

公有云综合应用实战

课程概述

随着互联网技术的不断发展，公有云服务得到的飞速的发展。2021年4月22日，IDC最新发布的《全球及中国公有云服务市场（2020年）跟踪》报告显示，2020年全球公有云服务整体市场规模（IaaS/PaaS/SaaS）达到3,124.2亿美元，同比增长24.1%，中国公有云服务整体市场规模达到193.8亿美元，同比增长49.7%，全球各区域中增速最高。IDC预计，到2024年中国公有云服务市场的全球占比将从2020年的6.5%提升为10.5%以上，如图-1

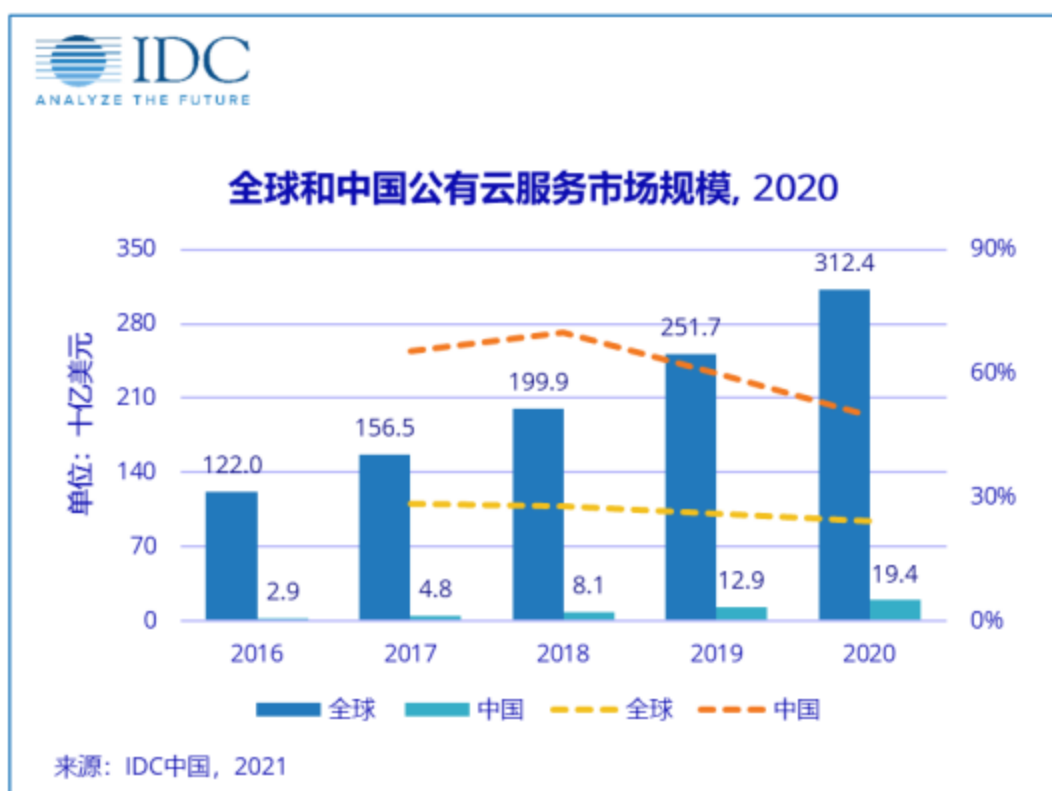


图-1

基于目前互联网的流行趋势，规划并设计了《公有云综合应用实战》教材。旨在通过基于公有云项目案例讲解和操作，提升学生基于公有云环境的应用、处理问题、解决问题的能力。课程涵盖了基础的Linux系统基本操作、文件及用

