

独立区域管理详解

(企业管理模块)

产品版本 : ZStack 2.5.1

文档版本 : V2.5.1

版权声明

版权所有©上海云轴信息科技有限公司 2018。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标说明

ZStack商标和其他云轴商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受上海云轴公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，上海云轴公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

| | |
|-------------------------|-----------|
| 版权声明 | 1 |
| 1 介绍 | 1 |
| 2 典型应用场景 | 2 |
| 2.1 环境准备..... | 3 |
| 2.2 admin创建两个平台管理员..... | 3 |
| 2.3 平台管理员-SH登录云平台..... | 5 |
| 2.4 平台管理员-BJ登录云平台..... | 16 |
| 2.5 验证..... | 17 |
| 术语表 | 20 |

1 介绍

企业管理主要为企业用户提供组织架构管理，以及基于项目的资源访问控制、工单审批、独立区域管理等功能。企业管理以单独的功能模块形式提供，需提前购买企业管理模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

独立区域管理是企业管理提供的子功能之一。

独立区域管理：

区域通常对应某地的一个真实数据中心。在对区域进行资源隔离的基础上，可对每个区域指定相应的区域管理员，实现各地机房的独立管理，同时admin可对所有区域进行巡查和管理。

本教程以典型应用场景为例，介绍独立区域管理功能。

2 典型应用场景

背景信息

场景设定：假定企业用户在上海、北京各有一个分公司，总部管理员（即：admin）分别指定相应的平台管理员，实现两地数据中心的独立管理。

如图 1: 独立区域管理示意图所示：

图 1: 独立区域管理示意图



以下为具体实践流程。

操作步骤

1. 环境准备；
2. admin创建两个平台管理员，分别管控上海、北京两个区域；
3. 平台管理员-SH登录云平台，构建上海分公司的组织架构，并创建相应的项目；
4. 平台管理员-SH登录云平台，构建北京分公司的组织架构，并创建相应的项目；
5. 验证：
 - 平台管理员划分区域后，只可管控所在区域内的资源；
 - 项目只可归属于一个区域，只可访问使用所属区域内的资源；
 - 项目负责人/项目管理员/项目成员只可访问使用所属项目内的资源；

- admin可对所有区域进行巡查和管理。

2.1 环境准备

- admin请提前安装最新版本ZStack
- admin请创建上海、北京两个区域，并分别对两个区域部署完成创建云主机必要的资源。

详情可参考[用户手册](#)安装部署章节。

- admin请提前购买企业管理模块许可证（ Plus License ），安装企业管理模块。

详情可参考[ZStack官网教程](#)《许可（ license ）更新说明》。

2.2 admin创建两个平台管理员

背景信息

admin创建两个平台管理员，分别管控上海、北京两个区域。

操作步骤

1. admin从主登录界面登录云平台。

使用Chrome浏览器或FireFox浏览器打开主登录界面（ http://your_machine_ip:5000/#/login ），admin输入相应用户名和密码登录云平台。

如图 2: 主登录界面所示：

图 2: 主登录界面



2. admin创建平台管理员-SH，并指定其管控上海区域的数据中心。

在ZStack私有云主菜单，点击**企业管理** > **平台管理员**按钮，进入**平台管理员**页面，点击**创建平台管理员**按钮，弹出**创建平台管理员**界面，可参考以下示例输入相应内容：

- **名称**：设置平台管理员名称，且作为登录名需全局唯一
- **简介**：可选项，可留空不填
- **密码**：设置平台管理员登录密码
- **确认密码**：再次输入登录密码
- **区域**：可选项，可为平台管理员划分管控区域，本场景下指定上海区域，可在创建平台管理员时直接指定，也可在创建平台管理员后再指定

如图 3: [创建平台管理员-SH](#)所示，点击**确定**，创建平台管理员-SH。

图 3: 创建平台管理员-SH



确定 取消

创建平台管理员

名称 * ?

平台管理员-SH

简介

密码 *

.....

确认密码 *

.....

