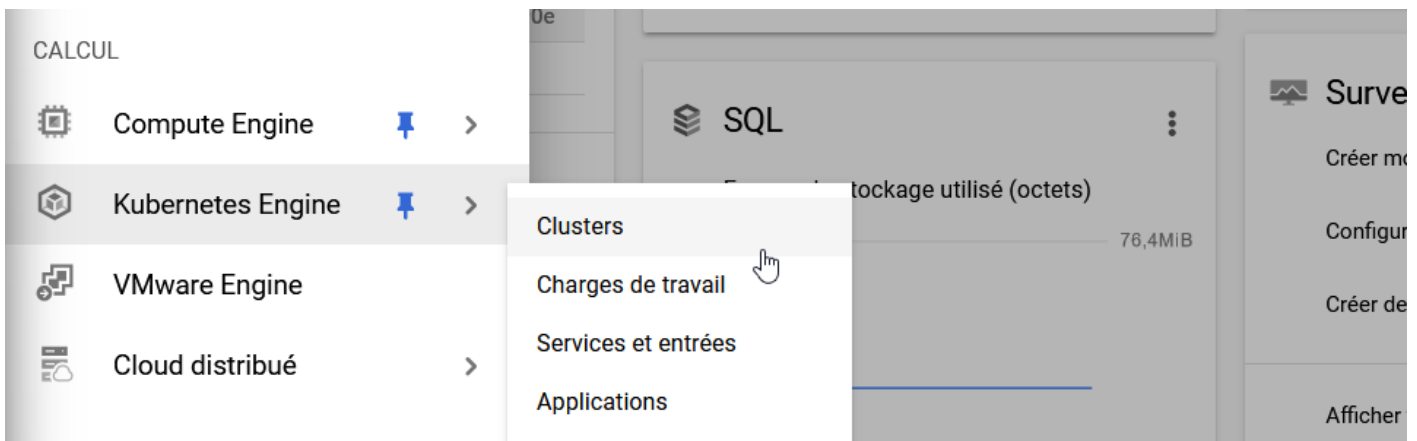


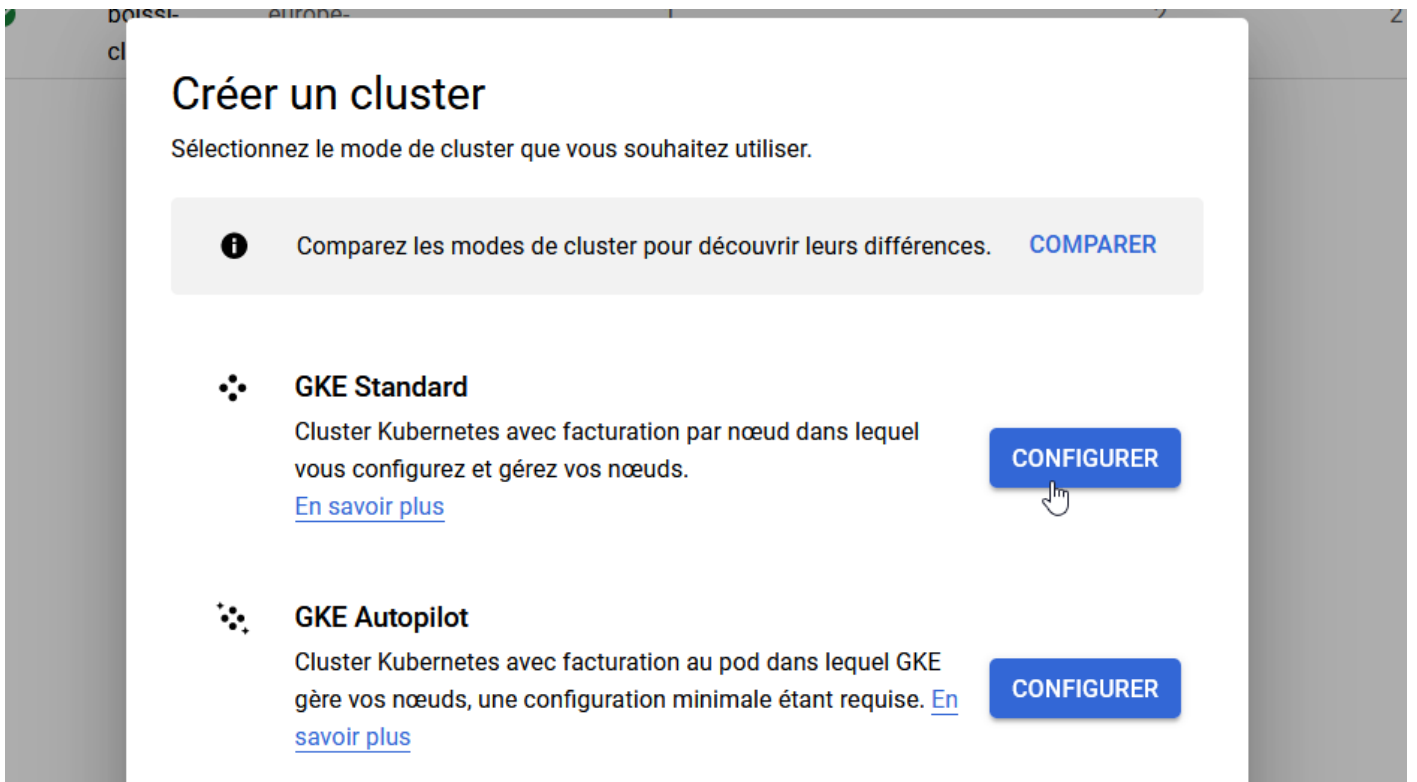
Google Kubernetes Engine

Mise en place d'un cluster GKE

Dans la section **CALCUL** de **GCP**, allez sur le service **Kubernetes Engine** > **Clusters**.



Une fois sur cette page, il peut vous être demandé d'activer GKE. Cela fait, cliquez sur le bouton **Créer** pour ajouter un nouveau cluster, puis choisissez le mode **GKE Standard**.



Configuration du cluster

Paramètres de base du cluster

- Donnez un nom à votre cluster
- Choisissez une zone proche de là où vous trouvez
- Choisissez une version de Kubernetes (celle proposée par défaut est très bien)

Paramètres de base du cluster

Le cluster sera créé avec le nom, la version et l'emplacement que vous indiquez ici. Une fois le cluster créé, le nom et l'emplacement ne peuvent pas être modifiés.



Pour effectuer des tests avec un cluster abordable, sélectionnez **Mon premier cluster** dans le menu **Guides de configuration des clusters**

Nom

cluster-1



Type d'emplacement

Le prix des ressources peut varier d'une région à l'autre. [En savoir plus](#)

Zonal

Régional

Zone

europa-central2-a



Spécifiez les emplacements de nœuds par défaut

Emplacements par défaut actuels : europa-central2-a

Version du plan de contrôle