户的安全设置、磁盘管理、软件管理、基于 Linux 系统的常用服务管理与配置、基于公有云的开发环境部署、云数据库、云 API 的应用、小程序开发等相关知识。

相关术语

- **云计算**：云计算是分布式计算的一种，指的是通过网络将海量的数据计算处理程序分解成无数的小程序，然后通过众多服务器组成的系统进行处理和分析这些小程序得到的结果并返回给用户。云计算的早期就是简单的分布式计算，解决任务分发、并行计算结果合并。现阶段的云计算服务已经不是简简单单的分布式计算，而是分布式计算、效用计算、负载均衡、并行计算、热备冗余和虚拟化等计算机技术的混合演进。在 2006 年 8 月 9 日，Google 首席执行官埃里克·施密特（Eric Schmidt）在搜索引擎大会（SESSanJose2006）首次提出“云计算”（Cloud Computing）的概念。这是云计算发展史上第一次正式地提出这一概念，有着巨大的历史意义。
- **公有云**：通常指第三方提供商为用户提供的能够使用的云，公有云一般可通过 Internet 使用，可能是免费或成本低廉的，公有云的核心属性是共享资源服务。
- **私有云**：私有云(Private Clouds)是为一个客户单独使用而构建的，因而提供对数据、安全性和服务质量的最有效控制。私有云可部署在企业数据中心的防火墙内，也可以将它们部署在一个安全的主机托管场所，私有云的核心属性是专有资源。
- **云 API**：是指开发者使用云服务商提供的云应用编程接口编码开发应用，该接口是云服务商提供的服务。也可以理解为把原来单独使用的 API 通过优化和技术升级部署在云端，对所有互联网用户开放。由于云 API 暴露在互联网上因此具有一定的安全风险，可能会危害到敏感的业务数据，这就要求使用云 API 时首先要确认该服务的安全性。用户通过云服务商提供的云 API，只需要少量的代码即可快速操作其相关云产品。在使用云服务商提供的云 API 时，需要查阅相关对应的云 API 文档，该文档内会包含接口信息、使用指南等。

- **云数据库：**云数据库是指被优化或部署到一个虚拟计算环境中的数据库，可以实现按需付费、按需扩展、高可用性以及存储整合等优势。根据数据库类型一般分为关系型数据库和非关系型数据库（NoSQL 数据库）。其特点主要表现为：实例创建快速、支持只读实例、读写分离、故障自动切换、数据备份、Binlog 备份、SQL 审计、访问白名单、监控与消息通知等。
- **微信小程序：**是一种不需要下载安装即可使用的应用，它实现了应用“触手可及”的梦想，用户扫一扫或者搜一下即可打开应用。也体现了“用完即走”的理念，用户不用关心是否安装太多应用的问题。应用将无处不在，随时可用，但又无需安装卸载。对于开发者而言，微信小程序开发门槛相对较低，难度不及 APP，能够满足简单的基础应用，适合生活服务类线下商铺以及非刚需低频应用的转换。微信小程序能够实现消息通知、线下扫码、公众号关联等七大功能。其中，通过公众号关联，用户可以实现公众号与微信小程序之间相互跳转，微信小程序不存在入口。

1. 项目一：操作系统运维与管理实战

项目背景

某公司系统运维工程师，在项目日常运行、管理、维护的过程中。工程师小王要对 Linux 系统中的程序与文件进行管理，所有需要创建一系列的用户以及用户组，对其进行合理的权限管理；并在项目维护过程中，需要对 Linux 系统的磁盘空间进行扩容、缩容、生成快照等等操作；以及掌握各种包管理工具的使用。

1.1. 管理用户帐户及用户帐户文件

任务要求

- 掌握 Linux 用户账号的概念
- 掌握/etc/passwd 与/etc/shadow 文件的作用
- 掌握 Linux 用户帐号的添加、删除与修改
- 用户口令的管理及用户帐户信息查看等操作命令

1.1.1. Linux 系统中用户的概述

用户帐户是用户的身份标识，用户通过用户帐户可以登录到系统。所有用户分为三类：

- 超级用户 (root)：它的 UID 为 0。对系统有绝对的控制权。
- 系统用户：一般不登陆系统，用于维持某个服务程序正常运行 (UID: 1 ~ 999)。
- 普通用户：管理员创建，权力受限 (UID 从 1000 开始)。

用户帐户信息都存放在/etc/passwd 文件中，该文件一行记录对应着一个用户

```
cat /etc/passwd
```

```
[root@VM-16-16-centos ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
libstoragemgmt:x:998:997:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
chrony:x:997:995:/:var/lib/chrony:/sbin/nologin
tcpdump:x:72:72:/:/sbin/nologin
syslog:x:996:994:/:home/syslog:/bin/false
alice:x:1000:1000:/:home/alice:/bin/bash
[root@VM-16-16-centos ~]#
```

