

# E-book

## The Ultimate Guide to Best Practices of Kubernetes Deployment



OPSTREE  
Relay on US



---

**By BuildPiper**  
An Opstree Product



# Table Of Contents

<b>Introduction .....</b>	<b>1</b>
<b>Kubernetes Demand .....</b>	<b>2</b>
<b>Challenges of Kubernetes Deployment .....</b>	<b>3</b>
<b>Security Challenges .....</b>	<b>4</b>
<b>Mitigating these Security Challenges .....</b>	<b>4.1</b>
<b>Best Security Practices .....</b>	<b>4.2</b>
<b>Monitoring &amp; Observability Challenges .....</b>	<b>5</b>
<b>Addressing Monitoring &amp; Observability Challenges .....</b>	<b>5.1</b>
<b>Best Monitoring &amp; Observability Practices .....</b>	<b>5.2</b>
<b>Networking Challenges .....</b>	<b>6</b>
<b>Remediating Networking Challenges .....</b>	<b>6.1</b>
<b>Best Networking Practices .....</b>	<b>6.2</b>
<b>General Best Practices of K8s deployment .....</b>	<b>7</b>

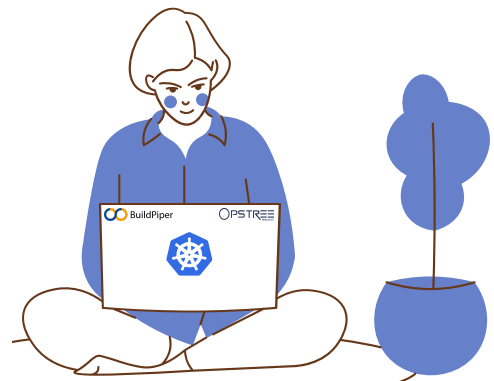


# Introduction

**Kubernetes** is an open-source platform for scheduling and automating the deployment, management and scaling of containerized applications. Also known as “k8s” or “kube” — this container orchestration platform enables cost-effective cloud-native development. ([Read this](#) to know more about Kubernetes, its architecture and Kubernetes components like nodes, pods, containers and much.

Enterprises across the globe are deploying Kubernetes via their preferred choices. Based on the cloud service, some choose to go for AKS deployment on Azure, others prefer to choose EKS deployment with AWS or some others choose standalone setup of Kubernetes for enabling seamless container management.

Along with all the advantages that come up with deploying Kubernetes, there are many challenges too. Engineering teams can be seen exploring ways to navigate through these complicated and often overwhelming Kubernetes challenges to get the most out of their investments. This ebook explains and walks you through the best practices of Kubernetes deployment.

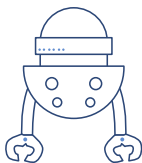


# Kubernetes Demand!



Kubernetes has quickly emerged as one of the leading container orchestration platforms—and, no doubt, for the good. It has become the de-facto standard for deploying containerized applications at scale in private, public and hybrid cloud environments in the market today.

## Features of Kubernetes



**Automated Scheduling**



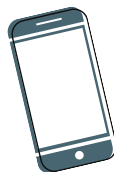
**Self Healing Capabilities**



**Automated Rollouts  
& Rollback**



**Enterprise Ready Features**



**Application Centric  
Management**




**Improved Resource Utilization**




**BuildPiper - By OpsTree**

# Kubernetes Demand!

According to a new forecast from Gartner, Inc, **the worldwide container management revenue will grow strongly from a small base of \$465.8 million in 2020, to reach \$944 million in 2024.** Moreover, the report suggests, among the various cloud technologies, public cloud container orchestration and serverless container offerings will experience the most significant growth.