区域

ZONE-SH ⊖

⊕

3. 同理，admin创建平台管理员-BJ，并指定其管控北京区域的数据中心。

2.3 平台管理员-SH登录云平台

背景信息

平台管理员-SH登录云平台，构建上海分公司的组织架构，并创建相应的项目。

操作步骤

1. 平台管理员-SH从项目登录入口登录云平台。

使用Chrome浏览器或FireFox浏览器打开项目登录界面（http://your_machine_ip:5000/#/project），平台管理员-SH输入相应用户名和密码登录云平台。

如图 4: 项目登录界面所示：

图 4: 项目登录界面



2. 平台管理员-SH构建上海分公司的组织架构。

a) 通过创建用户方式，将上海分公司人员录入云平台。

在ZStack私有云主菜单，点击**企业管理 > 组织架构 > 用户**按钮，进入**用户**页面，点击**创建用户**按钮，弹出**创建用户**界面，可参考以下示例输入相应内容：

- **姓名**：输入用户姓名
- **用户名(用于登录)**：设置用户名，作为登录名需全局唯一
- **密码**：设置用户登录密码
- **确认密码**：再次输入登录密码
- **简介**：可选项，可留空不填
- **手机号码**：可选项，输入用户手机号码
- **邮箱地址**：可选项，输入用户邮箱地址
- **编号**：可选项，输入用户编号，例如工号
- **项目**：可选项，可将用户加入到一个或多个项目
- **组织**：可选项，可将用户加入到一个或多个组织

如图 5: 创建用户所示：

图 5: 创建用户

确定 取消

创建用户

姓名 * ?

用户名 (用于登录) *

密码 *

确认密码 *

简介

手机号码

| | |
|-----|-------------|
| +86 | 14563589534 |
|-----|-------------|

邮箱地址

编号

项目

| | |
|----------|---|
| 开发项目A-SH | ⊖ |
| 开发项目B-SH | ⊖ |
| | ⊕ |

组织

| | |
|--------|---|
| Dev-SH | ⊖ |
| | ⊕ |

b) 构建上海分公司的组织架构。

在ZStack私有云主菜单，点击**企业管理 > 组织架构 > 组织**按钮，进入**组织**页面，点击**添加组织**按钮，弹出**添加组织**界面，可参考以下示例输入相应内容：

- **名称**：输入组织名称
- **简介**：可选项，可留空不填
- **类型**：选择组织类型，可选择添加部门或顶级部门



注：添加部门，需指定**上级部门**，在已添加的顶级部门或部门中选择。

- **部门负责人**：需指定相应的用户作为部门负责人



注：组织架构树中，部门负责人图标右下角有红色五角星标识。

- **用户**：可选项，可将已有相关用户加入到该组织

如图 6: 添加组织所示：

图 6: 添加组织

确定 取消

添加组织

名称 * ?

简介

类型

部门 顶级部门

上级部门 *

部门负责人 *

用户

c) 上海分公司的组织架构展示。

在**组织**界面，平台管理员-SH构建的上海分公司的组织架构如[图 7: 上海分公司的组织架构](#)所示：

图 7: 上海分公司的组织架构

| 名称 | 部门负责人 | 总人数 | 上级部门 | 创建日期 |
|-----------|-------|-----|-----------|---------------------|
| ZStack-BJ | Tomas | 4 | - | 2018-06-15 13:23:38 |
| ZStack-SH | Frank | 7 | - | 2018-06-07 21:04:23 |
| Dev-SH | Tom | 3 | ZStack-SH | 2018-06-07 21:04:45 |
| Tom | - | - | Dev-SH | 2018-06-07 21:02:40 |
| John | - | - | Dev-SH | 2018-06-07 21:03:12 |
| Jack | - | - | Dev-SH | 2018-06-07 21:02:54 |
| QA-SH | Bill | 3 | ZStack-SH | 2018-06-15 13:22:41 |
| Bill | - | - | QA-SH | 2018-06-15 13:10:40 |
| Chil | - | - | QA-SH | 2018-06-15 13:09:25 |
| Sam | - | - | QA-SH | 2018-06-15 13:10:04 |
| Frank | - | - | ZStack-SH | 2018-06-07 21:03:52 |

3. 平台管理员-SH创建相应的项目。

a) 创建项目。

在ZStack私有云主菜单，点击**企业管理 > 项目管理 > 项目**按钮，进入**项目**页面，点击**创建项目**按钮，弹出**创建项目**界面。



注:

