IB00109 云计算技术

授课教师：姜婧妍

jiangjingyan@sztu.edu.cn

2023年

第二章

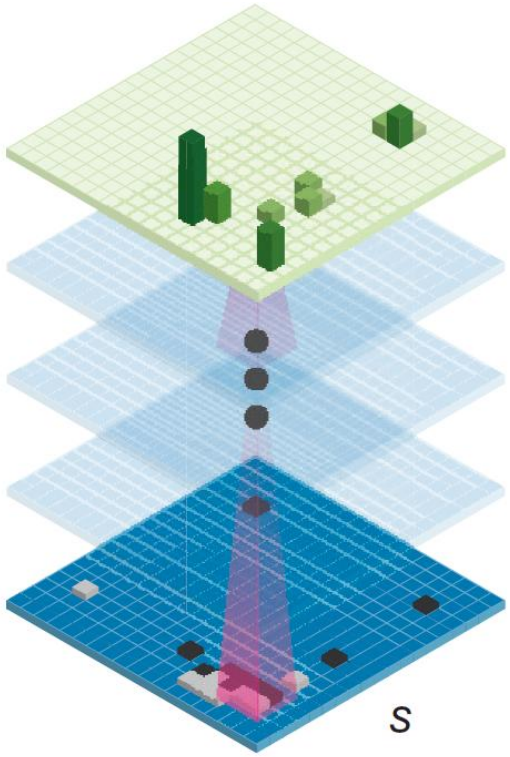
云计算概论与云计算基础

授课教师：姜婧妍

jiangjingyan@sztu.edu.cn

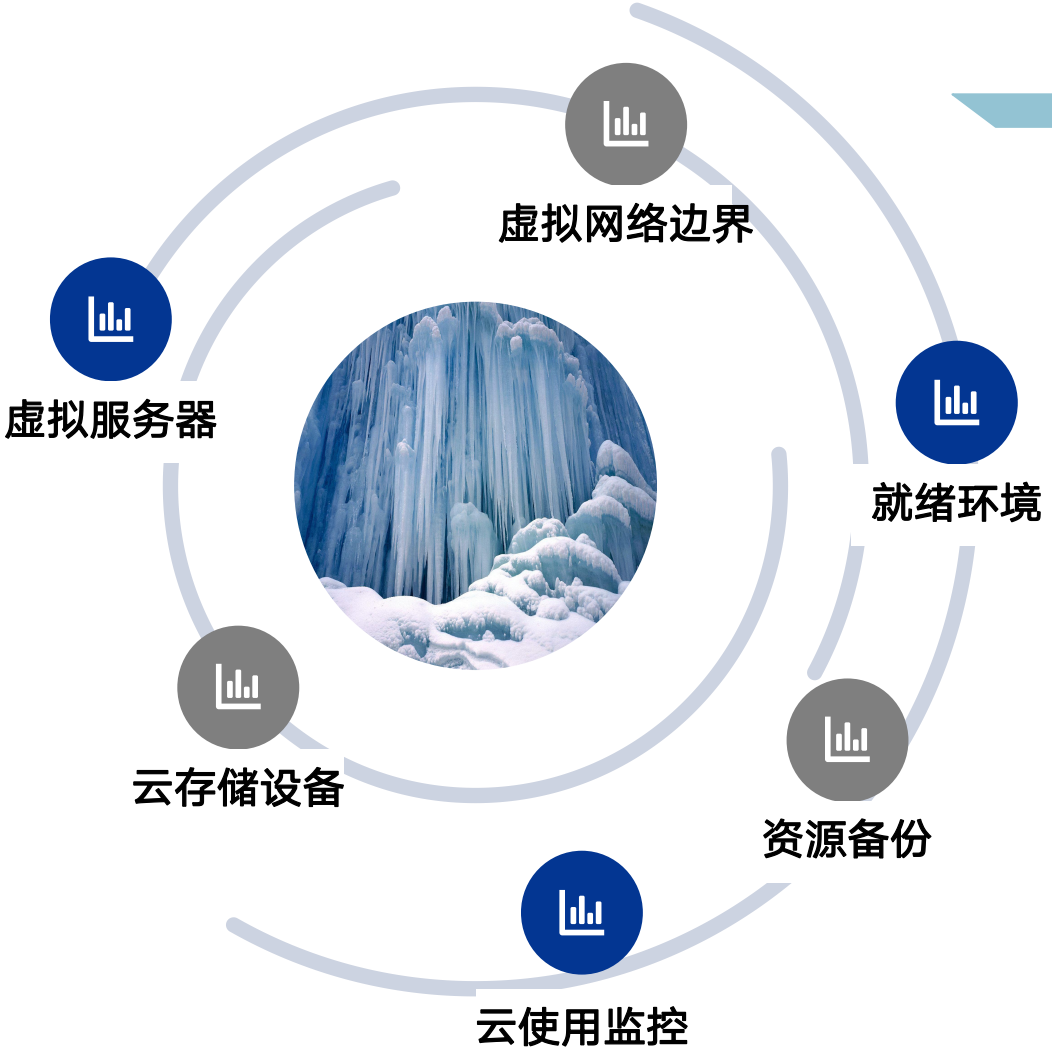
2023年

目录 CONTENTS



01 云基础设施机制

云基础设施机制



云基础设施机制是云环境的基础构建块，它是形成云技术架构基础的主要构件

虚拟网络边界

虚拟网络边界（virtual network perimeter）通常是由提供和控制数据中心连接的网络设备建立，一般是作为虚拟化环境部署的。例如虚拟防火墙、虚拟网络（VLAN、VPN）。