## How to Decide if your Business is ready for Kubernetes Deployment?



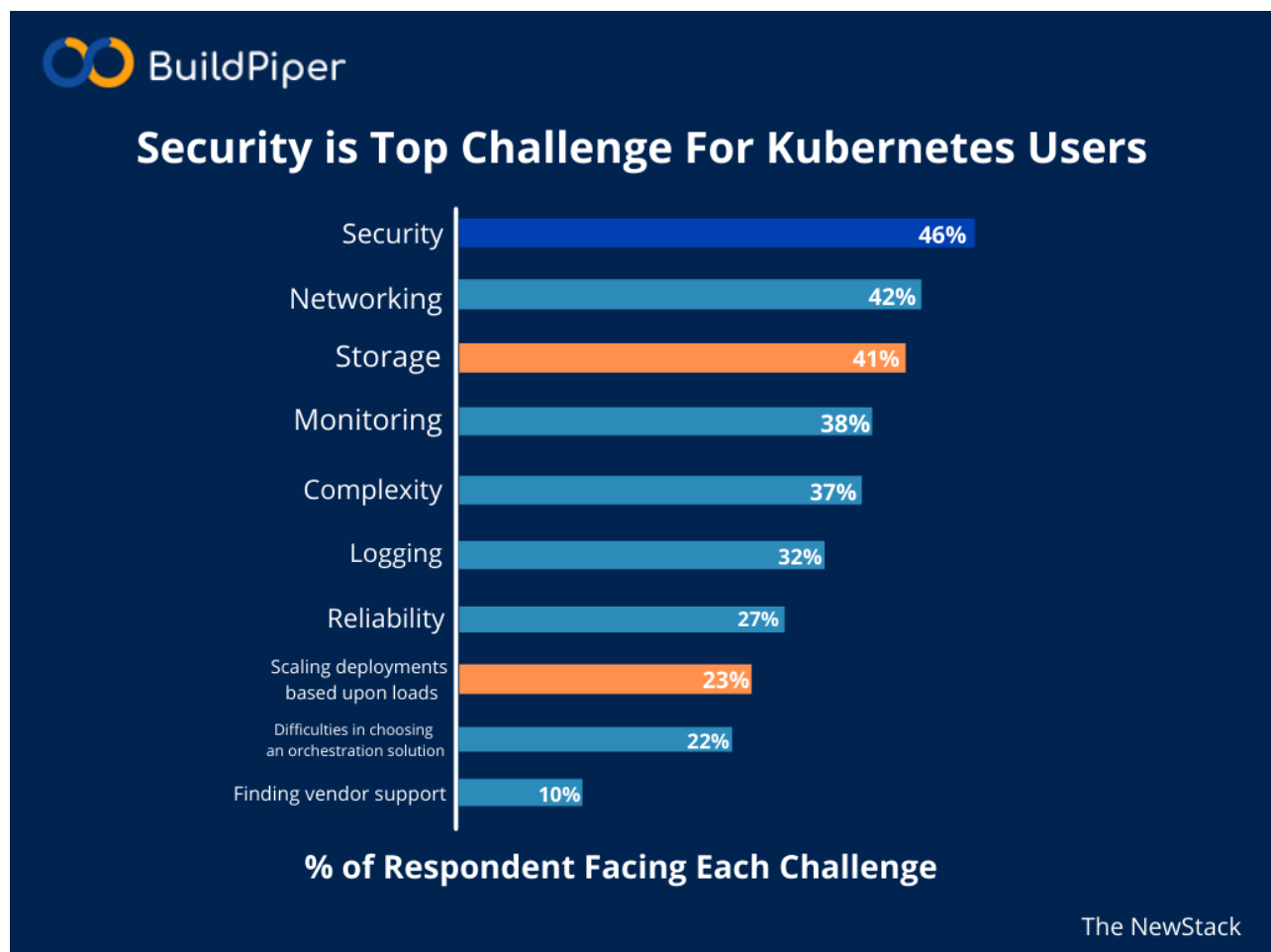
- Workload:** Have you identified the targeted workloads for containerization?
- DevOps:** Does your team have the required skills and the right platform strategy to enable agile software development?
- Deployment Platform:** Have you decided where the workloads will be deployed and which platform would you go for deploying Kubernetes?
- Return on Investment:** What will be the return on investment?
- Roles & Skills:** What additional skills/training would be required to make this implementation successful?
- Integration:** How will the platform integrate with the existing infrastructure?



**BuildPiper - By OpsTree**

# Challenges & Best Practices of Kubernetes Deployment!

According to a survey, shifting **hundreds or thousands of apps to** Kubernetes can be highly challenging. The survey suggests that initial deployment, monitoring and alerting, complexity and increased cost, and reliability were the major hurdles that enterprises faced during migration.



