第14章 云交付模型考量

§14.1 云交付模型：云提供者角度

- 构建IaaS环境
- 装备PaaS环境
- 优化SaaS环境

§14.2 云交付模型：云用户角度

- 使用IaaS环境
- 使用PaaS环境
- 使用SaaS环境

§14.1云交付模型：云提供者角度

- 如何将IPS这些基于云的环境集成到更大的环境中
- 如何把它们与不同的技术和云机制关联起来。
- 构建IaaS环境
- 装备PaaS环境
- 优化SaaS环境

构建IaaS环境

- IaaS的基本资源：
  - 虚拟服务器（VS）、云存储设备
- 主要的配置属性：
  - 操作系统
  - 主存容量
  - 处理能力
  - 虚拟化的存储容量

构建IaaS环境

- VS快照(snapshot)
  - VS当前状态、内存和环境配置的记录
  - 用于备份和复制、水平和垂直扩展
- 自定义VS镜像
  - 导入/出用户自定义构建的虚拟服务器映像
  - 私有格式或者标准格式

地理分布的数据中心

- 多数据中心的IaaS
  - 数据中心通过低延迟的高速通信网络连接
- 主要优势：
  - 多数集装箱集群可以连接起来以增加弹性。
  - 提高可用性和可靠性
  - 负载均衡、IT资源备份和复制以及增加存储容量。
  - 应对法律约束
    - 不同地域的用户受不同法律和法规要求限制

可展性与可靠性

- 在IaaS环境中，通过动态垂直扩展来自动提供虚拟服务器。
- 负载均衡机制是工作负载分布架构的一部分，可以
  - 用来在资源池中的IT资源间分布工作负载
  - 用来完成水平扩展的过程。
- 手工扩展需要云用户与管理程序交互
  - 明确地请求IT终于的扩展

监控

- IaaS环境中的云使用监控器
  - 通过虚拟机管理器VIM实现，或者
  - 采用专门的监控工具，这些工具直接包含虚拟化平台，并与之打交道。
- IaaS平台涉及监控的几个常见性能：
  - 虚拟服务器生命周期(virtual server lifecycle)
  - 数据存储(data storage)
  - 网络流量(network traffic)
  - 失效情况(failure condition)
  - 事件触发器(event trigger)

安全

- 与IaaS环境安全相关的云安全机制括：
  - 加密、哈希、数字签名和PKI机制，用来全面保护数据传输
  - IAM和SSO机制，用来访问安全系统内的服务和接口
  - 基于云的安全组，用于隔离虚拟环境
  - 强化的虚拟服务器映像，用于隔离虚拟环境
  - 各种云使用监控器，追踪提供的虚拟IT资源，来发现异常使用模式

