Amazon Elastic Kubernetes Service Platform Architecture Security Review

Amazon Web Services

Version 1.0 – November 10, 2025

While precautions have been taken in the preparation of this document, NCC Group the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NCC Group’s services does not guarantee the security of a system, or that computer intrusions will not occur.

Prepared By
Divya Natesan
Jonathan Leadbeater

Prepared For
Amazon Web Services

1 Executive Summary

Synopsis

In the second quarter of 2025, Amazon Web Services (AWS) engaged NCC Group to conduct an architecture review of the AWS managed Kubernetes service: Amazon Elastic Kubernetes Service (Amazon EKS) to evaluate how the system is designed in order to prevent AWS employees (Operators) from accessing Customer Content stored or processed by Amazon EKS, with a specific focus on validating a number of Data Security claims asserted by AWS. These are enumerated in the `Scope` section of the `Executive Summary`. The planning and execution of this engagement lasted for six calendar weeks.

The following is a short excerpt from the publicly available Amazon EKS documentation describing the service[1]:

> Amazon Elastic Kubernetes Service (EKS) provides a fully managed Kubernetes service that eliminates the complexity of operating Kubernetes clusters. With EKS, you can:
>
> - Deploy applications faster with less operational overhead
> - Scale seamlessly to meet changing workload demands
> - Improve security through AWS integration and automated updates
> - Choose between standard EKS or fully automated EKS Auto Mode

Scope

There are eight Security Design claims (enumerated below) made by AWS with respect to Amazon EKS Data Security Posture. AWS attests that production Amazon EKS Clusters will adhere to an explicit policy of protecting the security of Customer Content with the following claims:

1. There are no technical means for AWS personnel to gain interactive access to a managed Kubernetes Control Plane Instance.
2. There are no technical means available to AWS personnel to read, copy, extract, modify, or otherwise access Customer Content in a managed Kubernetes Control Plane Instance.
3. Internal Administrative APIs used by AWS personnel to manage the Kubernetes Control Plane Instances cannot access Customer Content in the Kubernetes Data Plane.
4. Changes to Internal Administrative APIs used to manage the Kubernetes Control Plane always require Multi-Party Review and Approval.
5. There are no technical means available to AWS personnel to access Customer Content in backup storage for the `etcd` database. No AWS personnel can access any plaintext encryption keys used for securing data in the `etcd` database.
6. AWS personnel can only interact with the Kubernetes Cluster API endpoint using Internal Administrative APIs without access to Customer Content in the managed Kubernetes Control Plane or Data Plane. All actions performed on the Kubernetes Cluster API endpoints by AWS personnel are visible to customers through customer-enabled audit logs.
7. Access to Internal Administrative APIs always requires authentication and authorization. All operational actions performed by Internal Administrative APIs are logged and audited.
8. A managed Kubernetes Control Plane Instance can only run tested software that has been deployed by a trusted pipeline. No AWS personnel can deploy software to a managed Kubernetes Control Plane Instance outside of this Pipeline.

[1] What is Amazon EKS? https://docs.aws.amazon.com/eks/latest/userguide/what-is-eks.html

NCC Group was able to thoroughly cover the scope and evaluate all the features explicitly asserted by AWS within the allocated time frame.

Limitations

This engagement represents a point-in-time evaluation of Amazon EKS. Security threats and attacker capabilities evolve rapidly, and the results of this assessment should not be interpreted as a guarantee of adequacy against future threats. All findings and observations reflect the system as it was presented during the engagement window and do not constitute assurance regarding any future changes in implementation, policy, or operational practice.

This review is based on the attestation of AWS staff and product design documents as presented to NCC Group. While AWS supplied suitable support in that regard, NCC Group cannot attest to the accuracy of the information or associated conclusions, or whether the implementation matches the design. Statements regarding the behavior or properties of Amazon EKS refer to its design as described and demonstrated during the review period.

2 Security Design Evaluation

It is an AWS goal to prevent unauthorized access by Amazon EKS Operators to Customer Content stored and processed on Amazon EKS Clusters. In particular, the focus is on the managed Amazon EKS Control Plane where there is limited visibility to customers.

Customer Content in Amazon EKS

In the operation of Amazon EKS, Operators encounter different types of data assigned to different tiers of sensitivity & confidentiality by AWS. AWS also has set customer expectations regarding how different content is managed & secured accordingly, based on the classification of data.