# Challenges & Best Practices of Kubernetes Deployment!

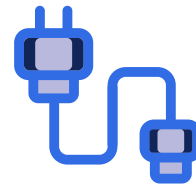
The major problem arises when organizations face a number of complexities while running Kubernetes. Here we'll explore three of the primary barriers, along with some of the best practices



**Security Challenges**



**Monitoring & Observability Challenges**



**Networking Challenges**





# Security Challenges

Among the many challenges that enterprises have to handle with Kubernetes deployment, security is one of them. In the current disruptive and highly competitive market, Kubernetes-related security attacks and incidents are on the rise. Many organizations are forced to hold back on their business plans because of their Kubernetes-related security concerns and partly for their inability to resolve them.

Security checks and addressing security issues can't be an afterthought. The security practices need to be embedded in the DevOps process - generally referred to as "DevSecOps". While talking about Kubernetes challenges here, or Kubernetes DevSecOps, Product teams need to plan for securing the containerized environment across the entire DevOps life cycle, which includes the build, deploy and run phases of an application.

Lately, security concerns have come out as one of the significant Kubernetes challenges for enterprises planning to deploy Kubernetes. When it comes to single out significant security challenges, it won't be wrong to consider these as the major barriers for implementing Kubernetes. **Let's hash these out.**

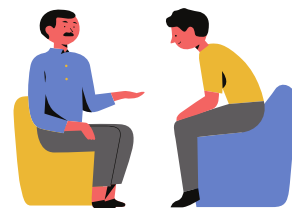
- **Communication between the pods**
- **Runtime security threats**





# Communication Between the Pods

The entire Kubernetes deployment comes down to pods or groups of one or more containers. **Pods** are the smallest deployable units of computing that can be created and managed within Kubernetes. A pod comprises the shared storage and network resources, and a specification for how to run the containers.



It makes sense that enterprises' efforts for resolving Kubernetes-related security concerns should begin here. Pod communication is an issue. Since all pods are non-isolated by default and accept traffic from any source. Thus, the intrusion of external malicious entities can take advantage of the fact and use the communication properties of the pod to contaminate the remaining pods.

This creates a problem in access control. Access control is determining who gets what kind of access to particular data. Restricting access to confidential systems or data helps in preventing risks associated with data exposure.



# Runtime Security Threats

Enterprises need to be aware of runtime security threats for a secured and hassle-free Kubernetes deployment. The runtime phase of Kubernetes deployment exposes containerized applications to a chunk of security threats that happen in real-time. As a result, a compromised container can execute a malicious process that ultimately affects the other containers in the environment.

A [survey](#) shows that 94% of organizations have experienced a serious security issue in the last 12 months in their container environment, with

69%

having detected  
misconfigurations

27%

experiencing runtime  
security incidents

24%

discovering significant  
vulnerabilities to remediate.



BuildPiper - By OpsTree

# Runtime Security Threats

Comprehensive Kubernetes monitoring and checking container activities can help organizations tackle these security-related Kubernetes challenges. Enterprises should primarily focus on network traffic in order to restrict and prevent unnecessary or insecure communication, as specified by their network policies. They can then use this data to harden the conditions of their network policies even further. Leveraging popular Kubernetes DevSecOps approaches can help in overcoming these challenges.

## Mitigating these Security Challenges

Security has been the first concern when it comes to deploying and running Kubernetes for container orchestration. Combining the latest Kubernetes DevSecOps approaches along with the best security practices, **BuildPiper** helps with secure, scalable and seamless K8s cluster management and deployment. Here is how BuildPiper commits to make your life easier.



# Mitigating these Security Challenges



## Secret Management with Hashicorp Vault:

Enables seamless secrets management within the same platform by default integration with Hashicorp Vault, thus providing the platform operations team with the ability to manage security from a centralised console with a Key-Value pair.



## RBAC

BuildPiper allows cluster creation backed by RBAC based safe & compliant interface, enabling secured K8s operations and access control management



## Access Management

With a 'Security - First' mindset, BuildPiper offers multiple options to securely manage access with custom ingress rules for the public, protected and private traffic flowing through the services.



**BuildPiper - By OpsTree**

# Best Security Practices

To restrict exposure of containerized applications from security threats and malicious attacks, considering Kubernetes DevSecOps practices can be leveraged. Here are a few recommended approaches and best practices to adopt in order to resolve security issues and extract the most out of the Kubernetes advantages and quick delivery of applications.



## Image Scanning Process

Integrate an image-scanning process to prevent vulnerabilities in the applications. Include the process as a part of the continuous integration/continuous delivery (CI/CD). Doing this makes sure that all the enterprise applications are scanned during the build and run phases of the software development life cycle.