该机制被定义为将一个网络环境与通信网络的其它部分隔开，形成一个虚拟网络边界，包含并隔离了一组相关的基于云的IT资源，这些资源在物理上可能是分布式的。

该机制可被用于如下的几个方面：

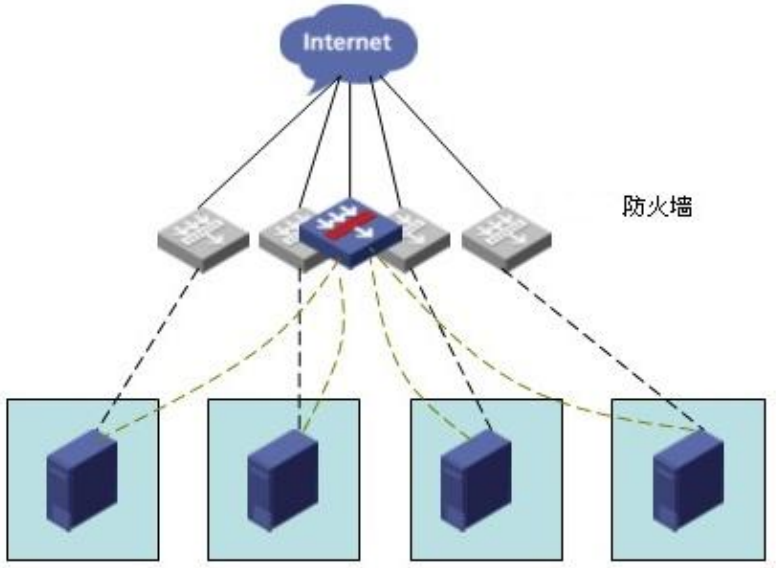
- 将云中的IT资源与非授权用户隔离；
- 将云中的IT资源与非用户隔离；
- 将云中的IT资源与云用户隔离；
- 控制被隔离IT资源的可用带宽

虚拟防火墙

每个虚拟防火墙能够实现防火墙的大部分特性，并且虚拟防火墙之间相互独立，一般情况下不允许相互通信。

虚拟防火墙技术特点：

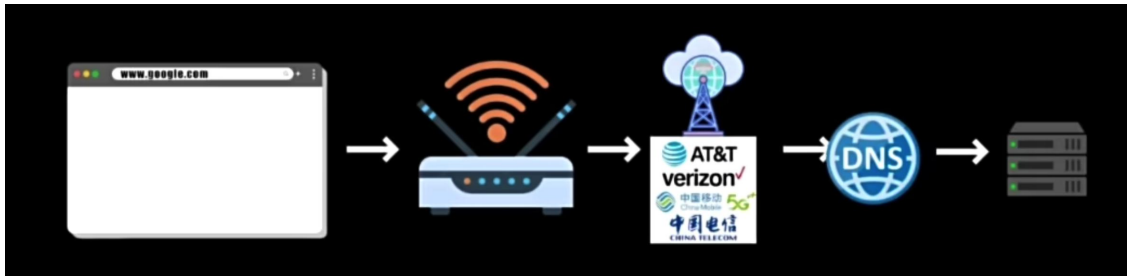
- 每个虚拟防火墙独立维护一组安全区域
- 每个虚拟防火墙独立维护一组资源对象（地址/地址组，服务/服务组等）
- 每个虚拟防火墙独立维护自己的包过滤策略
- 每个虚拟防火墙独立维护自己的ASPF策略、NAT策略、ALG策略
- 可限制每个虚拟防火墙占用资源数，如防火墙Session以及ASPF Session数目。