图14-1

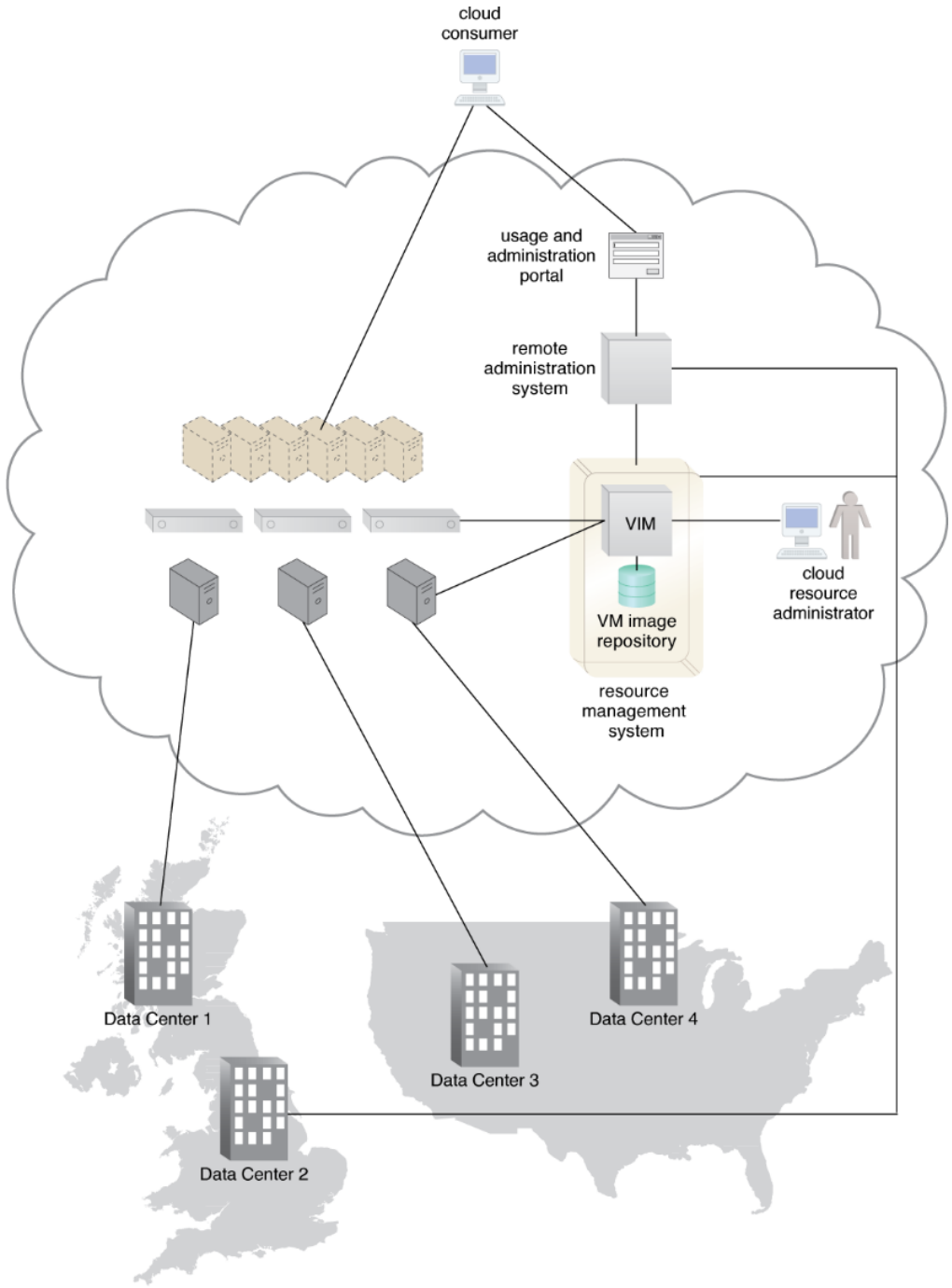


Figure 14.1

- The cloud provider's cloud resource administrator uses the resource management system to
  - set up the physical IT resources and virtualization platform,
  - build pre-configured virtual server images, and
  - generate virtual servers based on these pre-configured images.
- A cloud consumer accesses the usage and administration portal to
  - request the provisioning of Virtual Server A.
- The usage and administration portal interacts with the resource management system, which uses the VIM to
  - automatically locate the necessary physical server and
  - instruct the hypervisor to create the requested virtual server.
- The cloud consumer gains direct access to Virtual Server A and can proceed to deploy software and data.

装备PaaS环境

- PaaS环境一般需要
  - 配备一组选择出来的应用开发和部署平台，以容纳不同的编程模型、语言和框架。
  - 通常为每个编程栈创建一个独立的已就绪环境，包括运行专门为这个平台开发的应用程序所需的软件。
- 云提供者通常提供PaaS平台定制的资源管理系统
  - 云用户可以创建和控制带有已就绪环境的自定义虚拟服务器映像。

可扩展性和可靠性

- 部署在PaaS环境中的云服务和应用的可扩展性需求通常是借助于动态可扩展性和工作负载分配架构来处理的，这些架构依赖于使用本地自动扩展监听器和负载均衡器。
- 已就绪环境与它们承载的云服务和应用的可靠性可以用标准的故障转移系统机制与不中段服务重置架构来支持，从而使云用户免受故障转移情况的麻烦。