## CIS Benchmarks

Tighten the configurations for Kubernetes monitoring and detecting threats and vulnerabilities by using Center for Internet Security (CIS) benchmarks, which are available for Kubernetes, to enable a strong security system.



## Access Control

Restrict access to confidential systems or data. It helps to mitigate potential threats and risks associated with data exposure.



# Best Security Practices



## RBAC

Enable Kubernetes role-based access control (RBAC). Kubernetes RBAC controls the access authorization and also restricts the access to a cluster's Kubernetes API servers, both for service accounts and for users in the cluster.



## Secrets Management

Deploy tools and methods for managing digital authentication credentials (known as secrets), including passwords, keys, APIs, and tokens for getting access to applications, services, and other sensitive parts of the enterprise.

## Key Takeaway:

Security is an important aspect that needs to be taken care of right from the start. Ignoring potential security risks can expose applications to damaging threats leading to serious consequences. Considering effective security practices can fasten the delivery process and help businesses with enhanced agility and greater ROI. Platforms like BuildPiper can enable this out of the box and make your Kubernetes & Microservices Journey, hugely rewarding!





# Monitoring and Observability Challenges

Enterprises deploying Kubernetes clusters across on-premises, multiple public clouds, or hybrid clouds introduce a lot of fragmentation and complexity. To leverage the maximum value from the Kubernetes and to avoid overhead expenditure, security risks and performance issues, organizations need to have a complete view of the cluster components including pods, nodes, applications, namespaces etc and how they interact with each other.

Engineering teams struggle in gaining deep insights and detailed observability into the cluster environment, which delays the process of identifying failures and increases the MTTR (Mean Time to Resolution) for any production outage. Due to a large number of connected services and components within a cluster, monitoring needs special attention.

**Moreover**, since the environment is constantly changing, Kubernetes monitoring gets too complicated. As a result, platform teams fail to figure out what is actually happening and what resources are being utilized, and even the cost implications of the actions being taken on the cluster environment. This is why finding the **right cluster management** platform that supports deep insights and comprehensive observability is essential.



# Addressing Monitoring & Observability Challenges

BuildPiper provides a 360-degree view of the cluster with out-of-the-box microservice and cluster observability capabilities allowing users to view and monitor the performance, health status, availability, logs and other important metrics. To carry out concrete and comprehensive Kubernetes monitoring, BuildPiper has -



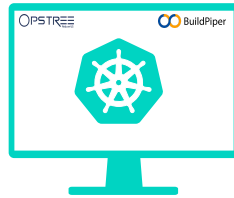
## Managed Kubernetes

With Managed Kubernetes as one of the core features, BuildPiper aims to make Kubernetes- Microservices Application ready, enabling highly intuitive cluster management with features like -





# Addressing Monitoring & Observability Challenges



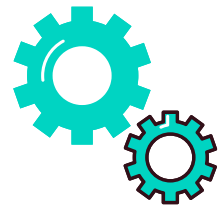
## Service Kubernetes Dashboard

The dashboard gives complete visibility into the service details in Kubernetes.



## Infrastructure Monitoring Tools

BuildPiper enables hassle-free integration and setup of infrastructure monitoring tools such as **Prometheus**, **Grafana**, **Alert Manager** for event monitoring and alerting.



## Log Management Tools

BuildPiper supports easy configuration of log management tools such as **ElasticSearch**, **Fluentd**, and **Kibana** to manage logs in Microservices architecture.



BuildPiper - By OpsTree

# Best Monitoring & Observability Practices

Monitoring & Observability plays an important part in empowering production-grade Kubernetes clusters. Here are a few practices to leverage comprehensive monitoring & clear observability of the cluster components.



## Granular View

Focus to gain deep insights into the cluster components by monitoring at a container granularity and across containers at a service level.



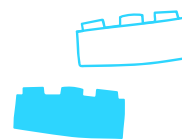
## Real-time details

Prioritize tools that have automated service discovery, can perform detailed application monitoring and provide action-oriented recommendations in real-time, using analytics and machine learning.



## Monitoring Tools

Leverage infrastructure monitoring tools such as Prometheus & Grafana and log management tools Kibana & Fluentd, that offer complete visibility into the cluster environment.