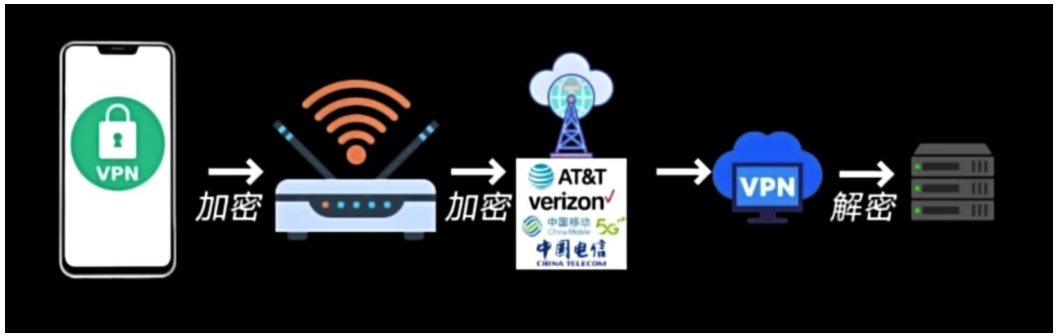


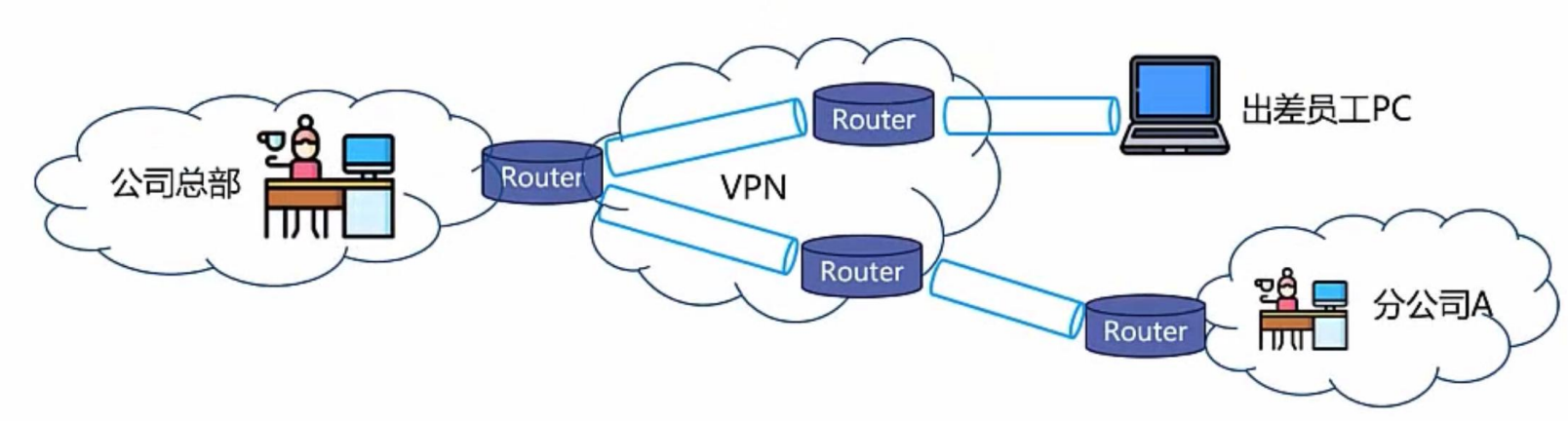
虚拟专用网络（VPN）

- 虚拟专用网络 (VPN, Virtual Private Network) 是一种通过公用网络（如 Internet）连接专用网络（如办公室网络）的方法。
- VPN 使用经过身份验证的链接来确保只有授权用户才能连接到自己的网络，而且这些用户使用**加密来确保他们通过 Internet 传送的数据不会被其他人截取和利用**。Windows 使用点对点隧道协议 (PPTP) 或第二层隧道协议 (L2TP) 实现此安全性。

