REDSEAL

# RedSeal Cloud

## EKS inventory

### Identify all your Amazon EKS resources

Containerized applications and Amazon Elastic Kubernetes Service (EKS) allow software developers to rapidly develop and deploy new capabilities, but require new types of security measures that are implemented by development teams.

These measure:

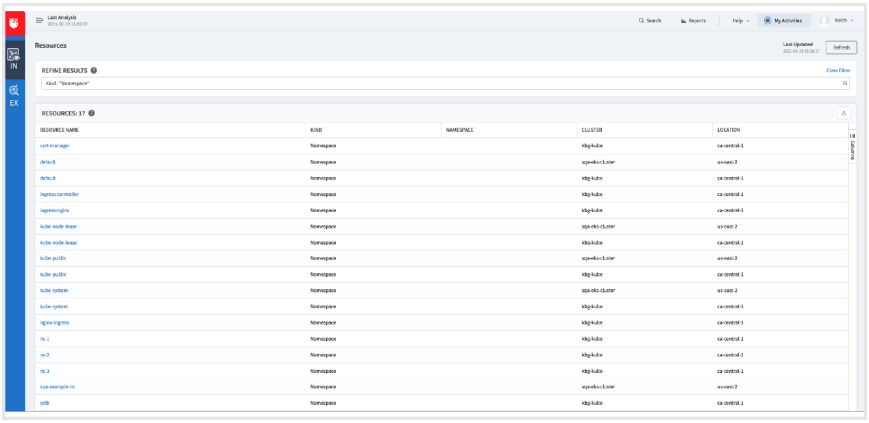
- Control communications between pods and clusters
- Manage services and user/group accounts access
- Define custom policies that are specific to the application deployment

Given this additional responsibility for developers and overall complexity of deployment environments, misconfigured controls are too common. Gartner estimates that by 2025, 99% of cloud security failures are caused by misconfigurations from the customer.

By collaborating with DevOps throughout the Software Development Lifecycle (SDL) security teams can learn the basics of containerized applications and define policies that ensure a stronger security posture.

**Define your security posture and prevent misconfigurations**
**By analyzing all EKS configurations, security teams can answer these key questions:**

- Are there overly permissive user and service accounts?
- Are there services exposed outside the cluster?
- Are there nodes exposed to the Internet?
- Is there unintended access between specific clusters?
- Is the proper RBAC access to the control plane in place?



RedSeal Cloud provides continuous monitoring of your Amazon Kubernetes resources

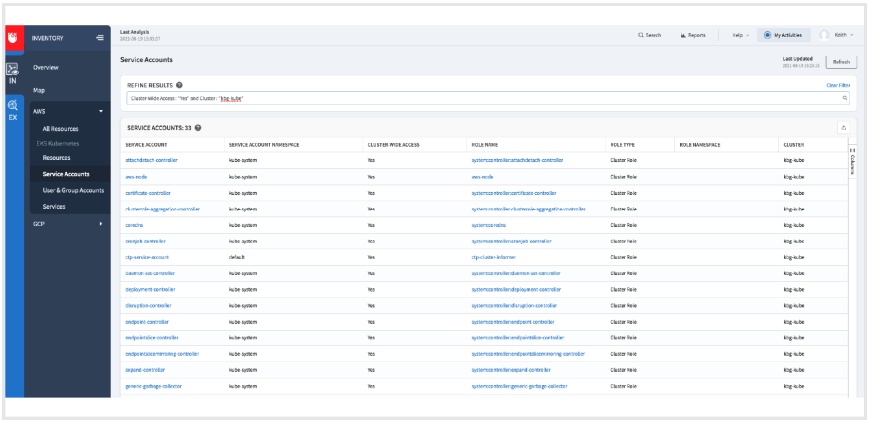
| NETWORK POLICY | NAMESPACE | POD SELECT… | IP BLOCK | NAMESPACE | POD SELECT… | PORTS |
|---|---|---|---|---|---|---|
| deny-ingress | default | | | default | name In hell… | |
| dummy-policy | default | app:apiserver | 172.20.0.0/8 except 17… | default | | TCP:5000, U… |

Identify network security policies which may be in place for both ingress and egress

# Understand your EKS resources

RedSeal Cloud's EKS Inventory provides continuous monitoring of your EKS resources, including filtering by type and detailed drill down of resources (namespace, pod, deployment, service), service accounts, user & group accounts, and services. By drilling down into service accounts and user/group accounts, specific roles are identified along with their types. This enables identification of overly permissive accounts that may allow unintended access across clusters or pods.

Examination of services shows what specific types of services exist that may violate desired access methods (e.g. ClusterIP and Node Port which are often used by developers but are not desired after deployment), including the details of IP addresses and ports. Detailed analysis of all resources also identifies network security policies which may be in place for both ingress and egress, and whether these policies properly enforce the desired security posture.



**Identify overly permissive accounts that may allow unintended access across clusters or pod**

SERVICES: 15

| SERVICE | SERVICE NA... | ACCESS TO CLU... | SERVICE TYPE | EX... | CLUSTER IP | PORTS | CLUSTER |
|---|---|---|---|---|---|---|---|
| apache-svc | default | No | Cluster IP | | 10.100.158.42 | TCP:80 | kbg-kube |
| cert-manager | cert-manager | No | Cluster IP | | 10.100.18.145 | TCP:9402 | kbg-kube |
| cert-manager-w... | cert-manager | No | Cluster IP | | 10.100.172.216 | TCP:443 | kbg-kube |

**Identify services that violate desired access methods, including IP address and port details**

Through this detailed examination of the configurations of all EKS resources, RedSeal Cloud enables security teams to:

- Have up-to-date detailed knowledge of all EKS resources and their relationships with each other
- Identify overly permissive user and service accounts
- Pinpoint unintended exposure to the internet from nodes, clusters, or pods
- Analyze communication channels/access between clusters that may create unintended internet exposure
- Validate network policies that have been defined to ensure that no unintended exposure has been allowed

## A critical piece of a comprehensive CSPM solution

As a key component of the RedSeal Cloud solution, EKS Inventory provides comprehensive visibility and analysis of security controls and policies throughout the entire cloud application environment.

Combined with other capabilities focused on AWS infrastructure, RedSeal Cloud provides a comprehensive cloud security posture management solution focused on stopping unintended exposure.