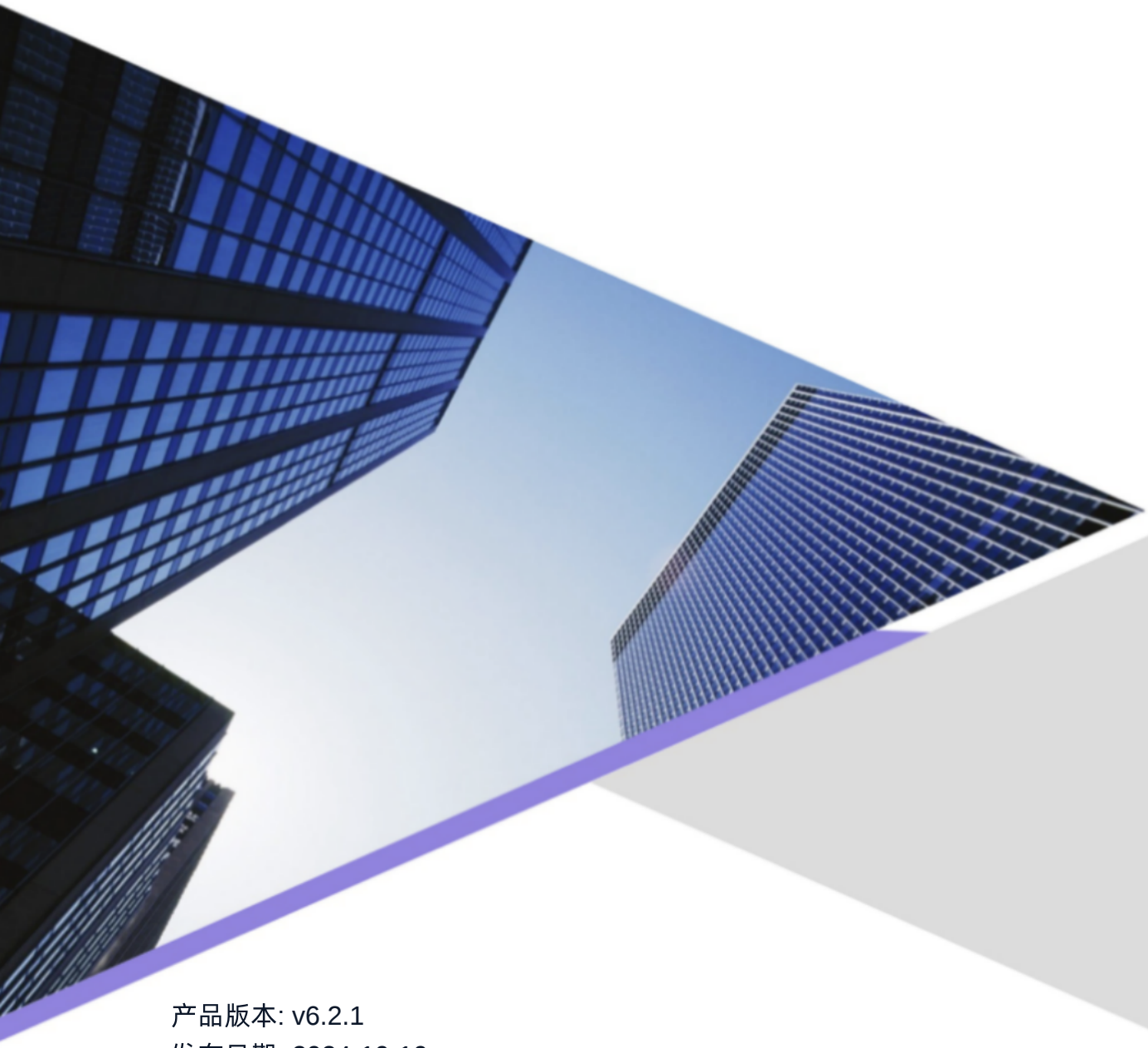
EasyStack
易捷行云

安全容器服务

快速入门



产品版本: v6.2.1
发布日期: 2024-10-10

© 北京易捷思达科技发展有限公司

目录

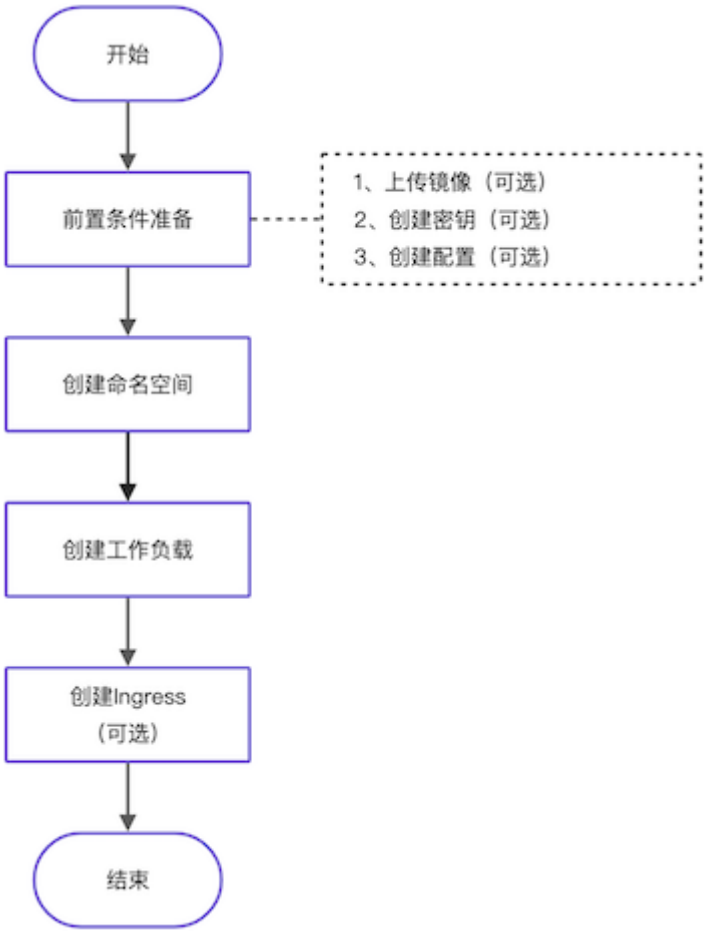
1 快速入门 ---------- 1
1.1 操作指引 ---------- 1
1.2 前置条件准备 ---------- 3
1.3 创建命名空间 ---------- 5
1.4 创建工作负载 ---------- 6
1.5 创建Ingress（可选） ---------- 17
1.6 使用Yaml创建资源（可选） ---------- 18

版权所有© 北京易捷思达科技发展有限公司

1 快速入门

1.1 操作指引

安全容器服务云产品的主线使用流程及具体说明如下：



操作流程		描述
前置条件准备	上传镜像（可选）	预先上传工作负载的容器创建时所需要的镜像文件。 请根据客户实际业务需求酌情创建。如已有可用镜像或使用第三方镜像时，可跳过本步骤。

操作流程		描述
	创建密钥（可选）	预先创建工作负载创建时所需要的密钥。 请根据客户实际业务需求酌情创建。如不使用开启密钥认证的第三方镜像，且数据卷、环境变量都不选择“密钥”类型时，可跳过本步骤。
	创建配置（可选）	预先创建工作负载创建时所需要的配置。 请根据客户实际业务需求酌情创建。如数据卷和环境变量都不选择“配置”类型时，可跳过本步骤。
创建命名空间		通过命名空间实现同一集群内不同资源之间的隔离。
创建工作负载		工作负载是对一组Pod的逻辑抽象，用于承载业务运行。
创建Ingress（可选）		通过Ingress为工作负载的服务提供外部访问时所需的路由规则集合。 请根据客户实际业务需求酌情配置。当工作负载已添加服务，且该服务需要配置对外访问的路由规则时，才需执行此操作。

1.2 前置条件准备

在创建工作负载前，请先完成以下准备工作。

上传镜像（可选）

本操作用于预先上传工作负载的容器创建时所需要的镜像文件，请根据客户实际业务需求酌情创建。如已有可用镜像或使用第三方镜像时，可跳过本步骤。

1. 在云平台的顶部导航栏中，依次选择[产品与服务]-[容器镜像服务]-[镜像管理]，进入“镜像管理”页面。

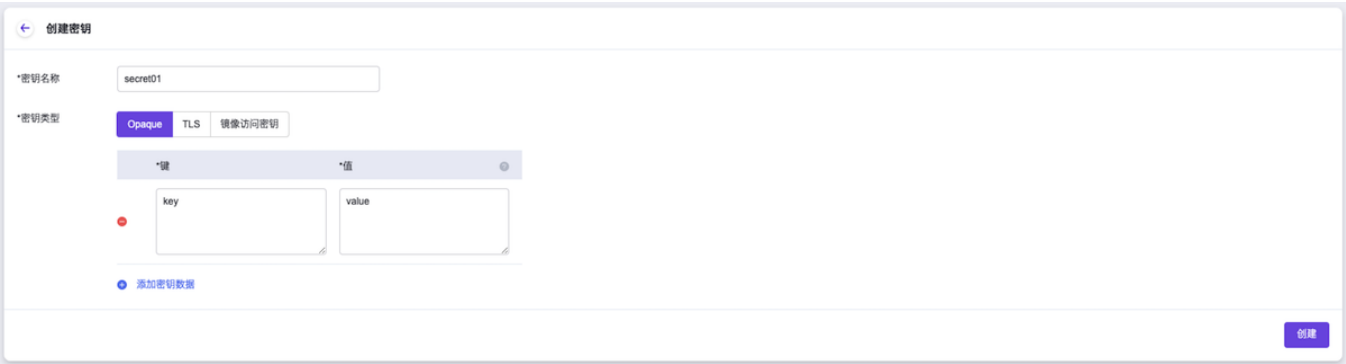
2. 单击 `上传镜像` 或 `Push镜像` ，弹出对应的对话框。

3. 配置参数后，完成操作。各参数的具体说明，请参考“容器镜像服务”帮助中“镜像管理”的相关内容。

创建密钥（可选）

本操作用于预先创建工作负载创建时所需要的密钥，请根据客户实际业务需求酌情创建。如不使用开启密钥认证的第三方镜像，且数据卷、环境变量都不选择“密钥”类型时，可跳过本步骤。

1. 在云平台顶部导航栏中，依次选择[产品与服务]-[安全容器服务]-[配置中心]，进入“配置中心”页面。
2. 在左侧导航栏选择[业务视图]，选择目标命名空间，选择[配置中心]-[密钥]，进入“密钥”页面。
3. 单击 `创建密钥` ，进入“创建密钥”页面。
4. 配置参数后，单击 `创建` 完成操作。



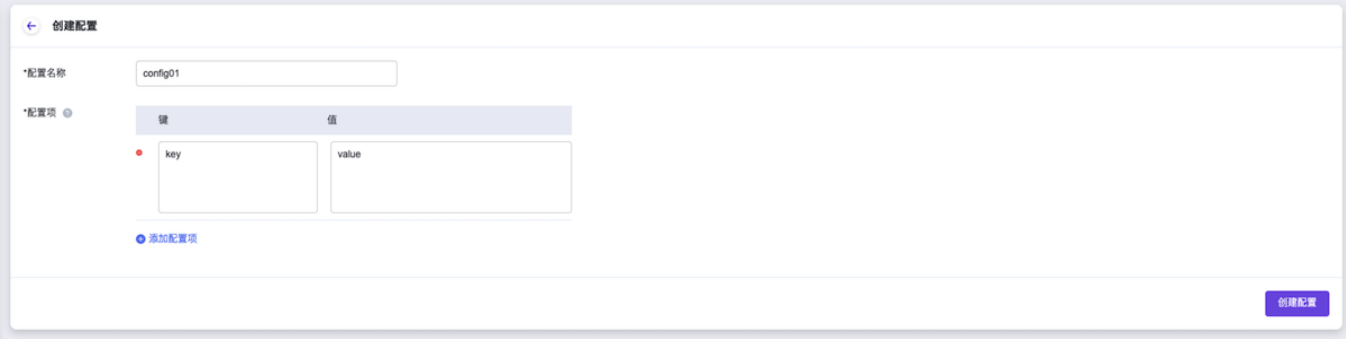
参数	说明

参数	说明
密钥类型	* Opaque：一般密钥类型。 * TLS：存放7层负载均衡服务所需的证书。 * 镜像访问密钥：存放拉取私有仓库镜像所需的认证信息。
密钥数据	* 当密钥类型为Opaque时，单击“添加密钥数据”，输入键、值。 * 当密钥类型为TLS时，上传证书和私钥文件。 * 当密钥类型为镜像访问密钥时，输入镜像仓库地址、用户名、密码和邮箱。

创建配置（可选）

本操作用于预先创建工作负载创建时所需要的配置，请根据客户实际业务需求酌情创建。如数据卷和环境变量都不选择“配置”类型时，可跳过本步骤。

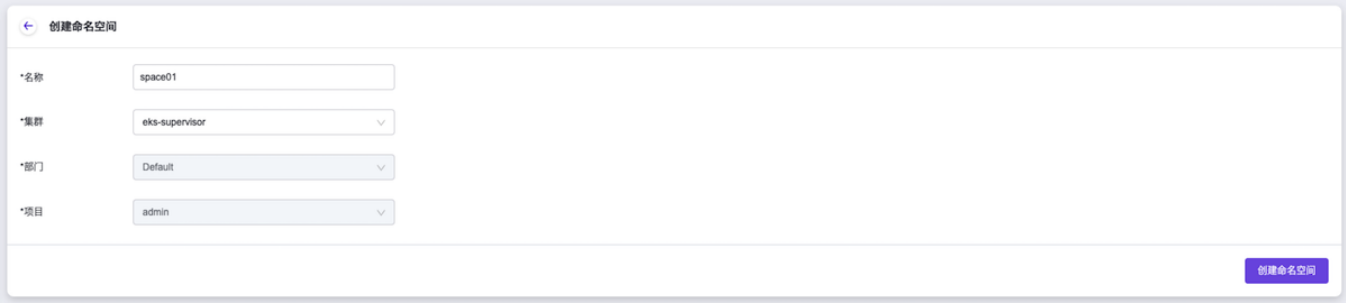
1. 在左侧导航栏选择[业务视图]，选择目标命名空间，选择[配置中心]-[配置]，进入“配置”页面。
2. 单击 创建配置 ，进入“创建配置”页面。
3. 填写参数后，单击 创建配置 ，完成操作。



1.3 创建命名空间

通过命名空间实现同一集群内不同项目资源之间的隔离。

1. 在顶部导航栏选择[产品与服务]-[安全容器服务]-[命名空间]，进入“命名空间”管理页面。
2. 单击 创建命名空间 ，跳转至“创建命名空间”页面。
3. 配置参数，单击 创建命名空间 完成操作。

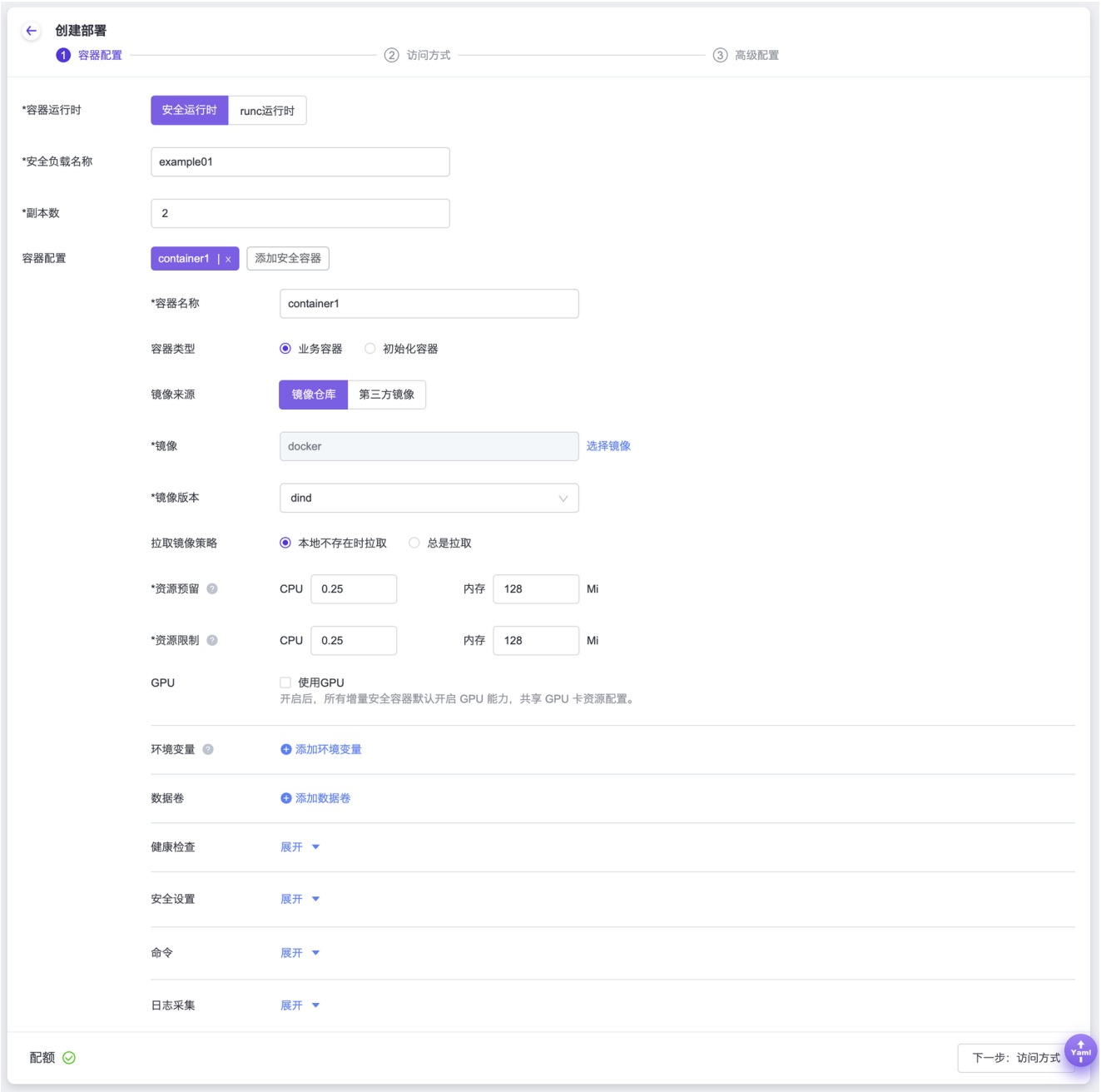


参数	说明
名称	选择命名空间的名称。
集群	选择命名空间所属集群。
部门/项目	用户所在部门和项目，不支持修改。

1.4 创建工作负载

工作负载是对一组Pod的逻辑抽象，用于承载业务运行。其类型包括部署（Deployment）、有状态副本集（StatefulSet）、守护进程集（DaemonSet）、任务（Job）、定时任务（CronJob），请根据客户实际业务需求酌情创建。创建方式支持界面创建和Yaml创建，本节将介绍界面创建方式，Yaml创建方式请参见 [如何使用Yaml创建资源]。

1. 在左侧导航栏选择[业务视图]页签-选择目标命名空间后，依据工作负载类型选择对应子菜单，进入对应页面。
2. 单击 `创建部署/有状态副本集/守护进程集/任务/定时任务` ，进入对应创建页面的“容器配置”页面。
3. 在“容器配置”页面中，配置参数后，单击 `下一步：访问方式` ，进入“访问方式”配置页面。其中，在“容器配置”区域框中，单击 `添加容器` ，可在该容器实例中添加多个容器，但是在容器添加过程中，请先确保已完成当前容器的配置。


创建部署
1 容器配置
2 访问方式
3 高级配置
*容器运行时
安全运行时
runc运行时
*安全负载名称
example01
*副本数
2
容器配置
container1
添加安全容器
*容器名称
container1
容器类型
业务容器
初始化容器
镜像来源
镜像仓库
第三方镜像
*镜像
docker
选择镜像
*镜像版本
dind
拉取镜像策略
本地不存在时拉取
总是拉取
*资源预留
CPU
0.25
内存
128
Mi
*资源限制
CPU
0.25
内存
128
Mi
GPU
使用GPU
开启后，所有增量安全容器默认开启 GPU 能力，共享 GPU 卡资源配置。
环境变量
添加环境变量
数据卷
添加数据卷
健康检查
展开
安全设置
展开
命令
展开
日志采集
展开
配额
下一步：访问方式

参数	说明

参数		说明
容器运行时		该工作负载中安全容器的运行时类型。该参数值可选“安全运行时”或“runc运行时”。 运行安全运行时的工作负载与运行runc运行时的工作负载相比，其进程隔离机制为内核级隔离，安全容器间的计算资源、网络资源具有更为彻底的隔离性。 runc运行时不支持内核隔离，不支持使用GPU。
副本数		仅当负载类型为“部署”或“有状态副本集”时可配置此参数。表示该工作负载包括的容器组个数。每个容器组都由相同的容器部署而成。设置多个容器组主要用于实现高可靠性，当某个实例故障时，工作负载还能正常运行。
容器配置	容器类型	包括业务容器和初始化容器。业务容器即真正运行业务的容器，初始化容器则运行于业务容器启动期间。若容器组中有多个初始化容器，这些容器会按顺序逐个运行，每个初始化容器必须运行成功，下一个才能够运行，当所有初始化容器运行完成时，集群才会正常运行业务容器。由于一个容器组中的存储卷是共享的，所以初始化容器中产生的数据可以被业务容器使用到。由于初始化容器提供了一种机制来阻塞或延迟业务容器的启动，可以应用于有启动顺序要求的容器组之间。
	镜像来源	包括镜像仓库和第三方镜像两种来源。选择镜像仓库则使用本集群对接的镜像仓库，选择第三方镜像则需要输入第三方镜像地址且保证网络可达。
	密钥认证	仅当镜像来源为“第三方镜像”时可配置。
	密钥	仅当镜像来源为“第三方镜像”且密钥认证为“是”时可配置。
	镜像	若镜像来源为“镜像仓库”，则单击 选择镜像 ，弹出选择镜像对话框。选择目标镜像，单击 确定 完成操作。若镜像来源为“第三方镜像”，则输入格式为ip:port/path/name的镜像地址。
	镜像版本	若镜像来源为“镜像仓库”，则在下拉框中选择目标版本；若镜像来源为“第三方镜像”，则手动输入目标版本。

参数		说明
	拉取镜像策略	包括“本地不存在时拉取”和“总是拉取”两种策略。
	资源预留	保证容器成功调度到节点的最小资源。 当需要勾选“使用GPU”时，建议此参数值的CPU大于等于1，内存大于等于1024MiB。
	资源限制	容器运行中允许使用的最大资源。
	使用GPU	仅当容器运行时为“安全运行时”时可配置此参数。表示容器是否使用GPU资源。 “守护进程集（DaemonSet）”和“定时任务（CronJob）”类型的工作负载不支持使用GPU。
	环境变量（可选）	容器在启动过程中需要的一些配置信息如启动命令、证书等，这类信息需要在容器组故障重启后仍然存在并重新加载到新容器组中，这类信息可以通过环境变量的形式单独存储。当前支持以下类型： * 普通变量：普通变量不需提前创建，直接输入即可。 * 配置：选择已创建好的配置。 * 密钥：选择已创建好的密钥。 * Pod字段：直接选择具体字段即可。 * 容器资源：直接选择具体资源即可。

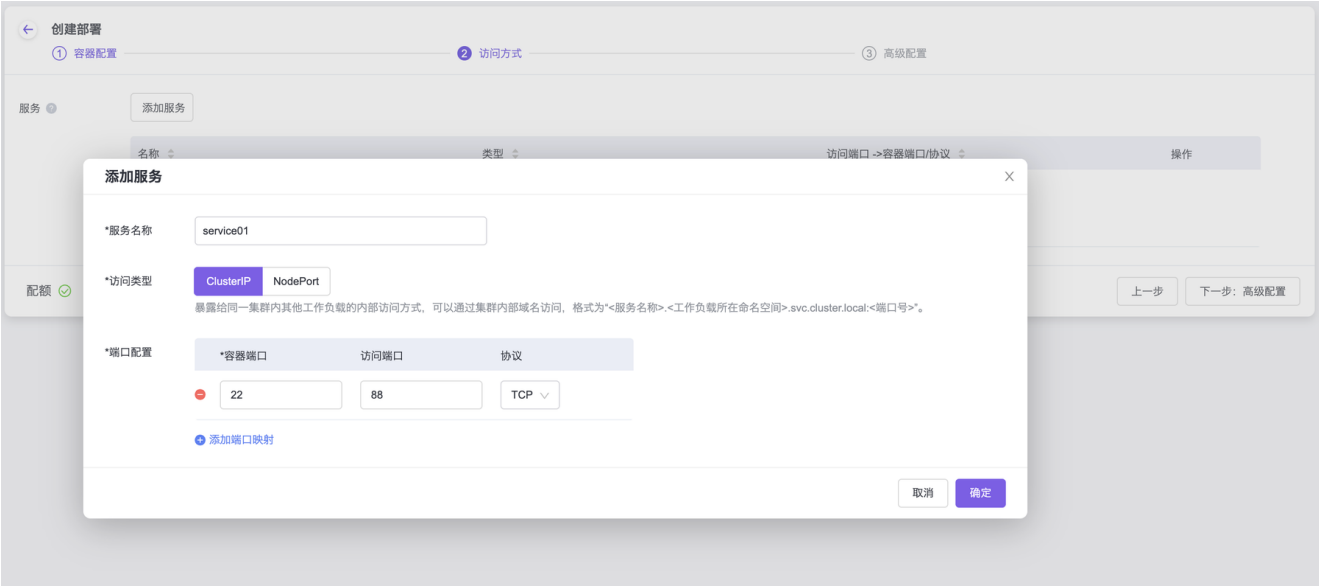
参数		说明
	数据卷（可选）	单击 `添加数据卷` ，弹出“添加数据卷”对话框。配置参数，单击 `确定` 完成操作。参数说明如下： * 类型： - 持久卷声明：仅工作负载类型为部署、任务、定时任务时可选择本类型。给容器挂载持久化存储，数据不会因容器的销毁或节点异常而消失。适用于需持久化存储、高磁盘IO等场景。持久卷声明需要事先创建，相关介绍请参考 创建持久卷声明。 - 存储类：仅工作负载类型为有状态副本集时可选择。不需事先创建持久卷声明，可直接通过指定存储类及所需存储容量创建持久卷，并挂载到指定的容器路径。各参数的具体说明，请参考 创建持久卷声明。 - 临时路径：将容器所在宿主机的临时目录挂载到容器的指定路径。 - 配置：选择已创建好的配置。 - 密钥：选择已创建好的密钥。 * 挂载路径(可选)：所选数据卷挂载至容器的绝对路径。
	健康检查（可选）	健康检查包括存活检查、就绪检查和启动检查功能。存活检查用于检测容器是否正常，如果容器的存活检查失败，集群会对该容器执行重启操作；若容器的存活检查成功则不执行任何操作。就绪检查用于检查用户业务是否就绪，如果容器的就绪检查失败，则不转发流量到当前容器组；若检查成功，则会开放对该容器组的访问。启动检查用于保护慢启动容器有充足时间完成启动，避免死锁状况发生。 * 检查方式： - HTTP/HTTPS方式：适用于提供HTTP/HTTPS服务的容器，集群周期性地对该容器发起HTTP/HTTPS GET请求，如果HTTP/HTTPS 返回状态码小于400，则证明检查成功、容器健康，否则检查失败。例如，方式选择HTTP，路径为/check，端口为80，则集群周期性向容器发起如下请求： `GET http://容器IP:80/check` 。 - TCP方式：适用于提供TCP通信服务的容器，集群周期性地检测端口是否为打开状态，若端口为打开状态，则检查成

参数		说明
		功、容器健康；若端口为关闭或进程为停止状态，则检查失败。例如：一个提供nginx服务的容器，服务端口为80，则配置TCP检查端口为80，那么集群会周期性检测该容器的80端口打开状态。 - 容器命令方式：该方式要求用户指定一个容器内的可执行命令，集群会周期性地在容器内执行该命令，若进程退出状态码为 0则检查成功、容器健康，否则检查失败。 * 公共参数： - 首次检查延时：容器启动后第一次进行健康检查的延迟时间，这段时间为预留给业务程序正常启动。例如，设置为10，表明容器启动后10秒才开始健康检查。 - 检查间隔：执行健康检查的时间间隔。例如，设置为30，则每间隔30秒执行一次健康检查。 - 超时时间：检查超时后的等待时间。例如，设置为10，表明执行健康检查的超时等待时间为10秒，如果超过这个时间，本次健康检查就被视为失败。 - 健康认定（）次成功：假设本参数设置为N，健康检查失败后，至少连续成功N次会认为容器健康。 - 不健康认定（）次失败：假设本参数设置为X，健康检查失败后，集群将继续尝试X次健康检查，若仍不符合健康条件，则放弃该容器。对于存活检查，放弃意味着重启容器；对于就绪检查，放弃意味着容器组将被标记为未就绪。
	安全设置（可选）	* 非root用户运行：要求容器组具有非零runAsUser值，或在镜像中定义了USER环境变量。 * 只读root文件系统：是否必须使用一个只读的root文件系统。 * runAsUser：用户ID。容器中的进程都以该用户ID运行。 * runAsGroup：Group ID。容器中的进程都以该Group ID运行。

参数		说明
	命令（可选）	* 启动命令：容器启动时运行的第一条命令，将覆盖镜像中的Entrypoint指令。 * 启动命令参数：覆盖镜像中的CMD执行，如已设置了运行命令，该条指令将被附加到运行命令的参数中。 * 启动后执行命令：该命令在创建容器之后立即执行。 * 停止前执行命令：这个命令在停止容器前执行，是否立即调用此命令取决于 API 的请求或者管理事件。
	日志采集（可选）	采集应用的运行日志，实现平台内应用与组件日志的全量采集与查询。 * 日志源：选择需采集日志的资源，支持容器标准日志（默认）和应用日志两种。 * 日志文件路径：当“日志源”选择“应用日志”时需配置。日志文件存放路径，需注意，该路径要求已挂载数据卷。

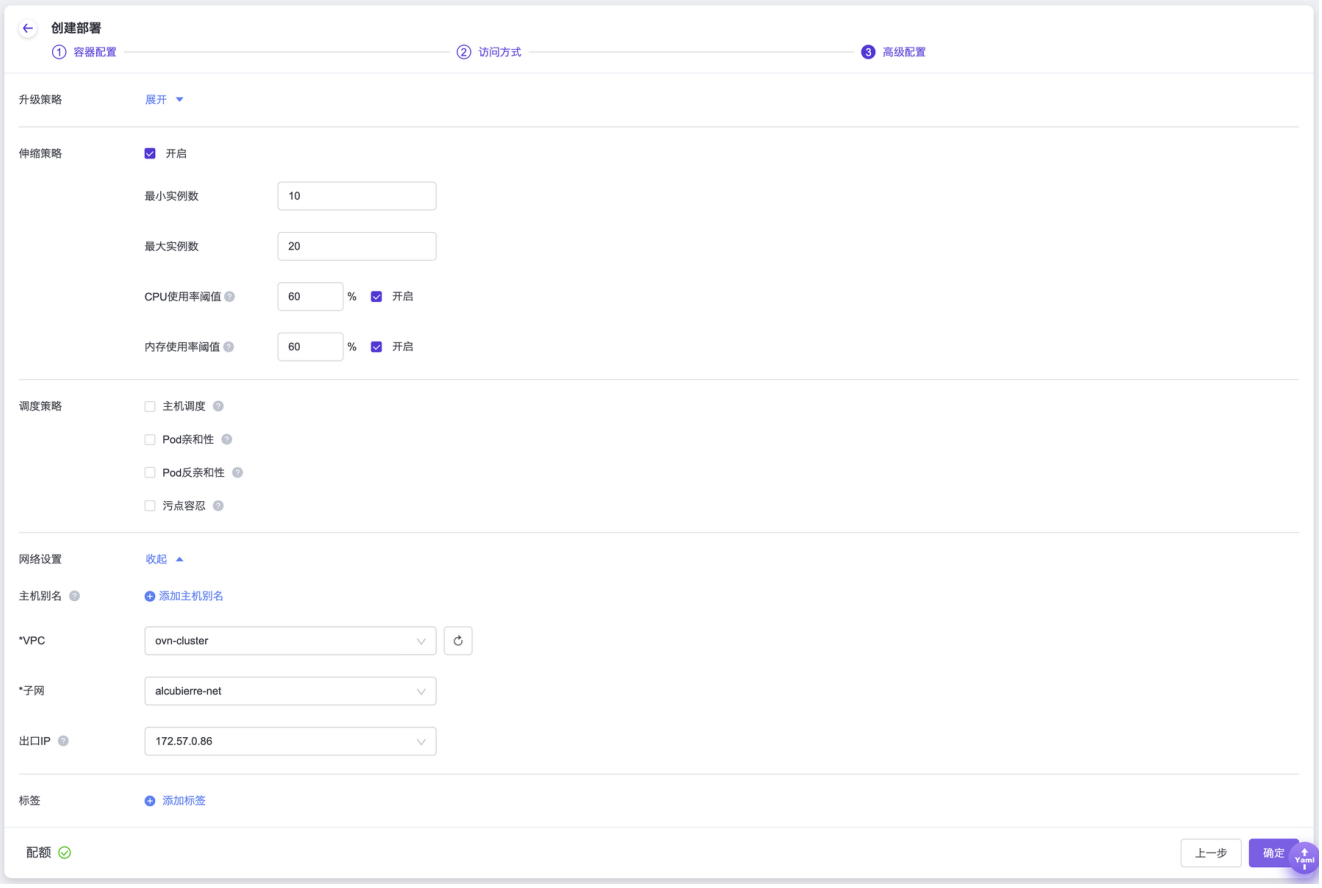
4. 在“访问方式”页面中，配置参数后，单击 `下一步：高级配置` ，进入“高级配置”配置页面。