一般上网是什么样的，什么是VPN？







VPN系统主要技术特点

安全保障

服务质量保证（QoS）

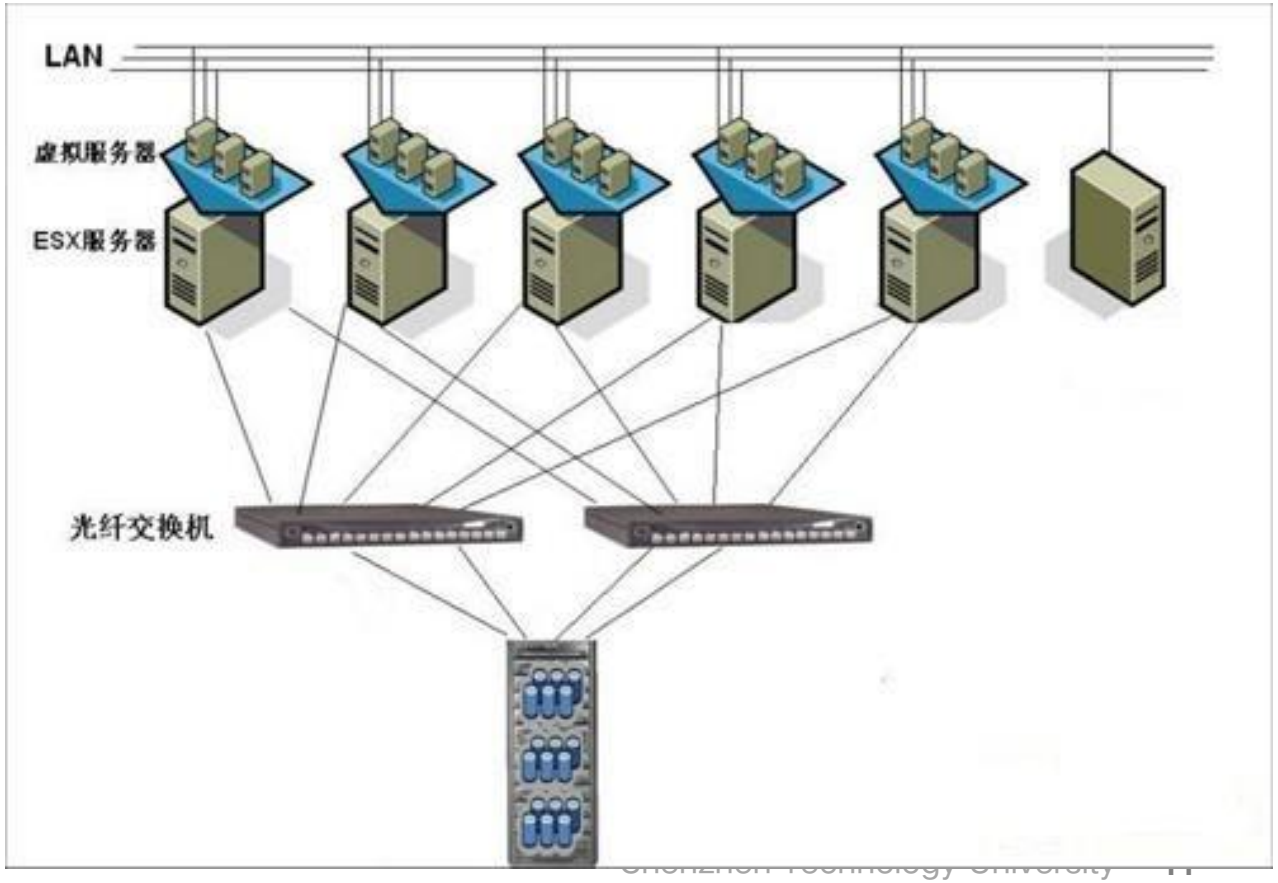
可管理性

可扩充性和灵活性

虚拟服务器

- 虚拟服务器（virtual server）是一种模拟物理服务器的虚拟化软件。
- 通过向云用户提供独立的虚拟服务实例，云提供者使多个云用户共享同一个物理服务器。
- 基本特性： 多实例、隔离性、封装性
- 虚拟服务器优点：
  - ✓实时迁移
  - ✓快速部署
  - ✓高兼容性
  - ✓提高资源利用率
  - ✓动态调度资源

虚拟服务器基本架构



云存储设备

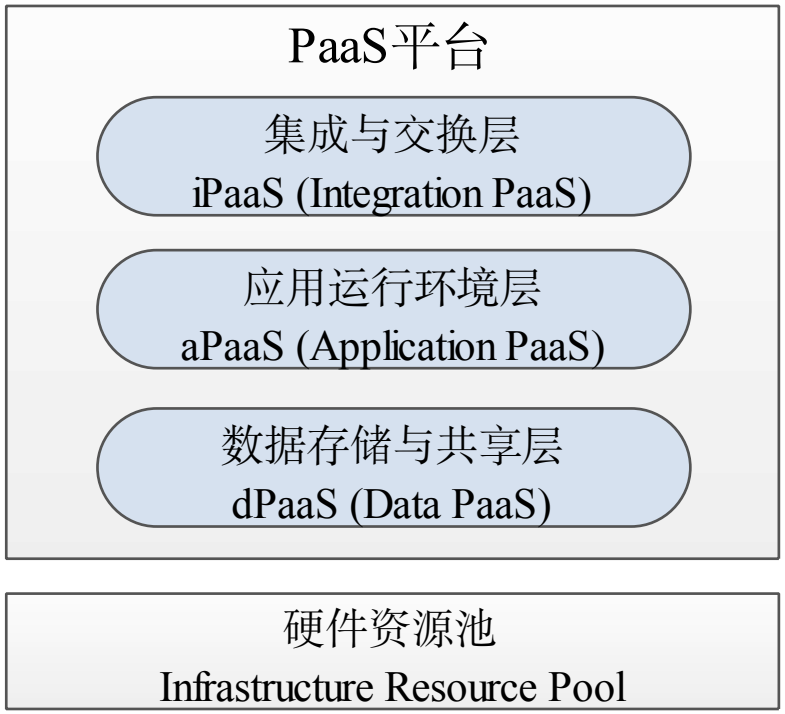
云存储设备（cloud storage device）机制是指专门为基于云配置所设计的的存储设备。这些设备的实例可以被虚拟化。其单位如下：

