: Insert into Table SQL Query

```
INSERT INTO %s (ObjectKey ,  
    BucketName ,  
    Result ,  
    Antivirus ,  
    Timestamp ,  
    VirusType) VALUES ($1 ,  
                        $2 ,  
                        $3 ,  
                        $4 ,  
                        $5 ,  
                        $6  
)  
// Where %s = tableName
```

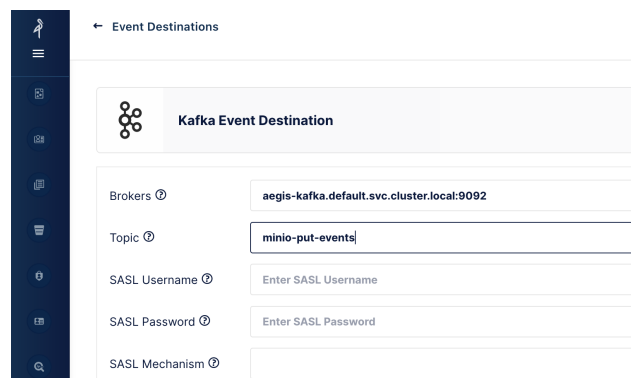




Figure 16: Configuring MinIO to Send Events to Kafka



Subscribe To Bucket Events



ARN

arn:minio:sqs::kafka

Prefix

Suffix

Select

Event

☒

PUT - Object Uploaded

☐

GET - Object accessed

☐

DELETE - Object Deleted

Cancel

Save

Listing 6: Aegis Scan Log

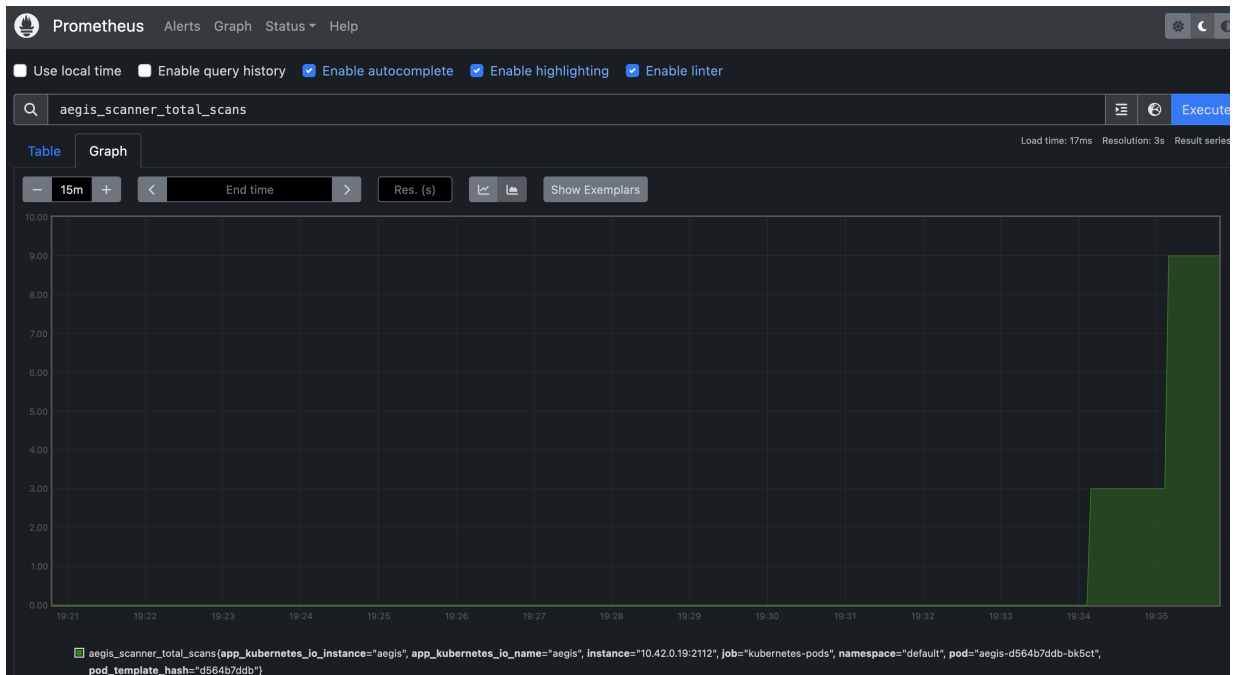


Figure 18: Exposed Prometheus Metrics

Listing 7: Example Audit Log

aegis_antivirus=# select * from aegis_audit_logs;							
id	objectkey	bucketname	result	antivirus	timestamp	virustype	
1	1cb3c3f91b2	test-bucket	infected	clamav	2023-05-10 10:06:09	Win. Trojan . Emotet -6396293-0	
2	0e969221c2e	test-bucket	infected	clamav	2023-05-10 10:06:09	Win. Trojan . Agent -1816988	
3	0b599447fdd	test-bucket	infected	clamav	2023-05-10 10:06:09	Win. Malware . Loki -6881381-0	
4	2a299b9d8f0c	test-bucket	infected	clamav	2023-05-10 10:06:09	Win. Coinminer . Generic -7151253-0	
5	sysclass.dll	test-bucket	clean	clamav	2023-05-10 10:06:18		
6	bidispl.dll	test-bucket	clean	clamav	2023-05-10 10:06:17		

(6 rows)

Listing 8: Output of kubectl get all

>>> kubectl get all					
NAME	READY	STATUS	RESTARTS	AGE	
pod/aegis-prometheus-node-exporter-stdb4	1/1	Running	0	3h49m	
pod/aegis-kube-state-metrics-776fb858c7-cvnc4	1/1	Running	0	3h49m	
pod/aegis-prometheus-pushgateway-75d654897c-kssmh	1/1	Running	0	3h49m	
