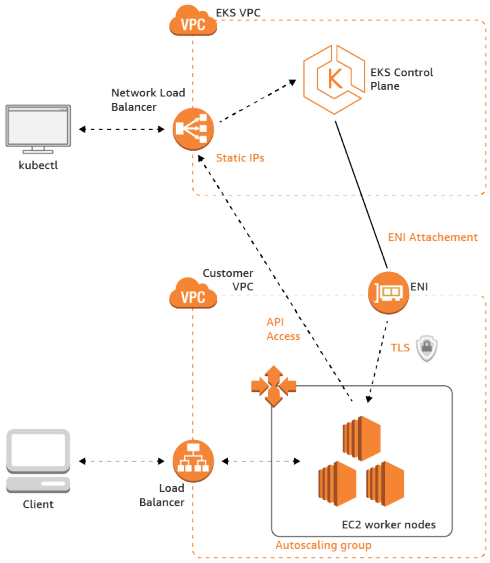
Automated Safeguards for EKS

Amazon Elastic Container Service for Kubernetes (Amazon EKS) makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS.

Amazon EKS runs the Kubernetes management infrastructure for you across multiple AWS availability zones to eliminate a single point of failure. Amazon EKS is certified Kubernetes conformant so you can use existing tooling and plugins from partners and the Kubernetes community. Applications running on any standard Kubernetes environment are fully compatible and can be easily migrated to Amazon EKS. EKS helps customers by configuring the control plane, and other infrastructure components of Kubernetes, allowing them to focus on their application and not configuring Kubernetes infrastructure.

EKS is priced based on the hourly usage of a Cluster, and the associated usage of the Worker Nodes. Please see Amazon EKS Pricing for details.

Amazon EKS requires a fully managed control plane, and Worker Nodes deployed into VPCs. The following diagram illustrates the EKS architecture



EKS Reference Architecture - Note that the EKS VPC is managed by AWS and does not require you to deploy a separate VPC.

> **Private EKS Clusters**
>
> At this time ClearDATA Automated Safeguards only support EKS Clusters with **public** endpoints. ClearDATA is working on enhancing the safeguard to support private endpoints, allowing customers to deploy fully private EKS clusters. This article will be updated once private endpoints are supported.

IAM Roles

EKS Clusters & Worker Nodes require an IAM role in order to properly deploy a Cluster and for Worker Nodes to join that Cluster. As ClearDATA is responsible for IAM role creation, ClearDATA pre-populates the necessary roles into all customers with Automated Safeguards.

- **Safeguards-EKSWorkerNode**: The name of the role to be used by the Worker Nodes. It contains the necessary Amazon Managed Policies for the Worker Nodes. This role is required by the Worker Nodes.
- **Safeguards-EKSServiceWorker**: The name of the role used by the ClearDATA Automated Safeguards for EKS. This role must be mapped with the necessary Kubernetes Permissions.
- **Safeguards-EKSCluster**: The name of the role to be used by the EKS Cluster and is referenced when you create the Cluster via the AWS Console or SDK.

> **Info**
>
> ClearDATA has created a CloudFormation Template and a Terraform Configuration that will easily deploy an EKS Cluster. Click on the links below to download the deployment method of your choice.
>
> Click here to download the Terraform Configuration. Instructions are found in the readme file.
>
> Click here to download the CloudFormation Template. Instructions are found in the template, and when the template is loaded into CloudFormation.

Administrative actions, via kubectl, are executed against the managed control plane, while users connect to applications hosted on EC2 Worker Nodes. ClearDATA provides customers a hardened EKS-optimized Worker Node AMI to be used for all Clusters. See the Automated Safeguards section for more information.

Please see Amazon EKS Features and Amazon EKS FAQs for more details.

IAM Roles & Pods

As of April 2019, EKS does not have a native solution for mapping IAM roles to Kubernetes pods. Amazon's Containers Roadmap (https://github.com/aws/containers-roadmap/issues) discusses the current state of this feature request. Until the feature is released, both Amazon and ClearDATA recommend the tool kube2iam. kube2iams solution is to redirect the traffic that is going to the ec2 metadata API for docker containers to a container running on each instance, make a call to the AWS API to retrieve temporary credentials and return these to the caller. Other calls will be proxied to the EC2 metadata API. This container will need to run with host networking enabled so that it can call the EC2 metadata API itself. The tool is available at https://github.com/jtblin/kube2iam.

