账户管理详解

产品版本：ZStack 3.3.0

文档版本：V3.3.0

ZStack

版权声明

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

1 简介

ZStack的多租户和亚马逊的Identity Access Management（IAM）系统基本一致，包含账户，用户，用户组等内容，可以对用户权限按照资源操作进行细节控制。

注: 绝大部分私有云场景使用账户级别进行资源的隔离管理就足够了，不需要使用用户。

本文将介绍多租户管理中的账户管理。

2 账户

账户是ZStack系统对资源控制引入的新概念，用来定义和隔离资源的所有者。

每个账户可以对属于自己的资源进行使用、修改、共享、召回等操作，也可以使用其他账户分享给自己的资源。这里使用的意思代表创建云主机，创建云盘等操作。账户分为admin账户和普通账户，其中admin账户是ZStack系统的特权用户。

系统安装完成后首次引导和其他关键资源需要admin账户进行配置和添加。普通账户由admin账户创建，默认情况下普通账户看不到admin账户创建的计算规格、云盘规格、物理主机、镜像和网络等关键资源。需要admin提前分享计算规格、网络等资源才可创建云主机。普通账户拥有创建、删除和管理云主机、镜像、云盘、安全组、用户组及用户的权限。

下表详述了admin账户和普通账户的区别和联系：

属性	admin账户	普通账户
生命周期	一直存在，不可删除	由admin账户创建，可被删除
默认权限	全局超级权限	部分权限
资源配额	全局使用	各项配额受admin控制
可拥有的资源种类	全局拥有（用户组除外）	云主机/镜像/云盘/安全组/用户组/用户
可分享/召回的资源	计算规格/云盘规格/网络/镜像	镜像（需admin分享）
其他账户云主机	全局可见、可控	不可见，不可控制其他账户资源
其他账户镜像	全局可见、可控	1.未经admin分享，不可见 2.admin分享后，只读权限
共享/召回方式	单个账户/批量账户/全局	1.暂不支持普通账户主动共享/召回 2.需经admin分享/召回
可支持的操作	全局操作（普通用户创建、修改权限除外）	支持对云主机、镜像、云盘、安全组、用户组、普通账户所属用户的所有操作
创建云主机的条件	配置Wizard引导完成	1.admin配置Wizard引导完成 2.admin共享计算规格、网络资源 3.本账户添加镜像文件或admin分享镜像资源(如需安装镜像，则同时需要admin分享云盘规格)

属性	admin账户	普通账户
删除后果	不支持删除	支持删除，但此账户下的所有资源被删除，包括云主机、镜像、云盘、安全组、用户组、用户所有资源
命名规则	不支持命名	支持命名，但账户名称不可重复