pod/aegis-alertmanager-0	1/1	Running	0	3h49m	
pod/aegis-prometheus-server-5cc5469468-bqztp	2/2	Running	0	3h49m	
pod/aegis-minio-8588645fc6-fdrbj	1/1	Running	0	3h49m	
pod/aegis-postgresql-0	1/1	Running	0	3h49m	
pod/aegis-zookeeper-0	1/1	Running	0	3h49m	
pod/aegis-kafka-0	1/1	Running	0	3h49m	
pod/aegis-clamav-668f695bc-t7r66	1/1	Running	0	92m	
pod/aegis-5d7698d4bf-45xq8	1/1	Running	1 (88m ago)	89m	
pod/aegis-clamav-cronjob-28062065-m9sxs	0/1	Completed	0	6m29s	
pod/aegis-clamav-cronjob-28062067-q9czz	0/1	Completed	0	4m14s	
pod/aegis-clamav-cronjob-28062069-bjb48	1/1	Running	0	119s	
NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
service/kubernetes	ClusterIP	10.43.0.1	<none>	443/TCP	3h52m
service/aegis-zookeeper-headless	ClusterIP	None	<none>	2181/TCP, 2888/TCP, 3888/TCP	3h49m
service/aegis-kafka-headless	ClusterIP	None	<none>	9092/TCP, 9093/TCP	3h49m
service/aegis-postgresql-hl	ClusterIP	None	<none>	5432/TCP	3h49m
service/aegis-alertmanager-headless	ClusterIP	None	<none>	9093/TCP	3h49m
service/aegis	ClusterIP	10.43.6.8	<none>	80/TCP	3h49m
service/aegis-kube-state-metrics	ClusterIP	10.43.180.151	<none>	8080/TCP	3h49m
service/aegis-zookeeper	ClusterIP	10.43.181.148	<none>	2181/TCP, 2888/TCP, 3888/TCP	3h49m
service/aegis-postgresql	ClusterIP	10.43.90.131	<none>	5432/TCP	3h49m
service/aegis-minio	ClusterIP	10.43.69.101	<none>	9000/TCP, 9001/TCP	3h49m
service/aegis-clamav	ClusterIP	10.43.20.200	<none>	3310/TCP	3h49m
service/minio	NodePort	10.43.234.39	<none>	9001:30001/TCP	3h49m
service/aegis-kafka	ClusterIP	10.43.208.56	<none>	9092/TCP	3h49m
service/postgresql	NodePort	10.43.231.175	<none>	5432:30080/TCP	3h49m