- 创建项目前，云平台内的基本资源（计算规格、镜像、网络等）建议提前共享或创建；
- 可按照弹出的智能操作助手进行相关操作，如图 8: 智能操作助手所示：

图 8: 智能操作助手



可参考以下示例输入相应内容：

- **名称**：设置项目名称
- **简介**：可选项，可留空不填
- **配额方式**：设置项目配额，对项目资源总量进行控制

设置项目配额方式有以下两种：

- **自定义**：

如选择自定义方式设置项目配额，需设置以下内容：

- **计算资源**：包括云主机数量、运行中云主机数量、CPU数量、内存、亲和组数量的配额设置
- **存储资源**：包括云盘快照数量、数据云盘数量、可用存储容量、镜像数量、所有镜像容量的配额设置
- **网络资源**：包括VXLAN网络数量、三层网络数量、安全组数量、虚拟IP数量、弹性IP数量、端口转发数量、负载均衡器数量、监听器数量的配额设置
- **其他**：包括定时任务数量、定时器数量的配额设置

如图 9: 自定义配额方式所示：

图 9: 自定义配额方式

- **项目模板：**

如选择项目模板方式设置项目配额，需设置以下内容：

- **项目模板：**选择已有的项目模板，可直接使用模板定义的配额来配置项目

如图 10: 项目模板配额方式所示：

图 10: 项目模板配额方式

关于项目模板的更多介绍，详情可参考[项目模板](#)章节。

- **区域：**需指定项目所属的区域，一个项目只可归属于一个区域
- **项目周期：**可选项，默认为无限制，也可选择定时回收

- **无限制：**

创建项目后，项目内资源默认一直处于启用状态。

- **定时回收：**

项目过期后，项目内资源按照指定的控制策略回收。

如选择定时回收，需设置以下内容：

- **截止时间：**设置项目到期时间，支持秒级粒度
- **回收策略：**提供以下三种回收策略
 - **禁止登录：**过期后，项目相关人员均禁止登录此项目，项目内云主机仍将正常运行
 - **停止资源：**过期后，项目内云主机会被停止，项目仍可正常登录
 - **删除项目：**过期后，项目会被删除，处于“已删除”状态，项目禁止登录，云主机会被停止

如图 11: 定时回收所示：

图 11: 定时回收

项目周期

定时回收

截止时间

2018-12-12 15:14

回收策略

禁止登录

- **项目负责人：**需指定相应的用户作为项目负责人
- **成员：**添加相关用户进入项目作为项目成员

如图 12: 创建项目所示：

图 12: 创建项目

确定 取消

创建项目

名称 ?

开发项目A-SH

简介

配额方式 ?

自定义 项目模板

项目模板 ?

开发项目模板

区域 ?

ZONE-SH

项目周期

定时回收

截止时间

2019-01-09 17:08

回收策略 ?

删除项目

项目负责人 ?

Jack

成员

Frank

John

Tom

+

b) 上海分公司的相应项目展示。

在**项目**界面，平台管理员-SH创建的上海分公司的相应项目如图 7: 上海分公司的组织架构所示：

图 13: 上海分公司的相应项目

| 名称 | 项目负责人 | 成员数 | 成员组数 | 启用状态 | 创建日期 |
|----------|-------|-----|------|------|---------------------|
| 开发项目A-SH | Jack | 4 | 0 | 启用 | 2018-06-15 17:41:40 |
| 测试项目A-SH | Bill | 3 | 0 | 启用 | 2018-06-15 13:35:45 |
| 开发项目B-SH | Tom | 3 | 0 | 启用 | 2018-06-07 21:10:00 |

2.4 平台管理员-BJ登录云平台

背景信息

同理，平台管理员-BJ登录云平台，构建北京分公司的组织架构，并创建相应的项目。

操作步骤

1. 北京分公司的组织架构展示。

在**组织**界面，平台管理员-BJ构建的北京分公司的组织架构如图 14: 北京分公司的组织架构所示：

图 14: 北京分公司的组织架构

| 名称 | 部门负责人 | 总人数 | 上级部门 | 创建日期 |
|-----------|-------|-----|-----------|---------------------|
| ZStack-BJ | Tomas | 4 | - | 2018-06-15 13:23:38 |
| Sales-BJ | Ben | 3 | ZStack-BJ | 2018-06-15 13:24:14 |
| Ben | - | - | Sales-BJ | 2018-06-15 13:13:22 |
| Shelly | - | - | Sales-BJ | 2018-06-15 13:12:01 |
| Amy | - | - | Sales-BJ | 2018-06-15 13:12:41 |
| Tomas | - | - | ZStack-BJ | 2018-06-15 13:16:15 |
| ZStack-SH | Frank | 7 | - | 2018-06-07 21:04:23 |