每行记录又被冒号(:)分隔为 7 个字段，其格式和具体含义如下：

用户名:口令:用户标识号:组标识号:注释性描述:主目录:登录 Shell

/etc/passwd: 每个字段的作用:

例如: root:x:0:0:root:/root:/bin/bash

用户名 : 密码占位符 : UID : GID : 用户描述 : 用户主目录 (bash 中"~"代表哪个) : 登录后使用的 shell

注意:

- 用户名不超过8个字符, 不要包含点字符(.), 且不使用连字符(-)和加号(+)开头。
- 登录Shell是/sbin/nologin是称为伪用户(pseudo users), 作用是方便系统管理, 但是不能登录。

root:\$6\$.BTyNB8Q397zR.KY\$412.....M8ZHWiidd/:16274: 0 : 99999 : 7 : : *

1 用户名 : 密码(REHLS 使用 MD5/RHEL6 使用 SHA512 加密)

2 被加密后的密码

3 最近更改密码的日期, 从 19700101 开始计算

4 密码不能更改的天数: 最近被改过之后几天后才可以再次更改。0 表示随时可以修改。

5 密码过期时间, 即多少天后必须再次修改。

6 密码需要更改期限到来前 7 发出警告。

7 宽限天数: 密码过了几天后还能改密码。

8 帐号过期时间。

9 保留。

/etc/shadow 中的记录行与/etc/passwd 中的一一对应, 它由 pwconv 命令根据 /etc/passwd 中的数据自动产生, 格式为:

登录名:加密口令:最后一次修改时间:最小时间间隔:最大时间间隔:警告时间:不活动时间:失效时间:标志

注意:

- 用户口令字长度为 13 个字符。如果为空, 则对应用户没有口令, 登录时不需要口令; 如果含有不属于集合 {./0-9A-Za-z} 中的字符, 则对应的用户不能登录。
- “最后一次修改时间”表示的是从某个时刻起, 到用户最后一次修改口令时的天数。时间起点对不同的系统可能不一样。一般在 Linux 中, 这个时间起点是 1970 年 1 月 1 日。
- “最小时间间隔”指的是两次修改口令之间所需的最小天数。

- “最大时间间隔”指的是口令保持有效的最大天数。
- “警告时间”字段表示的是从系统开始警告用户到用户密码正式失效之间的天数。
- “不活动时间”表示的是用户没有登录活动但账号仍能保持有效的最大天数。
- “失效时间”字段给出的是一个绝对的天数，如果使用了这个字段，那么就给出相应账号的生存期。期满后，该账号就不再是一个合法的账号，也就不能再用来登录了。

查看/etc/shadow 文件内容：

```
cat /etc/shadow
```

```

[root@VM-16-38-centos ~]# cat /etc/shadow
root:$1$WadeohPv$emnLU/wCBf6xDiyWioeKNO:18620:0:99999:7:::
bin:!:17834:0:99999:7:::
daemon:!:17834:0:99999:7:::
adm:!:17834:0:99999:7:::
lp:!:17834:0:99999:7:::
sync:!:17834:0:99999:7:::
shutdown:!:17834:0:99999:7:::
halt:!:17834:0:99999:7:::
mail:!:17834:0:99999:7:::
operator:!:17834:0:99999:7:::
games:!:17834:0:99999:7:::
ftp:!:17834:0:99999:7:::
nobody:!:17834:0:99999:7:::
systemd-network:!!:17962:::::
dbus:!!:17962:::::
polkitd:!!:17962:::::
libstoragemgmt:!!:17962:::::
rpc:!!:17962:0:99999:7:::
ntp:!!:17962:::::
abrt:!!:17962:::::
sshd:!!:17962:::::
postfix:!!:17962:::::
chrony:!!:17962:::::
tcpdump:!!:17962:::::
syslog:!!:18205:::::
alice:!!:18620:0:99999:7:::
albert:$1$8HaTfcjd$0Mx6gNtpN2zBF1XDpeIHG1:18620:0:99999:7:::

```

```

root:$6$.BTyNB8Q397zR.KY$412.....M8ZHwiidd/:16274: 0 : 99999 : 7 : : :