service/aegis-prometheus-pushgateway	ClusterIP	10.43.88.49	<none>	9091/TCP	3h49m
service/aegis-alertmanager	ClusterIP	10.43.78.103	<none>	9093/TCP	3h49m
service/aegis-prometheus-node-exporter	ClusterIP	10.43.213.77	<none>	9100/TCP	3h49m
service/aegis-prometheus-server	ClusterIP	10.43.195.143	<none>	80/TCP	3h49m
service/prometheus	NodePort	10.43.5.128	<none>	9090:30090/TCP	3h49m

NAME	DESIRED	CURRENT	READY	UP-TO-DATE	AVAILABLE	NODE SELECTOR	AGE
daemonset.apps/aegis-prometheus-node-exporter	1	1	1	1	1	<none>	3h49m

NAME	READY	UP-TO-DATE	AVAILABLE	AGE
deployment.apps/aegis-kube-state-metrics	1/1	1	1	3h49m
deployment.apps/aegis-prometheus-pushgateway	1/1	1	1	3h49m
deployment.apps/aegis-prometheus-server	1/1	1	1	3h49m
deployment.apps/aegis-minio	1/1	1	1	3h49m
deployment.apps/aegis-clamav	1/1	1	1	3h49m
deployment.apps/aegis	1/1	1	1	3h49m

NAME	DESIRED	CURRENT	READY	AGE
replicaset.apps/aegis-kube-state-metrics-776fb858c7	1	1	1	3h49m
replicaset.apps/aegis-prometheus-pushgateway-75d654897c	1	1	1	3h49m
replicaset.apps/aegis-prometheus-server-5cc5469468	1	1	1	3h49m
replicaset.apps/aegis-minio-8588645fc6	1	1	1	3h49m
replicaset.apps/aegis-clamav-659c5f8c69	0	0	0	3h49m
replicaset.apps/aegis-clamav-668f695bc	1	1	1	92m
replicaset.apps/aegis-d564b7ddb	0	0	0	3h49m
replicaset.apps/aegis-5d7698d4bf	1	1	1	89m

NAME	READY	AGE
statefulset.apps/aegis-alertmanager	1/1	3h49m
statefulset.apps/aegis-postgresql	1/1	3h49m
statefulset.apps/aegis-zookeeper	1/1	3h49m
statefulset.apps/aegis-kafka	1/1	3h49m

NAME	SCHEDULE	SUSPEND	ACTIVE	LAST SCHEDULE	AGE
cronjob.batch/aegis-clamav-cronjob	* * * * *	False	1	2m45s	3h49m

NAME	COMPLETIONS	DURATION	AGE
job.batch/aegis-clamav-cronjob-28062065	1/1	2m15s	6m29s
job.batch/aegis-clamav-cronjob-28062067	1/1	2m15s	4m14s
job.batch/aegis-clamav-cronjob-28062069	0/1	119s	119s

References

- Artifact Hub. 2022. Artifact hub, Available at: <https://artifacthub.io/>. [Accessed: 16 Apr 2023].
- Aslan, Aslan, O. and Refik, S. 2020. A comprehensive review on malware detection approaches. *IEEE Access* 8, pp. 6249–6271.
- Baresi, L., Quattrocchi, G. and Tamburri, D. A. 2022. *Microservice architecture practices and experience: a focused look on docker configuration files*, [Online].
- ClamAV. 2023a. Clamav, Available at: <https://www.clamav.net/>. [Accessed: 24 Mar 2023].
- ClamAV. 2023b. Clamav, Available at: <https://www.github.com/Cisco-Talos/clamav>. [Accessed: 24 Mar 2023].
- Doaa, A., Naglaa, G., Eman, E. and Lamiaa, D. 2022. The malware detection approach in the design of mobile applications. *Symmetry* 14(5). Available at: <https://www.mdpi.com/2073-8994/14/5/839>.
- Docker. 2022. Docker, Available at: <https://www.docker.com/>. [Accessed: 16 Apr 2023].
- Docker. 2023. Dockerfile documentation, Available at: <https://docs.docker.com/engine/reference/builder/>. [Accessed: 24 Apr 2023].
- Drake, J. D. and Worsley, J. C. 2002. *Practical PostgreSQL*. " O'Reilly Media, Inc."
- Gita, M., Wildan, S. and Ardiansyah", A. F. "2018". "personal extreme programming with moscow prioritization for developing library information system". *"IAES Indonesia Section"*