- 文件（file）
- 块（block）
- 数据集（dataset）
- 对象（object）

就绪环境

就绪环境机制是PaaS云交付模型的定义组件，基于云平台，已有一组安装好的IT资源，可以被云用户使用和定制。

- iPaaS：基于SOA、ESB、BPM等架构，是云内/云与企业间的集成平台；
- aPaaS共享：基于Java等应用技术架构，是应用的部署与运行环境平台；
- dPaaS可灵活伸缩：是数据存储与共享平台，提供多租户环境下高效与安全的数据访问；
- 硬件资源池：为PaaS平台提供所需要的高性能硬件资源系统。



Oracle的PaaS框架

02 云管理机制

云管理机制

	传统管理	云管理
管理对象	网络、存储、服务器、OS、数据库、中间件、应用	IaaS、PaaS、SaaS等各种云服务
管理目标	实现IT系统的正常运作	实现云服务的端对端交付
管理特色	需要专业的管理技能 手动管理 竖井式管理	通过封装屏蔽底层细节 自服务 多租户，共享管理平台
管理平台易用性	安装配置复杂	自配置、自修复、自优化
管理规模	100节点	10000节点+
用户	管理员	分层管理，多租户
整合	基于事件、数据库、私有接口的整合	面向服务的整合
管理手段	离散的工具	充分自动化

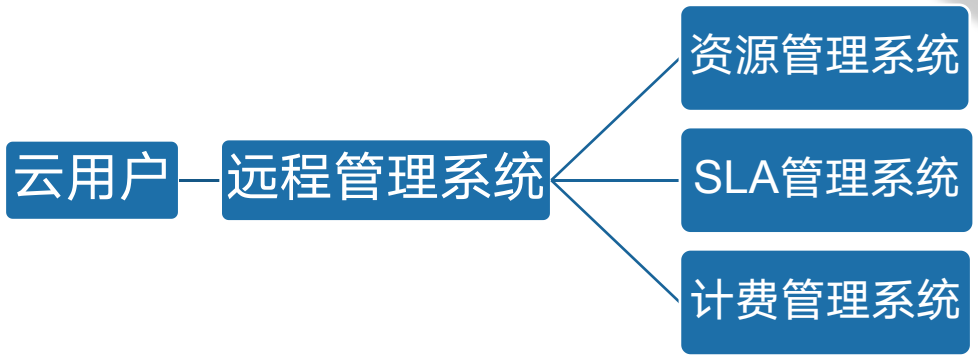
云管理机制

基于云的IT资源需要被建立、配置、维护和监控。远程管理系统是必不可少的，它们促进了形成云平台与解决方案的IT资源的控制和演化，从而形成了云技术架构的关键部分，与管理相关的机制如下

- 远程管理系统
- 资源池化系统
- SLA管理系统
- 计费管理系统
- 资源备份
- 云监控
- 自动化运维
- 服务模板管理
- 云CMDB及流程管理
- 服务目录管理
- 租户及用户管理
- 容量规划及管理
- ……

远程管理系统

远程管理系统（remote administration system）机制向外部的云资源管理者提供工具和用户界面来配置并管理基于云的IT资源。



资源池管理

资源池化管理系统（resource pool management system）是云管理平台的关键所在，因为在一个企业内部，传统数据中心往往打散在不同地区，不同地区的数据中心也会有不同的等级以及业务属性。

资源池是以资源种类为基础来进行划分的，资源池建设考虑以下五个要素

https://ecs.console.aliyun.com/home

SLA管理系统

SLA管理系统（Service Level Agreement Management，服务等级协议）机制代表的是一系列商品化的可用云管理产品。

产品提供的功能包括：SLA数据的管理、收集、存储、报告以及运行时通知，对相关数据的管理、收集、存储、报告以及运行时通知，通常会有一个服务资料测量库。

阿里云：https://help.aliyun.com/document_detail/111729.html?spm=a2c4g.112758.0.0.3917194aKJqJ1V