Choisissez une version disponible pour la gestion automatique de la version de votre cluster et de la fréquence de mise à niveau. Optez pour une version statique pour gérer la version de votre cluster de façon plus directe. [En savoir plus](#).

Version stable

Version disponible

Version disponible

Version standard (par défaut)



Version

1.21.10-gke.2000 (par défaut)



Ces versions ont réussi les tests de validation interne et sont considérées de qualité production, mais ne disposent pas de données historiques suffisantes pour garantir leur stabilité. Les problèmes connus ont généralement des solutions de contournement connues. [Notes de version](#)

Pools de nœuds

- Donnez un nom à votre pool
- Choisissez la taille
- Pour éviter une surfacturation, laissez décoché l'autoscaling

Le nombre de nœuds peut être redimensionnable manuellement après la création du cluster en cas de besoin

- Paramètres de base du cluster

POOLS DE NŒUDS

- default-pool ^
 - Nœuds
 - Sécurité
 - Métadonnées

CLUSTER

- Automatisation
- Réseau
- Sécurité
- Métadonnées
- Fonctionnalités

Détails du pool de nœuds

Le cluster sera créé avec au moins un pool de nœuds. Un pool de nœuds représente le modèle des groupes de nœuds créés dans ce cluster. D'autres pools de nœuds peuvent être ajoutés ou supprimés après la création du cluster.