- "Vol 5: EECSI 2018". Available at: <http://journal.portalgaruda.org/index.php/EECSI/article/view/1701/1140>.
- GNU. 2023. Makefile, Available at: <https://www.gnu.org/software/make/manual/make.html>. [Accessed: 25 Mar 2023].
- Go by Example. 2022a. Closing channels, Available at: <https://gobyexample.com/closing-channels>. [Accessed: 30 Mar 2023].
- Go by Example. 2022b. Ranging over channels, Available at: <https://gobyexample.com/range-over-channels>. [Accessed: 30 Mar 2023].
- Go by Example. 2022c. Waitgroups, Available at: <https://gobyexample.com/waitgroups>. [Accessed: 30 Mar 2023].
- Goverment, U. 2018. The data protection act 2018, Available at: <https://www.gov.uk/data-protection>. [Accessed: 28 Feb 2023].
- Helm. 2023. Helm documentation, Available at: <https://helm.min.io/>. [Accessed: 29 Apr 2023].
- Jayathilake, D. 2012. Towards structured log analysis. In: *2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*. pp. 259–264.
- John, G. and David, R. 2012. The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. *IDC iView: IDC Analyze the future* 2007(2012), pp. 1–16.
- K3d. 2023. K3d documentation, Available at: <https://k3d.io/v5.4.9/>. [Accessed: 24 Mar 2023].
- Kil, C. S., Iulian, M., Jiyong, J., John, T., David, B. and G., A. D. 2011. Splitscreen: Enabling efficient, distributed malware detection. *Journal of Communications and Networks* 13(2).
- Kubernetes. 2023. Kubernetes documentation, Available at: <https://kubernetes.io/>. [Accessed: 16 Apr 2023].
- Levy, E. 2022. Kafka vs rabbitmq: Architecture, performance, and use cases, Available at: <https://www.upsolver.com/blog/kafka-versus-rabbitmq-architecture-performance-use-case>. [Accessed: 24 Mar 2023].
- Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C. and Tung, K.-Y. 2013. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications* 36(1), pp. 16–24. Available at: <https://www.sciencedirect.com/science/article/pii/S1084804512001944>.
- M., F., K., M., D., N., O., R. and Satran, J. 2005. Object storage: the future building block for storage systems. In: *2005 IEEE International Symposium on Mass Storage Systems and Technology*. pp. 119–123.
- M, I. 2022. Installing apache kafka without zookeeper: Easy steps 101, Available at: <https://hevodata.com/learn/kafka-without-zookeeper/>. [Accessed: 24 Mar 2023].
- Martínez, J. 2022. Kubernetes services clusterip, nodeport and loadbalancer, Available at: <https://sysdig.com/blog/kubernetes-services-clusterip-nodeport-loadbalancer/>. [Accessed: 16 Apr 2023].

