Enhancing the Security & Integrity of IBM Kubernetes Offerings

Free Trial Instance and Sandbox: https://trial.shepherd.one

Solution page: https://www.wanclouds.net/shepherd.html

One of the major challenges customers face while managing multiple Kubernetes clusters in a hybrid or multi-cloud environments, is uniform visibility, monitoring and security policy management from a single pane of glass. Moreover, maintaining the integrity of multiple clusters is not actively addressed across different Linux distros and across various private and public clouds.

Shepherd is a single pane of glass security, integrity, and monitoring application for Kubernetes running on Linux machines across private and public clouds. Shepherd provides very detailed and uniform visibility to track the integrity of the Kubernetes clusters. It leverages SElinux and AppArmor to create, deploy, and manage Mandatory Access Control (MAC) policies across the clusters in a very simple and uniform way. It enforces these policies so the Linux hosts, hosting the Kubernetes cluster remain in a trusted state. While running containerized apps, It is not uncommon to see processes such as containers running with root capabilities or in an unconfined state which is considered security threat. An unconfined process can access any container or its mounted data folder with full privileges. To ensure such processes are kept in check, Shepherd leverages SElinux, AppArmor as well as other integrity monitoring techniques to make sure that even if a host is compromised, no harm is done to the containers and important files/DB volumes as the entire system is labelled correctly. In general, deploying and managing SElinux, AppArmor policies are very cumbersome, time-consuming to deploy, and hard to manage. There is no centralized utility today where you can build, deploy, and manage these MAC policies for your container and VM environments. Shepherd helps address these concerns.

Shepherd also supports firewall (FW) rules deployment for Kubernetes cluster as well as visibility of how the various PODs, deployments are communicating with each other. You can create and deploy firewall rules across your cluster to restrict or manage how certain PODs, Deployments talk to each other as well as create, deploy iptables rules on specific hosts.

The other key feature of Shepherd is the ability to track and monitor the integrity of one or multiple clusters deployed in hybrid and multiple clouds. This integrity is tracked on an

ongoing basis. In case a Kubernetes cluster is deployed on bare metal servers, Shepherd has built-in integration with Intel's Cloud Integrity Technology (CIT) solution which measures "integrity at rest" such as OS, boot process. You can run your clusters in a private in-house cloud, or public cloud and create policies, manage security, integrity and compliance from a single control point. Below diagram shows how Shepherd monitors different containerized clusters for security and integrity.

Key Features & Benefits

Shepherd supports Kubernetes running on various Linux distros such as Ubuntu, Centos, Oracle Linux, RHEL. You can add a mix of Kubernetes and Red Hat OpenShift clusters across both public and private clouds. Following are some of the key features;

Visibility and Support for Hybrid and Multi-Cloud

Shepherd provides very detailed and uniform visibility to track the integrity of any Kubernetes clusters, including OpenShift or IBM Cloud Kubernetes Service. It can be deployed inside your private enterprise cloud or in a public cloud. sAgent is used for a cluster not accessible with public IPs which are typically running in a private cloud or in public cloud with private IP addressing. sAgent is a light weight program that can be run on Linux or VM or as a container.

Tracking integrity

Shepherd creates uniform visibility of the attack surface by tracking the integrity of the cluster on an ongoing basis using its custom-built integrity tracking mechanism. It keeps track of the various modules, firewall rules, ports, or specific files and folders. If a cluster is deployed over bare-metal servers, Shepherd has built-in integration with Intel's Cloud Integrity Technology (CIT) for tracking integrity at rest for OS, boot sequence, geo tagging etc.

Firewall policies

Shepherd enables the admin to create, deploy, and manage firewall policies across clusters and for specific hosts using iptable rules. This allows you to manage inter-pod or inter-deployments traffic policies.

Mandatory Access Control (MAC) policies

Shepherd has greatly simplified to build, deploy, enforce, and manage mandatory access control policies across your cluster. It supports both SElinux (Security-Enhanced Linux) and AppArmor (Application Armor) Linux kernel security modules. It allows you to build a profile such as allowing only read and write privileges to a certain folder or process. You can then choose to group containers/PODs across different clusters and associate a specific profile to it. This way, you can pick and choose PODs and images that will inherit a specific MAC profile across one or multiple clusters.

Images tracking & inventory

Shepherd keeps track of the image inventory and enables the admin to white-label containers images for integrity, visibility and compliance across multiple clusters.

Health monitoring

It allows you to monitor your hosts, workloads, PODs for general health (CPU, memory utilization, Storage, network traffic and more.

Operational rules and alerts

An admin can create Integrity and Monitoring rules for their day to day management. For example, you can create rules for CPU or memory utilization or if particular port is opened on a host. Once the condition is met, Shepherd will send an alert to the specified admins/users. Alerts can be sent to ServiceNow, Slack, and email for any operational rules that gets violated.

Compliance

Uniform policies and active monitoring of the attack surface across different clouds and customer's own Data Centers. It strengthens infrastructure compliance for regulations such as GDPR to ensure access to user data is restricted.

Sharing and collaboration

Shepherd is a multi-tenant system by default and an admin can also share his/her account with other team members by adding them. Team members can be added with admin privileges or read-only privileges.

How Shepherd works with IBM managed Kubernetes service (IKS) and its private on-prem offering

IBM offers both managed Kubernetes service (IBM Cloud Kubernetes Service - IKS) as well as a private on-prem Kubernetes deployments (IBM Cloud Private - ICP). In the IKS offering, IBM exposes the Kubernetes dashboard as well as the nodes to its users. Shepherd can help manage and enforce various security & integrity policies as well as active health monitoring of the clusters. All of the above features can be leveraged when you add an IKS cluster. In addition, you can add other clusters such as ICP Kubernetes cluster or other clusters running in another public or private cloud. Shepherd allows you the visibility and helps you create, enforce, manage security and integrity policies enhancing your overall infrastructure compliance and control. Learn how to deploy a Kubernetes cluster in IBM cloud at https://www.ibm.com/blogs/bluemix/2018/06/improving-app-availability-multizone-clusters/.

You add the cluster by deploying the Shepherd sAgent on the IKS nodes following the IKS authentication mechanism. All of the Shepherd features can be utilized for both IKS and private on-prem offerings. All the communication between the cluster, nodes and Shepherd is fully secure using SSL.

Learn more

You can try Shepherd for free using https://trial.shepherd.one. We can deploy a private instance for you in IBM Cloud or at your own private cloud to enhance your cluster security and compliance.

Please contact Wanclouds for further queries at info@wanclouds.net or support@wanclouds.net. You can also find additional information the website at www.wanclouds.net.

For questions or comments, engage the IBM team via Slack. You can register here (https://bxcs-slack-invite.mybluemix.net) and join the discussion in the #questions channel on https://ibm-container-service.slack.com.