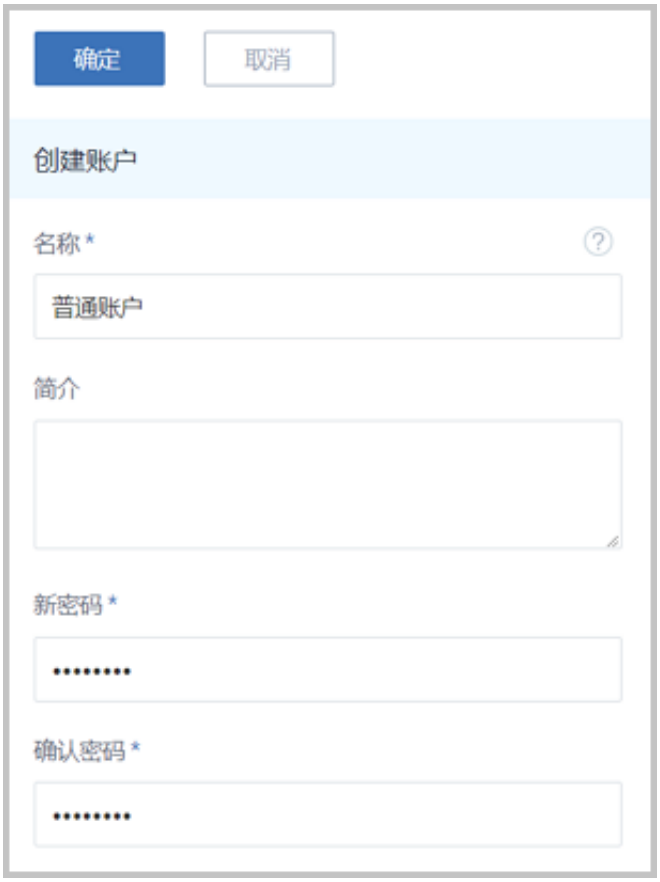
3 账户管理方法

操作步骤

1. 创建账户

   使用admin账户登录后，点击**平台管理**，在**账户**界面点击**创建账户**按钮后，弹出界面，输入相关信息，点击**确定**按钮。即可创建新账户，如图 *1:* 创建账户所示：

   图 1: 创建账户



2. 管理账户

   在**账户**界面，点击此账户名称可查看并修改此账户的相关信息。配额栏会显示此账户可使用的资源配额（即使用的上限），可点击相关配额进行修改，如图 *2:* 管理账户所示：

   图 2: 管理账户

3. 共享资源

admin账户创建的计算规格、镜像和网络默认不对普通账户分享。需提前分享给账户，普通账户才可使用，并创建云主机。下面以计算规格共享为例，其他资源共享均需同样的操作。

点击**云资源池 > 计算规格**进入**计算规格**页面，点击计算规格名称，再点击**共享**页面的**操作 > 共享**按钮，在弹出界面，选择待共享的账户，点击**确定**，使用此账户登录，创建云主机即可看到此资源，如图 3: admin分享计算规格所示：

图 3: admin分享计算规格

注: admin账户可以创建不同的资源，并选择共享不同的资源给不同的普通账户。使用这种方式可以对多租户使用的资源进行有效的隔离。

4. 使用普通账户登录

点击浏览器右上角的**登出**按钮，退出admin账户，使用刚创建的普通账户登录系统，如图 *4:* 普通账户登录所示：

图 4: 普通账户登录

普通账户登录后，首页显示了此账户的相关可用资源信息，此信息与admin账户管理的配额信息一致，如图 *5:* 普通账户界面所示：

图 5: 普通账户界面

登录后界面比admin账户界面缺少总物理主机CPU负载率、总物理主机内存负载率、总物理主机网络吞吐量、总物理主机磁盘IO、计算等资源管理界面。在普通账户界面中存储容量和镜像容量是指该账户的配额。

5. 创建云主机

创建云主机过程和admin账户模式下创建方法相同，在ZStack私有云主菜单，点击**云资源池** > **云主机**按钮，在**云主机**界面点击**创建云主机**，在弹出的**创建云主机**页面中，可参考以下示例输入相应内容：

- **添加方式**：选择添加云主机的方式
- **名称**：设置云主机的名称
- **简介**：可选项，可留空不填
- **计算规格**：选择适合的计算规格
- **根云盘规格**：选择合适的根云盘规格
- **镜像**：选择云主机的镜像
- **网络**：选择创建云主机的三层网络

如图 *6:* 创建云主机界面所示，点击**确定**按钮，完成云主机创建。

图 6: 创建云主机界面

注: 需要注意的是：

普通账户模式下，创建云主机所需的计算规格、镜像、网络等资源需要提前登录admin账户分享，或者重新创建/上传这些资源。

重新创建/上传的资源只属于该普通账户，如果删除该账户，其名下的资源也将被删除。

6. 删除账户

如果需要删除普通账户，需要登录admin账户，在**账户**界面选中需要删除的账户，点击**更多操作 > 删除**，即可删除该普通账户和该账户下的资源。如图 7: 删除账户所示：

图 7: 删除账户

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、、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。