The definition of Customer Content can be found here: https://aws.amazon.com/compliance/data-privacy-faq

The above URL defines Customer Content as software (including machine images), data, text, audio, video, or images that a customer or any end user transfers to AWS for processing, storage, or hosting by AWS services in connection with a customer's account, and any computational results that a customer or their end user derives from the foregoing through their use of AWS services.

For example, Customer Content in Amazon EKS includes Customer-owned Images and Containers associated with the Kubernetes Worker Nodes.

Please note that Customer Content does not include account information and information included in resource identifiers, metadata tags, access controls, rules, usage policies, permissions, and similar items related to the management of AWS resources.

AWS recommends that customers do not include personally identifying, confidential, or sensitive information in these items.

The Claims stated in the `Executive Summary` cover Customer Content only. Access to information that is not Customer Content is out of scope, as listed in one of the sections below.

Security Boundary

The overall security goal is to make the Amazon EKS Control Plane a well-defended boundary that the Amazon EKS Operators cannot cross unilaterally. "Unilaterally" means Amazon EKS Operators cannot access Customer Content (defined above) and all operations performed by them should be logged in internal AWS systems.

Out of Scope

The following elements were not in scope:

- A review of Threat Actors other than AWS personnel was not in scope, for example, machine service accounts having access to the EKS Control and Data Planes, and who has access to these machine service account credentials.
- The Claims stated in the `Executive Summary` cover Customer Content only. Access to information that is not Customer Content is out of scope.

  Note: Only those Kubernetes resources that store Customer Content are in scope.
- A detailed architecture review of the AWS CI-CD Process was not in scope, and only relevance-limited coverage of this connected system was performed.
- As part of this engagement, NCC Group only performed an architecture review and included all aspects of the in-scope systems with relevance-limited coverage of connected systems. The engagement did not include an in-depth review of the implementation of specific components or any active, dynamic hands-on testing or

technical validation. The assessment of claims was based on the degree to which the Amazon EKS design, as assessed and observed, provided the means to support these claims and ensure that they would be maintained. As this was an architecture-level review, any failure to meet this goal in the design itself would result in not considering a claim to be supported.

- Due to the nature of the engagement being an architecture review, the code snippets for the input validation logic itself, which includes all the specific commands in the allow list, were out of scope and not reviewed by NCC Group.

Amazon EKS Design Goals Evaluation

The security architecture of the EKS Operating model prevents any Operator from accessing any Customer Content in the service. Information that is not Customer Content in Amazon EKS has a controlled level of access to Operations using the Internal Administrative APIs. Discussions with the Amazon EKS Service team stated that this controlled access to this information is required for Amazon EKS Operators to troubleshoot and perform diagnostics on behalf of customers to maintain the availability and uptime of the service.

Least Privilege

The design of Amazon EKS adheres to the principle of least privilege. The following were noted:

- No access to Customer Content by Amazon EKS Operators
- No ability to gain an interactive shell or execute arbitrary commands on Amazon EKS Control Plane Instances
- No ability for Amazon EKS Operators to run commands other than the pre-approved ones
- No unrecorded activity
- No emergency procedures that bypass standard access controls

Confidentiality

Strong encryption is present throughout the design of Amazon EKS. The Nitro System protects data stored temporarily in RAM. All data in transit is encrypted either via the Nitro System or using TLS. Amazon EKS employs envelope encryption of all Kubernetes API data before being stored in the `etcd` database.

Redundancy and Zero Trust

Amazon EKS employs redundant and layered controls to enforce authentication, authorization, and operational boundaries. Changes to the system require Multi-Party Approval and proceed through defined and audited CI-CD Pipelines. Multiple checkpoints are in place to prevent unintended deployment or misconfiguration.

Auditing

Suitable logs are securely stored, enabling accountability for actions performed on Kubernetes Control Plane Instances.

Summary

The Amazon EKS service has been designed with strong controls around access, isolation, and operational integrity. Access to the Amazon EKS Control Plane is tightly constrained, with only a single, well-defined administrative path available to Amazon EKS Operators. This access path is limited in scope and does not permit access to Customer Content. Analysis determined that there is a single method by which Amazon EKS Operators can interact with Control Plane instances, and that there are no other ways to access the Control Plane, either through alternate interfaces or indirect mechanisms. Analysis also determined that no other employees of AWS, other than Amazon EKS Operators, have access.

No direct access is available to the Data Plane infrastructure. Security measures within the Amazon EKS environment align with best practices in cryptography, account hardening, and change control. AWS has implemented robust safeguards to ensure that all operational actions are restricted to authorized personnel, and subject to secure workflows.

