




 Search

[Option+S] 



More ▾



[App Runner](#)



Create service



CloudShell

[Feedback](#)



Console Mobile App

[Privacy](#)

[Terms](#)

[Cookie preferences](#)



[Option+S]



More ▾

☐ Source and deployment

Step 2

☐ Configure build

Step 3

☒ **Configure service**

Step 4

☐ Review and create

## Configure service [Info](#)

### Configure service

#### Service settings

##### Service name

scrybe-prod

##### Virtual CPU

1 vCPU ▾

##### Virtual memory

2 GB ▾

#### Runtime environment variables - optional [Info](#)

Add environment variables in plain text or reference them from [Secrets Manager](#) and [SSM Parameter Store](#). Update IAM Policies using the IAM Policy template given below to securely reference secrets and configurations as environment variables.

No environment variables have been configured.

[Add environment variable](#)

You can add up to 50 more items.

#### ▼ IAM policy templates for secrets

Copy the following IAM policy template to your Instance role to enable permissions to reference secrets and configurations from AWS Secrets Manager or SSM Parameter Store. [Visit the IAM Console](#)

[Secrets Manager](#)[SSM Parameter Store](#)

CloudShell

[Feedback](#)[Console Mobile App](#)[Privacy](#)[Terms](#)[Cookie preferences](#)



[Option+S]



More ▾

```
{
  "Action": [
    "secretsmanager:GetSecretValue",
    "kms:Decrypt*"
  ],
  "Effect": "Allow",
  "Resource": [
    "arn:aws:secretsmanager:us-east-1:318928518060:secret:<secret_name>",
    "arn:aws:kms:us-east-1:318928518060:key/<key_id>"
  ]
},
"Version": "2012-10-17"
}
```

## Auto scaling [Info](#)

Configure automatic scaling behavior.

### Auto scaling configurations

[Create ▾](#)

#### Existing configurations

DefaultConfiguration ▾

v1 ▾



Concurrency  
100 requests

[CloudShell](#)[Feedback](#)[Console Mobile App](#)[Privacy](#)[Terms](#)[Cookie preferences](#)



[Option+S]



More ▾

## Health check [Info](#)

Configure load balancer health checks.

### Protocol

The IP protocol that App Runner uses to perform health checks for your service.

TCP ▾

### Timeout

Amount of time the load balancer waits for a health check response.

5 ▾

seconds

### Interval

Amount of time between health checks of an individual instance.

10 ▾

seconds

### Unhealthy threshold

The number of consecutive health check failures that determine an instance is unhealthy.

5 ▾

requests

### Health threshold

The number of consecutive successful health checks that determine an instance is healthy.

1 ▾

requests



CloudShell

[Feedback](#)[Console Mobile App](#)[Privacy](#)[Terms](#)[Cookie preferences](#)



[Option+S]



More ▾

**Instance role — conditional**

Select an instance role to provide permission to your application code to call other AWS service actions (APIs). If you added environment variables stored in Secrets Manager or SSM Parameter Store, instance role is required. To create a custom role, use the [IAM console](#).

Choose an Instance role ▾

**AWS KMS key**

This key is used to encrypt the stored copies of your data.

Use an AWS-owned key

A key that AWS owns and manages for you.

Choose a different AWS KMS key

A key that you own or have permission to use.

**Web Application Firewall** [Info](#)

Activate WAF to define Web access control list (ACL) to protect against web exploits and bots. Learn more about [WAF and pricing](#).

☐ Activate**Networking** [Info](#)

Configure the way your service communicates with other applications, services, and resources.

**Incoming network traffic**

Select if your service is accessible publicly over the internet or only within a Virtual Private Cloud (VPC)

**Public endpoint**

Configure to make your service accessible to any client via the public internet.

**Private endpoint**

Configure a private connection between your VPC and App Runner using a VPC interface



CloudShell

[Feedback](#)[Console Mobile App](#)[Privacy](#)[Terms](#)[Cookie preferences](#)



[Option+S]



More ▾

### Outgoing network traffic

Select if the outgoing traffic is routed to only public internet or customize to access private VPC from Amazon Virtual Private Cloud (Amazon VPC)

#### Public access

Your service can send outgoing messages only to public network endpoints.

#### Custom VPC

Your service connects to an Amazon VPC of your choice. Your service can send outgoing messages to any endpoint (private or public) that the VPC can access.

## Observability

Configure observability tooling.

### Configure observability tooling



Tracing with AWS X-Ray

X-Ray tracing for your application. For pricing information, see [AWS X-Ray pricing](#).

## Tags [Info](#)

Use tags to search and filter your resources, track your AWS costs, and control access permissions.

### Tags — optional

A tag is a key-value pair that you assign to an AWS resource.


No tags associated with the resource.

[Add new tag](#)

You can add 50 more tags.

[CloudShell](#)[Feedback](#)[Console Mobile App](#)[Privacy](#)[Terms](#)[Cookie preferences](#)



[Option+S] 



More ▾



CloudShell

Feedback



Console Mobile App

Privacy

Terms

Cookie preferences