监控

- PaaS环境中专门的云使用监控器用来监控下面的内容：
  - 已就绪环境实例(ready-made environment instance)
  - 数据持久化(data persistence)
  - 网络使用(network usage)
  - 失效情况(failure condition)
  - 时间触发器(event trigger)

安全

- 默认情况下，除了那些已经提供给IaaS环境的安全机制，PaaS环境通常不需要引入新的云安全机制。

图14-2

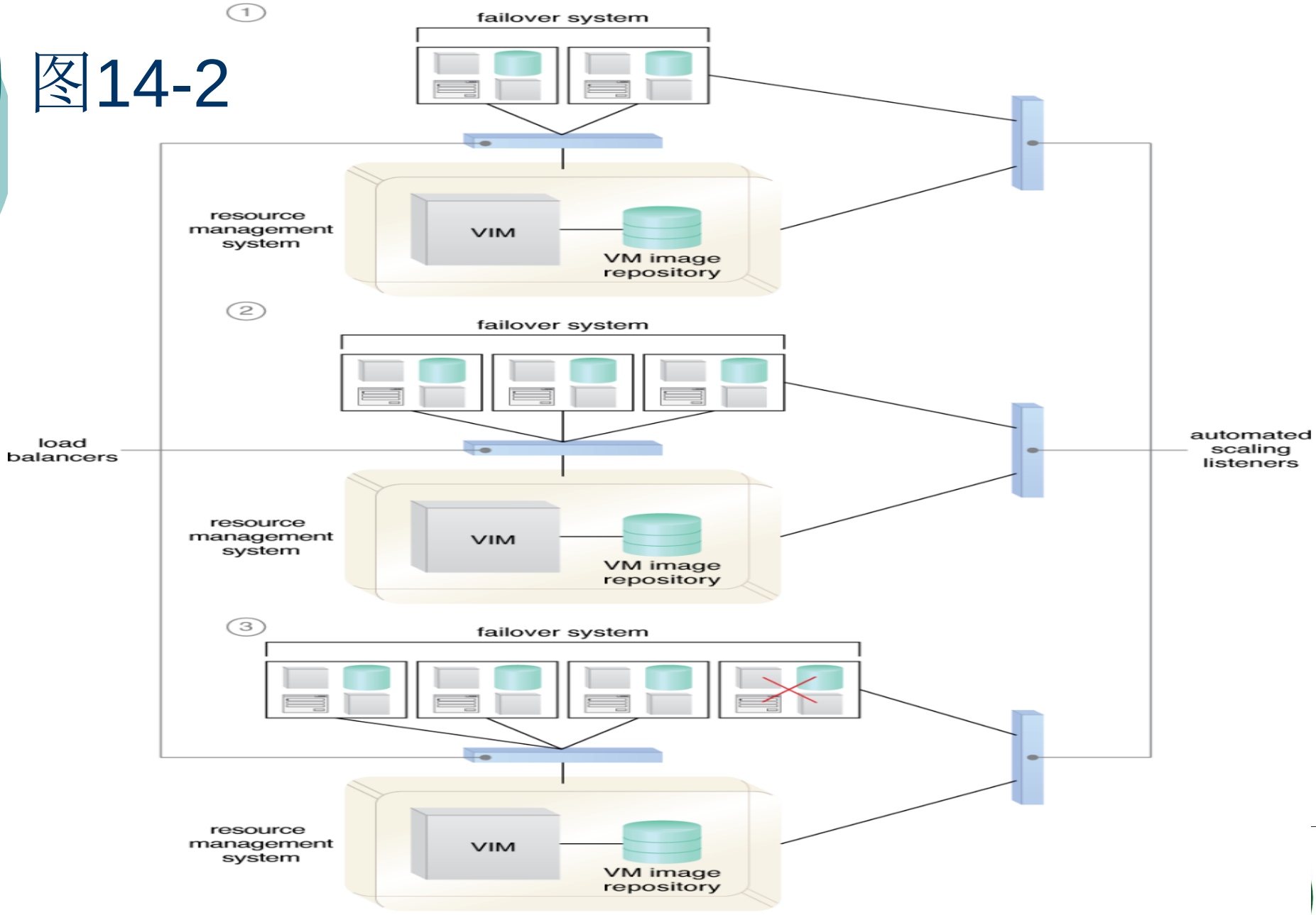


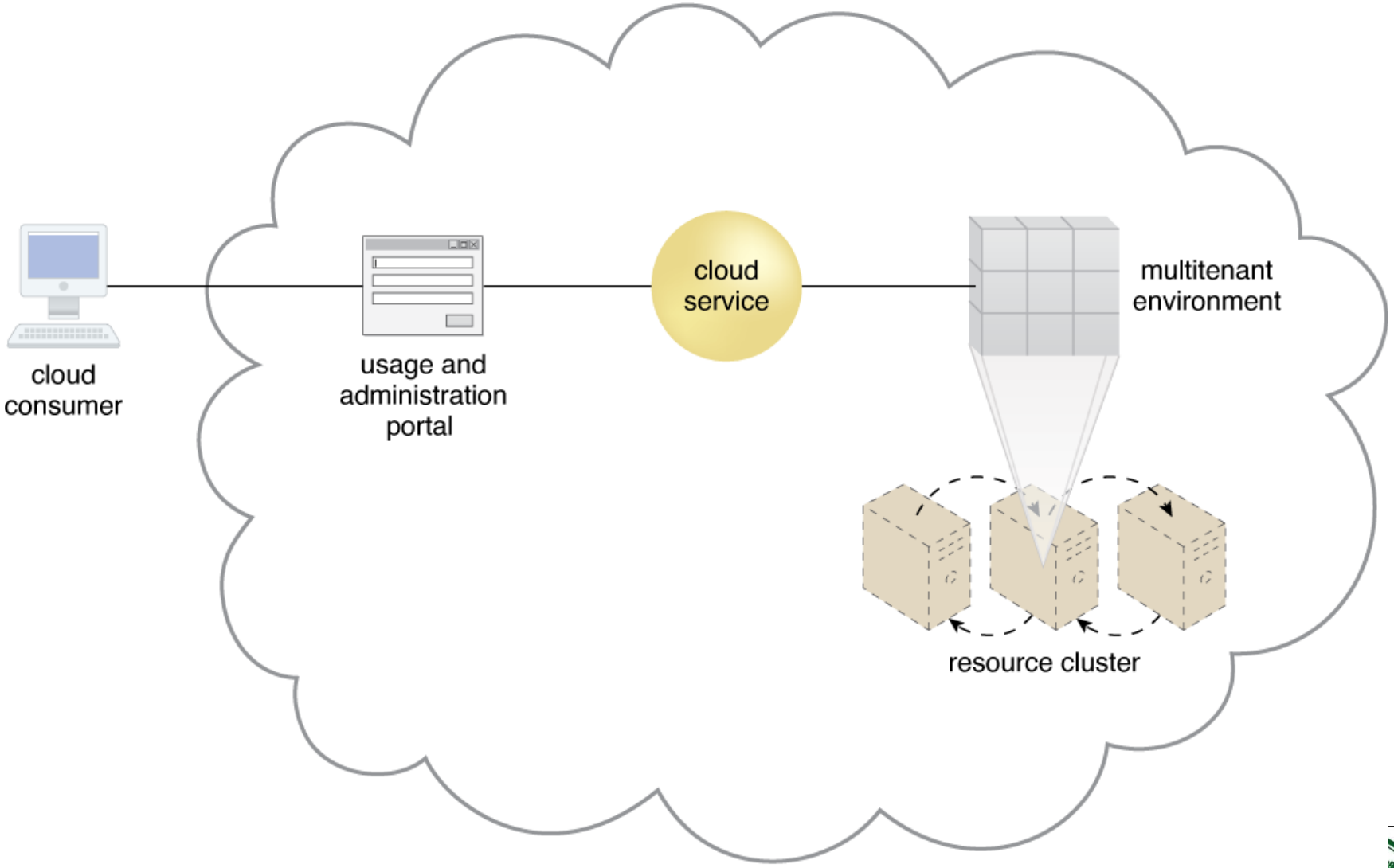
图14-2

- Load balancers are used to distribute ready-made environment instances that are part of a failover system
- Automated scaling listeners are used to monitor the network and instance workloads
- The ready-made environments are scaled out in response to an increase in workload
- The failover system detects a failure condition and stops replicating a failed ready-made environment