2. 北京分公司的相应项目展示。

在**项目**界面，平台管理员-BJ创建的北京分公司的相应项目如图 14: 北京分公司的组织架构所示：

图 15: 北京分公司的相应项目

| 名称 | 项目负责人 | 成员数 | 成员组数 | 启用状态 | 创建日期 |
|----------|-------|-----|------|------|---------------------|
| 销售项目A-BJ | Tomas | 4 | 0 | 启用 | 2018-06-15 13:36:46 |

2.5 验证

背景信息

验证：

- 平台管理员划分区域后，只可管控所在区域内的资源；
- 项目只可归属于一个区域，只可访问使用所属区域内的资源；
- 项目负责人/项目管理员/项目成员只可访问使用所属项目内的资源；
- admin可对所有区域进行巡查和管理。

操作步骤

1. 平台管理员划分区域后，只可管控所在区域内的资源。

例如，平台管理员-SH只可管控上海区域内的资源，北京区域资源不可见，如图 16: 平台管理员-SH视角所示：

图 16: 平台管理员-SH视角

| 名称 | CPU | 内存 | 默认IP | 物理机IP | 集群 | 启用状态 | 所有者 | 高可用级别 | 创建日期 |
|----------------|-----|------|-----------------|----------------|-----------|------|----------|-------|---------------------|
| 业务云主机-开发项目B-SH | 1 | 1 GB | 192.168.108.234 | 192.168.29.252 | Cluster-1 | 运行中 | 开发项目B-SH | None | 2018-06-15 20:48:54 |
| 业务云主机-开发项目A-SH | 1 | 1 GB | 192.168.108.246 | 192.168.29.252 | Cluster-1 | 运行中 | 开发项目A-SH | None | 2018-06-07 13:53:01 |

2. 项目只可归属于一个区域，只可访问使用所属区域内的资源。

例如，平台管理员-SH创建的项目只可归属于上海区域，只可访问使用上海区域内的资源，如图 17: 平台管理员-SH视角所示：

图 17: 平台管理员-SH视角



3. 项目负责人/项目管理员/项目成员只可访问使用所属项目内的资源

例如，上海区域内的项目**开发项目A-SH**，项目负责人**Jack**、项目管理员**Tom**、项目成员**Frank/John**均只可访问使用**开发项目A-SH**内的资源，如图 18: 平台管理员-SH视角、图 19: 项目负责人Jack视角、图 20: 项目管理员Tom视角、图 21: 项目成员Frank/John视角所示：

图 18: 平台管理员-SH视角



图 19: 项目负责人Jack视角



图 20: 项目经理Tom视角



图 21: 项目成员Frank/John视角



4. admin可对所有区域进行巡查和管理。

本场景下，admin可对上海区域和北京区域进行巡查和管理，如图 22: admin视角所示：

图 22: admin视角



后续操作

至此，独立区域管理功能介绍完毕。

术语表

区域 (Zone)

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群 (Cluster)

一个集群是类似物理主机 (Host) 组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统 (虚拟机管理程序, Hypervisor)，拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架 (Rack)。

管理节点 (Management Node)

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点 (Compute Node)

也称之为物理主机 (或物理机)，为云主机实例提供计算、网络、存储等资源的物理主机。

主存储 (Primary Storage)

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、Ceph、FusionStor、Shared Mount Point等类型。

镜像服务器 (Backup Storage)

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。

镜像仓库 (Image Store)

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机 (VM Instance)

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像 (Image)

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘 (Volume)

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格 (Instance Offering)

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格 (Disk Offering)

创建云盘容量大小的规格定义。

二层网络 (L2 Network)

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络 (L3 Network)

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络 (Public Network)

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络 (Private Network)

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池 (VXLAN Network Pool)

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络 (即 VXLAN 网络) ，这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络 (VXLAN)

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由 (vRouter)

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组 (Security Group)

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP (EIP)

公有网络接入到私有网络的IP地址。

快照 (Snapshot)

某一个时间点上某一个磁盘的数据备份。包括自动快照和手动快照两种类型。