- McKusick, M. K., Neville-Neil, G. V. and Watson, R. N. M. 2014. *Process Management in the FreeBSD Operating System*, Addison-Wesley Professional, p. 928. 2nd ed., Available at: <https://www.informit.com/articles/article.aspx?p=2249436&seqNum=8>.
- Miguel, H. R. 2021. Analysis of software engineering automation tools for go., Available at: <https://repositorio.uniandes.edu.co/handle/1992/54945>. [Accessed: 15 Apr 2023].
- MinIO. 2023a. Minio go sdk repository, Available at: <https://github.com/minio/minio-go>. [Accessed: 15 Mar 2023].
- MinIO. 2023b. Minio object storage, Available at: <https://min.io/>. [Accessed: 15 Mar 2023].
- MinIO. 2023c. Minio pricing, Available at: <https://min.io/pricing/> [Accessed: 24 Mar 2023].
- MinIO Erasure Coding. 2023. Minio erasure coding, Available at: <https://min.io/docs/minio/linux/operations/concepts/erasure-coding.html>. [Accessed: 25 Apr 2023].
- Momjian, B. 2001. *PostgreSQL: introduction and concepts*, vol. 192. Addison-Wesley New York.
- Naik, N., Jenkins, P., Cooke, R., Gillett, J. and Jin, Y. 2020. Evaluating automatically generated yara rules and enhancing their effectiveness. In: *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*. pp. 1146–1153.
- Nitin, N., Paul, J., Savage, N. and Longzhi, Y. 2019. Cyberthreat hunting - part 1: Triaging ransomware using fuzzy hashing, import hashing and yara rules. In: *2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. pp. 1–6.
- Nuha, A., Nour, A. and Roger, E. 2016. A systematic mapping study in microservice architecture. In: *2016 IEEE 9th International Conference on Service-Oriented Computing and Applications (SOCA)*. pp. 44–51.
- Omer, A. 2017. Performance comparison of static malware analysis tools versus antivirus scanners to detect malware. In: *International Multidisciplinary Studies Congress (IMSC)*.
- Ormandy, T. 2011. Sophail: A critical analysis of sophos antivirus. *Proc. of Black Hat USA* .
- Ot, A. 2022. The object storage market, Available at: <https://www.enterprisestorageforum.com/cloud/cloud-object-storage-market/>. [Accessed: 17 Mar 2023].
- Po-ching, L., Zhi-xiang, L., Ying-dar, L., Yuan-cheng, L., C, L. F. *et al.* 2006. Profiling and accelerating string matching algorithms in three network content security applications. *IEEE Commun. Surv. Tutorials* 8(1-4), pp. 24–37.
- Prometheus. 2023. Prometheus documentation, Available at: <https://prometheus.io/>. [Accessed: 24 Mar 2023].
- Ryer, M. 2020. Why you shouldn't use func main in go, Available at: <https://pace.dev/blog/2020/02/12/why-you-shouldnt-use-func-main-in-golang-by-mat-ryer.html>. [Accessed: 30 Mar 2023].
- Segmentio. 2022. Kafka go repository, Available at: <https://github.com/segmentio/kafka-go>. [Accessed: 24 Mar 2023].

- Sharma, V. 2022. Managing multi-cloud deployments on kubernetes with istio, prometheus and grafana. In: *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*. vol. 1, pp. 525–529.
- spf13. 2023. Viper, Available at: <https://github.com/spf13/viper>. [Accessed: 25 Mar 2023].
- Srinivasan, G., Eidelman, A. and Casmer, E. 2022. Integrating amazon s3 malware scanning into your application workflow with cloud storage security, Available at: <https://aws.amazon.com/blogs/apn/integrating-amazon-s3-malware-scanning-into-your-application-workflow-with-cloud-storage-security/>. [Accessed: 21 Mar 2023].
- Uber. 2023. Zap, Available at: <https://github.com/uber-go/zap>. [Accessed: 25 Mar 2023].
- Vlad, B., Dehelean, C. and Liviu, M. 2018. Object storage in the cloud and multi-cloud: State of the art and the research challenges. In: *2018 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*. IEEE, pp. 1–6.
- Wikipedia), U. h. n. . A., year = 2023. ??? Aegis in wikipedia.
- Yang, J. 2009. Analyzing uml sequence diagrams with utp. *2010 Fifth International Conference on Frontier of Computer Science and Technology* pp. 417–423.
- Zhelev, S. and Rozeva, A. 2019. Using microservices and event driven architecture for big data stream processing. *AIP Conference Proceedings* 2172(1). Available at: <https://doi.org/10.1063/1.5133587>. 090010.