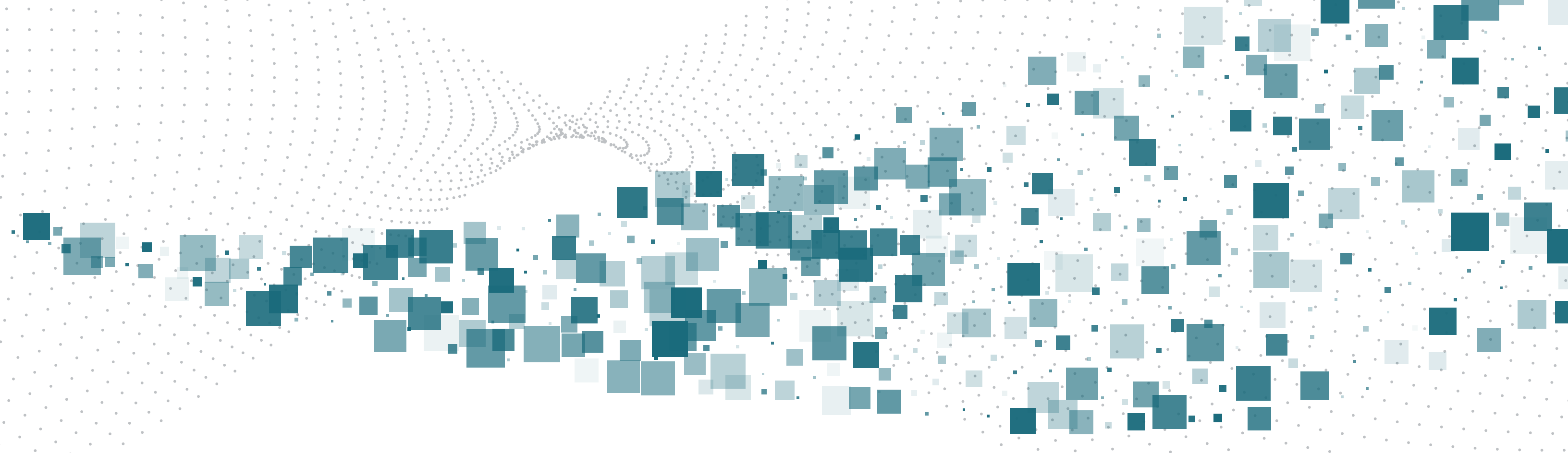
SOLUTION BRIEF | EKS INVENTORY

RedSeal Stratus

Identify All Your Amazon EKS Resources



STRATUS

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 measures:

- 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.

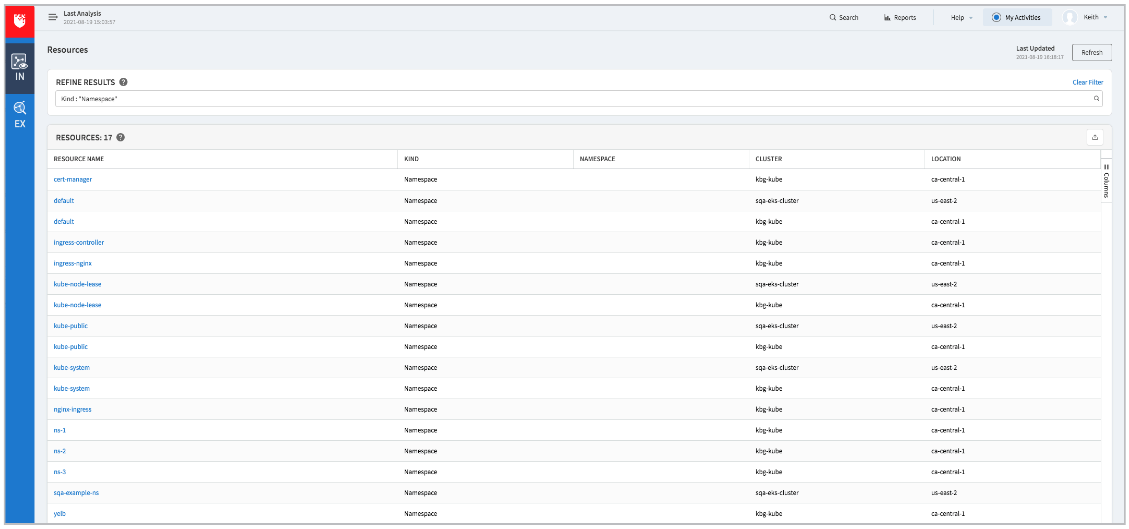
By collaborating with DevOps throughout the Software Development Lifecycle (SDL) security teams can learn the basics of containerized applications and define policies that ensure a stronger security posture.