计费管理系统

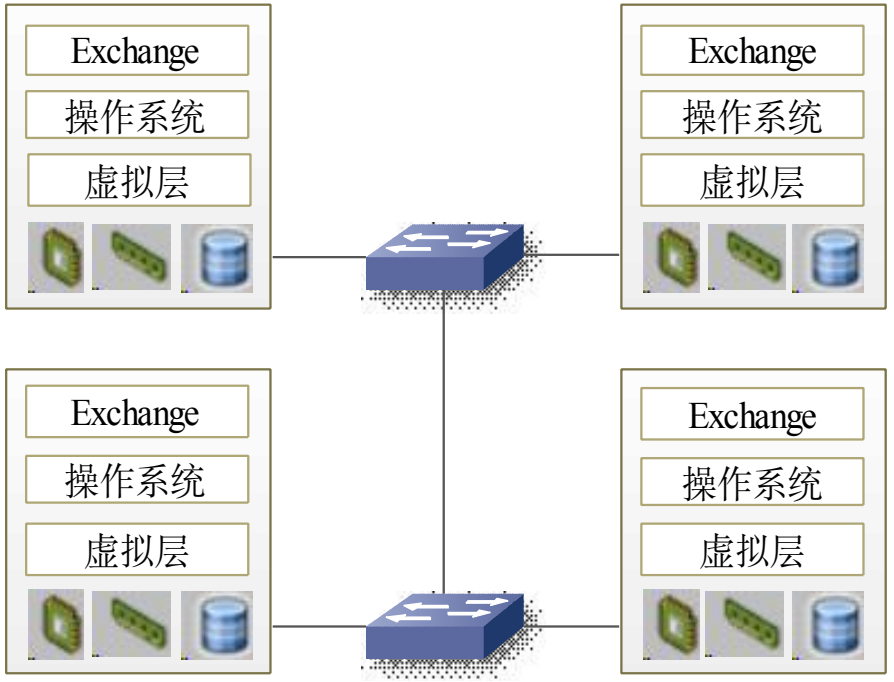
计费管理系统（billing management system）机制专门用于收集和处理使用数据，它涉及云提供者的结算和云用户的计费。

https://usercenter2.aliyun.com/home

计费管理系统组成

资源备份

资源备份（resource backup）可对同一个IT资源创建多个实例。



传统架构视角

云计算架构视角

云监控

为保证应用和服务的性能，开发者必须依据应用程序、服务的设计和实现机制估算工作负载，确定所需资源和容量的数量，避免资源供应不足或供应过量。

云计算使用付费监控器（pay-per-use monitor）机制测量基于云的IT资源使用，生成的使用日志可以用于计算费用，主要包括：

- 请求/响应消息数量
- 传送的数据量
- 带宽消耗量

自动化运维

资源创建后，面临更多时间是如何进行运维和保障，而在弹性自服务方式开通时，我们面对的资源是成几何倍数增长的，这种情况下，云平台的自动化运维就显得格外重要，从以下几个方面可以考虑运维的自动化：

配置	合规	补丁	自动发现
01	02	03	04

服务模版管理

服务模板管理也可以理解为服务蓝图。服务蓝图给出了一种可视化，架构式定义服务的全新方式。

- 提供服务的部署态视图——定义部署服务的一种或多种方式(如虚拟部署形态、物理部署形态、甚至公有云部署形态)
- 能够说明服务运行所需的资源
- 由服务器对象、存储对象和网络对象(含负载均衡/防火墙规则)组成

云CMDB及流程管理

CMDB存储与管理企业IT架构中设备的各种配置信息，它与所有服务支持和服务交付流程都紧密相联，支持这些流程的运转、发挥配置信息的价值，同时依赖于相关流程保证数据的准确性。

- 在云环境下的特点：
  - 资源开通都是用户自助方式开通
  - 对于资源配置的修改会对CI项产生影响

服务目录管理

从管理员的角度，云平台的服务目录应该具备的能力

- 服务目录应该支持对服务的生命周期管理
- 服务目录定义了IT服务的使用者与IT资源之间的标准接口
- 服务实例的管理
- 审批设定

租户及用户管理

- 云平台与传统系统一样，都需要涉及租户和用户的管理。对于不同租户的资源和数据隔离，通常可以通过VPC 逻辑区分，然后再通过VPC和相应的网络安全策略进行邦定，从而实现逻辑隔离。
- 除了租户外，还需要设计权限和用户以及用户组，权限可以赋予用户组也可以单独赋予某个用户，通过用户组可以更方便的划分用户属性。
- 在私有云中，还会涉及配额管理，在公有云中不会涉及。

容量规划及管理

容量规划是基础设施运维护服务的重要组成部分，有效的容量预测工具能够避免性能问题所造成的服务中断。容量信息也是硬件采购，系统扩容，以及节能减排等工作的重要依据。

系统支持业务场景下的容量分析：

- 指定业务KPI，分析特定条件下的容量需求
- 指定业务KPI，分析系统的最大业务容量
- 分析基础设施扩容
- 标识可能的性能瓶颈点
- 比较不同的硬件对系统容量的影响。支持定制化Benchmarks
- 提供容量面板，分析与规划报表