Nom
default-pool

Version du plan de contrôle : 1.21.10-gke.2000

Taille

Nombre de nœuds *
3

La plage d'adresses des pods limite la taille maximale du cluster. [En savoir plus](#)

Activer l'autoscaling ?

Spécifiez les emplacements de nœuds ?
Valeur par défaut : europe-central2-a

Automatisation

Activer la mise à niveau automatique ?

Activer la réparation automatique ?

Mise à niveau de la surutilisation ?

Surutilisation maximale *
1

Nombre maximal de nœuds indisponi...
0

- Côté nœuds, laissez le type d'image à **Container Optimized** pour minimiser la consommation de ressources
- Sélectionnez aussi le type de nœuds

En dessous de 2 Go de RAM cela va être limitée, surtout si vous souhaitez utiliser des annotations de demande de ressources dans vos pods car ceux présents de base prennent déjà quasiment tout.

- Taille du disque : 30 Go pour minimiser les frais
- Le reste des options peuvent être laissées par défaut

- Paramètres de base du cluster

POOLS DE NŒUDS

- default-pool

- **Nœuds**

- Sécurité

- Métadonnées

CLUSTER

- Automatisation

- Réseau

- Sécurité

- Métadonnées

- Fonctionnalités

Nœuds

Ces paramètres de nœud seront utilisés lorsque des nœuds seront créés à l'aide de ce pool de nœuds.

Type d'image

Container-Optimized OS avec containerd (cos_containerd) (par défaut)



Pour les clusters et les pools de nœuds récemment créés avec la version 1.21.10-gke.2000 ou une version ultérieure, l'image de nœud Linux par défaut est Container-Optimized OS avec Containerd. Pour les pools de nœuds Windows utilisant la version 1.21 ou une version ultérieure, Containerd est également l'environnement d'exécution recommandé. Étant donné que Dockershim devient obsolète dans le projet Kubernetes, [GKE va abandonner les images de nœuds Docker](#). Nous vous recommandons de [migrer vers des images de nœuds containerd](#) dès que possible. Apprenez-en plus sur les différentes [images de nœuds](#).

Configuration de la machine

Famille de machines

USAGE GÉNÉRAL

Types de machines pour les charges de travail courantes permettant d'optimiser les coûts et la flexibilité

Série

E2

Sélection de la plate-forme de processeur en fonction de la disponibilité

Type de machine

e2-small (2 processeurs virtuels, 2 Go de mémoire)



vCPU

Un cœur partagé

Memory

2 Go

PLATE-FORME DU PROCESSEUR ET GPU

Type de disque de démarrage

Disque persistant standard

- Nœuds
- Sécurité
- Métadonnées

CLUSTER

- Automatisation
- Réseau
- Sécurité
- Métadonnées
- Fonctionnalités

Taille du disque de démarrage (Go) ?

30

Activer le chiffrement géré par le client pour le disque de démarrage ?

Disques SSD locaux ?

Activer les nœuds Spot ?

Mise en réseau

i Les paramètres du cluster indiquent un maximum de 110 pods par nœuds, mais vous pouvez ignorer ce paramètre au niveau du pool de nœuds.

Nombre maximal de pods par nœud ?

110

Masque pour la plage d'adresses du pod par nœud : /24

Tags réseau ?