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



Resources

Last Updated
2021-08-19 16:18:17

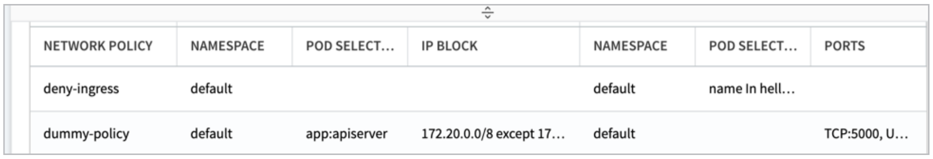
REFINE RESULTS

Kind : "Namespace"

RESOURCES: 17

RESOURCE NAME	KIND	NAMESPACE	CLUSTER	LOCATION
cert-manager	Namespace		kbg-kube	ca-central-1
default	Namespace		sqa-eks-cluster	us-east-2
default	Namespace		kbg-kube	ca-central-1
ingress-controller	Namespace		kbg-kube	ca-central-1
ingress-nginx	Namespace		kbg-kube	ca-central-1
kube-node-lease	Namespace		sqa-eks-cluster	us-east-2
kube-node-lease	Namespace		kbg-kube	ca-central-1
kube-public	Namespace		sqa-eks-cluster	us-east-2
kube-public	Namespace		kbg-kube	ca-central-1
kube-system	Namespace		sqa-eks-cluster	us-east-2
kube-system	Namespace		kbg-kube	ca-central-1
nginx-ingress	Namespace		kbg-kube	ca-central-1
ns-1	Namespace		kbg-kube	ca-central-1
ns-2	Namespace		kbg-kube	ca-central-1
ns-3	Namespace		kbg-kube	ca-central-1
sqa-example-ns	Namespace		sqa-eks-cluster	us-east-2
yelb	Namespace		kbg-kube	ca-central-1

RedSeal Stratus 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

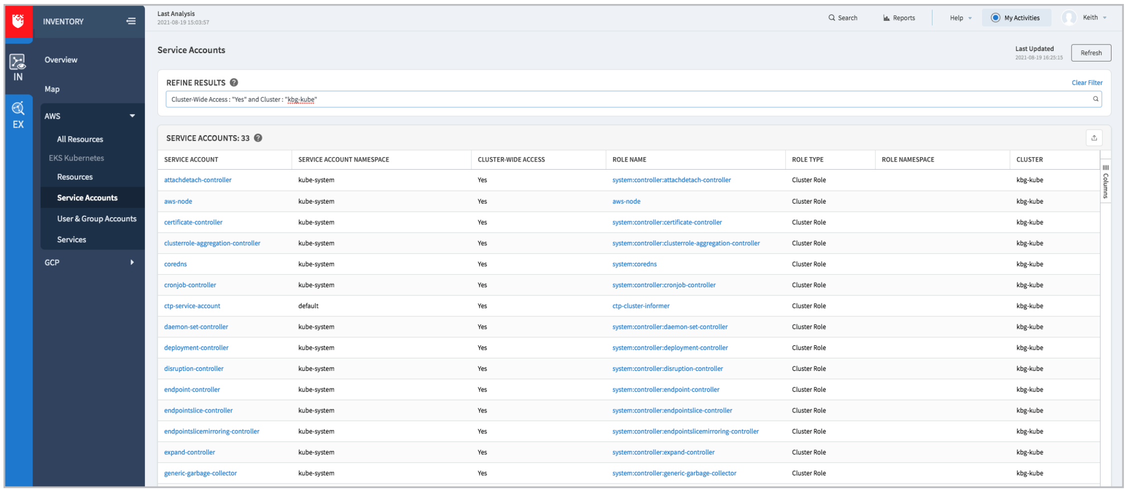
Understand Your EKS Resources

RedSeal Stratus' 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.