03 特殊云机制

特殊云机制

典型的云技术架构包括大量灵活的部分，这些部分应对IT资源和解决方案有不同的使用要求。有如下特殊云机制：

- 自动伸缩监听器
- 负载均衡器
- 故障转移系统
- 虚拟机监控器
- 资源集群
- 多设备代理
- 状态管理数据库

可以把所有这些机制看成对云基础设施的扩展。

自动伸缩监听器

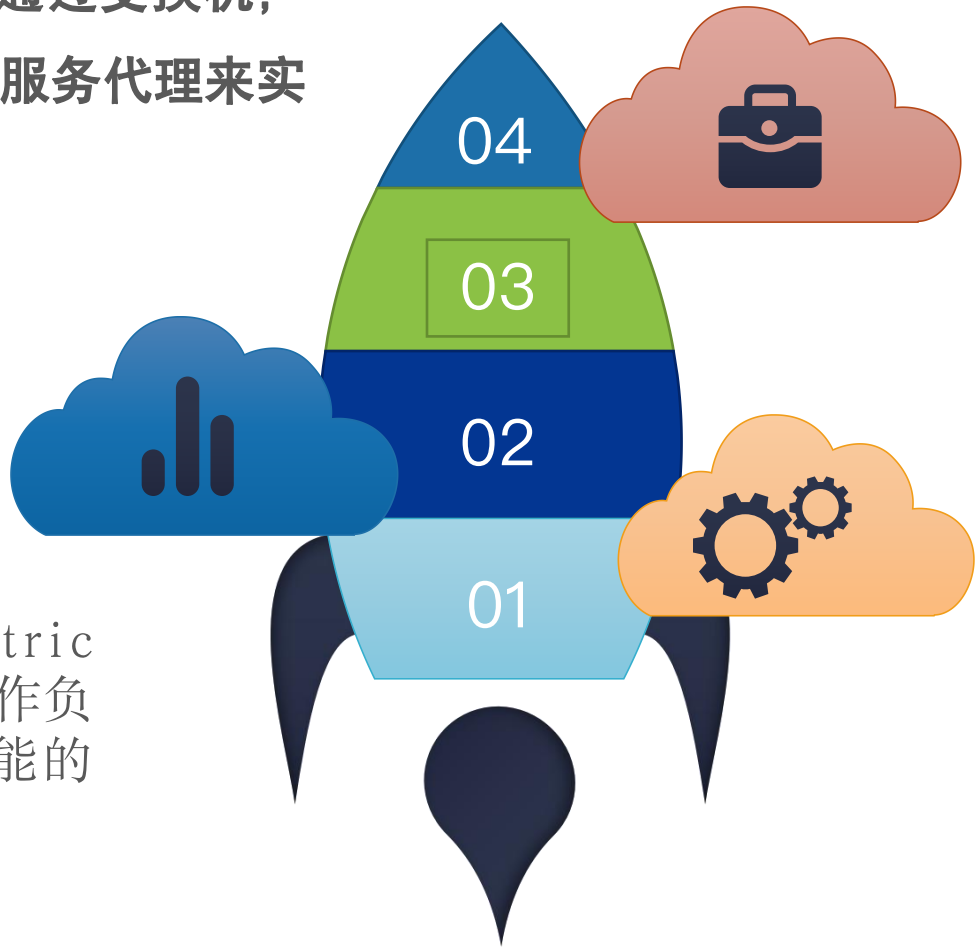
自动伸缩监听器（Automated Scaling Listener）机制是一个服务代理，它监听和追踪用户和云服务之间的通信或IT资源的使用情况。

对于不同负载波动的条件，自动伸缩监控器可以提供不同类型的响应，例如：

- 根据云用户实现定义的参数，自动伸缩IT资源；
- 当负载超过当前阈值或低于已分配资源时，自动通知云用户。

负载均衡器

负载均衡器（load balancer）机制是一个运行时代理，该机制可以通过交换机，专门的硬件/软件设备，以及服务代理来实现。



- 负载优先级（workload prioritization）：负载根据其优先级别进行调度、排队、丢弃和分配；
- 非对称分配（asymmetric distribution）：较大的工作负载被送到具有较强处理能的IT资源；
- 上下文感知的分配（content-aware distribution）：根据请求内容分配到不同的IT资源；