## Build & Deploy Logs

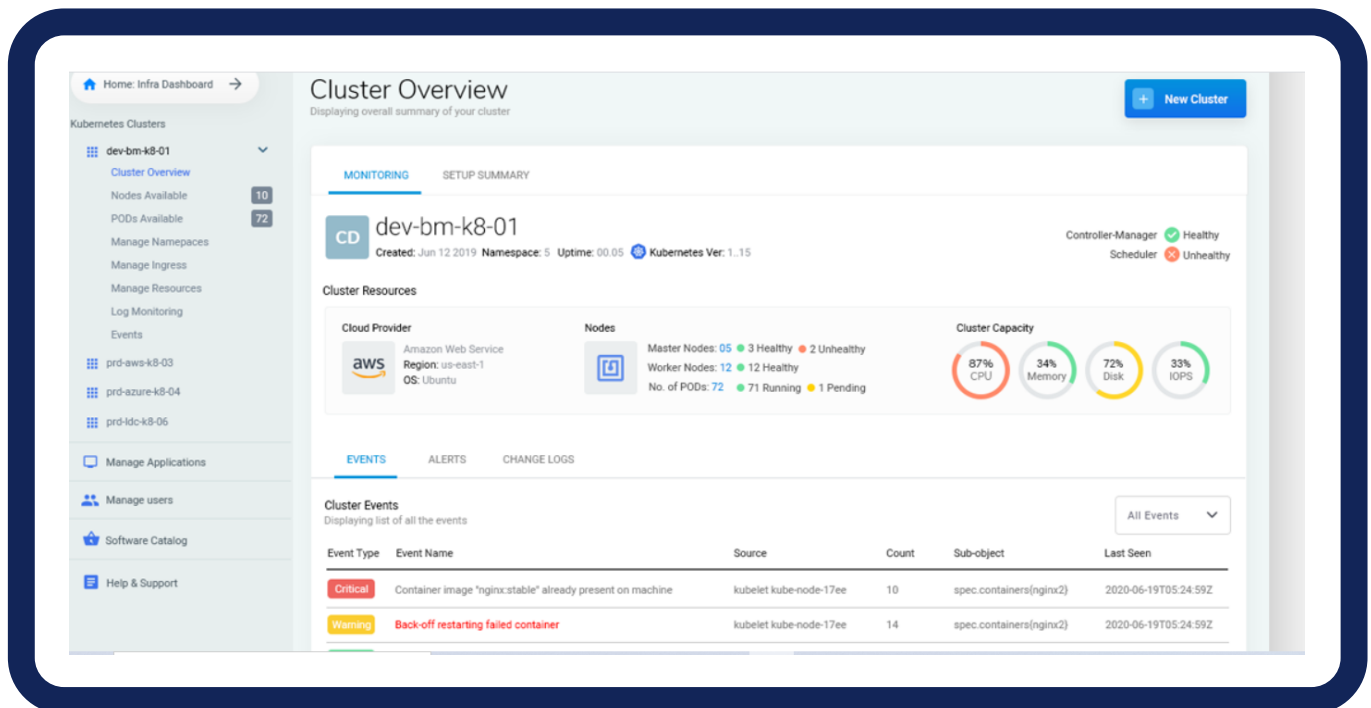
Get complete details of the Build & deploy logs and events to troubleshoot issues for seamless deployment.

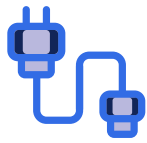


# Best Monitoring & Observability Practices

## Key Takeaway:

Tracing changes, monitoring health status and logging events in a large K8s cluster come with its own sets of added complexity. In such a complex system, monitoring is difficult but important to manage the complete lifecycle of applications. It helps in identifying issues that arise when the cluster is operational.





# Networking Challenges

Kubernetes networking can be complicated and managing these can take a toll on the productivity of the DevOps team. Troubleshooting typical Kubernetes networking issues for large-scale production deployments often becomes quite challenging for enterprises.

- **Network Communication Reliability**
- **Combining Virtual Machine Networking**

## Network Communication Reliability

Service-to-service communication in a Microservice architecture gets convoluted. As the number of services (and containers and Kubernetes pods) increases, the complexity of service communication increases, and so does the significance of reliable communications.

This is why enterprises often have to face communication reliability issues. Tightening the Kubernetes network policies (and other configurations) can help in making network communications reliable and more effective.



# Combining Virtual Machine Networking

While talking about the different challenges of Kubernetes networking, enterprises often have to face a common yet significant challenge. It is the need of combining the management and monitoring of VM-based deployments and Kubernetes-based deployments. Enterprises look for ways to manage both types of deployments.