NCC Group found no architectural gaps that would directly compromise the security claims asserted by AWS.

AWS must continue to innovate to address an evolving threat landscape, thus further strengthening Amazon EKS Architecture, while supporting a system that prioritizes strong isolation, access control, and operational transparency.

3 Review Methodology

The engagement was primarily conducted through interviews with the Amazon EKS Service team and by accessing documentation provided by AWS. AWS cooperated with NCC Group and provided all the necessary documentation and interviews for the engagement. NCC Group conducted interviews with multiple senior members of the Amazon EKS team. These interviews covered the design goals of the system in terms of the claims asserted by AWS as well as the security features put in place to eliminate access to Customer Content and limit access to information that is not Customer Content. Additionally, information was provided in documents and via screenshare to enable NCC Group to reach a thorough understanding of the security posture of Amazon EKS specific to the claims. The documentation provided covered extensive internal details of the Amazon EKS design. Finally, NCC Group also read public documentation related to specific in-scope topics around AWS Data Classification for Customer Content as described in the `Audit Policy` for Amazon EKS public document at https://docs.aws.amazon.com/eks/latest/best-practices/auditing-and-logging.html.

During the engagement, the following exercises were performed by NCC Group for the architecture review of the asserted claims in scope:

- Read-through of the documents detailing Amazon EKS Operational Security Controls specific to the claims asserted by AWS
- Iterative filling in and updating of the Artifact Request List (ARL) provided to the Amazon EKS Service Team
- Several meetings with the Amazon EKS Service Team around topics related to the claims
- Review of answers and evidence provided by Amazon EKS to questions documented in the ARL
- Evaluation of the security decisions made by AWS in designing Amazon EKS, specifically related to the claims asserted for review
- Identification of design patterns that are common among secure managed Kubernetes services. Then, the design of Amazon EKS was compared against the best practices, specifically in the features in scope.
- Formulation of observations discovered through the Architecture Security Review

The scope of analysis encompassed the verification of claims asserted by AWS, as well as the development and administrative processes that support the service. Several topics were identified as in-scope domains because they are directly related to the fulfillment of the claims asserted by AWS. NCC Group's evaluation included:

1. Access Flow to the Internal Administrative API (which enables Amazon EKS Operators to manage and operate the system without access to Customer Content)

   NCC Group considered the system from the perspective of "Operators", who are developers of Amazon EKS and other AWS employees.

   NCC Group examined the operational security controls in place that restrict Amazon EKS Operators from accessing Customer Content from the Amazon EKS Control and Data Plane instances.

   Additionally, NCC Group evaluated how Amazon EKS Operators can access the Internal Administrative APIs on EKS Control Plane Nodes from end-to-end. Access to the Internal Administrative APIs by Amazon EKS Operators is input validated by limiting them to running only specific pre-defined set of operational commands due to the enforcement of an allowlist of actions and their arguments.

An Architecture Review of the Internal Administrative APIs itself was conducted to further examine the privileges of the user running the commands executed on the Amazon EKS Control Plane and restrictions (if any) for Amazon EKS Operators to only run on specific Control Plane Nodes.

2. Amazon EKS Control Plane Architecture
3. Amazon EKS CI-CD Process for development and deployment, and maintenance of Amazon EKS with particular focus on change control, access management, Multi-Person Approval Process, and secure software engineering practices/workflows around changes to the Internal Administrative APIs
4. A review to confirm that no undocumented or alternative access mechanisms were present or required by Amazon EKS system’s design
5. Mechanisms to ensure appropriate isolation and access boundaries between components, including the enforcement of least privilege and network segmentation principles

4 Claims

AWS attests that production Amazon EKS Clusters will adhere to an explicit policy of protecting data security of customers with the following claims:

Claim Analysis

1. **There are no technical means for AWS personnel to gain interactive access to a managed Kubernetes Control Plane Instance.**

   Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. NCC Group finds that the architecture of Amazon EKS provides no mechanism by which interactive access can be initiated on a managed Kubernetes Control Plane instance. The only mechanism for Amazon EKS Operators to access Control Plane Instances is through the Internal Administrative APIs.

2. **There are no technical means available to AWS personnel to read, copy, extract, modify, or otherwise access Customer Content in a managed Kubernetes Control Plane Instance.**

   Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. There are no alternative mechanisms available to AWS employees to interact with the Amazon EKS Control Plane instances apart from the Internal Administrative APIs.

