

First Horizon National: CloudBees CI on modern cloud platforms Engagement Client Checklist

Table of Contents

[**Overview**](#_3t6c6sucizgv) **2**

[**CloudBees CI Pre-installation Configuration**](#_a38tg2xjlg9q) **3**

[Pre-Installation requirements](#_h10snypjo9ug) 3

[Customer Installation To Do List](#_6oqf4ig7q5wz) 3

[**Next Steps**](#_qmwcjssr7npw) **5**

[**Appendix A - Documentation**](#_vwoqzig0vh12) **6**

# 

# Overview

CloudBees met with First Horizon National on 2021-06-08 to review the Onboarding questionnaire, respond to client questions and list next actions to prepare for the installation

This is the CloudBees pre-installation guide for CloudBees CI on modern cloud platforms

Please review and contact your CSM if you have any questions.

Once you have reviewed this document and supplied the information requested, please return to your CSM so a followup validation call can be scheduled.

# 

# CloudBees CI Pre-installation Configuration

## Pre-Installation requirements

Review the [pre-installation documentation](https://docs.cloudbees.com/docs/cloudbees-ci/latest/kubernetes-install-guide/kubernetes-pre-install-requirements) for Kubernetes on premises

## Customer Installation To Do List

1. What version of Kubernetes will you be using?

|  |  |
| --- | --- |
| Version |  |

1. CloudBees CI on modern cloud platform requires an NGINX Ingress controller to be installed. Please confirm this is available and the version that is installed.

|  |  |
| --- | --- |
| NGINX Ingress version |  |

1. You need to ensure that a suitable Load balancer is set up to direct traffic to the Ingress controller, please confirm that this is in place and configured.
2. **Your** DNS configuration should be in place and traffic should successfully route through to your ingress controller.

|  |  |
| --- | --- |
| DNS Name |  |

1. Is SSL required for your environment?

|  |  |
| --- | --- |
| SSL Required? |  |

NOTE:

* Self-signed - please refer to the 'Using self-signed certificates in CloudBees CI' section of the installation documentation
* SSL certificates must be installed at the load balancer

1. It is recommended to use a CloudBees CI specific namespace in the cluster with permissions to create Role and RoleBinding objects. Typically this means having the cluster-admin super-user role in that namespace, and that namespace only.

NOTE:

* This is only needed during the installation. Services will run using the created roles with limited privileges.

|  |  |  |  |
| --- | --- | --- | --- |
| **Purpose** | **Namespace** | **CPU** | **Memory** |
| CloudBees CI |  |  |  |
| Builds |  |  |  |

1. Confirm you have a dedicated account, with admin access, within the Kubernetes namespaces.
2. By default, CloudBees CI will use whatever class is configured to be the Default Storage class. Verify that a default storage class for each namespace has been set. To confirm you have a default storage class, run the following command:

|  |
| --- |
| **kubectl get storageclass** |

In the output your should expect to see “default” next to one of the types, similar to below:

|  |
| --- |
| **NAME PROVISIONER**  **default kubernetes.io/aws-ebs**  **gp2 (default) kubernetes.io/aws-ebs** |

NOTE:

* The **NAME** and **PROVISIONER** are likely to be different in your own environment

|  |
| --- |
| **kubectl get storageclass** |
|  |
|  |

1. If default does not appear next to any Name, run the following command to set a default:

|  |
| --- |
| **kubectl patch storageclass <your-class-name> -p '{"metadata":**  **{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'** |

1. Confirm that the storage class configured and intended for use by CloudBees CI dynamically creates persistent volumes.

|  |  |
| --- | --- |
| Dynamic provisioning supported? |  |

# Action Items

During the review of the discovery questionnaire, we identified a few items that need additional information.

## Scans Performed on CAP Plugins

Security Scanning of plugins that are part of CAP, like all security, constantly evolves based on threats and technology. Today CloudBees is using Anchore.

## Plugin Catalogs

First Horizon has an internal compliance requirement to scan all plugins that are installed on CloudBees CI. Plugins that are managed by Beekeeper are scanned as part of CAP. First Horizon expects they will need plugins that are not part of CAP, and thus will need to be scanned to meet the compliance requirements. To do this, these plugins should be managed using a plugin catalog. [Here](https://docs.cloudbees.com/docs/admin-resources/latest/plugin-management/configuring-plugin-catalogs) is the documentation on how to install non-CAP plugins with a plugin catalog. [Here](https://docs.cloudbees.com/docs/admin-resources/latest/plugin-management/managing-plugins-secure-environment) is the documentation on how to configure a plugin catalog in a secured environment.

## External Load Balancer Configuration

First Horizon has an F5 Load balancer installed. CloudBees recommends terminating on the load balancer so that the load balancer’s performance is affected and not the Operations Center or the controller host.

The DNS entry should point to the Ingress Controller that was created. The external load balancer needs to drive traffic to the Ingress Controller.

For more information, see the [Kubernetes documentation](https://kubernetes.github.io/ingress-nginx/deploy/).

## Self-signed Certificates installation with Modern

First Horizon satisfies the SSL requirement using self-signed certificates. [Here](https://docs.cloudbees.com/docs/cloudbees-ci/latest/cloud-admin-guide/kubernetes-self-signed-certificates) is the documentation on how to implement self-signed certificates in CloudBees CI on Kubernetes

## Multi Cluster Setup

This item will be covered in more detail during a future engagement, but for now, the documentation on how it is configured can be found [here](https://docs.cloudbees.com/docs/cloudbees-ci/latest/cloud-admin-guide/multiple-clusters).

## 

# Next Steps

First Horizon is planning their initial Meeting with the Rancher team in the week of June 14th 2021 to plan their kubernetes cluster installation.

# Appendix A - Documentation

The [CloudBees Documentation](https://docs.cloudbees.com/) page contains information about all aspects of a CloudBees CI on modern cloud platforms environment, including installation, maintenance and best practices

* [CloudBees CI on modern platforms release notes](https://docs.cloudbees.com/docs/release-notes/latest/cloudbees-ci/modern-cloud-platforms/2.263.2.2)
* [CloudBess CI on modern platforms administration guide](https://docs.cloudbees.com/docs/cloudbees-ci/latest/cloud-admin-guide/)
* [Reference Architecture for kubernetes on premises](https://docs.cloudbees.com/docs/cloudbees-ci/latest/cloud-reference-architecture/ra-for-onprem/)
* [Kubernetes Network Policies](https://kubernetes.io/docs/concepts/services-networking/network-policies/)
* [Kubernetes Pod Security Policies](https://kubernetes.io/docs/concepts/policy/pod-security-policy/)
* [How to use Kubernetes Pod Security Policies with CloudBees CI](https://support.cloudbees.com/hc/en-us/articles/360034591531-How-to-use-Kubernetes-Pod-Security-Policies-with-CloudBees-Core-on-Modern-Cloud-Platforms)
* [Required URLs to allowlist](https://docs.cloudbees.com/docs/cloudbees-ci/latest/cloud-secure-guide/url-list)
* [Required Ports to open](https://docs.cloudbees.com/docs/cloudbees-ci/latest/traditional-secure-guide/configuring-network-requirements)