Plage d'adresses de pods de pools de nœuds

i Les paramètres du cluster spécifient une plage d'adresses de pods par défaut au niveau du cluster, mais vous pouvez remplacer ce paramètre au niveau du pool de nœuds.

Créer automatiquement des plages secondaires ?

Plage CIDR secondaire du pod ?

Réseau

Vous pouvez définir la visibilité de votre Cluster (par défaut public) ainsi que le réseau sur lequel il se trouve.

On peut laisser par défaut.

- Paramètres de base du cluster

POOLS DE NŒUDS

- default-pool ^
 - Nœuds
 - Sécurité
 - Métadonnées

CLUSTER

- Automatisation
- Réseau
- Sécurité
- Métadonnées
- Fonctionnalités

Mise en réseau

Définissez la manière dont les applications dans ce cluster communiquent entre elles et avec le plan de contrôle de Kubernetes, ainsi que la manière dont les clients peuvent accéder à vos applications.

Réseau *
default ▼ ?

Sous-réseau de nœud *
default ▼ ?

Cluster public
 Cluster privé ?

Options de mise en réseau avancées

Activer le routage du trafic de VPC natif (utilisation d'une adresse IP d'alias) ?

Créer automatiquement des plages secondaires ?

Plage d'adresses par défaut des pods dans le cluster ?

Exemple : 192.168.0.0/16

Nombre maximal de pods par nœud ?

110

Masque pour la plage d'adresses du pod par nœud : /24

Création

Cliquez ensuite sur **Créer** en bas de la page pour créer le cluster Kubernetes.

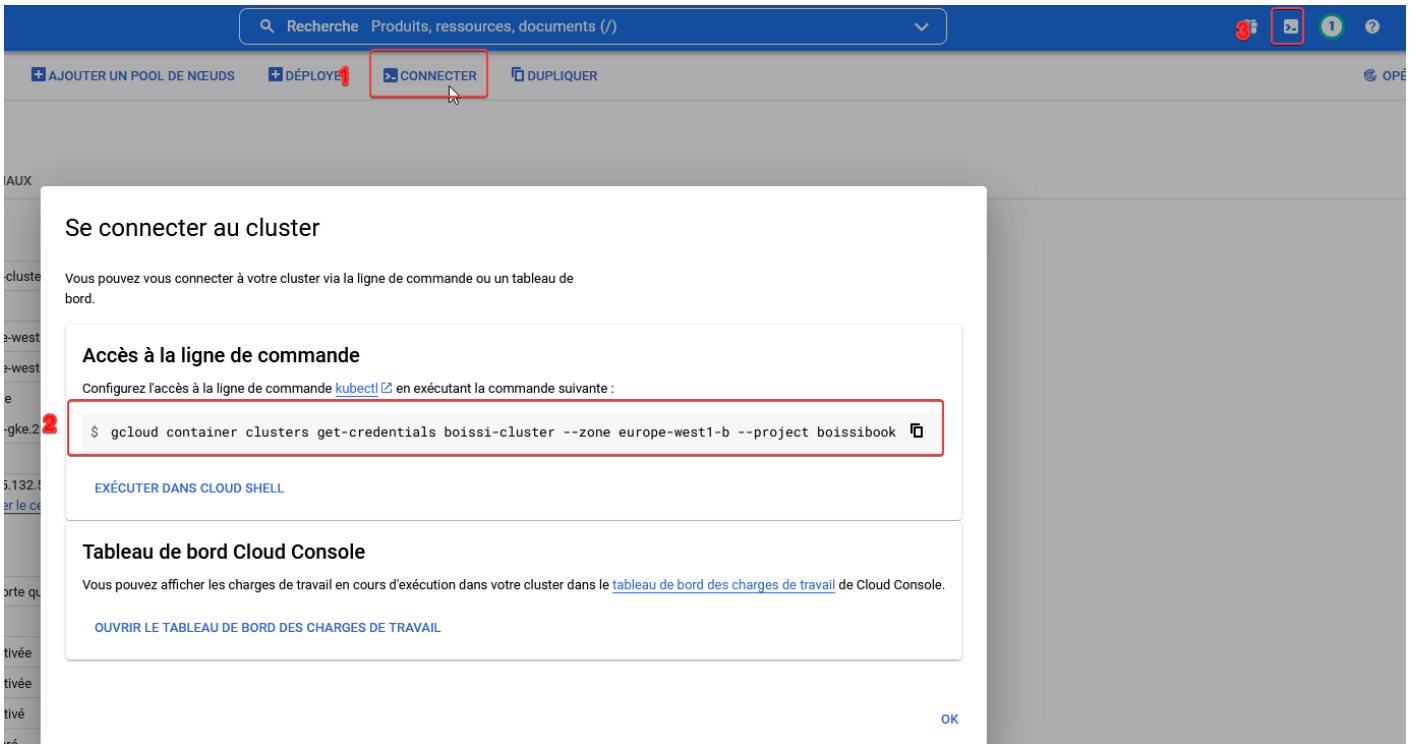
Après quelques minutes, ce dernier devrait apparaître dans la liste des clusters avec un état **Vert** signifiant qu'il est opérationnel.