```

- 1 用户名，密码(RHEL5 使用 MD5/RHEL6 使用 SHA512 加密)
- 2 被加密后的密码。
- 3 最近更改密码的日期，从 19700101 开始计算。
- 4 密码不能更改的天数：最近被改过之后几天后才可以再次更改。0 表示随时可以修改。
- 5 密码过期时间，即多少天后必须再次修改。
- 6 密码需要更改期限到来前 7 发出警告。
- 7 宽限天数：密码过了几天后还能改密码。
- 8 帐号过期时间。
- 9 保留。

1.1.2. Linux 系统用户的管理

1、添加自定义的帐号

例如：添加一个主目录为/home/albert，名为 albert 的账号。

```

useradd -d /home/albert albert

```

```
[root@VM-16-16-centos ~]# useradd -d /home/albert albert
```

```
[root@VM-16-16-centos ~]# ls /home
albert  alice
[root@VM-16-16-centos ~]#
```

useradd 命令的用法: useradd 选项 用户名

选项:

- -c comment 指定一段注释性描述。
- -d 目录 指定用户主目录, 如果此目录不存在, 则同时使用-m 选项, 可以创建主目录。
- -g 用户组 指定用户所属的用户组。
- -G 用户组, 用户组 指定用户所属的附加组。
- -s Shell 文件 指定用户的登录 Shell。
- -u 用户号 指定用户的用户号, 如果同时有-o 选项, 则可以重复使用其他用户的标识号。

增加用户就是在/etc/passwd 文件中为新用户增加一条记录, 同时更新其他系统文件如/etc/shadow, /etc/group 等。

Linux 提供了集成的系统管理工具 userconf, 它可以用来对用户账号进行统一管理。

2、删除帐号

如果一个用户的账号不再使用, 可以从系统中删除。删除用户账号就是要将/etc/passwd 等系统文件中的该用户记录删除, 必要时还删除用户的主目录。

删除一个已有的用户账号使用 userdel 命令, 其格式如下:

userdel 选项 用户名

选项:

- -r: 把用户的主目录一起删除。

例如：删除用户 albert，此命令删除用户 albert 在系统文件中（主要是 /etc/passwd, /etc/shadow, /etc/group 等）的记录，同时删除用户的主目录。

```
userdel -r albert
```

```
[root@VM-16-16-centos ~]# userdel -r albert  
[root@VM-16-16-centos ~]#
```

3、修改帐号属性

修改用户账号的属性就是根据实际情况更改用户的有关属性，如用户号、主目录、用户组、登录 Shell 等。用 usermod 命令，其格式如下：

```
usermod 选项 用户名
```

常用的选项包括 -c, -d, -m, -g, -G, -s, -u 以及 -o 等，这些选项的意义与 useradd 命令中的选项一样，可以为用户指定新的资源值。另外，有些系统可以使用选项：-l 新用户名，这个选项指定一个新的账号，即将原来的用户名改为新的用户名。

例如：将用户 brown 的登录 Shell 修改为 bash，主目录改为 /home/share，用户组改为 alice。

```
useradd brown  
usermod -s /bin/bash -d /home/share -g alice brown
```

```
[root@VM-16-38-centos ~]# useradd brown  
[root@VM-16-38-centos ~]# usermod -s /bin/bash -d /home/share -g alice brown  
[root@VM-16-38-centos ~]#
```

4、用户口令的管理

用户管理的一项重要内容是用户口令的管理。用户账号刚创建时没有口令，但是被系统锁定，无法使用，必须为其指定口令后才可以使⤵用。指定和修改用户口令的 Shell 命令是 `passwd`。超级用户可以为自己和其他用户指定口令，普通用户只能用它修改自己的口令。命令的格式为：

```
passwd 选项 用户名
```

选项：

- `-l` 锁定口令，即禁用账号。
- `-u` 口令解锁。
- `-d` 使账号无口令。
- `-f` 强迫用户下次登录时修改口令。

如果是超级用户，可以用下列形式指定任何用户的口令：

```
passwd alice
```

```
[root@VM-16-38-centos ~]# passwd alice
Changing password for user alice.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@VM-16-38-centos ~]#
```

如果是在 `root` 用户下怎么设置都可以，可以不受验证机制的约束，即便出来“BAD PASSWORD: it is based on a dictionary word”也可以修改成功。

但是普通用户修改自己的密码，不符合密码验证机制的话就修改不成功，会有各种报错。

“BAD PASSWORD: it’s WAY too short”，这是报密码太短，不符合 `/etc/login.defs` 的设置；