Last Analysis
2021-08-19 15:03:57

Service Accounts

Last Updated
2021-08-19 16:25:15

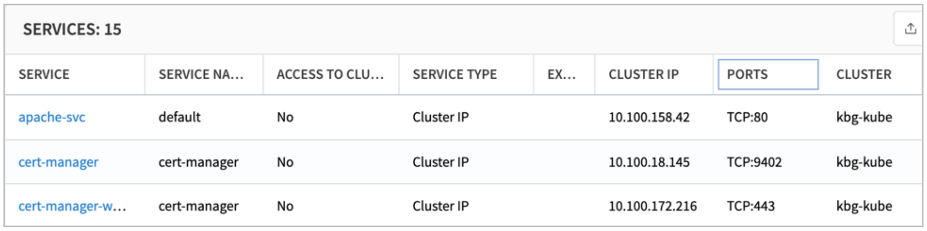
REFINE RESULTS

Cluster-Wide Access : "Yes" and Cluster : "kbg-kube"

SERVICE ACCOUNTS: 33

SERVICE ACCOUNT	SERVICE ACCOUNT NAMESPACE	CLUSTER-WIDE ACCESS	ROLE NAME	ROLE TYPE	ROLE NAMESPACE	CLUSTER
attachdetach-controller	kube-system	Yes	system:controller:attachdetach-controller	Cluster Role		kbg-kube
aws-node	kube-system	Yes	aws-node	Cluster Role		kbg-kube
certificate-controller	kube-system	Yes	system:controller:certificate-controller	Cluster Role		kbg-kube
clusterrole-aggregation-controller	kube-system	Yes	system:controller:clusterrole-aggregation-controller	Cluster Role		kbg-kube
coredns	kube-system	Yes	system:coredns	Cluster Role		kbg-kube
cronjob-controller	kube-system	Yes	system:controller:cronjob-controller	Cluster Role		kbg-kube
ctp-service-account	default	Yes	ctp-cluster-informer	Cluster Role		kbg-kube
daemon-set-controller	kube-system	Yes	system:controller:daemon-set-controller	Cluster Role		kbg-kube
deployment-controller	kube-system	Yes	system:controller:deployment-controller	Cluster Role		kbg-kube
disruption-controller	kube-system	Yes	system:controller:disruption-controller	Cluster Role		kbg-kube
endpoint-controller	kube-system	Yes	system:controller:endpoint-controller	Cluster Role		kbg-kube
endpointslice-controller	kube-system	Yes	system:controller:endpointslice-controller	Cluster Role		kbg-kube
endpointslicemirroring-controller	kube-system	Yes	system:controller:endpointslicemirroring-controller	Cluster Role		kbg-kube
expand-controller	kube-system	Yes	system:controller:expand-controller	Cluster Role		kbg-kube
generic-garbage-collector	kube-system	Yes	system:controller:generic-garbage-collector	Cluster Role		kbg-kube

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 Stratus 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 Stratus 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 Stratus provides a comprehensive cloud security posture management solution focused on stopping unintended exposure.

ABOUT REDSEAL (redseal.net)

RedSeal — through its cloud security solution and professional services — helps government agencies and Global 2000 companies measurably reduce their cyber risk and show where their resources are exposed to the internet.

Only RedSeal's award-winning cloud security solution can bring all network environments– public clouds (AWS, Microsoft Azure, Google Cloud Platform and Oracle Cloud), private clouds, and on premises — into one comprehensive, dynamic visualization. RedSeal verifies that networks align with security best practices; validates network segmentation policies; and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk.