DaoCloud Enterprise

DaoCloud Enterprise Product Documentation

DaoCloud

Copyright © 2016 - 2023 DaoCloud

Table of contents

1. Gproduct 3
   1.1 GProduct 如何对接全局管理 3
   1.2 对接导航栏 4
   1.3 接入路由和登录认证 8
2. Install 11
   2.1 使用国密网关代理 DCE 5.0 11
   2.2 离线升级全局管理模块 13
   2.3 自定义 DCE 5.0 反向代理服务器地址 17
   2.4 您的反向代理地址，例如：`export DCE_PROXY="https://demo-alpha.daocloud.io"` 17
   2.5 helm --set 参数备份文件 17
   2.6 获取当前 ghippo 的版本号 17
3. Intro 20
   3.1 功能总览 21
   3.2 常见术语 28
   3.3 全局管理 Release Notes 30
   3.4 什么是全局管理？ 34
4. Permissions 35
   4.1 应用工作台权限说明 35
   4.2 中间件数据服务权限说明 39
   4.3 服务网格权限说明 44
   4.4 微服务引擎权限说明 48
5. User guide 53
   5.1 审计日志 53
   5.2 登录 55
   5.3 开启/关闭审计日志 57
   5.4 密码重置 61
   5.5 Access control 68
   5.6 Personal center 106
   5.7 Platform setting 118
   5.8 Workspace 131

Copyright © 2016 - 2023 DaoCloud

1. Gproduct

1.1 GProduct 如何对接全局管理

GProduct 是 DCE 5.0 中除全局管理外的所有其他模块的统称，这些模块需要与全局管理对接后才能加入到 DCE 5.0 中。

对接什么

- 对接导航栏

  入口统一放在左侧导航栏。

- 接入路由和 AuthN

  统一 IP 或域名，将路由入口统一走全局管理的 Istio Gateway。

- 统一登录 / 统一 AuthN 认证

  登录统一使用全局管理 (Keycloak) 登录页，API authn token 验证使用 Istio Gateway。 GProduct 对接全局管理后不需要关注如何实现登录和认证。

Copyright © 2016 - 2023 DaoCloud

1.2 对接导航栏

以容器管理（开发代号 `kpanda`）为例，对接到导航栏。

对接后的预期效果如图：

Copyright © 2016 - 2023 DaoCloud

对接方法

参照以下步骤对接 GProduct：

Copyright © 2016 - 2023 DaoCloud

1. 通过 GProductNavigator CR 将容器管理的各功能项注册到导航栏菜单。

```yaml
apiVersion: ghippo.io/v1alpha1
kind: GProductNavigator
metadata:
  name: kpanda
spec:
  gproduct: kpanda
  name: 容器管理
  localizedName:
    zh-CN: 容器管理
    en-US: Container Management
  url: /kpanda
  category: 容器  # (1)
  iconUrl: /kpanda/nav-icon.png
  order: 10 # (2)
  menus:
  - name: 备份管理
    localizedName:
      zh-CN: 备份管理
      en-US: Backup Management
    iconUrl: /kpanda/bkup-icon.png
    url: /kpanda/backup
```

a. 当前只支持概览、工作台、容器、微服务、数据服务、管理，六选一

b. 数字越大排在越上面

全局管理的导航栏 `category` 配置在 ConfigMap，暂时不能以注册方式增加，需要联系全局管理团队来添加。

2. `Kpanda` 前端作为微前端接入到 DCE 5.0 父应用 Anakin 中

前端使用 qiankun 来接入子应用 UI， 可以参考快速上手。

在注册 GProductNavigator CR 后，接口会生成对应的注册信息，供前端父应用注册使用。 例如 `Kpanda` 就会生成以下注册信息：

```go
{
  "id": "kpanda",
  "title": "容器管理",
  "url": "/kpanda",
  "uiAssetsUrl": "/ui/kpanda/", // 结尾的/是必须的
  "needImportLicense": false
},
```

以上注册信息与 qiankun 子应用信息字段的对应关系是：

```yaml
{
    name: id,
    entry: uiAssetsUrl,
    container: '#container',
    activeRule: url,
    loader,
    props: globalProps,
}
```

container 和 loader 由前端父应用提供，子应用无需关心。 props 会提供一个包含用户基本信息、子产品注册信息等的 pinia store。

qiankun 启动时会使用如下参数：

```go
start({
  sandbox: {
```


Copyright © 2016 - 2023 DaoCloud

```
    experimentalStyleIsolation: true,
  },
  // 去除子应用中的favicon防止在Firefox中覆盖父应用的favicon
  getTemplate: (template) => template.replaceAll(/<link\s* rel="[\w\s]*icon[\w\s]*"\s*( href=".*?")?\s*\/?>/g, ''),
});
```

请参阅前端团队出具的 GProduct 对接 demo tar 包。

Copyright © 2016 - 2023 DaoCloud

1.3 接入路由和登录认证

接入后统一登录和密码验证，效果如下图：

各个 GProduct 模块的 API bear token 验证都走 Istio Gateway。

接入后的路由映射图如下：

Copyright © 2016 - 2023 DaoCloud

接入方法

以 `kpanda` 为例注册 GProductProxy CR。

```
# GProductProxy CR 示例, 包含路由和登录认证

# spec.proxies: 后写的路由不能是先写的路由子集, 反之可以
# spec.proxies.match.uri.prefix: 如果是后端 api, 建议在 prefix 末尾添加 "/" 表述这段 path 结束（特殊需求可以不用加）
# spec.proxies.match.uri: 支持 prefix 和 exact 模式; Prefix 和 Exact 只能 2 选 1; Prefix 优先级大于 Exact

apiVersion: ghippo.io/v1alpha1
kind: GProductProxy
metadata:
  name: kpanda  # (1)
spec:
  gproduct: kpanda  # (2)
  proxies:
  - labels:
      kind: UIEntry
    match:
      uri:
        prefix: /kpanda # (3)
    rewrite:
      uri: /index.html
    destination:
      host: ghippo-anakin.ghippo-system.svc.cluster.local
      port: 80
    authnCheck: false  # (4)
  - labels:
      kind: UIAssets
    match:
      uri:
        prefix: /ui/kpanda/ # (5)
    destination:
      host: kpanda-ui.kpanda-system.svc.cluster.local
      port: 80
    authnCheck: false
  - match:
      uri:
        prefix: /apis/kpanda.io/v1/a
    destination:
      host: kpanda-service.kpanda-system.svc.cluster.local
      port: 80
    authnCheck: false
  - match:
      uri:
        prefix: /apis/kpanda.io/v1 # (6)
    destination:
      host: kpanda-service.kpanda-system.svc.cluster.local
```


Copyright © 2016 - 2023 DaoCloud

```
      port: 80
    authnCheck: true
```

1. cluster 级别 CRD
2. 需要用小写指定 GProduct 名字
3. 还可支持 exact
4. 是否需要 istio-gateway 给该条路由 API 作 AuthN Token 认证，false 为跳过认证
5. UIAssets 建议末尾添加 `/` 表示结束（不然前端可能会出现问题）
6. 后写的路由不能是先写的路由的子集，反之可以

Copyright © 2016 - 2023 DaoCloud

2. Install

2.1 使用国密网关代理 DCE 5.0

参照以下步骤为 DCE 5.0 配置国密网关。

软件介绍

Tengine: Tengine 是由淘宝网发起的 Web 服务器项目。它在 Nginx 的基础上，针对大访问量网站的需求，添加了很多高级功能和特性。

Tongsuo: 铜锁/Tongsuo（原 BabaSSL）是一个提供现代密码学算法和安全通信协议的开源基础密码库，为存储、网络、密钥管理、隐私计算等诸多业务场景提供底层的密码学基础能力，实现数据在传输、使用、存储等过程中的私密性、完整性和可认证性，为数据生命周期中的隐私和安全提供保护能力。

准备工作

一台安装了 Docker 的 Linux 主机，并且确保它能访问互联网

编译和安装 Tengine & Tongsuo

注：此配置仅供参考

```
FROM docker.m.daocloud.io/debian:11.3

# Version
ENV TENGINE_VERSION="2.3.4" \
    TONGSUO_VERSION="8.3.2"

# Install required system packages and dependencies
RUN apt update && \
    apt -y install \
    wget \
    gcc \
    make \
    libpcre3 \
    libpcre3-dev \
    zlib1g-dev \
    perl \
    && apt clean

# Build tengine
RUN mkdir -p /tmp/pkg/cache/ && cd /tmp/pkg/cache/ \
    && wget https://github.com/alibaba/tengine/archive/refs/tags/${TENGINE_VERSION}.tar.gz -O tengine-${TENGINE_VERSION}.tar.gz \
    && tar zxvf tengine-${TENGINE_VERSION}.tar.gz \
    && wget https://github.com/Tongsuo-Project/Tongsuo/archive/refs/tags/${TONGSUO_VERSION}.tar.gz -O Tongsuo-${TONGSUO_VERSION}.tar.gz \
    && tar zxvf Tongsuo-${TONGSUO_VERSION}.tar.gz \
    && cd tengine-${TENGINE_VERSION} \
    && ./configure \
        --add-module=modules/ngx_openssl_ntls \
        --with-openssl=/tmp/pkg/cache/Tongsuo-${TONGSUO_VERSION} \
        --with-openssl-opt="--strict-warnings enable-ntls" \
        --with-http_ssl_module --with-stream \
        --with-stream_ssl_module --with-stream_sni \
    && make \
    && make install \
    && ln -s /usr/local/nginx/sbin/nginx /usr/sbin/ \
    && rm -rf /tmp/pkg/cache

EXPOSE 80 443
STOPSIGNAL SIGTERM
CMD ["nginx", "-g", "daemon off;"]
```

```
docker build -t tengine:0.0.1 .
```

生成 SSL 证书（SM2 和 RSA 证书）

注：此证书仅适用于测试环境

您可以参考官方文档使用 Tongsuo 生成 SSL 证书，或者访问 https://www.gmssl.cn/gmssl/index.jsp?go=CA 申请。

Copyright © 2016 - 2023 DaoCloud

SM2 证书

```
-rw-r--r-- 1 root root  749 Dec  8 02:59 sm2.*.io.enc.crt.pem
-rw-r--r-- 1 root root  258 Dec  8 02:59 sm2.*.io.enc.key.pem
-rw-r--r-- 1 root root  749 Dec  8 02:59 sm2.*.io.sig.crt.pem
-rw-r--r-- 1 root root  258 Dec  8 02:59 sm2.*.io.sig.key.pem
```

RSA 证书（可选）

```
-rw-r--r-- 1 root root  216 Dec  8 03:21 rsa.*.io
-rw-r--r-- 1 root root 4096 Dec  8 02:59 sm2.*.io
```

给 nginx 配置 SSL 证书

支持 SM2 和 RSA 两种证书。双证书的优点是：当浏览器不支持国密证书时，自动切换到 RSA 证书。

更多详细配置，请参考官方文档。

```
# 进入 nginx 配置文件存放目录
cd /usr/local/nginx/conf

# 创建 cert 文件夹，用于存放 SSL 证书
mkdir cert

# 把 SM2、RSA（可选）证书拷贝到 `/usr/local/nginx/conf/cert` 目录下
cp sm2.*.enc.crt.pem sm2.*.io.enc.key.pem  sm2.*.sig.crt.pem  sm2.*.sig.key.pem /usr/local/nginx/conf/cert
cp rsa.*.crt.pem  rsa.*.key.pem /usr/local/nginx/conf/cert

# 编辑 nginx.conf 配置
vim nginx.conf
...
server {
  listen 443          ssl;
  proxy_http_version  1.1;
  # 开启国密功能
  enable_ntls         on;

  # 国际 RSA 证书（可选）
  ssl_certificate                 /usr/local/nginx/conf/cert/rsa.demo-dev.daocloud.io.crt.pem;
  ssl_certificate_key             /usr/local/nginx/conf/cert/rsa.demo-dev.daocloud.io.key.pem;

  # 国密签名证书
  ssl_sign_certificate            /usr/local/nginx/conf/cert/sm2.demo-dev.daocloud.io.sig.crt.pem;
  ssl_sign_certificate_key        /usr/local/nginx/conf/cert/sm2.demo-dev.daocloud.io.sig.key.pem;
  # 国密加密证书
  ssl_enc_certificate             /usr/local/nginx/conf/cert/sm2.demo-dev.daocloud.io.enc.crt.pem;
  ssl_enc_certificate_key         /usr/local/nginx/conf/cert/sm2.demo-dev.daocloud.io.enc.key.pem;
  ssl_protocols                   TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;

  location / {
    proxy_set_header Host $http_host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header REMOTE-HOST $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_pass https://istio-ingressgateway.istio-system.svc.cluster.local;
  }
}
```

重新加载 nginx，使其配置生效

```
nginx -s reload
```

下一步

国密网关部署成功之后，自定义 DCE 5.0 反向代理服务器地址。

Copyright © 2016 - 2023 DaoCloud

2.2 离线升级全局管理模块

本页说明从下载中心下载全局管理模块后，应该如何安装或升级。

!!! info

```
下述命令或脚本内出现的 `ghippo` 字样是全局管理模块的内部开发代号。
```

从安装包中加载镜像

您可以根据下面两种方式之一加载镜像，当环境中存在镜像仓库时，建议选择chart-syncer同步镜像到镜像仓库，该方法更加高效便捷。

chart-syncer 同步镜像到镜像仓库

1. 创建 load-image.yaml

!!! note

```
该 YAML 文件中的各项参数均为必填项。您需要一个私有的镜像仓库，并修改相关配置。
```

=== "已安装 chart repo"

```
若当前环境已安装 chart repo，chart-syncer 也支持将 chart 导出为 tgz 文件。

```yaml title="load-image.yaml"
source:
  intermediateBundlesPath: ghippo-offline # (1)
target:
  containerRegistry: 10.16.10.111 # (2)
  containerRepository: release.daocloud.io/ghippo # (3)
  repo:
    kind: HARBOR # (4)
    url: http://10.16.10.111/chartrepo/release.daocloud.io # (5)
    auth:
    username: "admin" # (6)
    password: "Harbor12345" # (7)
  containers:
    auth:
      username: "admin" # (8)
      password: "Harbor12345" # (9)
```

1. 到执行 charts-syncer 命令的相对路径，而不是此 YAML 文件和离线包之间的相对路径
2. 需更改为你的镜像仓库 url
3. 需更改为你的镜像仓库
4. 也可以是任何其他支持的 Helm Chart 仓库类别
5. 需更改为 chart repo url
6. 你的镜像仓库用户名
7. 你的镜像仓库密码
8. 你的镜像仓库用户名
9. 你的镜像仓库密码
```

=== "未安装 chart repo"

```
若当前环境未安装 chart repo，chart-syncer 也支持将 chart 导出为 tgz 文件，并存放在指定路径。

```yaml title="load-image.yaml"
source:
  intermediateBundlesPath: ghippo-offline # (1)
target:
  containerRegistry: 10.16.10.111 # (2)
  containerRepository: release.daocloud.io/ghippo # (3)
  repo:
    kind: LOCAL
    path: ./local-repo # (4)
  containers:
    auth:
      username: "admin" # (5)
      password: "Harbor12345" # (6)
```

1. 到执行 charts-syncer 命令的相对路径，而不是此 YAML 文件和离线包之间的相对路径
2. 需更改为你的镜像仓库 url
3. 需更改为你的镜像仓库
4. chart 本地路径
5. 你的镜像仓库用户名
6. 你的镜像仓库密码
```

Copyright © 2016 - 2023 DaoCloud

2. 执行同步镜像命令。

   `shell`

   `charts-syncer sync --config load-image.yaml`

Docker 或 containerd 直接加载

解压并加载镜像文件。

1. 解压 tar 压缩包。

   `shell`

   `tar xvf ghippo.bundle.tar`

   解压成功后会得到 3 个文件：

- hints.yaml
- images.tar
- original-chart

2. 从本地加载镜像到 Docker 或 containerd。

   === "Docker"

   ```shell
   docker load -i images.tar
   ```

   === "containerd"

   ```shell
   ctr image import images.tar
   ```

   !!! note

   ```
   每个 node 都需要做 Docker 或 containerd 加载镜像操作，
   加载完成后需要 tag 镜像，保持 Registry、Repository 与安装时一致。
   ```

升级

有两种升级方式。您可以根据前置操作，选择对应的升级方案：

!!! note

```
当从 v0.11.x (或更低版本) 升级到 v0.12.0 (或更高版本) 时，需要将 `bak.yaml` 中所有 keycloak key 修改为 `keycloakx`。

这个 key 的修改示例：

```yaml title="bak.yaml"
USER-SUPPLIED VALUES:
keycloak:
    ...
```

修改为：

```yaml title="bak.yaml"
USER-SUPPLIED VALUES:
keycloakx:
    ...
```
```

=== "通过 helm repo 升级"

```
1. 检查全局管理 helm 仓库是否存在。

    ```shell
    helm repo list | grep ghippo
    ```

   若返回结果为空或如下提示，则进行下一步；反之则跳过下一步。
```

Copyright © 2016 - 2023 DaoCloud

```none
Error: no repositories to show
```

1. 添加全局管理的 helm 仓库。

```shell
heml repo add ghippo http://{harbor url}/chartrepo/{project}
```

1. 更新全局管理的 helm 仓库。

```shell
helm repo update ghippo # (1)
```

1. helm 版本过低会导致失败，若失败，请尝试执行 helm update repo

1. 选择您想安装的全局管理版本（建议安装最新版本）。

```shell
helm search repo ghippo/ghippo --versions
```

```none
[root@master ~]# helm search repo ghippo/ghippo --versions
NAME                  CHART VERSION  APP VERSION  DESCRIPTION
ghippo/ghippo  0.9.0          v0.9.0       A Helm chart for GHippo
...
```

1. 备份 `--set` 参数。

在升级全局管理版本之前，建议您执行如下命令，备份老版本的 `--set` 参数。

```shell
helm get values ghippo -n ghippo-system -o yaml > bak.yaml
```

1. 更新 ghippo crds

```shell
helm pull ghippo/ghippo --version 0.9.0 && tar -zxf ghippo-0.9.0.tgz
kubectl apply -f ghippo/crds
```

1. 执行 `helm upgrade`。

升级前建议您覆盖 bak.yaml 中的 `global.imageRegistry` 字段为当前使用的镜像仓库地址。

```shell
export imageRegistry={你的镜像仓库}
```

```shell
helm upgrade ghippo ghippo/ghippo \
  -n ghippo-system \
  -f ./bak.yaml \
  --set global.imageRegistry=$imageRegistry
  --version 0.9.0
```

=== "通过 chart 包升级"

1. 备份 `--set` 参数。

在升级全局管理版本之前，建议您执行如下命令，备份老版本的 `--set` 参数。

```shell
helm get values ghippo -n ghippo-system -o yaml > bak.yaml
```

1. 更新 ghippo crds

```shell
kubectl apply -f ./crds
```

1. 执行 `helm upgrade`。

升级前建议您覆盖 bak.yaml 中的 `global.imageRegistry` 为当前使用的镜像仓库地址。

```shell
export imageRegistry={你的镜像仓库}
```

```shell
helm upgrade ghippo . \
  -n ghippo-system \
  -f ./bak.yaml \
```


Copyright © 2016 - 2023 DaoCloud

```
  --set global.imageRegistry=$imageRegistry
```


Copyright © 2016 - 2023 DaoCloud

2.3 自定义 DCE 5.0 反向代理服务器地址

前置条件

要求 DCE 5.0 管理集群上的 ghippo-apiserver pod 必须能够访问通该反向代理入口地址，可在管理集群节点上 curl 反向代理入口地址来验证其连通性：

```
# 假设准备设置的反向代理入口地址为 https://demo-alpha.daocloud.io
curl -k "https://demo-alpha.daocloud.io"
```

如不满足连通性要求，则下述设置步骤无效

设置步骤

1. 设置环境变量，方便在下文中使用。

   ```shell

## 2.4 您的反向代理地址，例如：`export DCE_PROXY="https://demo-alpha.daocloud.io"`

export DCE_PROXY="https://domain:port"

## 2.5 helm --set 参数备份文件

export GHIPPO_VALUES_BAK="ghippo-values-bak.yaml"

## 2.6 获取当前 ghippo 的版本号

export GHIPPO_HELM_VERSION=$(helm get notes ghippo -n ghippo-system | grep "Chart Version" | awk -F ': ' '{ print $2 }') ```

2. 更新全局管理 Helm 仓库。

   `shell`

   `helm repo update ghippo`

3. 备份 --set 参数。

   `shell`

   `helm get values ghippo -n ghippo-system -o yaml > ${GHIPPO_VALUES_BAK}`

4. 添加您的反向代理地址。

   !!! note

   ```
   - 如果可以，您可以使用 `yq` 命令：

       ```shell
       yq -i ".global.reverseProxy = \"${DCE_PROXY}\"" ${GHIPPO_VALUES_BAK}
       ```

   - 或者您可以使用 `vim` 命令编辑并保存：

       ```shell
       vim ${GHIPPO_VALUES_BAK}

       USER-SUPPLIED VALUES:
       ...
       global:
         ...
         reverseProxy: ${DCE_PROXY} # 只需要修改这一行
       ```
   ```

5. 执行 `helm upgrade` 使配置生效。

   `shell`

   `helm upgrade ghippo ghippo/ghippo \`



Copyright © 2016 - 2023 DaoCloud
   ```

```
  -n ghippo-system \
  -f ${GHIPPO_VALUES_BAK} \
  --version ${GHIPPO_HELM_VERSION}
```

6. 使用 `kubectl` 重启全局管理 Pod，使配置生效。

```shell
kubectl rollout restart deploy/ghippo-apiserver -n ghippo-system
kubectl rollout restart statefulset/ghippo-keycloakx -n ghippo-system
```


Copyright © 2016 - 2023 DaoCloud

Copyright © 2016 - 2023 DaoCloud

3. Intro

Copyright © 2016 - 2023 DaoCloud

3.1 功能总览

本页说明全局管理的各项功能特性。

Copyright © 2016 - 2023 DaoCloud

1. 用户管理

   拥有用户帐号，是用户访问 DCE 平台的前提。 用户由平台管理员 Super Admin 或者用户与访问控制管理员 IAM Admin 在 `全局管理` -> `用户与访问控制` -> `用户` 页面创建，或者通过 LDAP 对接而来。 每位用户拥有独立的用户名和密码，通过给单个或者一组用户授予不同的权限，让不同的用户拥有不同资源的访问权限。

   ```mermaid graph LR

   ```
   admin([平台管理员或
用户与访问控制管理员]) --> |创建并管理用户|user[用户]
   user --> user1[用户 A]
   user --> user2[用户 B]
   user --> user3[用户 C]
   ```

   click user "https://docs.daocloud.io/ghippo/user-guide/access-control/user/"

   classDef plain fill:#ddd,stroke:#fff,stroke-width:0px,color:#000; classDef k8s fill:#326ce5,stroke:#fff,stroke-width:0px,color:#fff; classDef cluster fill:#fff,stroke:#bbb,stroke-width:2px,color:#326ce5; class admin plain; class user1,user2,user3 k8s; class user cluster ```

2. 用户组管理

   用户组是多个用户的集合。 用户可以通过加入用户组，实现继承用户组的角色权限。通过用户组批量地给用户进行授权，可以更好地管理用户及其权限。

   ```mermaid graph LR

   ```
   admin([平台管理员或<br>用户与访问控制管理员])
   admin --> user[创建用户]
   admin --> group[创建用户组]
   admin --> add[将用户加入用户组]
   ```

   click user "https://docs.daocloud.io/ghippo/user-guide/access-control/user/" click group "https://docs.daocloud.io/ghippo/user-guide/access-control/group/" click add "https://docs.daocloud.io/ghippo/user-guide/access-control/group/#_5"

   classDef plain fill:#ddd,stroke:#fff,stroke-width:0px,color:#000; classDef k8s fill:#326ce5,stroke:#fff,stroke-width:0px,color:#fff; classDef cluster fill:#fff,stroke:#bbb,stroke-width:2px,color:#326ce5; class admin plain; class user,group,add cluster ```

3. 角色管理

   一个角色对应一组权限。 权限决定了可以对资源执行的操作。向用户授予某个角色，即授予该角色所包含的所有权限。 您可以将不同模块的管理权限划分给不同的用户， 比如用户 A 管理容器管理模块，用户 B 管理应用工作台模块，共同管理可观测性模块。

4. 工作空间

   工作空间用于管理资源，包含层级和工作空间两部分。

   层级是资源层次结构中的节点，一个层级可以包含工作空间、其他层级或两者的组合。 可以将层级理解为有层次结构的部门、环境、供应商等多种概念。

   工作空间可以理解为部门下的项目，管理员通过层级和工作空间映射企业中的层级关系。

   虽然一个层级可以包含多个层级或工作空间，但是给定的层级或者工作空间只能有一个父级。

Copyright © 2016 - 2023 DaoCloud

5. 审计日志

   审计日志完整地记录用户的各项操作行为， 包括用户通过页面或 API 接口发起的操作以及各服务内部自触发的操作。 支持通过事件来源、资源类型、操作状态等多个维度进行组合查询，支持审计日志导出。

6. 平台设置

   平台设置包括账号安全设置、 外观定制、 邮件服务器等。 当需要对账号的安全信息、平台 logo、许可证授权、邮件服务器等平台级设置进行管理时，可以通过 `平台设置` 进行操作，平台设置仅平台管理员具有管理权限。

   ```mermaid graph LR

   ```
   admin([平台管理员]) --> |管理|about[平台设置]
   about --> password[用户密码等安全策略]
   about --> appear[平台外观定制]
   about --> mail[邮件服务器]
   about --> license[正版授权]
   ```

   click about "https://docs.daocloud.io/ghippo/user-guide/platform-setting/about/" click password "https://docs.daocloud.io/ghippo/user-guide/password/" click appear "https://docs.daocloud.io/ghippo/user-guide/platform-setting/appearance/" click mail "https://docs.daocloud.io/ghippo/user-guide/platform-setting/mail-server/" click license "https://docs.daocloud.io/dce/license0/"

   classDef plain fill:#ddd,stroke:#fff,stroke-width:0px,color:#000; classDef k8s fill:#326ce5,stroke:#fff,stroke-width:0px,color:#fff; classDef cluster fill:#fff,stroke:#bbb,stroke-width:2px,color:#326ce5; class admin plain; class about,password,appear,mail,license cluster ```


Copyright © 2016 - 2023 DaoCloud
   ```

功能清单

具体的功能清单如下所述。

Copyright © 2016 - 2023 DaoCloud

1. 用户与访问控制

a. 用户

- 列表展示用户名、描述、创建时间、最近一次登录时间
- 列表支持通过用户名搜索用户
- 列表支持给用户快捷授权
- 列表支持将用户快捷加入用户组
- 列表支持批量删除用户
- 列表支持创建用户
- 详情支持编辑用户基本信息，包括邮箱、描述、启用 / 禁用等
- 详情支持记录用户授权信息，支持添加 / 移除权限
- 详情支持记录用户加入用户组信息，支持用户加入新的用户组，支持将用户从老的用户组移除
- 支持管理员帮助用户修改密码
- 支持管理员帮助用户创建访问密钥

b. 用户组

- 列表展示用户组名、组内用户数、描述、创建时间
- 列表支持通过用户组名搜索
- 列表支持给用户组快捷授权
- 列表支持给用户组快捷添加用户
- 列表支持批量删除用户组
- 列表支持创建用户组
- 详情支持编辑用户组基本信息，例如描述
- 详情支持记录用户组授权信息，支持添加 / 移除权限
- 详情支持记录用户组成员信息，支持给用户组添加新成员，支持将成员从用户组移除

c. 角色

- 列表展示系统角色名称、描述
- 详情记录角色授权信息，支持将角色授予用户 / 用户组，支持将用户 / 用户组从该角色移除
- 支持 Folder Admin、Folder Editor、Folder Viewer 三种预定义文件夹角色
- 支持 Workspace Admin、Workspace Editor、Workspace Viewer 三种预定义工作空间角色

d. 身份提供商

- 支持 LDAP、OIDC 两种协议对接外部用户
- LDAP 协议支持手动 / 自动同步外部用户
- LDAP 协议支持手动同步外部用户组
- OIDC 协议支持手动同步外部用户

Copyright © 2016 - 2023 DaoCloud

2. 工作空间与层级

a. 文件夹

- 支持树状结构展示文件夹和工作空间
- 支持通过文件夹名称和工作空间名称搜索
- 支持 5 级文件夹映射企业层级
- 支持为文件夹添加用户 / 用户组并授权
- 支持权限继承，子文件夹、工作空间能够继承用户 / 用户组在上级文件夹权限
- 支持移动文件夹。映射企业中的部门变动，移动后其下的子文件夹、工作空间及其资源 / 成员均会跟随该文件夹移动，权限的继承关系重新发生变化

b. 工作空间

- 支持为工作空间添加用户 / 用户组并授权
- 支持添加资源到工作空间 - 资源组，支持 6 种资源类型
- 支持权限继承，资源组中的资源能够继承用户 / 用户组在工作空间和上级文件夹的角色
- 支持移动工作空间。映射企业中的项目变动，移动后其下的资源 / 成员均会跟随该工作空间移动，权限的继承关系重新发生变化（开发中）
- 支持添加资源到工作空间 - 共享资源，将一个集群资源共享给多个工作空间使用
- 支持针对每个共享的集群资源进行资源限额
- 支持通过 CPU Limit、CPU Request 、内存 Limit、内存 Request、存储请求总量 Request Storage、存储卷声明 PersistentVolumeClaim 六个维度进行资源限额

3. 审计日志

- 列表展示事件名称、资源类型、资源名称、状态、操作人、操作时间
- 列表支持查看审计日志详情
- 列表支持展示最近一天或自定义时间内的审计日志
- 列表支持通过状态、操作人、资源类型、资源名称搜索审计日志
- 列表支持 .csv 格式导出审计日志
- 默认采集全局管理的全部审计日志
- 默认保存 365 天内的审计日志
- 支持手动 / 自动两种方式清理全局管理的审计日志
- 支持开启 / 关闭收集 K8s 的审计日志
- 支持手动 / 自动两种方式清理 K8s 的审计日志

Copyright © 2016 - 2023 DaoCloud

4. 平台设置

a. 安全策略

- 支持自定义密码规则
- 支持自定义密码策略
- 支持自定义会话超时策略，超出时长自动退出当前账号
- 支持自定义账号锁定策略，限制时间内多次登录失败，账号将被锁定
- 支持登录登出策略，开启后关闭浏览器的同时退出登录

b. 邮件服务器设置：支持管理员配置邮件服务器，支持通过邮件方式找回用户密码，接收告警通知等

c. 外观定制

- 支持自定义登录页，包括更换平台 LOGO、登录页图标、标签页图标等
- 支持一键还原登录页外观配置
- 支持自定义顶部导航栏，包括导航栏图标、标签页图标等
- 支持一键还原顶部导航栏外观配置

d. 正版授权

- 列表展示许可证名称、所属模块、许可证级别、许可证状态过期时间
- 支持管理许可证，确保子模块在有效期内

e. 关于平台

- 支持展示模块版本
- 支持展示平台使用的开源软件
- 支持展示技术团队风采

5. 个人中心

a. 安全设置

- 支持用户更新登录密码
- 支持通过邮箱找回登录密码

b. 访问密钥：支持每个用户创建独立的 API 密钥，支持进行 API 密钥过期设置，以确保系统安全

c. 语言设置：支持多语言，支持简体中文、英文、自动检测您的浏览器首选语言三种方式确定语言

Copyright © 2016 - 2023 DaoCloud

3.2 常见术语

本节列出全局管理的常见术语。

IAM

IAM（Identity and access management）是用户与访问控制模块的简称，该模块的管理员被称为 IAM Admin，拥有该模块的最高权限。 被赋予 IAM Admin 的用户（用户组），将拥有用户与访问控制的全部且最高权限。

更多详细信息，参见什么是 IAM。

RBAC

RBAC（Role-based access control，基于角色的访问控制），基本理念是将角色这个概念赋予用户，在用户与权限之间通过角色进行关联，实现灵活配置。 RBAC 模型的三要素为：用户、角色、权限。使用 RBAC 机制授权 IAM 用户访问平台资源。

用户

用户是发起操作的主体，每个用户都有唯一的 ID，并被授予不同的角色。 默认创建的 IAM 用户没有任何权限，需要将其加入用户组，授予角色或策略，才能让用户获得对应的权限。

用户以用户名登录 DCE，按照被授予的权限操作平台资源和服务。 所以用户是资源归属的主体，对其拥有的资源具有相应权限。

用户可以在个人中心修改用户信息，设置密码、访问密钥和 UI 语言。

用户组

用户组是一个或多个用户的集合，IAM 可以通过用户组实现用户的授权。 通常先创建一个 IAM 用户，加入某个用户组，该用户将继承这个用户组的权限。当一个用户加入多个用户组时，该用户将同时拥有多个用户组的权限。

角色

角色是连接用户与权限的桥梁，一个角色对应一组权限，不同角色具有不同的权限。向用户授予某角色，即授予该角色所包含的所有权限。全局管理中有两种角色：

- 预定义角色：由系统创建，用户只能使用不能修改，每个子模块都有一个管理员 Admin 角色。
- 自定义角色：用户自主创建、更新和删除，自定义角色中的权限由用户自己维护。同时因为全局管理汇聚了多个子模块，各子模块也拥有相应的管理员角色，例如：
- IAM Admin：管理用户与访问控制，即管理用户/用户组以及授权
- Workspace Admin：管理层级及工作空间的权限，仅此权限可以创建层级
- Audit Admin：管理审计日志

权限

权限指是否允许用户对某种资源执行某种操作。 为了降低使用门槛，DCE 采用 RBAC 模型将权限聚合成一个个角色，管理员只需要将角色授权给用户，该用户就一次性得到了该角色下聚合的一组权限。

默认情况下，管理员创建的 IAM 用户没有任何角色权限，需要对其单独授予角色或将其加入用户组并给用户组授予角色，才能使得用户获得对应的角色权限，这一过程称为授权。 授权后，用户就可以基于被授予的角色权限对平台资源进行操作。

授权

授权指将用户完成具体工作所需的权限授予用户，授权通过系统角色或自定义角色的权限生效。 用户获得具体的权限后，可以对资源或服务进行操作。

Copyright © 2016 - 2023 DaoCloud

工作空间

通过工作空间协调全局管理和子模块的权限关系，解决资源聚合和映射层级关系。 通常一个工作空间对应一个项目，可以为每个工作空间分配不同的资源，指派不同的用户和用户组。

层级

参见上图，为了满足企业内各个部门的分支划分，DCE 引入了层级的概念，通常层级对应着不同的部门，每个层级可以包含一个或多个工作空间。

资源

资源（Resource）泛指 DCE 平台上通过各个子模块创建的资源，是完成授权的具体数据。 通常资源描述一个或多个操作对象，每个子模块拥有其各自的资源和对应的资源定义详情，如集群、Namesapce、网关等。

资源的拥有者是主账号 Super Admin。Super Admin 具有在各子模块创建/管理/删除资源的权限，普通用户在没有授权的情况下，不会自动拥有资源的访问权限，需要 Super Admin 进行授权。 工作空间支持跨子模块授权用户（用户组）对于资源的访问权限。

身份凭证

身份凭证是识别用户身份的依据，登录和使用资源时，需要有身份凭证才能通过系统的鉴权认证。 身份凭证包括密码和访问密钥，可以通过 IAM 管理自己以及下属 IAM 用户的身份凭证。

有关更多术语，请参阅本站收录的云原生词汇大全。

Copyright © 2016 - 2023 DaoCloud

3.3 全局管理 Release Notes

本页列出全局管理各版本的 Release Notes，便于您了解各版本的演进路径和特性变化。

2023-02-27

v0.14.0

功能

- 平台设置->外观定制->高级定制->登录页定制及登录后页面定制
- 支持 keycloak quarkus 架构在双栈环境运行
- CI 过程中加入 job 检测 helm chart 包中是否有不合规的镜像和检测安装参数是否正确
- 在 helm values 里设置开关，可以一键开关 audit 相关功能
- 审计日志支持记录 kpanda 页面操作

优化

- OpenAPI 调用方式优化

修复

- 修复部分错误的审计日志名称
- 修改 keycloak 启动探针 failureThreshold 值，提高启动成功率
- 修复绑定/解绑资源错误 i18n

2022-12-30

v0.13.2

修复

- 界面补充了缺少权限说明的英文文案
- 修复数据库表更新时，可能因为数据库编码导致报错

2022-12-28

v0.13.0

新功能

- 支持在 DCE 5.0 前面部署一个国密网关，并用国密浏览器来访问 DCE 5.0
- 在 helm values 里设置开关，可以一键开关 istio sidecar 功能
- 工作空间与层级增加 Workspace and Folder Owner 角色
- 拥有 Workspace/Folder Admin 和 Kpanda Owner 权限的用户才可进行资源绑定
- 对所用的库，进行开源 License 扫描
- 用户列表新增 `状态` 列
- 对内提供离线安装文档
- SDK 单元测试达 65%
- 界面支持发送测试邮件和无账号密码邮件服务器
- 界面支持对不符合系统要求的用户名进行提示

优化

- Ghippo 鉴权代码优化(减少内存使用量)

Copyright © 2016 - 2023 DaoCloud

- 前端界面低网络情况下预加载机制优化

修复

- 修复 OpenAPI cycle 为必填参数问题，修复后为可选参数

2022-11-30

v0.12.1

优化

- 通过 CI 自动构建纯离线包
- 优化 GHippo 升级文档

2022-11-28

v0.12.0

新功能

- 资源组里的 `模块` 改为 `来源`
- SDK 提供 Workspace 和 Resource 的绑定变化通知
- 完整对接 Insight metrics 和 otel tracing(加入 keycloak 和 db 链路)
- Keycloak 改成 Quarkus 架构
- Keycloak 镜像升级成 20.0.1 版本

优化

- 重构导出审计日志 http 接口为 gprc stream 接口
- SDK 内存使用量优化，峰值减少 50%
- 审计日志部分代码优化
- e2e 的 kind 镜像切到 1.25
- 提高资源使用效率到 40% 以上

修复

- 修复强绑定集群问题
- 修复配置身份提供商界面选择 `Client secret sent as basic auth` 没有保存到 keycloak 里的问题

2022-11-01

v0.11.2

修复

- 关闭资源组绑定集群功能
- 修复无工作空间时无法创建工作空间问题

2022-10-28

v0.11.0

新功能

- 给第三方应用提供接口在 Keycloak 创建 SSO 对接 Client
- 支持 Mysql8
- 对接 Insight(metrics, log, otel tracing)

Copyright © 2016 - 2023 DaoCloud

- License 模块名支持 i18n
- 支持一个 License 中可以包含多个 GProduct
- 资源组新增绑定集群类型资源
- 资源组列表增加“模块”字段
- 资源组列表增加已绑定标识
- 资源绑定接口支持 Registry 资源种类。

优化

- 资源种类改枚举
- GProduct license 是否需要灌入变量改为可配
- 优化 CICD 流程

修复

- 修复已经删除的集群依然存在问题
- 修复 keycloak jwks 变化后没有重置 istio 缓存问题
- 修复用户组创建时间零值问题
- 修复访问密钥 `最后使用时间` 字段在未使用时返回空字符

2022-09-28

v0.10.0

新功能

- 支持登录
- 支持忘记密码
- 支持站内信增删改查功能
- 支持 SMTP 设置邮件服务器
- 支持顶部导航栏获取查询
- 支持顶部导航栏更新
- 支持用户角色权限管理 CRUD
- 工作空间 -> 生命周期管理（创建/编辑/删除/查看/列表）
- 工作空间 -> 层级关系管理（绑定/列表）
- 工作空间 -> 工作空间与资源关系管理（绑定/解绑/列表）
- 工作空间 -> 工作空间和角色和用户（组）关系管理（绑定/解绑/列表）（API/SDK）
- 工作空间 -> 鉴权（API/SDK）
- 工作空间 -> GProduct 资源名字注册
- 关于 -> 产品版本（创建/编辑/删除/查看/列表）
- 关于 -> 开源软件（列表/初始化）
- 关于 -> 技术团队（列表/初始化）
- 许可证 -> 生命周期管理（创建/编辑/删除/查看/列表）
- 许可证 -> 获取 ESN 序列号
- 许可证 -> 未灌入或错误情况处理
- 工作空间 -> 资源配额管理（创建/编辑/删除/查看/列表/计算已分配）
- 工作空间 -> GProduct 资源配额注册
- 用户与访问控制 -> 鉴权（APIServer/SDK）
- 审计日志 -> 展示（查看/列表/清理设置/导出）

Copyright © 2016 - 2023 DaoCloud

- 审计日志 -> 批量插入
- 身份提供商 -> 对接 LDAP -> 用户/用户组同步设置（创建/编辑/删除/查看/同步）
- 平台设置 -> 安全策略 -> 密码策略设置
- 个人中心 -> 访问密钥(创建/编辑/删除/查看/列表)
- 审计日志 -> 全局管理操作插入审计日志
- 审计日志 -> 对接 Insight 来收集审计日志
- 平台设置 -> 安全策略 -> 账号锁定策略
- 平台设置 -> 安全策略 -> 浏览器关闭策略
- 身份提供商 -> 对接 IDP (OIDC 协议)
- 工作空间 -> 共享集群权限管理
- 工作空间 -> 共享集群配额管理 -> 存储
- 平台设置 -> 顶部导航外观定制 -> 重置功能
- 平台设置 -> 安全策略 -> 会话超时策略
- 审计日志 -> 自动清理功能
- 平台设置 -> 安全策略-账号锁定策略
- 平台设置 -> 顶部导航外观定制-还原功能
- 平台设置 -> 登录页外观定制-还原功能
- 产品导航 -> 首页仅对 admin 用户展示
- 工作空间 -> 用户仅能查看有权限的 workspace & folder 树状结构
- Keycloak 高可用
- 邮件服务器配置 -> 支持 Insight 和应用工作台发送邮件
- 满足 Helm 规范，支持安装器和离线化
- 审计日志 -> 数据库自动创建和合并分区
- 支持 ARM64 架构
- 支持 https
- 登录 -> 背景 theme 支持动画
- 授权鉴权 -> 给前端提供当前登录用户的权限列表
- 关于 -> 软件版本 -> 模块支持中文名
- 添加整体双语文档站结构及主要内容
- 文档站新增页面：什么是全局管理、常见术语、功能总览、快速入门/创建用户和授权、什么是用户访问和控制、用户、创建用户组并授权、用户组、登录、密码重置、全局管理角色、资源管理（按工作空间）、资源管理（按角色）、身份提供商、邮件服务器设置、外观定制、LDAP、OIDC、关于平台、审计日志、访问密钥、语言设置、安全设置 等文档

优化

- 授权鉴权 -> 提供一个 job 来确保 db 和 cr 的同步
- LDAP -> 配置错误检查
- 各功能操作反馈和提示语报错支持中英文
- 工作空间及层级 -> 删除前对是否存在子资源进行检查
- 优化 keycloak jvm 参数
- 通过 mockery 框架简化 mock

Copyright © 2016 - 2023 DaoCloud

3.4 什么是全局管理？

全局管理是以用户为中心的综合性服务板块，包含用户与访问控制、企业空间、审计日志、平台设置等基础服务模块。

- 用户与访问控制：帮助用户安全管理资源的访问权限。您可以通过用户与访问控制创建、管理、删除用户/用户组，并灵活配置用户/用户组权限，来完成用户职能权限的划分。
- 企业空间：具有层级结构和访问权限控制的资源隔离单元。您可以按照企业开发环境、部门结构等设置层级结构，并控制哪些人对哪些资源具有访问权限。
- 审计日志：提供资源的操作记录。通过操作记录您可以快速实现安全分析、资源变更、问题定位等。
- 平台设置：通过平台安全策略、邮件服务器、外观定制等，实现用户信息的安全性和平台的个性化。

全局管理优势

- 综合性汇总式服务

  将平台的基础服务模块汇聚在一起，减少菜单切换和功能分散带来的困扰，使平台管理员在一个菜单下就能够完成基础性平台设置和用户管理。
- 用户与租户相结合

  通过扁平化用户、用户组管理和层级式租户（工作空间）协作，多维度多场景实现基于平台的访问控制以及基于资源的权限划分。
- 个性化定制

  支持个性化定制平台外观，包括登录页定制和顶部导航栏定制，通过可视化页面轻轻松松配置一个属于您的个性化平台。
- 简化操作，上手即用

  预先为用户完成了绝大多数的平台设置，包括密码规则配置、会话超时策略等，简化用户操作，实现上手即用。

操作步骤

1. 使用 DCE 平台管理员（Admin）或具有管理员权限的用户登录 DCE 平台
2. 进入 `用户与访问控制`，创建用户并授权，创建用户组并授权，创建身份提供商
3. 进入 `工作空间`，创建层级（企业层级关系），创建工作空间（租户）
4. 进入 `审计日志`，查看并导出审计日志
5. 进入 `平台设置`，设置安全策略、邮件服务器、外观定制、正版授权

下载 DCE 5.0{ .md-button .md-button--primary } 安装 DCE 5.0{ .md-button .md-button--primary } 申请社区免费体验{ .md-button .md-button--primary }

Copyright © 2016 - 2023 DaoCloud

4. Permissions

4.1 应用工作台权限说明

应用工作台支持三种用户角色：

- Workspace Admin
- Workspace Editor
- Workspace Viewer

Copyright © 2016 - 2023 DaoCloud

每种角色具有不同的权限，具体说明如下。

Copyright © 2016 - 2023 DaoCloud

菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
应用	查看应用列表	&check	&check	&check
	查看详情（跳转到容器管理）	&check	&check	&check
	查看应用日志（跳转到可观测）	&check	&check	&check
	查看应用监控（跳转到可观测）	&check	&check	&check
	查看 RabbitMQ 详情 - 基本信息	&check	&check	&check
	查看服务网格（跳转到服务网格）	&check	&check	&check
	查看微服务引擎（跳转到微服务引擎）	&check	&check	&check
	创建应用	&check	&check	&cross
	编辑 YAML	&check	&check	&cross
	更新副本数量	&check	&check	&cross
	更新容器镜像	&check	&check	&cross
	编辑流水线	&check	&check	&cross
	应用分组	&check	&check	&cross
	删除	&check	&check	&cross
命名空间	查看	&check	&check	&check
	创建	&check	&cross	&cross
	编辑标签	&check	&cross	&cross
	编辑资源配额	&check	&cross	&cross
	删除	&check	&cross	&cross
流水线	查看流水线	&check	&check	&check
	查看运行记录	&check	&check	&check
	创建	&check	&check	&cross
	运行	&check	&check	&cross
	删除	&check	&check	&cross
	复制	&check	&check	&cross
	编辑	&check	&check	&cross
	取消运行	&check	&check	&cross
凭证	查看	&check	&check	&check
	创建	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
持续部署	查看	&check	&check	&check
	创建	&check	&check	&cross
	同步	&check	&check	&cross
	编辑	&check	&check	&cross

Copyright © 2016 - 2023 DaoCloud

菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
	删除	&check	&check	&check
代码仓库	查看	&check	&check	&cross
	导入	&check	&check	&cross
	删除	&check	&check	&cross
灰度发布	查看	&check	&check	&check
	创建	&check	&check	&cross
	发布	&check	&check	&cross
	继续发布	&check	&check	&cross
	终止发布	&check	&check	&cross
	更新	&check	&check	&cross
	回滚	&check	&check	&cross
	删除	&check	&check	&cross

!!! note

```
有关角色和权限管理的完整介绍，请参考[角色和权限管理](../user-guide/access-control/role.md)。
```


Copyright © 2016 - 2023 DaoCloud

4.2 中间件数据服务权限说明

中间件数据服务包括六大中间件：MySQL、RabbitMQ、Elasticsearch、Kafka、Redis、MinIO。中间件数据服务支持三种用户角色：

- Workspace Admin
- Workspace Editor
- Workspace Viewer

每种角色具有不同的权限，具体说明如下。

Copyright © 2016 - 2023 DaoCloud

中间件数据服务权限说明

Copyright © 2016 - 2023 DaoCloud

中间件模块	菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
MySQL	MySQL 实例列表	查看列表	&check	&check	&check
		实例名称搜索	&check	&check	&check
		创建实例	&check	&check	&cross
		更新实例配置	&check	&check	&cross
		删除实例	&check	&cross	&cross
	MySQL 实例详情	实例概览	&check	&check	&check
		实例监控	&check	&check	&check
		查看实例配置参数	&check	&check	&check
		修改实例配置参数	&check	&check	&cross
		查看实例访问密码	&check	&check	&cross
		查看实例备份列表	&check	&check	&check
		实例创建备份	&check	&check	&cross
		实例修改自动备份任务	&check	&check	&cross
		使用备份创建新实例	&check	&check	&cross
	备份配置管理	备份配置列表	&check	&cross	&cross
		创建备份配置	&check	&cross	&cross
		修改备份配置	&check	&cross	&cross
		删除备份配置	&check	&cross	&cross
RabbitMQ	RabbitMQ 实例列表	查看列表	&check	&check	&check
		实例名称搜索	&check	&check	&check
		创建实例	&check	&check	&cross
		更新实例配置	&check	&check	&cross
		删除实例	&check	&cross	&cross
	RabbitMQ 实例详情	实例概览	&check	&check	&check
		实例监控	&check	&check	&check
		查看实例配置参数	&check	&check	&check
		修改实例配置参数	&check	&check	&cross
		查看实例访问密码	&check	&check	&cross
Elasticsearch	Elasticsearch 实例列表	查看列表	&check	&check	&check

Copyright © 2016 - 2023 DaoCloud

中间件模块	菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
		实例名称搜索	&check	&check	&check
		创建实例	&check	&check	&cross
		更新实例配置	&check	&check	&cross
		删除实例	&check	&cross	&cross
	Elasticsearch 实例详情	实例概览	&check	&check	&check
		实例监控	&check	&check	&check
		查看实例配置参数	&check	&check	&check
		修改实例配置参数	&check	&check	&cross
		查看实例访问密码	&check	&check	&cross
Redis	Redis 实例列表	查看列表	&check	&check	&check
		实例名称搜索	&check	&check	&check
		创建实例	&check	&check	&cross
		更新实例配置	&check	&check	&cross
		删除实例	&check	&cross	&cross
	Redis 实例详情	实例概览	&check	&check	&check
		实例监控	&check	&check	&check
		查看实例配置参数	&check	&check	&check
		修改实例配置参数	&check	&check	&cross
		查看实例访问密码	&check	&check	&cross
Kafka	Kafka 实例列表	查看列表	&check	&check	&check
		实例名称搜索	&check	&check	&check
		创建实例	&check	&check	&cross
		更新实例配置	&check	&check	&cross
		删除实例	&check	&cross	&cross
	Kafka 实例详情	实例概览	&check	&check	&check
		实例监控	&check	&check	&check
		查看实例配置参数	&check	&check	&check
		修改实例配置参数	&check	&check	&cross
		查看实例访问密码	&check	&check	&cross

Copyright © 2016 - 2023 DaoCloud

中间件模块	菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
MinIO	MinIO 实例列表	查看列表	&check	&check	&check
		实例名称搜索	&check	&check	&check
		创建实例	&check	&check	&cross
		更新实例配置	&check	&check	&cross
		删除实例	&check	&cross	&cross
	MinIO 实例详情	实例概览	&check	&check	&check
		实例监控	&check	&check	&check
		查看实例配置参数	&check	&check	&check
		修改实例配置参数	&check	&check	&cross
		查看实例访问密码	&check	&check	&cross

Copyright © 2016 - 2023 DaoCloud

4.3 服务网格权限说明

服务网格支持几种用户角色：

- Admin
- Workspace Admin
- Workspace Editor
- Workspace Viewer

Copyright © 2016 - 2023 DaoCloud

这些角色的具体权限如下表所示。

Copyright © 2016 - 2023 DaoCloud

菜单对象	操作	Admin	Workspace Admin	Workspace Editor	Workspace Viewer
服务网格列表	创建网格	&check	&cross	&cross	&cross
	编辑网格	&check	&check	&check	&cross
	删除网格	&check	&check	&cross	&cross
	查看网格	&check	&check	&check	&check
网格概览	查看	&check	&check	&check	&check
服务列表	跳转至治理页面	&check	&check	&check	&cross
	查看	&check	&check	&check	&check
服务条目	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
虚拟服务	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
目标规则	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
网关规则	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
对等身份认证	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
请求身份认证	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
授权策略	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check

Copyright © 2016 - 2023 DaoCloud

菜单对象	操作	Admin	Workspace Admin	Workspace Editor	Workspace Viewer
命名空间边车管理	启用注入	&check	&check	&check	&cross
	禁用注入	&check	&check	&check	&cross
	查看	&check	&check	&check	&check
工作负载边车管理	启用注入	&check	&check	&check	&cross
	禁用注入	&check	&check	&check	&cross
	边车资源设置	&check	&check	&check	&cross
	查看	&check	&check	&check	&check
全局边车注入	启用注入	&check	&check	&check	&cross
	禁用注入	&check	&check	&check	&cross
	边车资源设置	&check	&check	&check	&cross
	查看	&check	&check	&check	&check
集群纳管	集群接入	&check	&check	&cross	&cross
	集群移除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
网格网关	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
Istio 资源管理	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
TLS 证书管理	创建	&check	&check	&cross	&cross
	编辑	&check	&check	&check	&cross
	删除	&check	&check	&cross	&cross
	查看	&check	&check	&check	&check
系统升级	Istio 升级	&check	&check	&check	&cross
	边车升级	&check	&check	&check	&cross
	查看	&check	&check	&check	&check
工作空间管理	绑定	&check	&cross	&cross	&cross
	解绑	&check	&cross	&cross	&cross
	查看	&check	&check	&check	&check

Copyright © 2016 - 2023 DaoCloud

4.4 微服务引擎权限说明

微服务引擎包括微服务治理中心和微服务网关两部分。微服务引擎支持三种用户角色：

- Workspace Admin
- Workspace Editor
- Workspace Viewer

每种角色具有不同的权限，具体说明如下。

Copyright © 2016 - 2023 DaoCloud

微服务治理中心权限说明

Copyright © 2016 - 2023 DaoCloud

菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
托管注册中心列表	查看列表	&check	&check	&check
托管注册中心	查看基础信息	&check	&check	&check
	创建	&check	&check	&cross
	重启	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&cross	&cross
	上/下线	&check	&check	&cross
微服务命名空间	查看	&check	&check	&check
	创建	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
微服务列表	查看	&check	&check	&check
	筛选命名空间	&check	&check	&check
	创建	&check	&check	&cross
	治理	&check	&check	&cross
	删除	&check	&check	&cross
服务治理规则-Sentinel	查看	&check	&check	&check
	创建	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
服务治理规则-Mesh	治理	&check	&check	&cross
实例列表	查看	&check	&check	&check
	上/下线	&check	&check	&cross
	编辑	&check	&check	&cross
服务治理策略-Sentinel	查看	&check	&check	&check
	创建	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
服务治理策略-Mesh	查看	&check	&check	&check
	创建	&check	&check	&cross
	YAML 创建	&check	&check	&cross
	编辑	&check	&check	&cross
	YAML 编辑	&check	&check	&cross
	删除	&check	&check	&cross
微服务配置列表	查看	&check	&check	&check

Copyright © 2016 - 2023 DaoCloud

菜单对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
	筛选命名空间	&check	&check	&check
	批量删除	&check	&check	&cross
	导出/导入	&check	&check	&cross
	创建	&check	&check	&cross
	克隆	&check	&check	&cross
	编辑	&check	&check	&cross
	历史查询	&check	&check	&check
	回滚	&check	&check	&cross
	监听查询	&check	&check	&check
业务监控	查看	&check	&check	&check
资源监控	查看	&check	&check	&check
请求日志	查看	&check	&check	&check
实例日志	查看	&check	&check	&check
插件中心	查看	&check	&check	&check
	开启	&check	&check	&cross
	关闭	&check	&check	&cross
	编辑	&check	&check	&cross
	查看详情	&check	&check	&check
接入注册中心列表	查看	&check	&check	&check
	接入	&check	&check	&cross
	编辑	&check	&check	&cross
	移除	&check	&cross	&cross
微服务	查看列表	&check	&check	&check
	查看详情	&check	&check	&check
	治理	&check	&check	&cross
服务治理策略-Mesh	查看	&check	&check	&check
	创建	&check	&check	&cross
	YAML 创建	&check	&check	&cross
	编辑	&check	&check	&cross
	YAML 编辑	&check	&check	&cross
	删除	&check	&check	&cross

Copyright © 2016 - 2023 DaoCloud

微服务网关权限说明

对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
网关列表	查看	&check	&check	&check
网关实例	查看	&check	&check	&check
	创建	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&cross	&cross
诊断模式	查看	&check	&check	&check
	调试	&check	&check	&cross
服务列表	查看	&check	&check	&check
	添加	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
服务详情	查看	&check	&check	&check
服务来源管理	查看	&check	&check	&check
	添加	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
API 列表	查看	&check	&check	&check
	创建	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&cross
请求日志	查看	&check	&check	&check
实例日志	查看	&check	&check	&check
插件中心	查看	&check	&check	&check
	启用	&check	&check	&cross
	禁用	&check	&check	&cross
插件配置	查看	&check	&check	&check
	启用	&check	&check	&cross
域名列表	查看	&check	&check	&check
	添加	&check	&check	&cross
	编辑	&check	&check	&cross
	删除	&check	&check	&check
监控告警	查看	&check	&check	&check

!!! note

```
有关角色和权限管理的完整介绍，请参考[角色和权限管理](../user-guide/access-control/role.md)。
```


Copyright © 2016 - 2023 DaoCloud

5. User guide

5.1 审计日志

审计日志帮助您监控并记录每个用户的活动，提供了与安全相关的、按时间顺序排列的记录的收集、存储和查询功能。 借助审计日志服务，您可以持续监控并保留用户在全局管理模块的使用行为，包括但不限于创建用户、用户登录/登出、用户授权以及与 Kubernetes 相关的用户操作行为。

功能特性

审计日志功能具有以下特点：

- 开箱即用：在安装使用该平台时，审计日志功能将会被默认启用，自动记录与用户相关的各种行为，如创建用户、授权、登录/登出等。默认可以在平台内查看 365 天的用户行为。
- 安全分析：审计日志会对用户操作进行详细的记录并提供导出功能，通过这些事件您可以判断账号是否存在风险。
- 实时记录：迅速收集操作事件，用户操作后可在审计日志列表进行追溯，随时发现可疑行为。
- 方便可靠：审计日志支持手动清理和自动清理两种方式，可根据您的存储大小配置清理策略。

下载和导出审计日志

1. 使用具有 `Admin` 或 `Audit Owner` 角色的用户登录 Web 控制台。

Copyright © 2016 - 2023 DaoCloud

2. 点击左侧导航栏底部的 全局管理 。

3. 导航至全局管理下的审计日志，选择 审计日志 。

4. 在 审计日志 下，选择时间范围，点击 导出 ，下载审计日志到本地。
5. 在 审计日志 下，点击 设置 ，配置以下信息完成清理审计日志策略的配置。

- 点击 清理全局管理审计日志 卡片中的 手动清理 -> 立即清理 按钮，输入清理天数，点击 立即清理 按钮，系统将自动清理该天数前的审计日志。 建议清理前先导出并保存。
- 点击 清理全局管理审计日志 卡片中的自动清理-设置按钮，输入最长保存时间，点击 确定 ，系统将自动清理该时间以外的所有日志。建议清理前先导出并保存。

6. 审计日志中与 Kubernetes 相关的日志记录由可观测性模块提供，为减轻审计日志的存储压力，全局管理默认不采集 Kubernetes 相关日志。 如需记录请先前往 xxxxx 开启该服务。开启后的清理功能与全局管理的清理功能一致，但互不影响。

Copyright © 2016 - 2023 DaoCloud

5.2 登录

用户在使用一个新系统前，在这个系统中是没有任何数据的，系统也无法识别这个新用户。为了标识用户身份、绑定用户数据，用户需要一个能唯一标识用户身份的帐号。

DCE 5.0 在 `用户与访问控制` 中通过管理员创建新用户的方式为用户分配一个附有一定权限的账号。该用户产生的所有行为都将关联到自己的帐号。

用户通过账号/密码进行登录，系统验证身份是否合法，如果验证合法，则用户成功登录。

!!! note

```
如果用户登录后 2 小时内无任何操作，将自动退出登录状态。如果登录的用户始终活跃，将持续处于登录状态。
```

用户登录的简单流程如下图。

```
graph TB

user[输入用户名] --> pass[输入密码] --> judge([点击登录并校验用户名和密码])
judge -.正确.->success[登录成功]
judge -.错误.->fail[提示错误]

classDef plain fill:#ddd,stroke:#fff,stroke-width:1px,color:#000;
classDef k8s fill:#326ce5,stroke:#fff,stroke-width:1px,color:#fff;
classDef cluster fill:#fff,stroke:#bbb,stroke-width:1px,color:#326ce5;

class user,pass cluster;
class judge plain
class success,fail k8s
```

用户登录界面如下图。具体登录画面，请与实际产品为准。

Copyright © 2016 - 2023 DaoCloud

Copyright © 2016 - 2023 DaoCloud

5.3 开启/关闭审计日志

默认 Kubernetes 集群不会输出审计日志信息。通过以下配置，可以开启 Kubernetes 的审计日志功能。

1. 准备审计日志的 Policy 文件
2. 配置 API 服务器，开启审计日志
3. 重启并验证

准备审计日志 Policy 文件

??? note "点击查看审计日志 Policy YAML 文件"

```yaml  title="policy.yaml"
apiVersion: audit.k8s.io/v1
kind: Policy
# Don't generate audit events for all requests in RequestReceived stage.
omitStages:
  - "ResponseStarted"
  - "RequestReceived"
  - "Panic"
rules:
  # The following requests were manually identified as high-volume and low-risk,
  # so drop them.
  - level: None
    users: ["system:kube-proxy"]
    verbs: ["watch"]
    resources:
      - group: "" # core
        resources: ["endpoints", "services", "services/status"]
  - level: None
    # Ingress controller reads `configmaps/ingress-uid` through the unsecured port.
    # TODO(#46983): Change this to the ingress controller service account.
    users: ["system:unsecured"]
    namespaces: ["kube-system"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["configmaps"]
  - level: None
    users: ["kubelet"] # legacy kubelet identity
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes", "nodes/status"]
  - level: None
    userGroups: ["system:nodes"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["nodes", "nodes/status"]
  - level: None
    users:
      - system:kube-controller-manager
      - system:kube-scheduler
      - system:serviceaccount:kube-system:endpoint-controller
    verbs: ["get", "update"]
    namespaces: ["kube-system"]
    resources:
      - group: "" # core
        resources: ["endpoints"]
  - level: None
    users: ["system:apiserver"]
    verbs: ["get"]
    resources:
      - group: "" # core
        resources: ["namespaces", "namespaces/status", "namespaces/finalize"]
  # Don't log HPA fetching metrics.
  - level: None
    users:
      - system:kube-controller-manager
    verbs: ["get", "list"]
    resources:
      - group: "metrics.k8s.io"
  # Don't log these read-only URLs.
  - level: None
    nonResourceURLs:
      - /healthz*
      - /version
      - /swagger*
  # Don't log events requests.
  - level: None
    resources:
      - group: "" # core
```


Copyright © 2016 - 2023 DaoCloud

```
      resources: ["events"]

  # new start
  # 忽略所有访问非认证端口的 API，通常是系统组件如 Kube-Controller 等。
  - level: None
    users: ["system:unsecured"]

  # 忽略 kube-admin 的审计日志
  - level: None
    users: ["kube-admin"]
  # 忽略所有资源状态更新的 API need add
  - level: None
    resources:
    - group: "" # core
      resources: ["events", "nodes/status", "pods/status", "services/status"]
    - group: "authorization.k8s.io"
      resources: ["selfsubjectrulesreviews"]
  # 忽略leases need add
  - level: None
    resources:
    - group: "coordination.k8s.io"
      resources: ["leases"]
  - level: Request
    verbs: ["create", "update", "patch", "delete"]
    users: ["kube-admin"]
  #new end

  # Secrets, ConfigMaps, and TokenReviews can contain sensitive & binary data,
  # so only log at the Metadata level.
  - level: Metadata
    resources:
      - group: "" # core
        resources: ["secrets", "configmaps"]
      - group: authentication.k8s.io
        resources: ["tokenreviews"]
    omitStages:
      - "RequestReceived"
  # Get responses can be large; skip them.
  - level: Request
    verbs: ["get", "list", "watch"]
    resources:
      - group: "" # core
      - group: "admissionregistration.k8s.io"
      - group: "apiextensions.k8s.io"
      - group: "apiregistration.k8s.io"
      - group: "apps"
      - group: "authentication.k8s.io"
      - group: "authorization.k8s.io"
      - group: "autoscaling"
      - group: "batch"
      - group: "certificates.k8s.io"
      - group: "extensions"
      - group: "metrics.k8s.io"
      - group: "networking.k8s.io"
      - group: "policy"
      - group: "rbac.authorization.k8s.io"
      - group: "settings.k8s.io"
      - group: "storage.k8s.io"
    omitStages:
      - "RequestReceived"
  # Default level for known APIs
  - level: RequestResponse
    resources:
      - group: "" # core
      - group: "admissionregistration.k8s.io"
      - group: "apiextensions.k8s.io"
      - group: "apiregistration.k8s.io"
      - group: "apps"
      - group: "authentication.k8s.io"
      - group: "authorization.k8s.io"
      - group: "autoscaling"
      - group: "batch"
      - group: "certificates.k8s.io"
      - group: "extensions"
      - group: "metrics.k8s.io"
      - group: "networking.k8s.io"
      - group: "policy"
      - group: "rbac.authorization.k8s.io"
      - group: "settings.k8s.io"
      - group: "storage.k8s.io"
    omitStages:
      - "RequestReceived"
  # Default level for all other requests.
  - level: Metadata
    omitStages:
      - "RequestReceived"
```

将以上审计日志文件放到 `/etc/kubernetes/audit-policy/` 文件夹下，并取名为 `apiserver-audit-policy.yaml`。

Copyright © 2016 - 2023 DaoCloud

配置 API 服务器

打开 API 服务器的配置文件 kube-apiserver.yaml，一般会在 `/etc/kubernetes/manifests/` 文件夹下，并添加以下配置信息：

这一步操作前请备份 kube-apiserver.yaml，并且备份的文件不能放在 `/etc/kubernetes/manifests/` 下，建议放在 `/etc/kubernetes/tmp`。

1. 在 `spec.containers.command` 下添加命令：

```yaml
--audit-log-maxage=30
--audit-log-maxbackup=1
--audit-log-maxsize=100
--audit-log-path=/var/log/audit/kube-apiserver-audit.log
--audit-policy-file=/etc/kubernetes/audit-policy/apiserver-audit-policy.yaml
```

2. 在 `spec.containers.volumeMounts` 下添加：

```yaml
- mountPath: /var/log/audit
  name: audit-logs
- mountPath: /etc/kubernetes/audit-policy
  name: audit-policy
```

3. 在 `spec.volumes` 下添加：

```yaml
- hostPath:
    path: /var/log/kubernetes/audit
    type: ""
  name: audit-logs
- hostPath:
    path: /etc/kubernetes/audit-policy
    type: ""
  name: audit-policy
```

测试并验证

稍等一会，API 服务器会自动重启，在 `/var/log/kubernetes/audit` 目录下查看是否有审计日志生成。

如果想关闭，去掉 `spec.containers.command` 中的相关命令即可。

开启审计日志的采集

通过 FluentBit 来采集审计日志。默认 FluentBit 不会采集 `/var/log/kubernetes/audit` 下的日志文件（Kubernetes 审计日志）。

Copyright © 2016 - 2023 DaoCloud

如需开启审计日志，按以下步骤操作：

1. 保存当前 value

   `shell`
   `helm get values insight-agent -n insight-system -o yaml > insight-agent-values-bak.yaml`

2. 获取当前版本号 ${insight_version_code}，然后更新配置

   `shell`
   `insight_version_code=`helm list -n insight-system |grep insight-agent | awk {'print $10'}`

   `shell`
   `helm upgrade --install --create-namespace --version ${insight_version_code} --cleanup-on-fail insight-agent insight-release/insight-agent -n insight-system -f insight-agent-values-bak.yaml --set global.exporters.auditLog.kubeAudit.enabled=true`

   如果因为版本未找到而升级失败，请检查命令中使用的 helm repo 是否有这个版本。 若没有，请尝试更新 helm repo 后重试。

   `shell`
   `helm repo update insight-release`

3. 重启所有 Pod

   重启所有 master 节点的 FluentBit Pod，重启后的 FluentBit 将会采集 `/var/log/kubernetes/audit` 下的日志。

禁用审计日志的采集

如需禁用 K8s 审计日志，按以下步骤操作：

1. 保存当前 value

   `shell`
   `helm get values insight-agent -n insight-system -o yaml > insight-agent-values-bak.yaml`

2. 获取当前版本号 ${insight_version_code}，然后更新配置

   `shell`
   `insight_version_code=`helm list -n insight-system |grep insight-agent | awk {'print $10'}`

   与开启相比，以下这条命令只是将 true 改为了 false。

   `shell`
   `helm upgrade --install --create-namespace --version ${insight_version_code} --cleanup-on-fail insight-agent insight-release/insight-agent -n insight-system -f insight-agent-values-bak.yaml --set global.exporters.auditLog.kubeAudit.enabled=false`

   如果因为版本未找到而升级失败，请检查命令中使用的 helm repo 是否有这个版本。 若没有，请尝试更新 helm repo 后重试。

   `shell`
   `helm repo update insight-release`

3. 重启所有 Pod

   重启所有 master 节点的 FluentBit Pod，重启后的 FluentBit 将不再采集 `/var/log/kubernetes/audit` 下的日志。

!!! note

```
此外，如果想停止全局管理的审计日志采集，可以执行 `kubectl edit cm insight-agent-fluent-bit-config -n insight-system`，删除以下 INPUT 即可：

```console
[INPUT]
Name                tail
Tag                 audit_log.ghippo.*
Parser              docker
Path                /var/log/containers/*_ghippo-system_audit-log*.log
DB                  /run/flb_audit.db
Mem_Buf_Limit       15MB
Buffer_Chunk_Size   1MB
Buffer_Max_Size     5MB
#DB.Sync            Normal
Refresh_Interval    10
```
```

Copyright © 2016 - 2023 DaoCloud

5.4 密码重置

如果您忘记密码，可以按本页面说明重置密码。

Copyright © 2016 - 2023 DaoCloud

重置密码步骤

管理员最初创建一个用户时，会为其设置用户名和密码。 该用户登录后，在 `个人中心` 填写邮箱并修改密码。 若该用户未设置邮箱，则只能联系管理员进行密码重置。

Copyright © 2016 - 2023 DaoCloud

1. 如果用户忘记了密码，可以在登录界面点击 忘记密码 。

2. 输入用户名，点击 提交 。

   为防止滥发邮件，点击 提交 后，该按钮将变灰并显示一个为期 1 分钟的倒计时。 如果 1 分钟后还未收到邮件，请再次点击此按钮。

Copyright © 2016 - 2023 DaoCloud

3. 在邮箱中找到密码重置邮件，点击 `密码重置` 按钮。

Copyright © 2016 - 2023 DaoCloud

邮件名称：DaoCloud Enterprise-密码重置

DCE LOGO

用户密码重置

尊敬的用户您好！

请点击以下链接，完成密码重置。

密码重置

或者复制以下链接到浏览器中完成验证：

http://qwefgertbvsaghuryea

此致

DaoCloud Enterprise团队

4. 按照屏幕提示，设置新密码，点击 `确定` 。设置新密码的要求与创建用户时的密码规则一致。

Copyright © 2016 - 2023 DaoCloud

5. 屏幕提示密码修改成功。

Copyright © 2016 - 2023 DaoCloud

重置密码流程

整个密码重置的流程示意图如下。

```
graph TB

pass[忘记密码] --> usern[输入用户名]
--> button[点击发送验证邮件的按钮] --> judge1[判断用户名是否正确]

    judge1 -.正确.-> judge2[判断是否绑定邮箱]
    judge1 -.错误.-> tip1[提示用户名不正确]

        judge2 -.已绑定邮箱.-> send[发送重置邮件]
        judge2 -.未绑定邮箱.-> tip2[提示未绑定邮箱<br>联系管理员重置密码]

send --> click[点击邮件中的链接] --> reset[重置密码]
--> success[成功重置密码]

classDef plain fill:#ddd,stroke:#fff,stroke-width:1px,color:#000;
classDef k8s fill:#326ce5,stroke:#fff,stroke-width:1px,color:#fff;
classDef cluster fill:#fff,stroke:#bbb,stroke-width:1px,color:#326ce5;

class pass,usern,button,tip1,send,tip2,send,click,reset,success plain;
class judge1,judge2 k8s
```


Copyright © 2016 - 2023 DaoCloud

5.5 Access control

全局管理模式

适用场景

如果您需要为子模块设置管理员，通过管理员进一步管理用户/用户组权限，那么可以通过用户与访问控制中的角色实现。拥有该角色表示拥有该子模块的最高管理权限。

!!! note

```
权限管理有三种模式，当前为全局管理模式。用户与访问控制中的角色代表各个子模块的最高权限。具体查看[权限管理](role.md)。
```

```
graph TB

gadmin[平台管理员] --> control[用户与访问控制] --> create[创建用户/用户组以及授权角色]
create --> admin[Admin]
create --> iam[IAM Owner]
create --> audit[Audit Owner]
create --> rm[RM Owner]
create --> kpanda[Kpanda Owner]

classDef plain fill:#ddd,stroke:#fff,stroke-width:1px,color:#000;
classDef k8s fill:#326ce5,stroke:#fff,stroke-width:1px,color:#fff;
classDef cluster fill:#fff,stroke:#bbb,stroke-width:1px,color:#326ce5;

class gadmin,control,create,admin,iam,audit,rm,kpanda k8s
```

一个角色对应一组权限。权限决定了可以对资源执行的操作。向用户授予某角色，即授予该角色所包含的所有权限。

用户与访问控制角色

在用户与访问控制中预定义了 4 个角色，分别是：Admin、IAM Owner、Audit Owner 和 Kpanda Owner。这 4 个角色由系统创建，用户只能使用不能修改。角色对应的权限如下：

角色名称	角色类型	所属模块	角色权限
Admin	系统角色	全部	平台管理员，管理所有平台资源，代表平台的最高权限
IAM Owner	系统角色	用户与访问控制	用户与访问控制的管理员，拥有该服务下的所有权限，如管理用户/用户组及授权
Audit Owner	系统角色	审计日志	审计日志的管理员，拥有该服务下的所有权限，如设置审计日志策略，导出审计日志
Kpanda Owner	系统角色	容器管理	容器管理的管理员，拥有该服务下的所有权限，如创建/接入集群，部署应用，给用户/用户组授予集群/命名空间相关的权限

Copyright © 2016 - 2023 DaoCloud

用户组

用户组是用户的集合，用户可以通过加入用户组，继承用户组的角色权限。通过用户组批量地给用户进行授权，可以更好地管理用户及其权限。

适用场景

当用户权限发生变化时，只需将其移到相应的用户组下，不会对其他用户产生影响。

当用户组的权限发生变化时，只需修改用户组的角色权限，即可应用到组内的所有用户。

创建用户组

前提：拥有平台管理员 Super Admin 权限或者用户与访问控制管理员 IAM Admin 权限。

1. 管理员进入 `用户与访问控制`，选择 `用户组`，进入用户组列表，点击右上方的 `创建用户组`。

2. 在 `创建用户组` 页面填写用户组信息。

3. 点击 `确定`，创建用户组成功，返回用户组列表页面。列表中的第一行是新创建的用户组。

Copyright © 2016 - 2023 DaoCloud

为用户组授权

前提：该用户组已存在。

Copyright © 2016 - 2023 DaoCloud

1. 管理员进入 用户与访问控制 ，选择 用户组 ，进入用户组列表，点击 ... -> 授权 。

2. 在 授权 页面勾选需要的角色权限（可多选）。

3. 点击 确定 完成为用户组的授权。自动返回用户组列表，点击某个用户组，可以查看用户组被授予的权限。

Copyright © 2016 - 2023 DaoCloud

给用户组添加用户

1. 管理员进入 用户与访问控制 ，选择 用户组 进入用户组列表，在某个用户组右侧，点击 `...` -> 添加用户 。

2. 在 添加用户 页面点选需要添加的用户（可多选）。若没有可选的用户，点击 前往创建新用户 ，先前往创建用户，再返回该页面点击 刷新 按钮，显示刚创建的用户。

Copyright © 2016 - 2023 DaoCloud

3. 点击 确定 完成给用户组添加用户。

!!! note

用户组中的用户会继承用户组的权限；可以在用户组详情中查看加入该组的用户。

Copyright © 2016 - 2023 DaoCloud

删除用户组

说明：删除用户组，不会删除组内的用户，但组内用户将无法再继承该组的权限

Copyright © 2016 - 2023 DaoCloud

1. 管理员进入 `用户与访问控制`，选择 `用户组` 进入用户组列表，在某个用户组右侧，点击 `...` -> `删除`。

2. 点击 `移除` 删除用户组。

3. 返回用户组列表，屏幕上方将提示删除成功。

Copyright © 2016 - 2023 DaoCloud

!!! note

说明：删除用户组，不会删除组内的用户，但组内用户将无法再继承该组的权限。

Copyright © 2016 - 2023 DaoCloud

什么是用户与访问控制

IAM（Identity and Access Management，用户与访问控制）是全局管理的一个重要模块，您可以通过用户与访问控制模块创建、管理和销毁用户（用户组），并使用系统角色和自定义角色控制其他用户使用 DCE 平台的权限。

优势

- 简洁流畅

  企业内部的结构和角色可能非常复杂，项目、工作小组及授权的管理都在不断地变化。用户与访问控制采用清晰整洁的页面，打通用户、用户组、角色之间的授权关系，以最短链路实现对用户（用户组）的授权。

- 适当的角色

  用户与访问控制为每个子模块预定义了一个管理员角色，无需用户维护，您可以直接将平台预定义的系统角色授权给用户，实现平台的模块化管理（细粒度权限请参阅[权限管理](../01UserandAccess/role.md)）。

- 企业级访问控制

  当您希望本企业员工可以使用企业内部的认证系统登录 DCE 平台，而不需要在 DCE 平台创建对应的用户，您可以使用用户与访问控制的身份提供商功能，建立您所在企业与 DCE 的信任关系，通过联合认证使员工使用企业已有账号直接登录 DCE 平台，实现单点登录。

使用流程

1. 使用 DCE 平台主账号（Super Admin）或具有管理员权限的用户账号登录 DCE 平台。
2. 创建用户，参见用户。
3. 为用户授权，参见权限管理。
4. 创建用户组，参见用户组。
5. 创建自定义角色，参见自定义角色。

Copyright © 2016 - 2023 DaoCloud

6. 创建身份提供商，参见身份提供商。

Copyright © 2016 - 2023 DaoCloud

身份提供商

全局管理支持基于 LDPA 和 OIDC 协议的单点登录，如果您的企业或组织已有自己的账号体系，同时希望管理组织内的成员使用 DCE 5.0 资源，您可以使用全局管理提供的身份提供商功能，而不必在您的 DCE 5.0 中为每一位组织成员创建用户名/密码。您可以向这些外部用户身份授予使用 DCE 5.0 资源的权限。

基本概念

- 身份提供商（Identity Provider，简称 IdP）

  负责收集和存储用户身份信息、用户名、密码等，在用户登录时负责认证用户的服务。在企业与 DCE 5.0 进行身份认证的过程中，身份提供商指企业自身的身份提供商。

- 服务提供商（Service Provider，简称 SP）

  服务提供商通过与身份提供商 IdP 建立信任关系，使用 IDP 提供的用户信息，为用户提供具体的服务。在企业与 DCE 5.0 进行身份认证的过程中，服务提供商指 DCE 5.0。

- LDAP

  LDAP 指轻型目录访问协议（Lightweight Directory Access Protocol），常用于单点登录，即用户可以在多个服务中使用一个账号密码进行登录。全局管理支持 LDAP 进行身份认证，因此与 DCE 5.0 通过 LDAP 协议建立身份认证的企业 IdP 必须支持 LDAP 协议。关于 LDAP 的详细描述请参见：欢迎使用 LDAP。

- OIDC

  OIDC 是 OpenID Connect 的简称，是一个基于 OAuth 2.0 协议的身份认证标准协议。全局管理支持使用 OIDC 协议进行身份认证，因此与 DCE 5.0 通过 OIDC 协议建立身份认证的企业 IdP 必须支持 OIDC 协议。关于 OIDC 的详细描述请参见：欢迎使用 OpenID Connect。

- OAuth 2.0

  OAuth 2.0 是 Open Authorization 2.0 的简称，是一种开放授权协议，授权框架支持第三方应用程序以自己的名义获取访问权限。

功能特性

- 管理员无需重新创建 DCE 5.0 用户

  使用身份提供商进行身份认证前，管理员需要在企业管理系统和 DCE 5.0 中分别为用户创建账号；使用身份提供商进行身份认证后，企业管理员只需要在企业管理系统中为用户创建账号，用户即可同时访问两个系统，降低了人员管理成本。

- 用户无需记住两套平台账号

  使用身份提供商进行身份认证前，用户访问企业管理系统和 DCE 5.0 需要使用两个系统的账号登录；使用身份提供商进行身份认证后，用户在本企业管理系统中登录即可访问两个系统。

Copyright © 2016 - 2023 DaoCloud

LDAP

LDAP 英文全称为 Lightweight Directory Access Protocol，即轻型目录访问协议，这是一个开放的、中立的工业标准应用协议，通过 IP 协议提供访问控制和维护分布式信息的目录信息。

如果您的企业或组织已有自己的账号体系，同时您的企业用户管理系统支持 LDAP 协议，就可以使用全局管理提供的基于 LDAP 协议的身份提供商功能，而不必在 DCE 5.0 中为每一位组织成员创建用户名/密码。 您可以向这些外部用户身份授予使用 DCE 5.0 资源的权限。

Copyright © 2016 - 2023 DaoCloud

在全局管理中，其操作步骤如下：

Copyright © 2016 - 2023 DaoCloud

1. 使用具有 `admin` 角色的用户登录 Web 控制台。点击左侧导航栏的左上角的 全局管理 。

2. 导航至 全局管理 下的 用户与访问控制 ，选择 创建身份提供商 。

3. 在 `LDAP` 页签中，填写以下字段后点击 保存 ，建立与身份提供商的信任关系及用户的映射关系。

Copyright © 2016 - 2023 DaoCloud

字段	描述	举例值
服务器	LDAP 服务的地址和端口号	10.6.165.2:30061
用户名称	登录 LDAP 服务的用户名	cn=admin,dc=daocloud,dc=io
密码	登录 LDAP 服务的密码	password
基准 DN	LDAP admin 的 DN，用于访问 LDAP 服务器	dc=daocloud,dc=io
用户对象过滤器	LDAP 用户的 LDAP objectClass 新建的用户将与所有这些对象类一起写入 LDAP，并且只要它们包含所有这些对象类，就会找到现在的 LDAP 用户记录。 DCE 5.0 已经帮用户自动填入，如需修改可直接编辑。	inetOrgPerson, organizationalPerson
自动同步	每十分钟自动同步一次。启用后仍可通过手动同步按钮，随时同步用户	勾选
是否启用 TLS	启用后将加密 DCE 5.0 与 LDAP 的连接	否
全名映射	姓-sn；名-cn	不可更改
邮箱映射	mail	不可更改

4. 在 `同步用户组` 页签中，填写以下字段配置用户组的映射关系后，再次点击 `保存`。

Copyright © 2016 - 2023 DaoCloud

字段	描述	举例值
基准 DN	用户组在 LDAP 树状结构中的位置	ou=groups,dc=example,dc=org
用户组对象过滤器	用户组的对象类，如果需要更多类，则用逗号分隔。在典型的 LDAP 部署中，通常是“groupOfNames”，系统已自动填入，如需更改请直接编辑。* 表示所有。	*
用户组名	cn	不可更改

!!! note

```
1. 当您通过 LDAP 协议将企业用户管理系统与 DCE 5.0 建立信任关系后，可通过手动同步或每十分钟自动同步一次的方式，将企业用户管理系统中的用户或用户组一次性同步至 DCE 5.0。
1. 同步后管理员可对用户组/用户组进行批量授权，同时用户可通过在企业用户管理系统中的账号/密码登录 DCE 5.0。
1. 有关实际操作教程，请参阅 [LDAP 操作演示视频](../../../videos/ghippo.md#ldap)。
```


Copyright © 2016 - 2023 DaoCloud

OIDC

OIDC（OpenID Connect）是建立在 OAuth 2.0 基础上的一个身份层，是基于 OAuth2 协议的身份认证标准协议。

如果您的企业或组织已有自己的账号体系，同时您的企业用户管理系统支持 OIDC 协议，可以使用全局管理提供的基于 OIDC 协议的身份提供商功能，而不必在 DCE 5.0 中为每一位组织成员创建用户名/密码。 您可以向这些外部用户身份授予使用 DCE 5.0 资源的权限。

Copyright © 2016 - 2023 DaoCloud

具体操作步骤如下。

Copyright © 2016 - 2023 DaoCloud

1. 使用具有 `admin` 角色的用户登录 Web 控制台。点击左侧导航栏底部的 `全局管理`。

2. 导航至 `全局管理` 下的 `用户与访问控制`，选择 `身份提供商` -> `OIDC`，点击 `创建身份提供商`。

3. 填写表单字段，建立与身份提供商的信任关系后，点击 `保存`。

Copyright © 2016 - 2023 DaoCloud

字段	描述
重定向 URL	重定向到 DCE 5.0 的 URL
提供商名称	显示在登录页上，是身份提供商的入口
认证方式	客户端身份验证方法。如果 JWT 使用私钥签名，请下拉选择 `JWT signed with private key`。具体参阅 Client Authentication。
客户端 ID	客户端的 ID
客户端密钥	客户端密码
客户端 URL	可通过身份提供商 well-known 接口一键获取登录 URL、Token URL、用户信息 URL 和登出 URL
自动关联	开启后当身份提供商用户名/邮箱与 DCE 5.0 用户名/邮箱重复时将自动使二者关联

!!! note

```
1. 当用户通过企业用户管理系统完成第一次登录 DCE 5.0 后，用户信息才会被同步至 DCE 5.0 的`用户与访问控制` -> `用户列表`。
1. 初次登录的用户不会被赋予任何默认权限，需要有管理员给其赋权（管理员可以是平台管理员、子模块管理员或资源管理员）。
1. 有关实际操作教程，请参阅 [OIDC 操作演示视频](../../../videos/ghippo.md#oidc)，也可参考 [Azure OpenID Connect (OIDC) 接入流程](https://learn.microsoft.com/zh-cn/azure/active-directory/develop/v2-protocols-oidc)。
```

用户身份认证交互流程

用户身份认证的交互流程为：

Copyright © 2016 - 2023 DaoCloud

1. 使用浏览器发起单点登录 DCE 5.0 的请求。
2. DCE 5.0 根据登录链接中携带的信息，查找 `全局管理` -> `用户与访问控制` -> `身份提供商` 中对应的配置信息，构建 OIDC 授权 Request，发送给浏览器。
3. 浏览器收到请求后，转发 OIDC 授权 Request 给企业 IdP。
4. 在企业 IdP 的登录页面中输入用户名和密码，企业 IdP 对提供的身份信息进行验证，并构建携带用户信息的 ID Token，向浏览器发送 OIDC 授权 Response。
5. 浏览器响应后转发 OIDC 授权 Response 给 DCE 5.0。
6. DCE 5.0 从 OIDC 授权 Response 中取出 ID Token，并根据已配置的身份转换规则映射到具体的用户列表，颁发 Token。
7. 完成单点登录，访问 DCE 5.0。

Copyright © 2016 - 2023 DaoCloud

角色和权限管理

一个角色对应一组权限。权限决定了可以对资源执行的操作。向用户授予某角色，即授予该角色所包含的所有权限。

权限管理存在以下三种模式，能够灵活、有效地解决您在权限上的使用问题：

- 全局管理模式
- 子模块管理模式
- 基于资源的管理模式

Copyright © 2016 - 2023 DaoCloud

全局管理模式

全局管理模式是指您在全局管理模块通过系统角色给用户（用户组）配置权限的方式。 平台为每个子模块预定义了一个管理员角色，用于实现对子模块的分块化管理。 比如用户与访问控制的 IAM Owner、容器管理的 Kpanda Owner 等，每个子模块管理员均拥有该模块的最高权限。 子模块管理员角色需要在全局管理模块配置，可以通过以下几种途径获得：