Kubernetes Permissions

In order for ClearDATA's Automated Safeguards to ensure initial and ongoing compliance, privileged access to the EKS Cluster is required. EKS maps the IAM principal of the Cluster creator to the Kubernetes system:masters role, and that is the only IAM principal that can access the Cluster after it is created. In order for ClearDATA to ensure a Cluster is compliant we require that IAM principal to map a IAM role to system:masters. This role, named Safeguards-EKSServiceWorker, has limited IAM access with only the AWS Managed EC2 Read Only policy. As directed by the Getting Started with Amazon EKS implementation guide the last step of provisioning a Cluster is to allow the Worker Nodes to join the Cluster through the **AWS authenticator configuration map** YAML file. Customers must allow ClearDATA's Automated Safeguard role, named to the aws-auth-cm.yaml file to map the role to the proper Kubernetes role. The aws-auth-cm.yaml should look like

aws-auth-cm.yaml

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: aws-auth
  namespace: kube-system
data:
  mapRoles: |
    - rolearn: arn:aws:iam::{AWSACCOUNTID}:role/Safeguards-EKSWorkerNode
      username: system:Node:{{EC2PrivateDNSName}}
      groups:
        - system:bootstrappers
        - system:Nodes
    - rolearn: arn:aws:iam::{AWSACCOUNTID}:role/Safeguards-EKSServiceWorker
      username: kubernetes-admin
          groups:
                - system:masters
```

where the instance profile is the ARN of the **Safeguards-EKSWorkerNode** role in your account and {AWSACCOUNTID} is the actual account number of your AWS account**.** The aws-auth-cm.yaml can now be applied to the EKS Cluster.

> **Note**
>
> The Terraform Configuration above will automatically generate the aws-auth-cm.yaml file for you. The CloudFormation Template does not automatically create it, and therefore the file will need to be created.

Non-Compliant Clusters

ClearDATA's Automated Safeguards for EKS monitor the status of Clusters and Worker Nodes and ensure the Worker Nodes have the proper rights to the EKS Cluster.

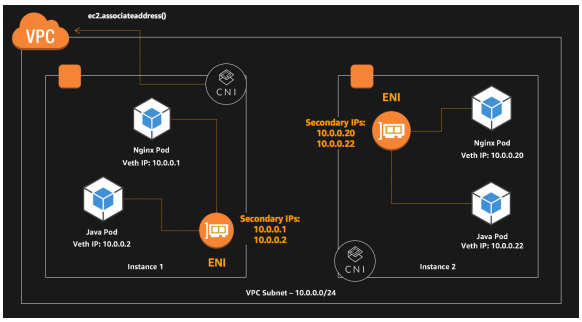
Remediation

If the Worker Nodes do not connect to the Cluster and notify the Safeguards that they have applied the necessary permissions to the EKS Cluster, the Worker Nodes may be marked as non-compliant and may be terminated.

VPC

Customers can use the existing VPC for the Cluster & Worker Nodes, or a new and dedicated VPC for EKS. If you wish to use a new VPC please contact ClearDATA Support for a new VPC. Note that the reference architecture diagram shows an EKS VPC, but that is part of the Control Plane managed by AWS and is not required to be deployed by you or ClearDATA.

Amazon EKS supports native VPC networking via the Amazon VPC CNI plugin for Kubernetes. Using this CNI plugin allows Kubernetes pods to have the same IP address inside the pod as they do on the VPC network. This CNI plugin is an open-source project that is maintained on GitHub.



The CNI plugin is responsible for allocating VPC IP addresses to Kubernetes nodes and configuring the necessary networking for pods on each node. The plugin consists of two primary components:

- The L-IPAM daemon is responsible for attaching elastic network interfaces to instances, assigning secondary IP addresses to elastic network interfaces, and maintaining a "warm pool" of IP addresses on each node for assignment to Kubernetes pods when they are scheduled.
- The CNI plugin itself is responsible for wiring the host network (for example, configuring the interfaces and virtual Ethernet pairs) and adding the correct interface to the pod namespace.

For more information about the design and networking configuration, see Proposal: CNI plugin for Kubernetes networking over AWS VPC.

