

PROTECTING KUBERNETES CLUSTERS IN AWS AND AZURE

Kubernetes computing services such as Amazon Elastic Kubernetes Service (Amazon EKS) and Azure Kubernetes Service (AKS) have become extremely popular as organizations scale up and adopt lightweight application deployment methodologies.

However, the rapid adoption of Kubernetes computing services creates challenges for organizations looking to obtain visibility and assess security risks across their cloud deployments.

Gain visibility into your Kubernetes entry points and mitigate risks

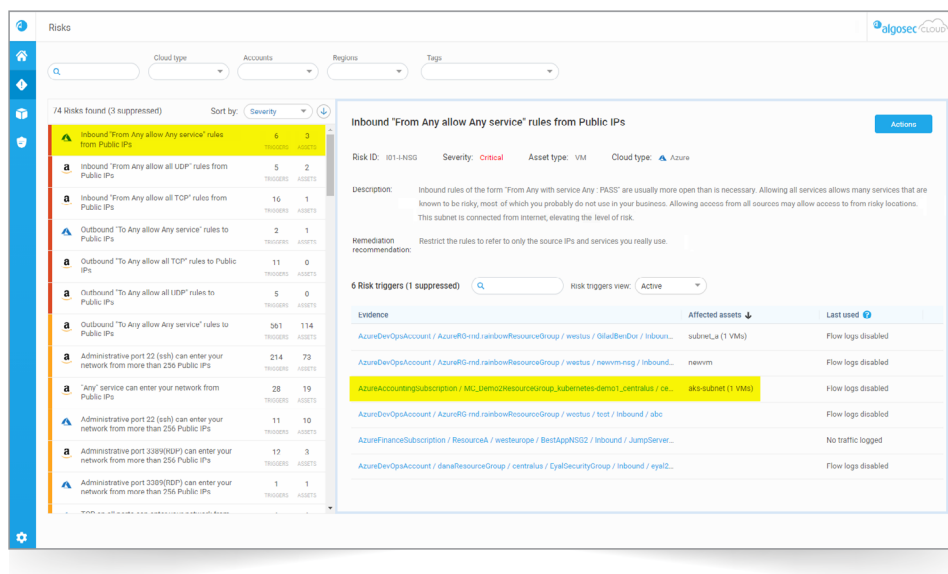
Complete visibility: You can't protect what you can't see

Full visibility is essential to avoid security breaches at the entry point to your Kubernetes nodes and pods. AlgoSec makes the security measures in place, visible at all entry or exit points to your Kubernetes environments. These entry and exit points either direct inbound traffic from the Internet (Public IPs) and Internal Networks (Private IPs), or direct outbound traffic to the Internet from the Internal Networks.

Visibility into the security rules governing the Kubernetes services ensures that an organization can detect over-permissive permissions and vulnerabilities. As a result, security breaches can be minimized.

Risk Analysis

AlgoSec can be used to run an ongoing risk analysis of the Kubernetes services to prevent network breaches. For example, customers that expose their Kubernetes nodes to the Internet with an "any" source and an "any" service in their security group rules are placing their Kubernetes nodes at risk. Identifying and mitigating such risks minimizes the chances of a network breach.



Risks

Cloud type: Accounts: Regions: Tags:

74 links found (8 suppressed) Sort by: Severity

Risk ID	Severity	Asset type	Cloud type
101-LANGSD	Critical	VM	Azure

Inbound "From Any allow Any service" rules from Public IPs

Description: Inbound rules of the form "From Any with service Any - PASS" are usually more open than is necessary. Allowing all services allows many services that are known to be risky, most of which you probably do not use in your business. Allowing access from all sources may allow access to from risky locations. This subnet is connected from internet, elevating the level of risk.

Remediation recommendation: Restrict the rules to refer to only the source IPs and services you really use.

6 Risk triggers (1 suppressed) Risk triggers view: Active

Evidence	Affected assets	Last used
AzureDevOpsAccount / AzureRM-mid-rainbowResourceGroup / westus / 01ac8e8e / Inbound...	subnet_La (1 VMs)	Flow logs disabled
AzureDevOpsAccount / AzureRM-mid-rainbowResourceGroup / westus / newmming / Inbound...	newmm	Flow logs disabled
AzureAccountSubscription / MC_DemoResourceGroup_kubernetesdemo1_centralus / ce...	aks-subnet (1 VMs)	Flow logs disabled
AzureDevOpsAccount / AzureRM-mid-rainbowResourceGroup / westus / test / Inbound / abc		Flow logs disabled
AzureFranceSubscription / ResourceA / westeurope / BestAppNS02 / Inbound / JumpServer...		No traffic logged
AzureDevOpsAccount / dataResourceGroup / centralus / CylSecurityGroup / Inbound / eya12...		Flow logs disabled