当该工作负载需要提供对外访问的服务时，请单击 `添加服务` ，在弹出的对话框中配置参数后，单击 `确定` ，完成服务添加。否则，可直接跳过本步骤。



参数		说明
服务（可选）	服务名称	该工作负载中用于提供外部访问的服务的名称。
	访问类型	* ClusterIP：适用于集群内部访问场景，集群为服务分配一个固定的集群内虚拟IP，集群内其它pod可以通过集群内部域名访问，格式为“<服务名称>.<工作负载所在命名空间>.svc.cluster.local:<端口号>”。集群外无效。 * NodePort：适用于集群外部访问场景，集群除了会给服务分配一个内部的虚拟IP，还会在每个节点上为服务分配静态端口号，集群外部可通过集群任一节点IP和静态端口号访问服务。
	端口配置	* 容器端口：容器镜像中工作负载实际监听的端口。 * 访问端口：容器端口映射到节点IP上的端口。当访问方式为“NodePort”时，支持随机生成。 * 协议：包括TCP、UDP，根据业务类型选择。

5. 在“高级配置”页面中，配置参数后，单击 `确定` ，完成操作。



参数		说明
升级策略	工作负载类型为“部署”	* 先启动新Pod，再停止旧Pod/先停止旧Pod，再启动新Pod：可定义每次启动或停止Pod的数量。例如选择先启动新Pod，再停止旧Pod，批量大小设置为1，则每次先启动1个新的Pod，新的Pod成功后停止1个旧Pod，以此类推。 * 停止所有Pod，再启动新Pod：先停止所有老版本容器组，再启动新版本容器组，升级过程中业务会中断。 * 自定义：“最大超量”表示更新过程中容器组数量可以超过期望副本的数量或百分比。“最多不可用数”表示升级过程中允许的最多不可用容器组数量，如果等于期望副本数量有业务中断风险（最小存活容器组数量=期望副本数量-最多不可用数）。

参数		说明
	工作负载类型为“有状态副本集”或“守护进程集”	* 滚动：滚动升级将逐步用新版本的实例替换旧版本的实例，升级的过程中，业务流量会同时负载均衡分布到新老的实例上，因此业务不会中断。其中，“最多不可用数”表示升级过程中允许的最多不可用容器组数量，如果等于期望副本数量则有业务中断风险（最小存活容器组数量=期望副本数量-最多不可用数）。 * 手动删除时更新：集群不会自动更新工作负载中的容器组，需手动删除容器组以使集群创建新的容器组。
伸缩策略		仅当工作负载类型为“部署”时可配置。当达到设置的条件后自动扩展或收缩容器组数量。 * 最小实例数：期望容器组数量的最小值。 * 最大实例数：期望容器组数量的最大值。 * CPU使用率阈值：所有容器组平均cpu使用率超过阈值自动扩展，n-1（n为容器组总数）个容器组平均内存使用率低于阈值自动收缩。需勾选“开启”后才能输入阈值。 * 内存使用率阈值：所有容器组平均内存使用率超过阈值自动扩展，n-1（n为容器组总数）个容器组平均内存使用率低于阈值自动收缩。需勾选“开启”后才能输入阈值。
调度策略（可选）	主机调度	* 指定主机：可选择集群内任一节点，该工作负载内的容器将被调度到所选节点上。 * 自定义规则：包括必须满足条件和尽量满足条件。必须满足条件是硬性要求，必须满足才能成功调度，支持添加多条规则，多条规则间是“且”的关系，即需要满足所有规则才可以调度；尽量满足条件表示集群会尽量将容器调度到符合规则的主机上，支持添加多条规则，多条规则间是“或”的关系，不满足规则的主机也会进行调度，根据规则的权重值，权重值越高越会被优先调度。

参数		说明
	Pod亲和性/Pod反亲和性	Pod亲和性决定哪些工作负载的Pod部署在同一个拓扑域，可根据业务需求进行工作负载的就近部署，容器间通信就近路由，减少网络消耗。Pod反亲和性决定工作负载的Pod不和哪些工作负载的Pod部署在同一个拓扑域，互相干扰的工作负载反亲和部署，避免干扰，减少宕机影响。拓扑域是由一个或多个节点组成的，这些节点在所指定的属性上具有相同的值，例如拓扑域为kubernetes.io/hostname，则具有相同hostname的节点成为一个拓扑域（即同一节点）。必须满足条件是硬性要求，支持添加多条规则，多条规则间是“且”的关系，即需要满足所有规则才可以调度；尽量满足条件表示集群会尽量将容器调度到符合规则的主机上，多条规则间是“或”的关系，不满足规则的主机也会进行调度，根据规则的权重值，权重值越高越会被优先调度。
	污点容忍	调度工作负载时能够容忍具有指定污点的节点。支持添加多条污点规则，多条规则间是“或”的关系，即满足任一规则即可调度。
网络设置		* 主机别名：添加主机别名后即可通过域名访问对应IP地址的主机。 * VPC：该工作负载的私有网络名称。支持选择系统默认生成的ovn-cluster，也支持自定义VPC和各网络的子网，具体操作请参考 如何自定义VPC网络。 * 子网：该工作负载的子网名称。 * 出口IP：该工作负载提供对外访问服务时，所使用的公网IP地址。
标签（可选）		通过标签可以方便地标识及筛选对象。

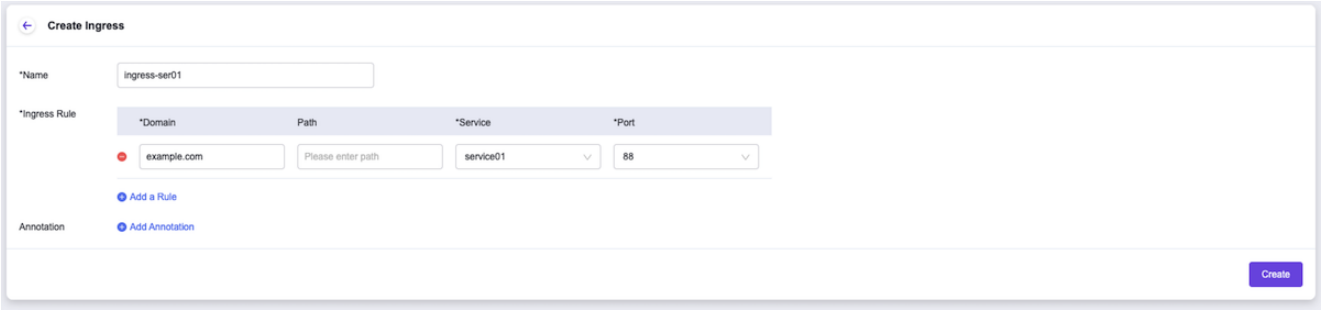
1.5 创建Ingress（可选）

通过Ingress可以为工作负载的服务提供外部访问时所需的路由规则集合，请根据客户实际业务需求酌情创建。当工作负载已添加服务，且该服务需要配置对外访问的路由规则时，才需执行此操作。

1. 在左侧导航栏选择[业务视图]，选择目标命名空间，选择[网络管理]-[Ingress]，进入“Ingress”页面。

2. 单击 `创建Ingress` ，进入“创建Ingress”页面。

3. 配置参数后，单击 `创建` 完成操作。



参数	说明
Ingress规则	是一种HTTP方式的路由转发机制。例如域名填写为example.com，路径填写为/path，服务选择已创建的名称为“app”的服务，则外部可通过 `http://example.com/path` 访问名称为“app”的服务。
注解	Ingress经常使用注解（annotations）来配置一些选项，具体取决于Ingress控制器。

1.6 使用Yaml创建资源（可选）

本章节主要描述如何使用Yaml创建安全容器服务资源。工作负载、持久卷声明和配置、密钥、服务、Ingress、自定义资源描述等资源不仅可以通过云平台页面进行创建，还可以通过Yaml文件进行创建。用户可以根据实际的业务场景，灵活选择适合的资源创建方案。

1. 在顶部导航栏选择[产品与服务]-[安全容器服务]任意一个子菜单，进入“安全容器服务”页面。
2. 在左侧导航栏选择[业务视图]页签-选择目标命名空间。
3. 单击页面右下角的“Yaml”图标，进入“导入Yaml”页面。

4. 直接粘贴Yaml文件内容，或单击编辑区域右上角的“导入”图标，选择本地存储的Yaml文件。

> 说明：
> 请关注调试结果。该调试主要针对格式校验，若有错误可点击错误信息，跳至目标行进行修改。

为了更清晰地说明，下面以创建名为"demo"的"部署"类型的工作负载为例，介绍如何使用Yaml创建资源。以下是一个示例Yaml内容:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  creationTimestamp: null
  labels:
    app: demo
  name: demo
spec:
  replicas: 1
  selector:
    matchLabels:
      app: demo
  strategy: {}
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: demo
    spec:
      containers:
      - image: nginx:latest
        name: nginx
        resources: {}
status: {}
```

5. 待调试通过后，单击 `导入` ，完成操作。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区23号楼华胜天成科研大楼一层东侧120-123
南京分公司：
江苏省南京市雨花台区软件大道168号润和创智中心B栋一楼西101
上海office：
上海黄浦区西藏中路336号华旭大厦22楼2204
成都分公司：
成都市高新区天府五街168号德必天府五街WE602

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)
training@easystack.cn (培训咨询)
hr@easystack.cn (招聘咨询)

版权所有© 北京易捷思达科技发展有限公司