Worker Node Image

ClearDATA provides a hardened, EKS-optimized AMI for use with EKS Clusters. If you wish to use EKS please contact ClearDATA Support and request the EKS AMI be created in the appropriate account and region. Once the AMI is available, it can be used for all EKS Worker Nodes.

ClearDATA Automated Safeguards are designed to provide additional technical controls for EKS Clusters that may process PHI or other sensitive healthcare data. ClearDATA provides an optimized AMI that is hardened against CIS Benchmarks for both the OS and Kubernetes to be used for the Cluster Worker Nodes, as well as tooling to ensure that containers running on the Cluster do not contain vulnerabilities. Please contact ClearDATA Support for a full list of configurations on the Worker Nodes.

Compliance Guidance

Encrypted Storage

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption as an addressable standard and strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (PHI). ClearDATA's interpretation of this regulation is that all storage must be encrypted. All EKS Worker Nodes enforce the use of encrypted EBS storage.

Audit Logging

HIPAA Technical Safeguard 45 CFR § 164.312(b) requires a Covered Entity to “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” ClearDATA Automated Safeguards configures the Worker Nodes to send all the Kubernetes or EKS logs to CloudWatch Logs to have a centralized and unified view of all the logs from the Cluster, both from the Nodes and from each container stdout. All logs are sent to Amazon CloudWatch.

Vulnerability Scanning

HIPAA Technical Safeguards CFR 164.306 and 164.308(a)(5)(ii)(B) require a covered entity or business associate to protect against any reasonably anticipated threats or hazards to the security or integrity of PHI. This includes implementing procedures for guarding against, detecting, and reporting malicious software. ClearDATA Automated Safeguards ensure that all EKS Clusters contain enterprise grade vulnerability scanning tools that have visability at the container level, ensuring that the components that will be processing the sensitive data do not contain any known vulnerabilities.

Twistlock - Overview

Twistlock is a container security platform ClearDATA utilizes for Amazon EKS. The installation of Twistlock is an automated installation process which is triggered by a `CreateCluster` EKS Cluster Operations event.

Twistlock - Installation

The Twistlock Console is installed as a replication controller with persistent storage, allowing the Console to be resilient to Node failures. Defenders are deployed to Kubernetes Nodes using DaemonSets. DaemonSets make Defender deployment simple and automatic, regardless of how large your Cluster or how frequently you add Nodes to it. With DaemonSets, rather than manually installing Twistlock Defenders on each Node, Twistlock generates a configuration file that you load into your Kubernetes Master. Kubernetes uses the configuration to ensure that every Node in the Cluster runs a Defender. As new Nodes are added, Defenders are automatically installed on them.

Twistlock - Accessing the console

The Twistlock Console serves as the user interface within Twistlock. The graphical user interface (GUI) lets you define policy, configure and control your Twistlock deployment, and view the overall health (from a security perspective) of your container environment.

Follow the instructions provided below to access the Twistlock Console:

Setup port forward

You will need to forward the port 8083 to your local computer. This will allow you access to the Twistlock Console from your local computer.

Use the command below to setup the port forward:

```
$ kubectl port-forward $(kubectl -n twistlock get pod | fgrep console |
awk '{print $1}') 8083:8083 -n twistlock
```

Access the Console

Navigate to **https://localhost:8083/** to open the Console user interface (you may need to accept a certificate exception). Access to the console does require logon credentials. Please contact ClearDATA to obtain logon credentials for your Twistlock installation.

Twistlock - Vulnerability Explorer

Most scanners find and list vulnerabilities, but Vulnerability Explorer takes it a step further by analyzing the data within the context of your environment. Because Twistlock can see how the containers run in your environment, we can identify the biggest risks and prioritize them for remediation. To view Vulnerability Explorer, open Console, then go to **Monitor** > **Vulnerabilities** > **Vulnerability Explorer**.

Roll-Ups

The charts at the top of the Vulnerability Explorer help identify how many images you need to fix. For each object type (container, image, host), the chart reports a count of the highest severity vulnerability in each object class in your environment as a function of time.

Top ten lists

Vulnerability Explorer gives you ranked lists of the most critical vulnerabilities in your environment based on a scoring system. There are top ten lists for the images in your environment and the hosts in your environment. The search tool at the top of the table lets you determine if any image or host in your environment is impacted by a specific vulnerability (whether it is in the top ten list or not).

Risk trees

Risk trees lists all the images, containers, and hosts that are vulnerable to a specific CVE. Risk trees are useful because they show you how you are exposed to a given vulnerability.

Recalculating statistics

Statistical data is calculated every 24 hours. You can force Console to recalculate the statistics for the current day with the current data by clicking the Refresh button in the top left of Vulnerability Explorer.

Compliance

Compliance Explorer gives you a picture of the overall compliance of the entities in your container environment. To view Compliance Explorer, go to **Monitor** > **Compliance** > **Compliance Explorer**. Compliance Explorer consists of two parts:

- Roll-up charts—Show the overall compliance for each entity type (images, containers, and hosts) as a percentage of total checks passed over total checks enabled. A grade of 100% means there are no compliance issues. The trend charts shows how your compliance has changed over the past 30 days.
- Table of compliance issues—Lists all compliance checks that failed. The checks that are evaluated are determined by the rules you've defined in **Defend** > **Compliance** > **Policy**. Issues are listed by compliance ID. Clicking on a row opens a dialog that lists all entities that do not comply with the given ID.

Statistical data is calculated every 24 hours. You can force the console to recalculate the statistics for the current day with the current data by clicking the Refresh button in the top left of Compliance Explorer.

Further Information

For more information and documentation about Twistlock please contact ClearDATA Support.

Shared Responsibility

Encrypted Connections

HIPAA Technical Safeguard 45 CFR 164.312(a)(2)(iv) requires encryption and decryption as an addressable standard and strongly suggests that you implement a mechanism to encrypt and decrypt electronic protected health information (PHI). ClearDATA's interpretation of this regulation is that all connections between Worker Nodes, and both to and from the EKS Cluster, must be encrypted. ClearDATA does not offer a managed TLS solution for EKS, allowing customers to choose the toolset that is appropriate to their business. ClearDATA recommends Istio for network policy management, including TLS.

Istio Installation

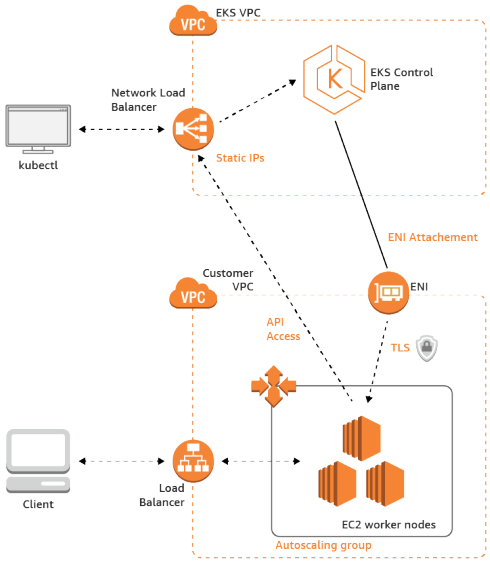
Instructions for installing Istio on Amazon EKS can be found here: Getting Started with Istio on Amazon EKS

TLS Configuration

Further information on how to use Istio for TLS management can be found here: Istio Mutual TLS Deep-Dive

Exclusion

Exclusions can be done on an AWS account basis, meaning that any account that contains PHI must use the Automated Safeguards for EKS for all Clusters, unless there is a security exception in place. Please contact ClearDATA Support for more information.



Users can be added to the **Safeguards-EKS** group to gain access to create and manage EKS Clusters.

Item	Clear DATA	Cust omer
Initial Cluster creation	IC	RA

Map ClearDATA Safeguards-EKSServiceWorker role to system:masters as directed above	IC	RA
Encrypt data in motion through the load balancer and between containers using industry standard services, such as Istio or Weave	IC	RA
Encrypt data in motion between Cluster Worker Nodes using industry standard services, such as Istio or Weave	IC	RA
Encrypt data in motion between EKS Cluster and all other services including but not limited to EC2, S3, RDS, & Redshift	IC	RA
Define Cluster type, instance type, scaling parameters	IC	RA
Create, Update, Delete container images	IC	RA
Create, Update, Delete Kubernetes objects	IC	RA
Indicate if Cluster will process PHI (before initial creation)	IC	RA
Capture and archive Cluster logs	RA	IC
Configure and run container image vulnerability scanning software	RA	IC
Configure initial vulnerability scanning software user	RA	IC
Configure and maintain additional vulnerability scanning software users	IC	RA
Create vulnerability alerting in accordance with your policies and procedures	IC	RA
Remediate container image vulnerabilities	IC	RA
Configure, maintain, remediate host Cluster security	RA	IC
Upgrade Kubernetes version	IC	RA
Provide regularly updated EKS optimized AMI	RA	IC
Update Kubernetes Worker Nodes	IC	RA