Clusters Kubernetes								OPÉRATIONS ▾
APERÇU		OPTIMISATION DES COÛTS						
Filtre Saisissez le nom ou la valeur de la propriété								
État	Nom ↑	Zone	Nombre de nœuds	Nombre total de processeurs virtuels	Mémoire totale	Notifications	Libellés	
<input type="checkbox"/> ✔	boissi-cluster	europa-west1-b	1	2	2 Go		⋮	

Connexion au Cluster via la console GCP

pour manipuler notre cluster, on peut s'y connecter via la console GCP.

En allant voir les détails du cluster, cliquez sur **Connecter**, puis copiez collez la commande de connexion dans votre console Cloud Shell.



```
noelarrieulacoste@cloudshell:~ (boissibook)$ gcloud container clusters get-credentials boissi-cluster --zone europe-west1-b --project boissibook
Fetching cluster endpoint and auth data.
kubeconfig entry generated for boissi-cluster.
noelarrieulacoste@cloudshell:~ (boissibook)$
```

On peut désormais effectuer quelques tests avec la commande **kubect!**

```
noelarrieulacoste@cloudshell:~ (boissibook)$ kubect! top nodes
NAME CPU(cores) CPU% MEMORY(bytes) MEMORY%
gke-boissi-cluster-pool-2-3eb7953f-9pxb 123m 13% 810Mi 59%
noelarrieulacoste@cloudshell:~ (boissibook)$ kubect! get pods --all-namespaces
NAMESPACE NAME READY STATUS RESTARTS AGE
default boissibook-68dfd59d4c-wd4gc 1/1 Running 0 152m
kube-system event-exporter-gke-5479fd58c8-pzkhs 2/2 Running 0 179m
kube-system fluentbit-gke-pjmmv 2/2 Running 0 3h6m
kube-system gke-metrics-agent-m69r7 1/1 Running 0 3h6m
kube-system konnectivity-agent-6f44578758-4645b 1/1 Running 0 3h6m
kube-system konnectivity-agent-autoscaler-7fd5dd4f5-vgpg8 1/1 Running 0 179m
kube-system kube-dns-56494768b7-4wzsq 4/4 Running 0 160m
kube-system kube-dns-autoscaler-f4d55555-r6fqb 1/1 Running 0 179m
kube-system kube-proxy-gke-boissi-cluster-pool-2-3eb7953f-9pxb 1/1 Running 0 3h6m
kube-system 17-default-backend-69fb9fd9f9-fhb7s 1/1 Running 0 179m
kube-system metrics-server-v0.4.5-bbb794dcc-6fwgn 2/2 Running 0 179m
kube-system pdcsi-node-qhr8h 2/2 Running 0 3h6m
noelarrieulacoste@cloudshell:~ (boissibook)$
```

Configuration d'un Ingress

Mise en place d'un LoadBalancer

Lorsqu'une application tourne sur votre cluster, elle n'est pas directement exposée sur internet. Le mieux est de la rendre visible derrière un **LoadBalancer** autogéré par GCP.

Pour cela, votre déploiement doit être exposé par service de type **LoadBalancer** :

```
kind: Service
apiVersion: v1
metadata:
  name: <deploymentName>
spec:
  selector:
    run: <deploymentName>
  ports:
    - protocol: TCP
      port: <WantedExposedPort>
      targetPort: <podExposedPort>
  type: LoadBalancer
```

En vous rendant sur **GCP > Kubernetes Engine > Services et entrées**, vous devriez pouvoir vérifier que votre **LoadBalancer** fonctionne et pointe correctement sur votre déploiement.

Services et entrées [ACTUALISER](#) [CRÉER UN INGRESS](#) [SUPPRIMER](#)

Cluster: boissi-cluster Espace de noms: default, kube-node-lease, ... [RÉINITIALISER](#) [SAVE](#)

SERVICES ENTRÉE

Les services sont des ensembles de pods avec un point de terminaison de réseau pouvant servir pour la détection et l'équilibrage de charge. Les Ingress sont des ensembles de règles qui permettent de router le trafic HTTP(S) externe vers les services.

Filtre Est un objet système : Faux Filtrer les services et les Ingress

<input type="checkbox"/>	Nom ↑	État	Type	Points de terminaison	Pods	Espace de noms	Clusters
<input type="checkbox"/>	boissibook	OK	Équilibreur de charge externe	34.78.19.44:8080	1/1	default	boissi-cluster

Vérifier que votre accès à votre service fonctionne correctement en vous rendant sur le **Point de terminaison**

Activation d'un Ingress

Il faut maintenant activer l'exposition de ce LoadBalancer derrière un domaine et avec un certificat HTTPS.

Pour faire cela, cochez votre LoadBalancer puis cliquez sur **Créer un Ingress**

Services et entrées ACTUALISER CRÉER UN INGRESS SUPPRIMER

Cluster: boissi-cluster Espace de noms: default, kube-node-lease, ... RÉINITIALISER SAVE

SERVICES ENTRÉE

Les services sont des ensembles de pods avec un point de terminaison de réseau pouvant servir pour la détection et l'équilibrage de charge. Les Ingress sont des ensembles de règles qui permettent de router le trafic HTTP(S) externe vers les services.

Filtre Est un objet système : Faux Filtrer les services et les Ingress

✓	Nom ↑	État	Type	Points de terminaison	Pods	Espace de noms	Clusters
✓	boissibook	OK	Équilibreur de charge externe	34.78.19.44:8080	1/1	default	boissi-cluster

Donnez un nom à votre entrée

An Ingress has 3 parts:

1. Backend configuration
2. Host and path rules configuration
3. Forwarding rules

Type d'entrée

Équilibreur de charge HTTP/S externe

Nom *

boissibook-ingress



Backend configuration

Vous avez configuré 1 backend

Services Kubernetes de backend

Nom	Port	Pods actifs	Cluster
boissibook	8080	1	boissi-cluster

Définissez ensuite les règles d'accès à votre **LoadBalancer**, notamment le domaine par lequel y accéder

Une fois l'IP publique de ce point d'entrée définis, il faudra bien sûr aller mettre à jour l'enregistrement DNS de type A et AAAA pour qu'il pointe sur ce dernier

← Créer une entrée Kubernetes

An Ingress has 3 parts:

1. Backend configuration
2. Host and path rules configuration
3. Forwarding rules

Type d'entrée

Équilibreur de charge HTTP/S externe

Nom *

boissibook-ingress



Backend configuration

Vous avez configuré 1 backend



Host and path rules

Vous avez configuré 2 règles

Configuration des règles d'hôte et de chemin d'accès

Host and path rules determine how your traffic will be directed. You can direct traffic to a backend kubernetes service. Any traffic not explicitly matched with a host and path rule will be sent to the default service selected on the first row.

Hosts 1

Paths 1

Backends 1

boissibook

Hosts 2

boissibook.fr

Paths 2

/*

Backends 2

boissibook

+ AJOUTER UNE RÈGLE D'HÔTE ET DE CHEMIN D'ACCÈS

Dans la section **Frontend Configuration**, vous pouvez définir si ce dernier sera accessible en HTTP/HTTPS

Vous pouvez soit fournir un certificat existant, soit laisser GCP gérer ça pour vous.

An Ingress has 3 parts:

1. Backend configuration
2. Host and path rules configuration
3. Forwarding rules

Type d'entrée
Équilibreur de charge HTTP/S externe

Nom *
boissibook-ingress

Backend configuration
Vous avez configuré 1 backend

Host and path rules
Vous avez configuré 2 règles

Frontend configuration
Protocole HTTPS configuré

Preview setup and YAML (facultatif)
Preview the Ingress

Configuration de l'interface

Kubernetes Engine créera l'adresse IP frontend. Si le protocole SSL est spécifié, un certificat doit également être attribué.

Protocole
HTTPS

IP
Allouée automatiquement (IPv4)

Port
443

Espace de noms
default

Certificat

Certificat 1

boissibook-certificat
Géré par Google

Recherche Produits, ressources, documents (/)

Configuration de l'interface

Kubernetes Engine créera l'adresse IP frontend. Si le protocole SSL est spécifié, un certificat doit également être attribué.

Protocole
HTTPS

IP
Allouée automatiquement (IPv4)

Port
443

Créer un certificat

Nom
mon-certificat-autogere

Mode de création

Upload my certificate
Utilisez votre certificat de clé publique, votre chaîne de certificats et votre clé privée

Create Google-managed certificate
Google fournira automatiquement un certificat SSL une fois la configuration de l'entrée terminée et fera pointer le DNS du domaine spécifié vers l'adresse IP associée à l'entrée.

Domaine
boissibook.fr

Vérifier que votre configuration est bonne, puis cliquez sur **Créer**

An Ingress has 3 parts:

1. Backend configuration
2. Host and path rules configuration
3. Forwarding rules

Type d'entrée
Équilibreur de charge HTTP/S externe

Nom *
boissibook-ingress

✓ Backend configuration
Vous avez configuré 1 backend

✓ Host and path rules
Vous avez configuré 2 règles

✓ Frontend configuration
Protocole HTTPS configuré

4 Preview setup and YAML (facultatif)
Preview the Ingress

CREATE

CANCEL

Aperçu

INFORMATIONS SUR L'ENTRÉE

YAML DE L'ENTRÉE

Interface

Protocole	Adresse IP	Port	Certificats
HTTP/S	Allouée automatiquement (IPv4)	443	boissibook-certificate
HTTP	Allouée automatiquement (IPv4)	80	

Règles d'hôte et de chemin d'accès

Hôtes	Chemins d'accès	Services Kubernetes de backend
		boissibook
boissibook.fr	/*	boissibook

Services Kubernetes de backend

1. boissibook

Protocole du point de terminaison Numéro de port
TCP 8080

Nom du pod	État	Redémarrages	Créées le
boissibook-68dfd59d4c-wd4gc	Running	0	15 mai 2022, 16:05:42

Après quelques minutes, notre déploiement Ingress devrait apparaître dans la section **Services réseau > Équilibrage de charge**

Équilibrage de charge + CRÉER UN ÉQUILIBREUR DE CHARGE ACTUALISER SUPPRIMER

ÉQUILIBREURS DE CHARGE BACKENDS INTERFACES

Filtre Saisissez le nom ou la valeur de la propriété

<input type="checkbox"/>	Nom	Type d'équilibreur de charge ↑	Protocoles	Région	Backends
<input type="checkbox"/>	k8s2-um-ite13j67-default-boissi-ingress-ry5p4zjs	HTTP(S) (classique)	HTTP et HTTPS		✓ 1 service backend (0 groupe d'instances, 1 groupe de points de terminaison du réseau)

En allant consulter les détails, on peut y retrouver l'adresse IP attribuée ainsi que d'autres informations sur son fonctionnement, notamment les certificats utilisés.

k8s2-um-ite13j67-default-boissi-ingress-ry5p4zjs

DÉTAILS SURVEILLANCE MISE EN CACHE

Interface

Protocole ↑	IP:Port	Certificat	Règle SSL	Niveau de réseau ?
HTTP		1:80	-	Premium
HTTPS	04.102.200.12:1:443	boissi-ssl, mcrt-dfe051a3-f4df-4e28-80e8-cfe60dc708b9	tls-1-3	Premium

Règles d'hôte et de chemin d'accès

Hôtes ↑	Chemins d'accès	Backend
Sans correspondance (par défaut)	Sans correspondance (par défaut)	k8s1-ef3e34e3-default-boissibook-8080-e5de6c85
boissibook.nospy.fr	/*	k8s1-ef3e34e3-default-boissibook-8080-e5de6c85
boissibook.nospy.fr	/*	k8s1-ef3e34e3-default-boissibook-8080-e5de6c85

Backend

Services de backend

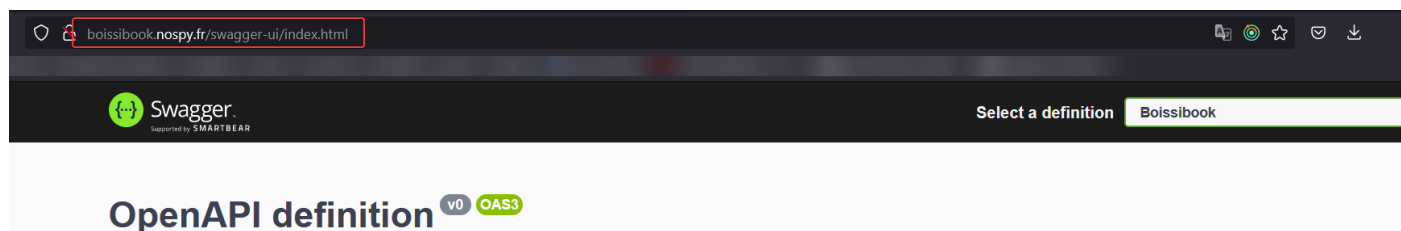
1. k8s1-ef3e34e3-default-boissibook-8080-e5de6c85

Protocole du point de terminaison	Délai avant expiration	Vérification de l'état	Cloud CDN	Journalisation
HTTP	30 secondes secondes	k8s1-ef3e34e3-default-boissibook-8080-e5de6c85	Désactivé	Activé (taux d'échantillonnage : 1)

▼ CONFIGURATIONS AVANCÉES

Nom ↑	Type	Zone	Opérationnelles	Autoscaling	Mode d'équilibrage	Capacité
k8s1-ef3e34e3-default-boissibook-8080-e5de6c85	Groupe de points de terminaison du réseau zonal	europé-west-1-b	✔ 1 sur 1	Aucune configuration	Nombre maximal de RPS : 1 (par point de terminaison)	100%

Une fois votre zone DNS mis à jour et votre cache DNS rafraichis, vous pouvez accéder à votre service via votre domaine.



La génération du certificat peut prendre un peu de temps (~1h)

Revision #5

Created 2022-05-15 15:27:38 UTC by Noé Larrieu-Lacoste

Updated 2022-05-15 17:32:24 UTC by Noé Larrieu-Lacoste