负载均衡实现方式

1. 软件负载均衡技术
2. 硬件负载均衡技术
3. 本地负载均衡技术
4. 全局负载均衡技术（也称为广域网负载均衡）
5. 链路集合负载均衡技术

故障转移系统

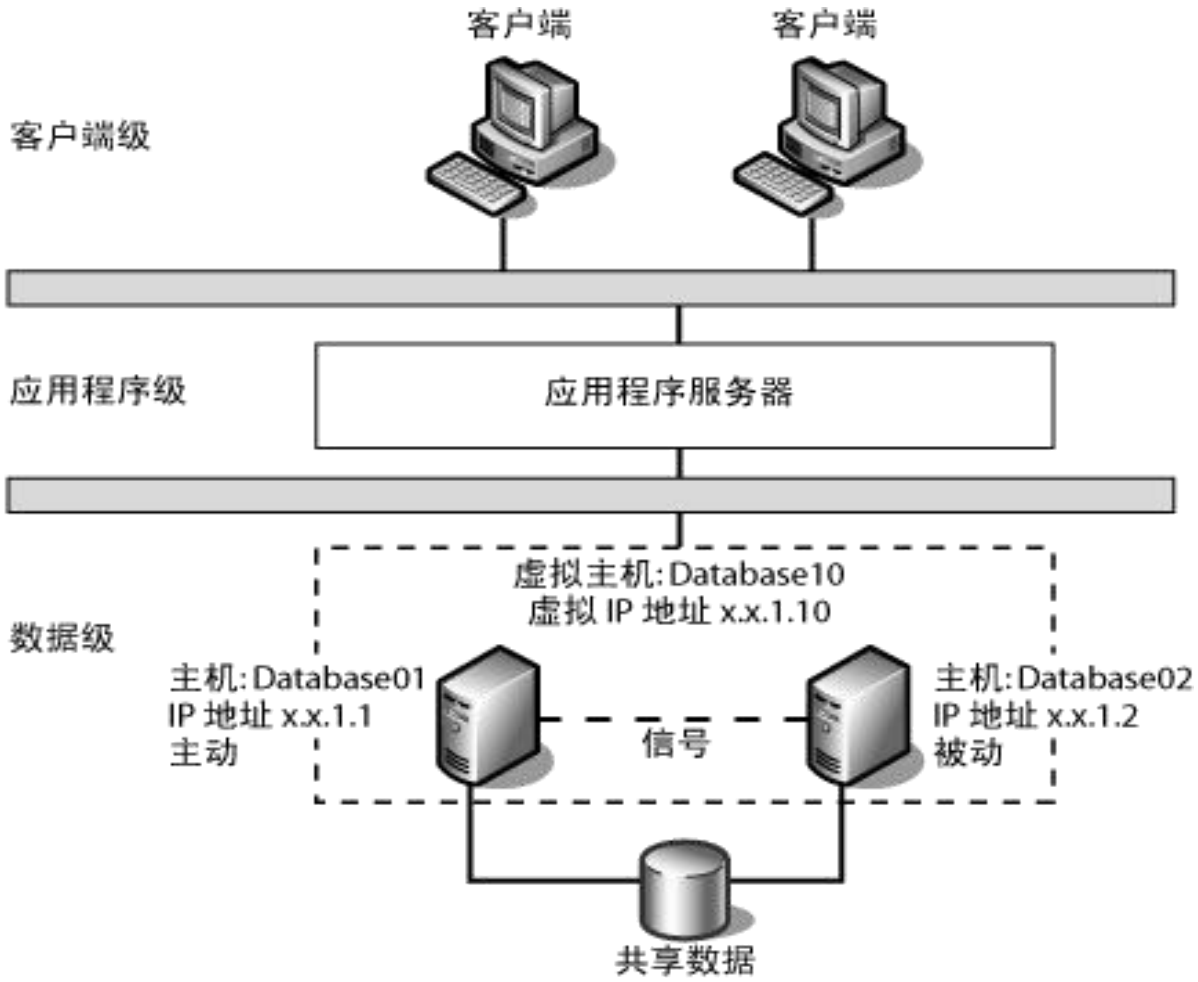
故障转移系统（failover system）通过集群技术提供冗余实现IT资源的可靠性和可用性。

一台服务器接管发生故障的服务器的过程通常称为“故障转移”。如果一台服务器变为不可用，则另一台服务器自动接管发生故障的服务器并继续处理任务。

集群中的每台服务器在集群中至少有一台其它服务器确定为其备用服务器。故障转移系统有两种基本配置：

- 主动-主动
- 主动-被动

故障转移工作原理


客户端
客户端
客户端级
应用程序级
应用程序服务器
数据级
虚拟主机: Database10
虚拟 IP 地址 x.x.1.10
主机: Database01
IP 地址 x.x.1.1
主动
信号
主机: Database02
IP 地址 x.x.1.2
被动
共享数据

资源集群

资源集群（resource cluster）将多个IT资源实例合并成组，使之能像一个IT资源那样进行操作。

HA集群是资源集群的一种，Heartbeat就是Linux-HA项目中的一个组件，其中包括**节点、资源、事件和动作**四个相关术语。

- 服务器集群
- 数据库集群
- 大数据集集群

多设备代理

多设备代理（multi-device broker）机制用来帮助运行时的数据转换，使得云服务被更广泛的用户程序和设备所用。

多设备代理通常是作为网关存在的，或者包含有网关的组件，例如：XML网关、云存储网关以及移动设备网关。多设备代理机制可以创建的转换逻辑层次包括：

1. 传输协议
2. 消息协议
3. 存储设备协议
4. 数据模型/数据模式

状态管理数据库

状态管理数据库（state management database）是一种存储设备，用来暂时地存储软件的状态数据，可以使软件程序和周边的基础设施都具有更大的可扩展性。

本章小结

基础机制是指在IT行业内确立的具有明确定义的IT构件，它通常区别于具体的计算模型和平台。云计算具有以技术为中心的特点，这就需要建立一套正式机制作为探索云技术架构的基础。本章介绍了云计算里常用的云计算机制，在实现过程中可以将它们组成不同的组合形式来具体应用。

深圳技术大学
SHENZHEN TECHNOLOGY UNIVERSITY
SZTU

Thank You!
感谢您的时间！