优化SaaS环境

- 在SaaS实现中，云服务通常是基于多租户环境的
  - 并发的云用户访问成为可能
- SaaS环境中IT 资源分割通常不发生在其基础设施层次上
  - 与IaaS和PaaS环境不同。

图14-3



优化SaaS环境

- SaaS严重依赖于本地动态可扩展和工作负载分布架构提供的特性。
- SaaS依赖不中断服务重置来保证故障转移情况不影响基于SaaS的云服务的可用性。
- SaaS环境的设计高度专有化
  - 每个SaaS部署都有它独特的架构、功能和运行时要求
  - 由于SaaS的功能多样性、实现技术多样化、实现媒介冗余化

优化SaaS环境

- SaaS依赖的一些架构模型：
  - 服务负载均衡(service load balancing)
  - 动态失效检测和恢复(dynamic failure detection and recovery)
  - 存储维护窗口(storage maintenance wondow)
  - 弹性资源容量(elastic resource capacity/elastic network capacity)
  - 云负载均衡(cloud balancing)

SaaS监控

- SaaS环境通常也会监控数据存储、网络流量、失效情况和时间的触发器
  - 类似于IaaS和PaaS
- SaaS可以使用特殊的云使用监控器追踪指标：
  - 租户订阅周期(tenant subscription period)
  - 应用使用(application usage)
  - 租户应用功能模块(tenant application functional module)