3. **Internal Administrative APIs used by AWS personnel to manage the Kubernetes Control Plane Instances cannot access Customer Content in the Kubernetes Data Plane.**

   Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. The Internal Administrative APIs are not able to access Customer Content. This is achieved because Amazon EKS Operators are input validated by limiting them to running only specific commands due to the enforcement of an allowlist of actions and their arguments. Please refer to the `Out of Scope` section in *Security Design Evaluation* for more details around scope for this claim.

4. **Changes to Internal Administrative APIs used to manage the Kubernetes Control Plane always require Multi-Party Review and Approval.**

   Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. NCC Group finds that the CI-CD process governing the Internal Administrative APIs includes formal controls to ensure that all modifications are subject to Multi-Party review and approval. These processes are supported by access management, secure software engineering practices & workflows, and appropriate segregation of duties. Please refer to the `Out of Scope` section in Security Design Evaluation for more details around scope for this claim. In general, Amazon EKS CI-CD Process follows the established AWS CI-CD Pipeline procedures and mechanisms.

5. **There are no technical means available to AWS personnel to access Customer Content in backup storage for the `etcd` database. No AWS personnel can access any plaintext encryption keys used for securing data in the `etcd` database.**

   Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. Amazon EKS enforces suitable encryption for `etcd` storage and backup. AWS personnel have no means of retrieving or decrypting Customer Content from these backups.

6. **AWS personnel can only interact with the Kubernetes Cluster API endpoint using Internal Administrative APIs without access to Customer Content in the managed Kubernetes Control Plane or Data Plane. All actions performed on the Kubernetes Cluster API endpoints by AWS personnel are visible to customers through customer-enabled audit logs.**

Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. NCC Group finds that access to Kubernetes Cluster API Endpoints by Amazon EKS Operators is exclusively through the Internal Administrative APIs, which do not have access to Customer Content.

7. **Access to Internal Administrative APIs always requires authentication and authorization. All operational actions performed by Internal Administrative APIs are logged and audited.**

   Analysis: **Confirmed.** NCC Group finds that the architecture of Amazon EKS fully supports this claim. NCC Group finds that access to the overarching internal Administrative APIs is protected by authentication and authorization mechanisms. Operational actions taken through these APIs are logged in a manner that supports traceability and auditability.

8. **A managed Kubernetes Control Plane Instance can only run tested software that has been deployed by a trusted pipeline. No AWS personnel can deploy software to a managed Kubernetes Control Plane Instance outside of this Pipeline.**

   Analysis: Confirmed. NCC Group finds that the architecture of Amazon EKS fully supports this claim. NCC Group finds that the software deployment process for Amazon EKS Control Plane instances is tightly controlled through a trusted CI-CD Pipeline. Please refer to the `Out of Scope` section in *Security Design Evaluation* for more details around scope for this claim.

5 Documents Reviewed

The following AWS documents were reviewed during this assessment. The internal AWS documents were kept on an AWS system for reading and no copies were made.

- **Data Privacy FAQs public document** - https://aws.amazon.com/compliance/data-privacy-faq
- **Audit Policy for Amazon EKS** public document - https://docs.aws.amazon.com/eks/latest/best-practices/auditing-and-logging.html
- **Amazon EKS Operational Security Controls Document** - The document provides a thorough description of the security designs and controls used to protect customer data in Amazon EKS from AWS employees.
- **Amazon EKS Default Envelope Encryption for Kubernetes API Data - Security Design and Configurations** - Documentation on the use of default envelope encryption for all Kubernetes API data.
- **Amazon EKS Kubernetes Control Plane - Network Security Configurations & Launch Templates** - The document focuses on the architecture of the managed Kubernetes Control Plane, its VPC network security configurations, and the launch templates used to provision the Control Plane instances.
- **Amazon EKS Kubernetes Control Plane - Internal Administrative APIs** - Documentation on the system which ensures that only a limited set of commands can be run on Kubernetes Control Plane instances.
- Evidence to demonstrate that S3 buckets used for AWS Security Logs is restricted by authorization to select personnel only, encrypted using Server-side Encryption with AWS Key Management Service (KMS), and subject to versioning.
- Evidence to demonstrate that EKS Operator access is based on time-bound, oncall group membership

6 Contact Info

The team from NCC Group has the following primary members:

- Divya Natesan – Technical Lead
  divya.natesan@nccgroup.com
- Jonathan Leadbeater – Consultant
  jonathan.leadbeater@nccgroup.com
- Michael Svoboda – Project Manager
  michael.svoboda@nccgroup.com
- Ben Walker – Account Manager
  ben.walker@nccgroup.com