Since there are many differences between the VMs and containers that results in organizations failing to overcome the issue. There arises a need for a platform that can offer an API to address the needs of development teams that have adopted Kubernetes for containers, along with the ability to carry out deployments based on virtual machines.

Since there are many differences between the VMs and containers that results in organizations failing to overcome the issue. There arises a need for a platform that can offer an API to address the needs of development teams that have adopted Kubernetes for containers, along with the ability to carry out deployments based on virtual machines.



# Remediating Networking Challenges

Adopt some of the following ways with a custom setup or leverage comprehensive platforms like BuildPiper.

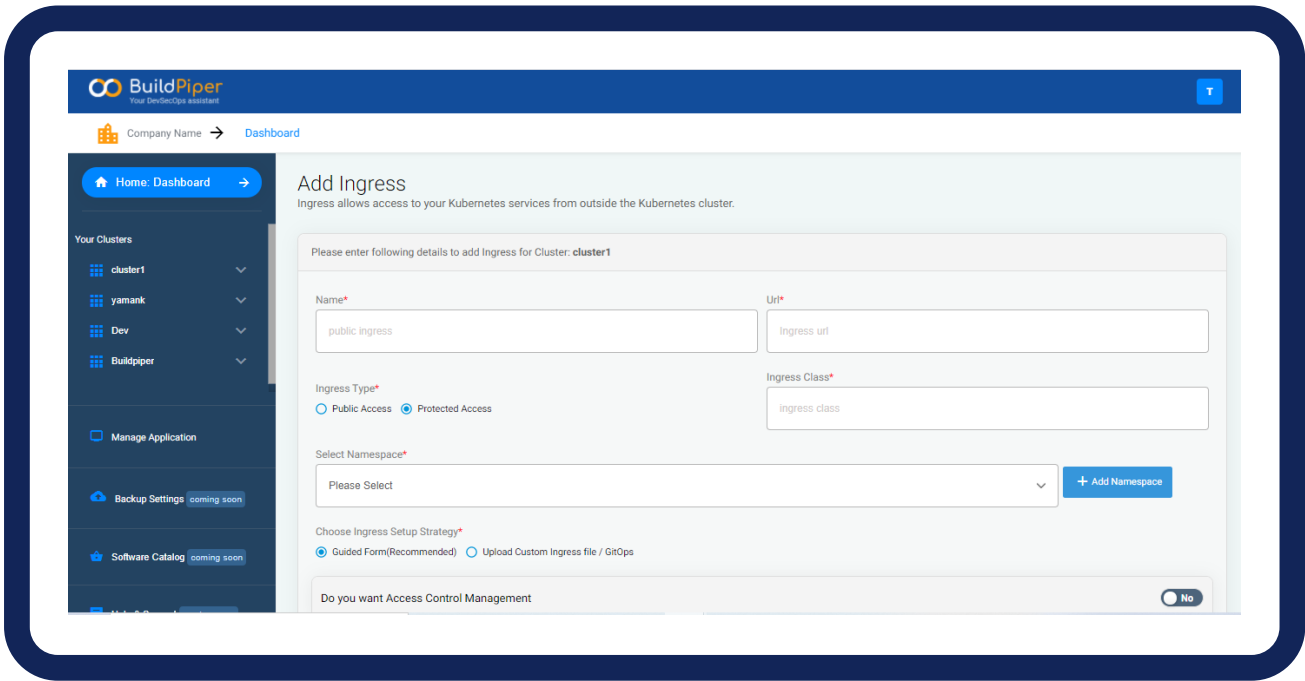
## **ISTIO:**

BuildPiper allows extremely easy setup and integration of ISTIO, which is an open-source service mesh, to manage the traffic flow across microservices. It checks and monitors the communication between microservices and helps in preventing internal and external threats spanning across the data, endpoints, communication, and platform.

## **Public & Protected Ingress:**

Deploying the “convention over configuration” approach to make Kubernetes cluster management extremely simple and highly secure, BuildPiper provides an option to create Public and Protected Ingress.





# Best Networking Practices

Using these practices can help organizations overcome the Kubernetes networking challenges.



## Container Networking Interface

Identify whether your Kubernetes distribution platform or software-defined networking (SDN) solution supports Kubernetes networking. If it does not, then choose a Container Networking Interface. A CNI plugin helps in inserting a network interface into the container network namespace.