Copyright © 2016 - 2023 DaoCloud

- 在 全局管理 -> 用户与访问控制 -> 用户 的用户列表中，找到该用户；点击 ...，选择 授权，为该用户赋予系统预定义的子模块管理员权限。

- 在 全局管理 -> 用户与访问控制 -> 用户组 的用户组列表中创建用户组，将该用户加入用户组，并给用户组授权（具体操作为：在用户组列表找到该用户组，点击 ...，选择 授权，为该用户组赋予系统预定义的子模块管理员权限）。

- 在 全局管理 -> 用户与访问控制 -> 角色 的角色列表中，找到相应的子模块管理员角色，点击角色名称进入详情，点击 关联成员 按钮，选中该用户或用户所在的用户组，点击 确定。

Copyright © 2016 - 2023 DaoCloud

支持此模式的子模块：用户与访问控制（IAM）、审计日志（Audit）、容器管理（Kpanda） 同时，平台的管理员角色（Admin）也可通过以上方式进行授权

Copyright © 2016 - 2023 DaoCloud

!!! note

```
- Admin          平台管理员
- IAM Owner      用户与访问控制模块管理员
- Kpanda Owner   容器管理模块管理员
- Audit Owner    审计日志模块管理员
```

子模块管理模式

子模块管理模式是指您可以通过子模块将不同的资源按需分配给不同的用户，同时对于同一种资源不同的用户也可以拥有不同的使用权限。 平台在子模块中为每个资源预定义了三种角色，分别是 Admin、Editor 和 Viewer。

- Admin 角色对该资源具有管理权限，并且能够将该资源授权给其他人使用；
- Editor 角色对资源具有使用权限，能够编辑、查看资源；
- Viewer 角色对资源仅具有查看权限。

比如容器管理中集群 A 下的 Namespace01 中的 NS Admin 角色能够管理、编辑、查看 Namespace01，并且能够授权给其他用户 NS Admin、NS Editor 和 NS Viewer 角色。 Namespace01 的 NS Editor 角色能够编辑、查看 Namespace01，能够部署应用。 Namespace01 的 Viewer 角色仅能够查看 Namespace01。

支持此模式的子模块：容器管理

您可以在 `容器管理` -> `权限管理`，选择 `添加授权`，为用户/用户组授予 Cluster 或 Namespace 的权限。

!!! note

```
本手册中 Cluster 是指集群；NS 是 Namespace 的缩写，即命名空间。
```

基于资源的管理模式

1. 基于资源的管理模式依赖于工作空间，通过集中统一的访问控制策略，将用户/用户组在工作空间中的角色权限应用到工作空间下的资源上，实现跨子模块授权用户（用户组）对于资源的访问权限。 比如用户 A 在工作空间 01 中是 Workspace Editor 角色，那么对于工作空间 01 下的全部资源，用户 A 都有 Editor 权限。 工作空间通常用于指代一个项目或环境，每个工作空间中的资源相对于其他工作空间中的资源是物理隔离的。 您可以通过工作空间

Copyright © 2016 - 2023 DaoCloud

中的“授权”，授予用户（用户组）同一组资源的不同访问权限。 同时，工作空间中包含不同模块中的多种类型资源，不同类型的资源在工作空间中有不同的呈现方式。

- 模块名称：应用工作台、微服务引擎

  由于这些模块不支持全局管理模式和子模块管理模式的授权方式，仅依靠工作空间来获取授权。 因此所有的资源均在工作空间下创建，创建后资源自动绑定到工作空间上，以确保这些资源在创建后能够被授权使用。 这些资源被创建后，不会自动显示在工作空间的资源组或者共享资源中，仅能够在各个模块的资源列表中呈现。（拥有Workspace的任意角色即可进入上述模块）

- 容器管理

  容器管理支持全局管理模式、子模块管理模式和基于资源的管理三种授权方式。 因此在容器管理模块您可以选择通过用户与访问控制模块授予用户/用户组 Kpanda Owner 角色，或者通过容器管理模块本身的权限管理功能授予用户/用户组某个资源的相应权限，或者通过将资源（cluster 或 Namespace）绑定到工作空间的方式继承用户/用户组在工作空间的角色权限。 由于容器管理中的资源存在绑定和未绑定工作空间两种状态，因此为了区分两种不同的状态，绑定到工作空间中的资源将会在工作空间-资源组中呈现，且工作空间-资源组和容器管理的资源列表均提供了资源的绑定/解绑入口。 （Admin 角色或者 Workspace admin + Kpanda Owner 角色能够进行资源绑定）

- 服务网格

  服务网格由于自身资源的特殊性，也存在绑定和未绑定两种状态。 因此，您可以通过 Admin 角色管理服务网格中的资源，或者将资源（Mesh 或 Mesh-Namespace）绑定到工作空间，使用户/用户组通过工作空间获得服务网格中资源的权限，被绑定的资源将在工作空间的资源组中进行显示。 当前仅服务网格模块提供了资源绑定入口。（Admin 角色能够进行资源绑定）

2. 支持此模式的子模块：应用工作台、微服务引擎、中间件、容器管理、服务网格。
3. 您可以通过 `全局管理` -> `工作空间与层级`，创建工作空间，并在 `工作空间-授权` 中给用户/用户组授予 Workspace Admin、Workspace Editor、Workspace Viewer 角色。

Copyright © 2016 - 2023 DaoCloud

!!! note

资源（Resource）泛指 DCE 平台上通过各个子模块创建的资源，是完成授权的具体数据。通常资源描述一个或多个操作对象，每个子模块拥有其各自的资源和对应的资源定义详情。
如集群、Namespace、网关等。资源的拥有者是主账号 Admin，Admin 具有在各子模块创建/管理/删除资源的权限，普通用户在没有授权的情况下，不会自动拥有资源的访问权限，需要资源拥有者授权。
通常资源拥有者将一组资源加入到某个工作空间，再通过工作空间给用户（用户组）授权，使用户/用户组获得某些资源的操作权限。

Copyright © 2016 - 2023 DaoCloud

用户

用户指的是由平台管理员 Admin 或者用户与访问控制管理员 IAM Admin 在 `全局管理` -> `用户与访问控制` -> `用户` 页面创建的用户，或者通过 LDAP / OIDC 对接过来的用户。 用户名代表账号，用户通过用户名和密码登录 DaoCloud Enterprise 平台。

拥有一个用户账号是用户访问平台的前提。新建的用户默认没有任何权限，例如您需要给用户赋予相应的角色权限，比如在 `用户列表` 或 `用户详情` 授予子模块的管理员权限。 子模块管理员拥有该子模块的最高权限，能够创建、管理、删除该模块的所有资源。 如果用户需要被授予具体资源的权限，比如某个资源的使用权限，请查看资源授权说明。

本页介绍用户的创建、授权、禁用、启用、删除等操作。

Copyright © 2016 - 2023 DaoCloud

创建用户

前提：拥有平台管理员 Admin 权限或者用户与访问控制管理员 IAM Admin 权限。

1. 管理员进入 `用户与访问控制`，选择 `用户`，进入用户列表，点击右上方的 `创建用户`。

2. 在 `创建用户` 页面填写用户名和登录密码。如需一次性创建多个用户，可以点击 `创建用户` 后进行批量创建，一次性最多创建 5 个用户。根据您的实际情况确定是否设置用户在首次登录时重置密码。

3. 点击 `确定`，创建用户成功，返回用户列表页。

!!! note

此处设置的用户名和密码将用于登录平台。

Copyright © 2016 - 2023 DaoCloud

为用户授予子模块管理员权限

前提：该用户已存在。

Copyright © 2016 - 2023 DaoCloud

1. 管理员进入 `用户与访问控制`，选择 `用户`，进入用户列表，点击 `...` -> `授权`。

2. 在 `授权` 页面勾选需要的角色权限（可多选）。

Copyright © 2016 - 2023 DaoCloud

3. 点击 `确定` 完成为用户的授权。

!!! note

在用户列表中，点击某个用户，可以进入用户详情页面。

将用户加入用户组

1. 管理员进入 `用户与访问控制`，选择 `用户`，进入用户列表，点击 `...` -> `加入用户组`。

Copyright © 2016 - 2023 DaoCloud

2. 在 加入用户组 页面勾选需要加入的用户组（可多选）。若没有可选的用户组，点击 创建用户组 创建用户组，再返回该页面点击 刷新 按钮，显示刚创建的用户组。

3. 点击 确定 将用户加入用户组。

!!! note

用户会继承用户组的权限，可以在`用户详情`中查看该用户已加入的用户组。

Copyright © 2016 - 2023 DaoCloud

启用/禁用用户

禁用用户后，该用户将无法再访问平台。与删除用户不同，禁用的用户可以根据需要再次启用，建议删除用户前先禁用，以确保没有关键服务在使用该用户创建的密钥。

1. 管理员进入 `用户与访问控制`，选择 `用户`，进入用户列表，点击一个用户名进入用户详情。

2. 点击右上方的 `编辑`，关闭状态按钮，使按钮置灰且处于未启用状态。

3. 点击 `确定` 完成禁用用户的操作。

Copyright © 2016 - 2023 DaoCloud

忘记密码

前提：需要设置用户邮箱，有两种方式可以设置用户邮箱。

- 管理员在该用户详情页面，点击 `编辑`，在弹出框输入用户邮箱地址，点击 `确定` 完成邮箱设置。

- 用户还可以进入 `个人中心`，在 `安全设置` 页面设置邮箱地址。

如果用户登录时忘记密码，请参考重置密码。

删除用户

!!! warning

```
删除用户后，该用户将无法再通过任何方式访问平台资源，请谨慎删除。
在删除用户之前，请确保您的关键程序不再使用该用户创建的密钥。
```


Copyright © 2016 - 2023 DaoCloud

如果您不确定，建议在删除前先禁用该用户。
如果您删除了一个用户，然后再创建一个同名的新用户，则新用户将被视为一个新的独立身份，它不会继承已删除用户的角色。

1. 管理员进入 用户与访问控制 ，选择 用户 ，进入用户列表，点击 `...` -> 删除 。

2. 点击 移除 完成删除用户的操作。

Copyright © 2016 - 2023 DaoCloud

5.6 Personal center

访问密钥

访问密钥可用于访问开放API和持续发布，用户可在个人中心参照以下步骤获取密钥并访问 API。Ghippo版本≥v0.14请参照该文档，旧版本请参照：访问密钥（Ghippo版本＜v0.14）

获取密钥

登录 DCE 5.0，在右上角的下拉菜单中找到 `个人中心`，可以在 `访问密钥` 页面管理账户的访问密钥。

Copyright © 2016 - 2023 DaoCloud

访问密钥信息仅显示一次。如果您忘记了访问密钥信息，您需要重新创建新的访问密钥。

使用密钥访问 API

在访问 DCE 5.0 openAPI 时，在请求中加上请求头 `Authorization:Bearer ${token}` 以标识访问者的身份，其中 `${token}` 是上一步中获取到的密钥，具体接口信息参见接口文档。

请求示例

```
curl -X GET -H 'Authorization:Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IkRKVjlBTHRBLXZ4MmtQUC1TQnVGS0dCSWc1cnBfdkxiQVVqM2U3RVByWnMiLCJ0eXAiOiJKV1QifQ.eyJleHAiOjE2NjE0MTU5NjksImlhdCI6MTY2MDgxMTE2OSwiaXNzIjoi
_mB1BubvWCBsDdUjIhCQfT39rk6EQozMjb-1X1sbLwzkfzKMls-oxkjagI_RFrYlTVPwT3Oaw-qOyulRSw7Dxd7jb0vINPq84vmlQIsI3UuTZSNO5BCgHpubcWwBss-Aon_DmYA-Et_-
QtmPBA3k8E2hzDSzc7eqK0I68P25r9rwQ3DeKwD1dbRyndqWORRnz8TLEXSiCFXdZT2oiMrcJtO188Ph4eLGut1-4PzKhwgrQ' https://demo-dev.daocloud.io/apis/ghippo.io/v1alpha1/users?
page=1&pageSize=10 -k
```

请求结果

```
{
    "items": [
        {
            "id": "a7cfd010-ebbe-4601-987f-d098d9ef766e",
            "name": "a",
            "email": "",
            "description": "",
            "firstname": "",
            "lastname": "",
            "source": "locale",
            "enabled": true,
            "createdAt": "1660632794800",
            "updatedAt": "0",
            "lastLoginAt": ""
        }
    ],
    "pagination": {
        "page": 1,
        "pageSize": 10,
        "total": 1
    }
}
```


Copyright © 2016 - 2023 DaoCloud

语言设置

本节说明如何设置界面语言。目前支持中文、English 两个语言。

语言设置是平台提供多语言服务的入口，平台默认显示为中文，用户可根据需要选择英语或自动检测浏览器语言首选项的方式来切换平台语言。 每个用户的多语言服务是相互独立的，切换后不会影响其他用户。

平台提供三种切换语言方式：中文、英语-English、自动检测您的浏览器语言首选项。

Copyright © 2016 - 2023 DaoCloud

操作步骤如下。

Copyright © 2016 - 2023 DaoCloud

1. 使用您的用户名/密码登录 Web 控制台。点击左侧导航栏底部的 全局管理 。

2. 点击右上角的用户名位置，选择 个人中心 。

3. 点击 语言设置 页签。

Copyright © 2016 - 2023 DaoCloud

4. 切换语言选项。

Copyright © 2016 - 2023 DaoCloud

访问密钥

每个用户登录或访问资源都需要一个访问密钥。参照以下步骤获取密钥、token 并访问 API。

获取密钥

登录 DCE 5.0，在右上角的下拉菜单中找到 `个人中心`，可以在 `平台设置` 页面管理账户的访问密钥对。

!!! note

```
若进入到该页面中无密钥，则点击`创建密钥`按钮，最多可以创建 2 对密钥。
```

根据密钥对生成 token

!!! note

```
token 有效期默认 3 天，可以在生成时修改参数 `cycle`。
```

生成 token 的请求 URL 为：

```
/api/v1/cube/key/token?ak=&sk=&cycle=
```

Method：GET

描述：根据密钥对生成 token，token 有效期根据 cycle 生成，默认为 3 天。

请求参数

参数名	说明	参数类型	是否必填
ak	密钥对 Ak	string	是
sk	密钥对 Sk	string	是
cycle	生命周期	int	否

返回参数

参数名	说明	参数类型
token	可以用于访问DCE 5.0 OpenAPI的token	string

Copyright © 2016 - 2023 DaoCloud

请求示例

```
curl -X GET 'https://demo-alpha.daocloud.io/apis/ghippo.io/v1alpha1/token?ak=0f70e597-31a7-4e34-a43c-400deadb4109&sk=1718672b-9c40-4538-a129-
d9316a36ddff&cycle=7'
```

请求结果


```
{
  "token":
"eyJhbGciOiJSUzI1NiIsImtpZCI6IkRKVjlBTHRBLXZ4MmtQUC1TQnVGS0dCSWc1cnBfdkxiQVVqM2U3RVByWnMiLCJ0eXAiOiJKV1QifQ.eyJleHAiOjE2NjE0MTU5NjksImlhdCI6MTY2MDgxMTE2OSwiaXNzIjo
_mB1BubvWCBsDdUjIhCQfT39rk6EQozMjb-1X1sbLwzkfzKMls-oxkjagI_RFrYlTVPwT3Oaw-qOyulRSw7Dxd7jb0vINPq84vmlQIsI3UuTZSNO5BCgHpubcWwBss-Aon_DmYA-Et_-
QtmPBA3k8E2hzDSzc7eqK0I68P25r9rwQ3DeKwD1dbRyndqWORRnz8TLEXSiCFXdZT2oiMrcJtO188Ph4eLGut1-4PzKhwgrQ"
}
```


使用 token 访问 API

在访问 DCE 5.0 openAPI 时，在请求中加上请求头 `Authorization:Bearer ${token}` 以标识访问者的身份，其中 `${token}` 是上一步中获取到的 token 值，具体接口信息参见接口文档。

请求示例

```
curl -X GET -H 'Authorization:Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IkRKVjlBTHRBLXZ4MmtQUC1TQnVGS0dCSWc1cnBfdkxiQVVqM2U3RVByWnMiLCJ0eXAiOiJKV1QifQ.eyJleHAiOjE2NjE0MTU5NjksImlhdCI6MTY2MDgxMTE2OSwiaXNzIjoi
_mB1BubvWCBsDdUjIhCQfT39rk6EQozMjb-1X1sbLwzkfzKMls-oxkjagI_RFrYlTVPwT3Oaw-qOyulRSw7Dxd7jb0vINPq84vmlQIsI3UuTZSNO5BCgHpubcWwBss-Aon_DmYA-Et_-
QtmPBA3k8E2hzDSzc7eqK0I68P25r9rwQ3DeKwD1dbRyndqWORRnz8TLEXSiCFXdZT2oiMrcJtO188Ph4eLGut1-4PzKhwgrQ' https://demo-dev.daocloud.io/apis/kpanda.io/v1alpha1/
clusters/kpanda-global-cluster/deployments -k
```

请求结果


```
{
    "items": [
        {
            "id": "a7cfd010-ebbe-4601-987f-d098d9ef766e",
            "name": "a",
            "email": "",
            "description": "",
            "firstname": "",
            "lastname": "",
            "source": "locale",
            "enabled": true,
            "createdAt": "1660632794800",
            "updatedAt": "0",
            "lastLoginAt": ""
        }
    ],
    "pagination": {
        "page": 1,
        "pageSize": 10,
        "total": 1
    }
}
```


Copyright © 2016 - 2023 DaoCloud

安全设置

功能说明：用于填写邮箱地址和修改登录密码。

- 邮箱：当管理员配置邮箱服务器地址之后，用户能够通过登录页的忘记密码按钮，填写该处的邮箱地址以找回密码。
- 密码：用于登录平台的密码，建议定期修改密码。

Copyright © 2016 - 2023 DaoCloud

具体操作步骤如下：

Copyright © 2016 - 2023 DaoCloud

1. 使用您的用户名/密码登录 Web 控制台。点击左侧导航栏底部的 全局管理 。

2. 点击右上角的用户名位置，选择 个人中心 。

3. 点击 安全设置 页签。填写您的邮箱地址或修改登录密码。

Copyright © 2016 - 2023 DaoCloud

Copyright © 2016 - 2023 DaoCloud

5.7 Platform setting

关于平台

关于平台 主要呈现平台各个子模块当前更新的版本，声明了平台使用的各个开源软件，并以动画视频的方式致谢了平台的技术团队。

Copyright © 2016 - 2023 DaoCloud

查看步骤：

Copyright © 2016 - 2023 DaoCloud

1. 使用具有 `Admin` 角色的用户登录 Web 控制台。点击左侧导航栏底部的 `全局管理`。

2. 点击 `平台设置`，选择 `关于平台`，查看产品版本、开源软件声明和技术团队。

产品版本

Copyright © 2016 - 2023 DaoCloud

License 声明

技术团队

Copyright © 2016 - 2023 DaoCloud

Copyright © 2016 - 2023 DaoCloud

外观定制

在 DCE 5.0 中，可通过 外观定制 更换登录界面及顶部导航栏的 logo，帮助用户更好地辨识产品。

定制登录页和顶部导航栏

1. 使用具有 `admin` 角色的用户登录 Web 控制台。点击左侧导航栏底部的 全局管理 -> 平台设置 。

2. 选择 外观定制 。

Copyright © 2016 - 2023 DaoCloud

3. 在 登录页定制 页签中，修改登录页的图标和文字后，点击 保存 。

4. 点击 顶部导航栏定制 页签，修改导航栏的图标和文字后，点击 保存 。

!!! note

如果想要恢复默认设置，可以点击`一键还原`。请注意，一键还原后将丢弃所有自定义设置。

高级定制

高级定制能够通过 CSS 样式来修改整个容器平台的颜色、字体间隔、字号等。 您需要熟悉 CSS 语法。删除黑色输入框的内容，可恢复到默认状态，当然也可以点击 一键还原 按钮。

Copyright © 2016 - 2023 DaoCloud

登录页定制的 CSS 样例：

```
.test {
  width: 12px;
}

#kc-login {
 /* color: red!important; */
}
```

登录后页面定制的 CSS 样例：

```
.dao-icon.dao-iconfont.icon-service-global.dao-nav__head-icon {
   color: red!important;
}
.ghippo-header-logo {
  background-color: green!important;
}
.ghippo-header {
  background-color: rgb(128, 115, 0)!important;
}
.ghippo-header-nav-main {
  background-color: rgb(0, 19, 128)!important;
}
.ghippo-header-sub-nav-main .dao-popper-inner {
  background-color: rgb(231, 82, 13) !important;
}
```


Copyright © 2016 - 2023 DaoCloud

邮件服务器

DCE 5.0 会在用户忘记密码时，向用户发送电子邮件以验证电子邮件地址，确保用户是本人操作。 要使 DCE 5.0 能够发送电子邮件，需要先提供您的邮件服务器地址。

Copyright © 2016 - 2023 DaoCloud

具体操作步骤如下：

Copyright © 2016 - 2023 DaoCloud

1. 使用具有 `admin` 角色的用户登录 Web 控制台。点击左侧导航栏底部的 全局管理 。

2. 点击 平台设置 ，选择 邮件服务器设置 。

Copyright © 2016 - 2023 DaoCloud

填写以下字段配置邮件服务器：

字段	描述	举例值
SMTP 服务器地址	能够提供邮件服务的 SMTP 服务器地址	smtp.163.com
SMTP 服务器端口	发送邮件的端口	25
用户名	SMTP 用户的名称	test@163.com
密码	SMTP 账户的密码	123456
发件人邮箱	发件人的邮箱地址	test@163.com
使用 SSL 安全连接	SSL 可以用于加密邮件，从而提高通过邮件传输的信息的安全性，通常需为邮件服务器配置证书	不开启

3. 配置完成后点击 `保存`，点击 `测试邮件服务器`。

Copyright © 2016 - 2023 DaoCloud

4. 屏幕右上角出现成功发送邮件的提示，则表示邮件服务器被成功设置。

常见问题

问：邮件服务器设置后用户仍无法找回密码是什么原因？

答：用户可能未设置邮箱或者设置了错误的邮箱地址；此时可以让 admin 角色的用户在 `全局管理` -> `用户与访问控制` 中通过用户名找到该用户，并在用户详情中为该用户设置新的登录密码。

如果邮件服务器没有连通，请检查邮件服务器地址、用户名及密码是否正确。

Copyright © 2016 - 2023 DaoCloud

5.8 Workspace

普通用户授权规划

普通用户是指能够使用 DCE 大部分产品模块及功能（管理功能除外），对权限范围内的资源有一定的操作权限，能够独立使用资源部署应用。

对这类用户的授权及资源规划流程如下图所示。

```
graph TB

    start([开始]) --> user[1. 创建用户]
    user --> ns[2. 准备 Kubernetes 命名空间]
    ns --> ws[3. 准备工作空间]
    ws --> ws-to-ns[4. 工作空间绑定命名空间]
    ws-to-ns --> authu[5. 给用户授权 Workspace Editor]
    authu --> complete([结束])

click user "https://docs.daocloud.io/ghippo/user-guide/access-control/user/"
click ns "https://docs.daocloud.io/kpanda/user-guide/namespaces/createns/"
click ws "https://docs.daocloud.io/ghippo/user-guide/workspace/workspace/"
click ws-to-ns "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-to-ns/"
click authu "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-permission/"

 classDef plain fill:#ddd,stroke:#fff,stroke-width:4px,color:#000;
 classDef k8s fill:#326ce5,stroke:#fff,stroke-width:4px,color:#fff;
 classDef cluster fill:#fff,stroke:#bbb,stroke-width:1px,color:#326ce5;
 class user,ns,ws,ws-to-ns,authu cluster;
 class start,complete plain;
```

授权后普通用户在各模块的权限为：

- 应用工作台
- 微服务引擎
- 服务网格（需要重复 2 - 4 准备网格/网格命名空间并绑定到工作空间）
- 可观测性

Copyright © 2016 - 2023 DaoCloud

将集群分配给多个工作空间（租户）

集群资源通常由运维人员进行管理。在分配资源分配时，他们需要创建命名空间来隔离资源，并设置资源配额。 这种方式有个弊端，如果企业的业务量很大，手动分配资源需要较大的工作量，而想要灵活调配资源额度也有不小难度。

DCE 为此引入了工作空间的概念。工作空间通过共享资源可以提供更高维度的资源限额能力，实现工作空间（租户）在资源限额下自助式创建 Kubernetes 命名空间的能力。

举例而言，如果想要让几个部门共享不同的集群。

	Cluster01（普通）	Cluster02（高可用）
部门（工作空间）A	50 quota	10 quota
部门（工作空间）B	100 quota	20 quota

可以参照以下流程将集群分享给多个部门/工作空间/租户：

```
graph TB

preparews[准备工作空间] --> preparecs[准备集群]
--> share[将集群共享到工作空间]
--> judge([判断工作空间剩余额度])
judge -.大于剩余额度.->modifyns[修改命名空间额度]
judge -.小于剩余额度.->createns[创建命名空间]

classDef plain fill:#ddd,stroke:#fff,stroke-width:1px,color:#000;
classDef k8s fill:#326ce5,stroke:#fff,stroke-width:1px,color:#fff;
classDef cluster fill:#fff,stroke:#bbb,stroke-width:1px,color:#326ce5;

class preparews,preparecs,share, cluster;
class judge plain
class modifyns,createns k8s

click preparews "https://docs.daocloud.io/ghippo/user-guide/workspace/cluster-for-multiws/#_2"
click preparecs "https://docs.daocloud.io/ghippo/user-guide/workspace/cluster-for-multiws/#_3"
click share "https://docs.daocloud.io/ghippo/user-guide/workspace/cluster-for-multiws/#_4"
click createns "https://docs.daocloud.io/amamba/user-guide/namespace/namespace/#_3"
click modifyns "https://docs.daocloud.io/amamba/user-guide/namespace/namespace/#_4"
```


Copyright © 2016 - 2023 DaoCloud

准备一个工作空间

工作空间是为了满足多租户的使用场景，基于集群、集群命名空间、网格、网格命名空间、多云、多云命名空间等多种资源形成相互隔离的资源环境，工作空间可以映射为项目、租户、企业、供应商等多种概念。

Copyright © 2016 - 2023 DaoCloud

1. 使用 admin/folder admin 角色的用户登录 Web 控制台，点击左侧导航栏底部的 全局管理 。

2. 点击左侧导航栏的 工作空间与层级 ，点击右上角的 创建工作空间 按钮。

3. 填写工作空间名称、所属文件夹等信息后，点击 确定 ，完成创建工作空间。

Copyright © 2016 - 2023 DaoCloud

准备一个集群

工作空间是为了满足多租户的使用场景，基于集群、集群命名空间、网格、网格命名空间、多云、多云命名空间等多种资源形成相互隔离的资源环境，工作空间可以映射为项目、租户、企业、供应商等多种概念。

参照以下步骤准备一个集群。

1. 点击左侧导航栏底部的 容器管理 ，选择 集群列表 。

2. 点击 创建集群 创建一个集群，或点击 接入集群 接入一个集群。

Copyright © 2016 - 2023 DaoCloud

在工作空间添加集群

返回 全局管理 ，为工作空间添加集群。

1. 依次点击 全局管理 -> 工作空间与层级 -> 共享资源 ，点击某个工作空间名称后，点击 新增共享资源 按钮。

2. 选择集群，填写资源限额后，点击 确定 。

下一步：将集群资源分配给多个工作空间后，用户可以前往 应用工作台 在这些工作空间下创建命名空间并部署应用。

Copyright © 2016 - 2023 DaoCloud

文件夹权限说明

文件夹具有权限映射能力，能够将用户/用户组在本文件夹的权限映射到其下的子文件夹、工作空间以及资源上。

若用户/用户组在本文件夹是 Folder Admin 角色，映射到子文件夹仍为 Folder Admin 角色，映射到其下的工作空间则为 Workspace Admin； 若在 `工作空间与层级 -> 资源组` 中绑定了 Namespace，则映射后该用户/用户组同时还是 Namespace Admin。

!!! note

文件夹的权限映射能力不会作用到共享资源上，因为共享是将集群的使用权限共享给多个工作空间，而不是将管理权限受让给工作空间，因此不会实现权限继承和角色映射。

应用场景

文件夹具有层级能力，因此将文件夹对应于企业中的部门/供应商/项目等层级时，

- 若用户/用户组在一级部门具有管理权限（Admin），其下的二级、三级、四级部门或项目同样具有管理权限；
- 若用户/用户组在一级部门具有使用权限（Editor），其下的二级、三级、四级部门或项目同样具有使用权限；
- 若用户/用户组在一级部门具有只读权限（Viewer），其下的二级、三级、四级部门或项目同样具有只读权限。

对象	操作	Folder Admin	Folder Editor	Folder Viewer
对文件夹本身	查看	&check	&check	&check
	授权	&check	&cross	&cross
	修改别名	&check	&check	&cross
对子文件夹	创建	&check	&cross	&cross
	查看	&check	&check	&check
	授权	&check	&cross	&cross
	修改别名	&check	&check	&cross
对其下的工作空间	创建	&check	&cross	&cross
	查看	&check	&check	&check
	授权	&check	&cross	&cross
	修改别名	&check	&check	&cross
对其下的工作空间 - 资源组	查看	&check	&check	&check
	资源绑定	&check	&cross	&cross
	解除绑定	&check	&cross	&cross
对其下的工作空间 - 共享资源	查看	&check	&check	&check
	新增共享	&check	&cross	&cross
	解除共享	&check	&cross	&cross
	资源限额	&check	&cross	&cross

Copyright © 2016 - 2023 DaoCloud

文件夹最佳实践

文件夹代表一个组织机构（例如一个部门），是资源层次结构中的一个节点。

一个文件夹可以包含工作空间、子文件夹或两者的组合。 它提供了身份管理、多层级和权限映射能力，能够将用户/用户组在文件夹中的角色映射到其下的子文件夹、工作空间和资源上。 因此借助于文件夹，企业管理者能够集中管控所有资源。

1. 构建企业层级关系

   首先要按照现有的企业层级结构，构建与企业相同的文件夹层级。 DCE 支持 5 级文件夹，可以根据企业实际情况自由组合，将文件夹和工作空间映射为企业中的部门、项目、供应商等实体。

   文件夹不直接与资源挂钩，而是通过工作空间间接实现资源分组。

2. 用户身份管理

   文件夹提供了 Folder Admin、Folder Editor、Folder Viewer 三种角色。 查看角色权限，可通过授权给同一文件夹中的用户/用户组授予不同的角色。

3. 角色权限映射

   企业管理者：在根文件夹授予 Folder Admin 角色。他将拥有所有部门、项目及其资源的管理权限。

   部门管理者：在各个子文件夹、工作空间单独授予管理权限。

   项目成员：在工作空间、资源层级单独授予管理权限。

Copyright © 2016 - 2023 DaoCloud

创建/删除文件夹

文件夹具有权限映射能力，能够将用户/用户组在本文件夹的权限映射到其下的子文件夹、工作空间以及资源上。

Copyright © 2016 - 2023 DaoCloud

参照以下步骤创建一个文件夹。

Copyright © 2016 - 2023 DaoCloud

1. 使用 admin/folder admin 角色的用户登录 Web 控制台，点击左侧导航栏底部的 全局管理 。

2. 点击左侧导航栏的 工作空间与层级 ，点击右上角的 创建文件夹 按钮。

3. 填写文件夹名称、上一级文件夹等信息后，点击 确定 ，完成创建文件夹。

Copyright © 2016 - 2023 DaoCloud

!!! tip

```
创建成功后文件夹名称将显示在左侧的树状结构中，以不同的图标表示工作空间和文件夹。

![工作空间和文件夹](../../images/ws04.png)
```

!!! note

```
选中某一个文件夹或文件夹，点击右侧的 `...` 可以进行编辑或删除。

- 当该文件夹下资源组、共享资源中存在资源时，该文件夹无法被删除，需要将所有资源解绑后再删除。

- 当微服务引擎模块在该文件夹下存在接入注册中心资源时，该文件夹无法被删除，需要将所有接入注册中心移除后再删除文件夹。
```


Copyright © 2016 - 2023 DaoCloud

资源限额

共享资源并非意味着被共享者可以无限制地使用被共享的资源。 Admin、Kpanda Owner 和 Workspace Admin 可以通过共享资源中的 资源配额 功能限制某个用户的最大使用额度。 若不限制，则表示可以无限制使用。

- CPU 请求（Core）
- CPU 限制（Core）
- 内存请求（MB）
- 内存限制（MB）
- 存储请求总量（GB）
- 存储卷声明（个）

一个资源（集群）可以被多个工作空间共享，一个工作空间也可以同时使用多个共享集群中的资源。

Copyright © 2016 - 2023 DaoCloud

资源组和共享资源

共享资源和资源组中的集群资源均来自容器管理，但是集群绑定和共享给同一个工作空间将会产生两种截然不同的效果。

Copyright © 2016 - 2023 DaoCloud

1. 绑定资源

   使工作空间中的用户/用户组具有该集群的全部管理和使用权限，Workspace Admin 将被映射为 Cluster Admin。 Workspace Admin 能够进入容器管理模块管理该集群。

!!! note

```
当前容器管理模块暂无 Cluster Editor 和 Cluster Viewer 角色，因此 Workspace Editor、Workspace Viewer 还无法映射。
```

2. 新增共享资源

   使工作空间中的用户/用户组具有该集群资源的使用权限，能够使用资源配额前往应用工作台创建命名空间（Namespace）。

Copyright © 2016 - 2023 DaoCloud

与资源组不同，将集群共享到工作空间时，用户在工作空间的角色不会映射到资源上，因此 Workspace Admin 不会被映射为 Cluster admin。

本节展示 3 个与资源配额有关的场景。

Copyright © 2016 - 2023 DaoCloud

创建命名空间

创建命名空间时会涉及到资源配额。

1. 在工作空间 ws01 新增一个共享集群。

2. 在应用工作台选择工作空间 ws01 和共享集群，创建命名空间 ns01。

- 若在共享集群中未设置资源配额，则创建命名空间时可不设置资源配额。
- 若在共享集群中已设置资源配额（例如 CPU 请求 = 100 core），则创建命名空间时 `CPU 请求 ≤ 100 core`。

Copyright © 2016 - 2023 DaoCloud

命名空间绑定到工作空间

前提：工作空间 ws01 已新增共享集群，操作者为 Workspace Admin + Kpanda Owner 或 Admin 角色。

以下两种绑定方式的效果相同。

- 在容器管理中将创建的命名空间 ns01 绑定到 ws01

- 若在共享集群未设置资源配额，则命名空间 ns01 无论是否已设置资源配额，均可成功绑定。
- 若在共享集群已设置资源配额 `CPU 请求 = 100 core`，则命名空间 ns01 必须满足 `CPU 请求 ≤ 100 core` 才能绑定成功。
- 在全局管理中，将命名空间 ns01 绑定到 ws01

- 若在共享集群未设置资源配额，则命名空间 ns01 无论是否已设置资源配额，均可成功绑定。
- 若在共享集群已设置资源配额 `CPU 请求 = 100 core`，则命名空间 ns01 必须满足 `CPU 请求 ≤ 100 core` 才能绑定成功。

Copyright © 2016 - 2023 DaoCloud

从工作空间解绑命名空间

以下两种解绑方式的效果相同。

- 在容器管理中将命名空间 ns01 从工作空间 ws01 解绑

- 若在共享集群中未设置资源配额，则命名空间 ns01 无论是否已设置资源配额，解绑后均不会对资源配额产生影响。
- 若在共享集群已设置资源配额 `CPU 请求 = 100 core`，命名空间 ns01 也设置了资源配额，则解绑后将释放相应的资源额度。
- 在全局管理中将命名空间 ns01 从工作空间 ws01 解绑

- 若在共享集群未设置资源配额，则命名空间 ns01 无论是否已设置资源配额，解绑后均不会对资源配额产生影响。
- 若在共享集群已设置资源配额 `CPU 请求 = 100 core`，命名空间 ns01 也设置了资源配额，则解绑后将释放相应的资源额度。

Copyright © 2016 - 2023 DaoCloud

创建/删除工作空间

工作空间是一种资源范畴，代表一种资源层级关系。 工作空间可以包含集群、命名空间、注册中心等资源。 通常一个工作空间对应一个项目，可以为每个工作空间分配不同的资源，指派不同的用户和用户组。

Copyright © 2016 - 2023 DaoCloud

参照以下步骤创建一个工作空间。

Copyright © 2016 - 2023 DaoCloud

1. 使用 admin/folder admin 角色的用户登录 Web 控制台，点击左侧导航栏底部的 全局管理 。

2. 点击左侧导航栏的 工作空间与层级 ，点击右上角的 创建工作空间 按钮。

3. 填写工作空间名称、所属文件夹等信息后，点击 确定 ，完成创建工作空间。

Copyright © 2016 - 2023 DaoCloud

```
!!! tip

创建成功后工作空间名称将显示在左侧的树状结构中，以不同的图标表示文件夹和工作空间。

![文件夹与工作空间](../../images/ws04.png)
```

```
!!! note

选中某一个工作空间或文件夹，点击右侧的 `...` 可以进行编辑或删除。

- 当该工作空间下资源组、共享资源中存在资源时，该工作空间无法被删除，需要将所有资源解绑后再删除。

- 当微服务引擎模块在该工作空间下存在接入注册中心资源时，该工作空间无法被删除，需要将所有接入注册中心移除后再删除工作空间。
```


Copyright © 2016 - 2023 DaoCloud

工作空间最佳实践

工作空间是一种资源分组单元，大多数资源都可以绑定到某一个工作空间中。 而工作空间通过授权和资源绑定，能够实现用户与角色的绑定关系，并一次性应用到工作空间的所有资源上。

通过工作空间，可以轻松管理团队与资源，解决跨模块、跨集群的资源授权问题。

工作空间的功能

工作空间包含三个功能：授权、资源组和共享资源。主要解决资源统一授权、资源分组及资源配额问题。

Copyright © 2016 - 2023 DaoCloud

Copyright © 2016 - 2023 DaoCloud

1. 授权：为用户/用户组授予该工作空间的不同角色，并将角色应用到工作空间的资源上。

   最佳实践：普通用户想要使用应用工作台、微服务引擎、服务网格、中间件模块功能，或者需要拥有容器管理、服务网格中部分资源的使用权限时，需要管理员授予该工作空间的使用权限（Workspace Admin、Workspace Edit、Workspace View）。 这里的管理员可以是 Admin 角色、该工作空间的 Workspace Admin 角色或该工作空间上层的 Folder Admin 角色。 查看 Folder 与 Workspace 的关系。

2. 资源组：资源组和共享资源是工作空间的两种资源管理模式。

   资源组支持 Cluster、Cluster-Namespace (跨集群)、Mesh、Mesh-Namespace 四种资源类型。 一个资源只能绑定一个资源组，资源被绑定到资源组后，工作空间的所有者将拥有该资源的所有管理权限，相当于该资源的所有者，因此不受资源配额的限制。

   最佳实践：工作空间通过“授权”功能可以给部门成员授予不同角色权限，而工作空间能够把人与角色的授权关系一次性应用到工作空间的所有资源上。因此运维人员只需将资源绑定到资源组，将部门中的不同角色加入不同的资源组，就能确保资源的权限被正确分配。

部门	角色	集群 Cluster	跨集群 Cluster-Namespace	Mesh	Mesh-Namespace
部门管理员	Workspace Admin	&check	&check	&check	&check
部门核心成员	Workspace Edit	&check	&cross	&check	&cross
其他成员	Workspace View	&check	&cross	&cross	&cross

3. 共享资源：共享资源功能主要针对集群资源。

   一个集群可以共享给多个工作空间（指工作空间中的共享资源功能）；一个工作空间也可以同时使用多个集群的资源。 但是资源共享不意味着被共享者（工作空间）可以无限制地使用共享的资源（集群），因此通常会限制共享者（工作空间）能够使用的资源限额。

   同时，与资源组不同，工作空间成员只是共享资源的使用者，能够在资源限额下使用集群中的资源。比如前往应用工作台创建命名空间、部署应用等，但并不具备集群的管理权限，限制后在该工作空间下创建/绑定的命名空间的资源配额总和不能超过集群在该工作空间设置的资源使用上限。

   最佳实践：运维部门手中有一个高可用集群 01，想要分配给部门 A（工作空间 A）和部门 B（工作空间 B）使用，其中部门 A 分配 CPU 50 核，部门 B 分配 CPU 100 核。 那么可以借用共享资源的概念，将集群 01 分别共享给部门 A 和部门 B，并限制部门 A 的 CPU 使用额度为 50，部门 B 的 CPU 使用额度为 100。 那么部门 A 的管理员（工作空间 A Admin）能够在应用工作台创建并使用命名空间，其中命名空间额度总和不能超过 50 核，部门 B 的管理员（工作空间 B Admin）能够在应用工作台创建并使用命名空间，其中命名空间额度总和不能超过 100 核。 部门 A 的管理员和部门 B 管理员创建的命名空间会被自动绑定在该部门，部门中的其他成员将对应的拥有命名空间的 Namesapce Admin、Namesapce Edit、Namesapce View 角色（这里部门指的是工作空间，工作空间还可以映射为组织、供应商等其他概念）。整个过程如下表：

部门	角色	集群 Cluster	资源配额
部门管理员 A	Workspace Admin	CPU 50 核	CPU 50 核
部门管理员 B	Workspace Admin	CPU 100 核	CPU 100 核
部门其他成员	Namesapce Admin Namesapce Edit Namesapce View	按需分配	按需分配

工作空间对 DCE 模块的作用

1. 模块名称：应用工作台、微服务引擎

   进入上述几个模块的前提是拥有某个工作空间的权限，因此在使用模块功能前必须具有 Admin 角色或者拥有某个工作空间的一定角色权限。

- 工作空间的角色会自动应用到工作空间包含的资源上。比如当您拥有工作空间 A 的 Workspace Admin 角色，那么对于该工作空间中的所有资源您都是 Admin 角色；
- 如果您是 Workspace Edit，那么对于工作空间中的所有资源您都是 Edit 角色；
- 如果您是 Workspace View，那么对于工作空间中的所有资源您都是 View 角色。

   另外，您在这些模块创建的资源也将自动被绑定到对应的工作空间中，而不需要其他额外的操作。

2. 模块名称：容器管理、服务网格

   由于功能模块的特殊性，在容器管理模块创建的资源不会自动被绑定到某个工作空间。

   如果您需要通过工作空间对人和资源进行统一授权管理，可以手动将需要的资源绑定到某个工作空间中，从而将用户在该工作空间的角色应用到资源上（这里的资源是可以跨集群的）。

Copyright © 2016 - 2023 DaoCloud

另外，在资源的绑定入口上容器管理与服务网格稍有差异，工作空间提供了容器管理中的 Cluster 和 Cluster-Namesapce 资源的绑定入口，但尚未开放对服务网格的 Mesh 和 Mesh-Namespace 资源的绑定。

对于 Mesh 和 Mesh-Namespace 资源，可以在服务网格的资源列表进行手动绑定。

工作空间的使用场景

- 映射为不同的部门、项目、组织等概念，同时可以将工作空间中 Workspace Admin、Workspace Edit 和 Workspace View 角色对应到部门、项目、组织中的不同角色
- 将不同用途的资源加入不同的工作空间中分开管理和使用
- 为不同工作空间设置完全独立的管理员，实现工作空间范围内的用户与权限管理
- 将资源共享给不同的工作空间使用，并限制工作空间能够使用的资源额度上限

Copyright © 2016 - 2023 DaoCloud

工作空间与层级

工作空间与层级 是一个具有层级的资源隔离和资源分组特性，主要解决资源统一授权、资源分组以及资源限额问题。

工作空间与层级 有两个概念：工作空间和文件夹。

工作空间

工作空间可通过 授权 、 资源组 和 共享资源 来管理资源，使用户（用户组）之间能够共享工作空间中的资源。

Copyright © 2016 - 2023 DaoCloud

- 资源

  资源处于资源管理模块层级结构的最低层级，资源包括 Cluster、Namespace、Pipeline、网关等。 所有这些资源的父级只能是工作空间，而工作空间作为资源容器是一种资源分组单位。

- 工作空间

  工作空间通常代指一个项目或环境，每个工作空间的资源相对于其他工作空间中的资源时逻辑隔离的。 您可以通过工作空间中的授权，授予用户（用户组）同一组资源的不同访问权限。

  从层次结构的底层算起，工作空间位于第一层，且包含资源。 除共享资源外，所有资源有且仅有一个父项。所有工作空间也有且仅有一个父级文件夹。

  资源通过工作空间进行分组，而工作空间中存在两种分组模式，分别是 `资源组` 和 `共享资源` 。

- 资源组

  一个资源只能加入一个资源组，资源组与工作空间一一对应。 资源被加入到资源组后，Workspace Admin 将获得资源的管理权限，相当于该资源的所有者。

- 共享资源

  而对于共享资源来说，多个工作空间可以共享同一个或者多个资源。 资源的所有者，可以选择将自己拥有的资源共享给工作空间使用，一般共享时资源所有者会限制被共享工作空间能够使用的资源额度。 资源被共享后，Workspace Admin 仅具有资源限额下的资源使用权限，无法管理资源或者调整工作空间能够使用的资源量。

  同时共享资源对于资源本身也具有一定的要求，只有 Cluster（集群）资源可以被共享。 Cluster Admin 能够将 Cluster 资源分享给不同的工作空间使用，并且限制工作空间在此 Cluster 上的使用额度。

  Workspace Admin 在资源限额内能够创建多个 Namespace，但是 Namespace 的资源额度总和不能超过 Cluster 在该工作空间的资源限额。 对于 Kubernetes 资源，当前能够分享的资源类型仅有 Cluster。

Copyright © 2016 - 2023 DaoCloud

文件夹

文件夹可用于构建企业业务层级关系。

- 文件夹是在工作空间基础之上的进一步分组机制，具有层级结构。 一个文件夹可以包含工作空间、其他文件夹或两者的组合，能够形成树状的组织关系。
- 借助文件夹您可以映射企业业务层级关系，按照部门对工作空间进行分组。 文件夹不直接与资源挂钩，而是通过工作空间间接实现资源分组。
- 文件夹有且仅有一个父级文件夹，而根文件夹是层次结构的最高层级。 根文件夹没有父级，文件夹和工作空间均挂靠到根文件夹下。

另外，用户（用户组）在文件夹中能够通过层级结构继承来自于父项的权限。 用户在层次结构中的权限来自当前层级的权限以及继承其父项权限的组合结果，权限之间是加合关系不存在互斥。

Copyright © 2016 - 2023 DaoCloud

工作空间权限说明

工作空间具有权限映射和资源隔离能力，能够将用户/用户组在工作空间的权限映射到其下的资源上。 若用户/用户组在工作空间是 Workspace Admin 角色，同时工作空间-资源组中绑定了资源 Namespace，则映射后该用户/用户组将成为 Namespace Admin。

!!! note

```
工作空间的权限映射能力不会作用到共享资源上，因为共享是将集群的使用权限共享给多个工作空间，而不是将管理权限受让给工作空间，因此不会实现权限继承和角色映射。
```

应用场景

通过将资源绑定到不同的工作空间能够实现资源隔离。 因此借助权限映射、资源隔离和共享资源能力能够将资源灵活分配给各个工作空间（租户）。

通常适用于以下两个场景：

- 集群一对一

普通集群	部门/租户（工作空间）	用途
集群 01	A	管理和使用
集群 02	B	管理和使用

- 集群一对多

集群	部门/租户（工作空间）	资源限额
集群 01	A	100 核 CPU
	B	50 核 CPU

权限说明

操作对象	操作	Workspace Admin	Workspace Editor	Workspace Viewer
本身	查看	&check	&check	&check
-	授权	&check	&cross	&cross
-	修改别名	&check	&check	&cross
资源组	查看	&check	&check	&check
-	资源绑定	&check	&cross	&cross
-	解除绑定	&check	&cross	&cross
共享资源	查看	&check	&check	&check
-	新增共享	&check	&cross	&cross
-	解除共享	&check	&cross	&cross
-	资源限额	&check	&cross	&cross
-	使用共享资源 ^1	&check	&cross	&cross

```
有关 Workspace Admin、Workspace Editor、Workspace Viewer 角色在各产品模块的操作范围，请查阅各模块的权限说明：

- [应用工作台权限说明](../../permissions/amamba.md)
- [服务网格权限说明](../../permissions/mspider.md)
- [中间件权限说明](../../permissions/mcamel.md)
- [微服务引擎权限说明](../../permissions/skoala.md)
- [容器管理权限说明](../../../kpanda/user-guide/permissions/permission-brief.md)
```


Copyright © 2016 - 2023 DaoCloud

工作空间（租户）绑定跨集群的命名空间

工作空间（租户）下绑定来自不同集群的命名空间，能够使工作空间（租户）灵活纳管平台上任意集群下的 Kubernetes Namespace。 同时平台提供了权限映射能力，能够将用户在工作空间的权限映射到绑定的命名空间身上。

当工作空间（租户）下绑定一个或多个跨集群的命名空间时，管理员无需再次给工作空间中的成员授权， 成员们在工作空间上的角色将根据以下映射关系自动映射完成授权，避免了多次授权的重复性操作：

- Workspace Admin 对应 Namespace Admin
- Workspace Editor 对应 Namespace Editor
- Workspace Viewer 对应 Namespace Viewer

以下是一个例子：

用户	工作空间	角色
用户 A	Workspace01	Workspace Admin

将一个命名空间绑定到工作空间后：

用户	所属范畴	角色
用户 A	Workspace01	Workspace Admin
	Namespace01	Namespace Admin

实现方案

将来自不同集群的不同命名空间绑定到同一工作空间（租户），给工作空间（租户）下的成员使用流程如图。

```
graph TB

preparews[准备工作空间] --> preparens[准备命名空间]
--> judge([命名空间是否与绑定到其他工作空间])
judge -.未绑定.->nstows[将命名空间绑定到工作空间] --> wsperm[管理工作空间访问权限]
judge -.已绑定.->createns[创建新的命名空间]

classDef plain fill:#ddd,stroke:#fff,stroke-width:1px,color:#000;
classDef k8s fill:#326ce5,stroke:#fff,stroke-width:1px,color:#fff;
classDef cluster fill:#fff,stroke:#bbb,stroke-width:1px,color:#326ce5;

class preparews,preparens,createns,nstows,wsperm cluster;
class judge plain

click preparews "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-to-ns/#_3"
click preparens "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-to-ns/#_4"
click nstows "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-to-ns/#_5"
click wsperm "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-to-ns/#_6"
click createns "https://docs.daocloud.io/ghippo/user-guide/workspace/ws-to-ns/#_4"
```

!!! tip

```
一个命名空间只能被一个工作空间绑定。
```


Copyright © 2016 - 2023 DaoCloud

准备工作空间

工作空间是为了满足多租户的使用场景，基于集群、集群命名空间、网格、网格命名空间、多云、多云命名空间等多种资源形成相互隔离的资源环境。工作空间可以映射为项目、租户、企业、供应商等多种概念。

Copyright © 2016 - 2023 DaoCloud

1. 使用 admin/folder admin 角色的用户登录 Web 控制台，点击左侧导航栏底部的 全局管理 。

2. 点击左侧导航栏的 工作空间与层级 ，点击右上角的 创建工作空间 按钮。

3. 填写工作空间名称、所属文件夹等信息后，点击 确定 ，完成创建工作空间。

Copyright © 2016 - 2023 DaoCloud

提示：若平台中已存在创建好的命名空间，点击某个工作空间，在 资源组 页签下，点击 绑定资源 ，可以直接绑定命名空间。

准备命名空间

命名空间是更小的资源隔离单元，将其绑定到工作空间后，工作空间的成员就可以进行管理和使用。

Copyright © 2016 - 2023 DaoCloud

参照以下步骤准备一个还未绑定到任何工作空间的命名空间。

1. 点击左侧导航栏底部的 `容器管理` 。

2. 点击目标集群的名称，进入 `集群详情` 。

   集群详情

3. 在左侧导航栏点击 `命名空间` ，进入命名空间管理页面，点击页面右侧的 `创建` 按钮。

   创建命名空间

4. 填写命名空间的名称，配置工作空间和标签（可选设置），然后点击 `确定` 。

   !!! info

   ```
   工作空间主要用于划分资源组并为用户（用户组）授予对该资源的不同访问权限。有关工作空间的详细说明，可参考[工作空间与层级](workspace.md)。
   ```

   填写

5. 点击 `确定` ，完成命名空间的创建。在命名空间列表右侧，点击 `⋮` ，可以从弹出菜单中选择 `绑定工作空间` 。

   确定和绑定

Copyright © 2016 - 2023 DaoCloud

将命名空间绑定到工作空间

除了在命名空间列表中绑定外，也可以返回 全局管理 ，按照以下步骤绑定工作空间。

1. 依次点击 全局管理 -> 工作空间与层级 -> 资源组 ，点击某个工作空间名称后，点击 绑定资源 按钮。

2. 选中要绑定的工作空间（可多选），点击 确定 完成绑定。

为工作空间添加成员并授权

1. 在 工作空间与层级 -> 授权 中，点击某个工作空间名称后，点击 添加授权 按钮。

Copyright © 2016 - 2023 DaoCloud

2. 选择要授权的 `用户/用户组` 、 `角色` 后，点击 `确定` 完成授权。

Copyright © 2016 - 2023 DaoCloud