# Best Networking Practices



## Ingress

Ensure that the Kubernetes platform you've chosen provides ingress controller support for load balancing across hosts in the cluster.



## Networking Tools

Provide the networking team with hands-on training on the latest Linux networking and network automation tools to enhance agility.



## Service Mesh

Deploy a service mesh. A service mesh integrates with the infrastructure layer of the application. It helps in making the communications between services over the network secure and reliable.

## Key Takeaway

Reliable and secured network communication is a must for smooth application delivery. Restricting the traffic flow and access control through Ingress can help in safe and secure communication between the services.





# General Best Practices of Kubernetes Deployment

Here are some of the general practices preferred by leading enterprises for smooth, secure and compliant Kubernetes deployment. Let's explore these!

## Cost Optimization with Spot Instances



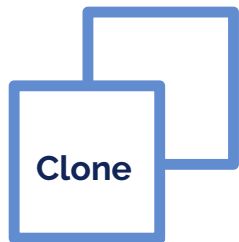
A majority of organizations have some workloads that are mission-critical and other workloads that are not nearly as important. It is possible to reduce the cost of these less-important workloads by taking advantage of Spot instances. Spot Instances let enterprises to take advantage of the unused EC2 capacity in the cloud. Through these spot instances, cloud providers offer excess capacity at a massive discount to drive usage and to nullify the loss of idle infrastructure.

BuildPiper enables software teams to use spot instances for running various stateless, fault-tolerant, or flexible applications such as containerized workloads, CI/CD, web servers, high-performance computing (HPC), and test & development workloads.



# General Best Practices of Kubernetes Deployment

## Start/Stop/Cloning an Environment



Build with a developer-friendly mindset, BuildPiper allows quick and hassle-free cloning of the environment details. While BuildPiper makes adding a new environment to the service extremely simple and easy, it also enables seamless modification and cloning of the build & deploy details from an already created environment.

This ability to clone environment details and makes the entire process of creating a new environment extremely smooth and painless. Unlike BuildPiper, not all management platforms available in the market have this out-of-the-box functionality to support trouble-free configuration of build & deploy details from an existing environment.

## Replica Sets



ReplicaSet's objective is to maintain a stable set of replica Pods that are running at any point in time. It is used to ensure and guarantee the availability of a specified number of identical Pods.



# General Best Practices of Kubernetes Deployment

A ReplicaSet is defined with fields that mainly include,

## Selector

for specifying how to identify Pods that it can acquire.

## Number of replicas

that indicates how many Pods should be maintained,

## Pod template

specifying the data of new Pods that should be created to meet the number of replicas criteria.

A ReplicaSet completes its task by creating and deleting Pods as needed to reach the desired number. A ReplicaSet uses its Pod template when it needs to create new Pods.

## Managed Services (Like ECS) vs Native Kubernetes Setup

Leveraging Managed Kubernetes services such as Amazon's ECS, Microsoft's AKS, and Google's GKE can help enterprises in solving security, observability & monitoring and networking challenges. Using a native Kubernetes setup with baked-in features like security, compliance and observability is an alternative too. BuildPiper is one such K8s deployment platform that helps in making **Kubernetes-Microservices application ready** along with the ability to run zero-touch, fully - automated & secured CI/CD pipelines.



# A Unified approach to Kubernetes & Microservices Application Management

BuildPiper emerges from our cumulative experience of managing platforms and DevSecOps for 100+ microservices journeys and making Kubernetes simple & effective for application developers. With Managed Kubernetes, BuildPiper solves cluster management issues and enables secure and hassle-free cluster creation or onboarding and with its capabilities, help enterprises in mitigating internal & external security threats and security risks within the cloud environment. It provides real-time insights into data and helps in automating compliance and security management.

With best-in-class capabilities for Ingress & Namespace Management, 360-degree cluster view, use of monitoring & log management tools, extensive focus on Cost Optimisations, BuildPiper brings in a holistic and proactive approach to observability spanning infrastructure, environments, data, and applications. It empowers the product and engineering teams to derive value with 10X reduced time & investments required on your Kubernetes & microservices Journey.

Explore its functionalities like Microservices Management, Security, Compliance & Observability and Secure CI/CD Pipelines setup along with Managed Kubernetes. for your use cases. [Take a demo today!](#)