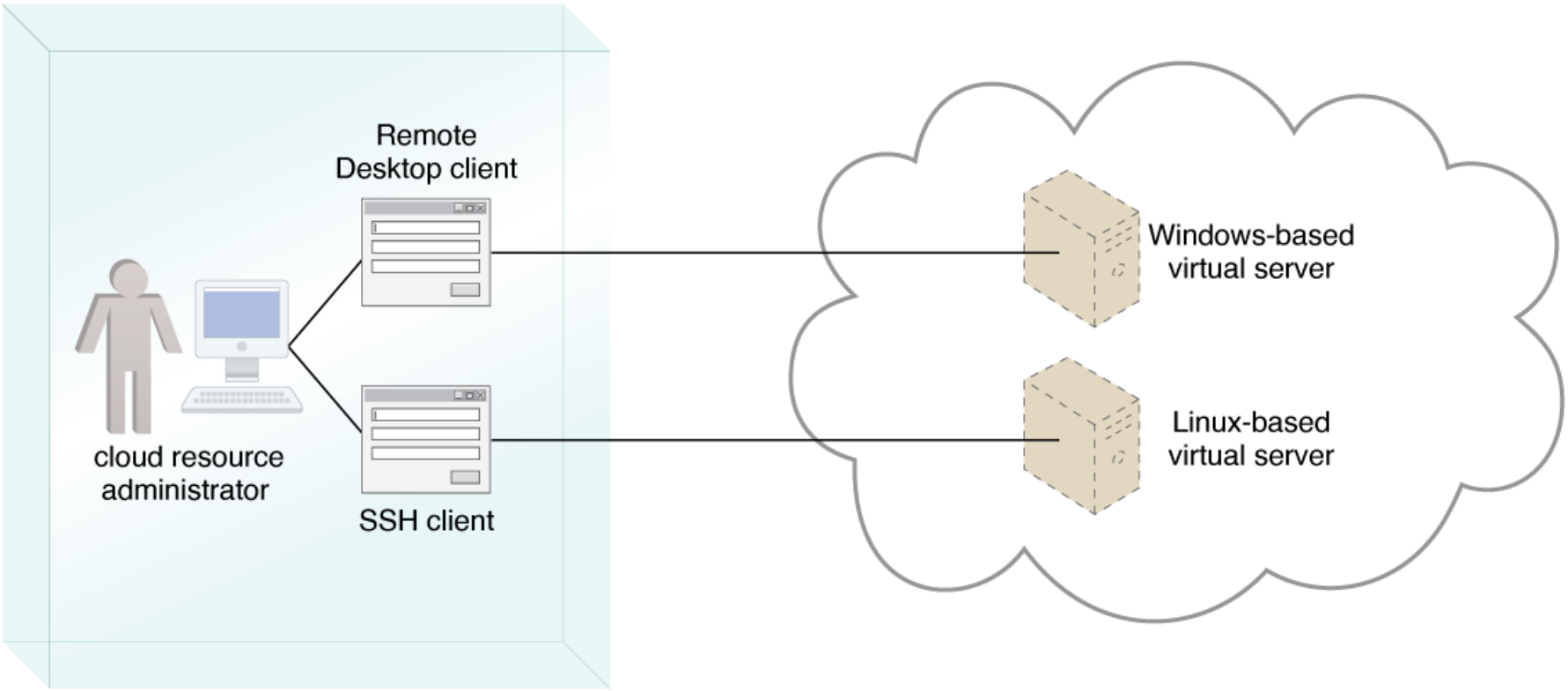
SaaS安全

- SaaS的实现通常依赖于其部署环境内在的安全控制基础。

§14.2 云交付模型：云用户角度

- 访问IaaS服务
  - 通过使用远程终端应用，在操作系统层面上访问虚拟服务器
  - 使用的客户端软件类型直接依赖于虚拟服务器上运行的操作系统类型
- 常见客户端：
  - 远程桌面客户端
  - SSH客户端

图14-4



访问IaaS服务

- 云存储访问有两种方式
- 云储存设备直接附加到虚拟服务器上
  - 通过操作系统提供的虚拟服务器管理功能接口进行访问
- 云存储设备附加到位于云之外的IT资源上
  - 例如一个通过WAN或VPN连接的企业内部设备
  - 常用的管理和传输云存储数据的格式如下所示：
    - 网络连接的文件系统(Networked File System)
    - 存储区域网设备(Storage Area Network Device)
    - 基于Web的资源(Web-based Resource)

IaaS环境下IT资源提供考量

- 云用户对如何提供IT资源以及提供到什么程度的控制权，如：
  - 控制可扩展性特性
  - 控制性能IT资源的生命周期
  - 控制虚拟网络环境和网络访问规则
  - 建立和暂时服务供给合约
  - 管理附加的云存储设备
  - 管理基于云的IT资源的预分配
  - 管理云资源管理员的证书和密码

IaaS环境下IT资源提供考量（con't）

- 管理基于云的安全组证书，这个安全组通过IAM访问虚拟化的IT资源
- 管理与安全相关的配置
- 管理自定义的虚拟服务器映像存储
- 对高可用选项进行选择
- 选择和监控SLA指标
- 选择基本的软件配置
- 从大量可用的与硬件相关的配置和选项中选择IaaS资源实例
- 选择基于云的IT 资源应该放置的地理区域
- 追踪和管理开销

使用PaaS环境

- 一个典型的PaaS的IDE可以提供范围广泛的工具和编程资源
  - 软件库、类库、框架、API
  - 各种运行时能力
- PaaS还允许应用把云存储设备作为独立的数据存储系统来使用
  - 用来存放于开发有关的数据。
  - 一般同时支持SQL和NoSQL的数据库结构。

PaaS环境下IT资源提供考量

- PaaS环境提供的管理控制权少于IaaS环境。
- 例如：
  - 建立和展示服务供给合约，例如账户情况和使用条款
  - 为已就绪环境选择软件平台和开发框架
  - 选择实例类型，最常见的是前端实例或后端实例
  - 选择已就绪环境中使用的云存储设备
  - 控制PaaS开发的应用的生命周期（部署、启动、关闭、重启和释放）
  - 控制部署的应用会和模块的版本

PaaS环境下IT资源提供考量（con't）

- 配置可用性和可靠性相关机制
- 使用IAM来管理开发者和云资源管理员的证书
- 管理通用的安全设置，例如可访问的网络端口
- 选择和监控PaaS相关的SLA指标
- 管理和监控使用情况和IT资源开销
- 控制可扩展性特性，例如使用配额、活跃实例的界限、自动扩展监听器和负载均衡机制的配置和部署

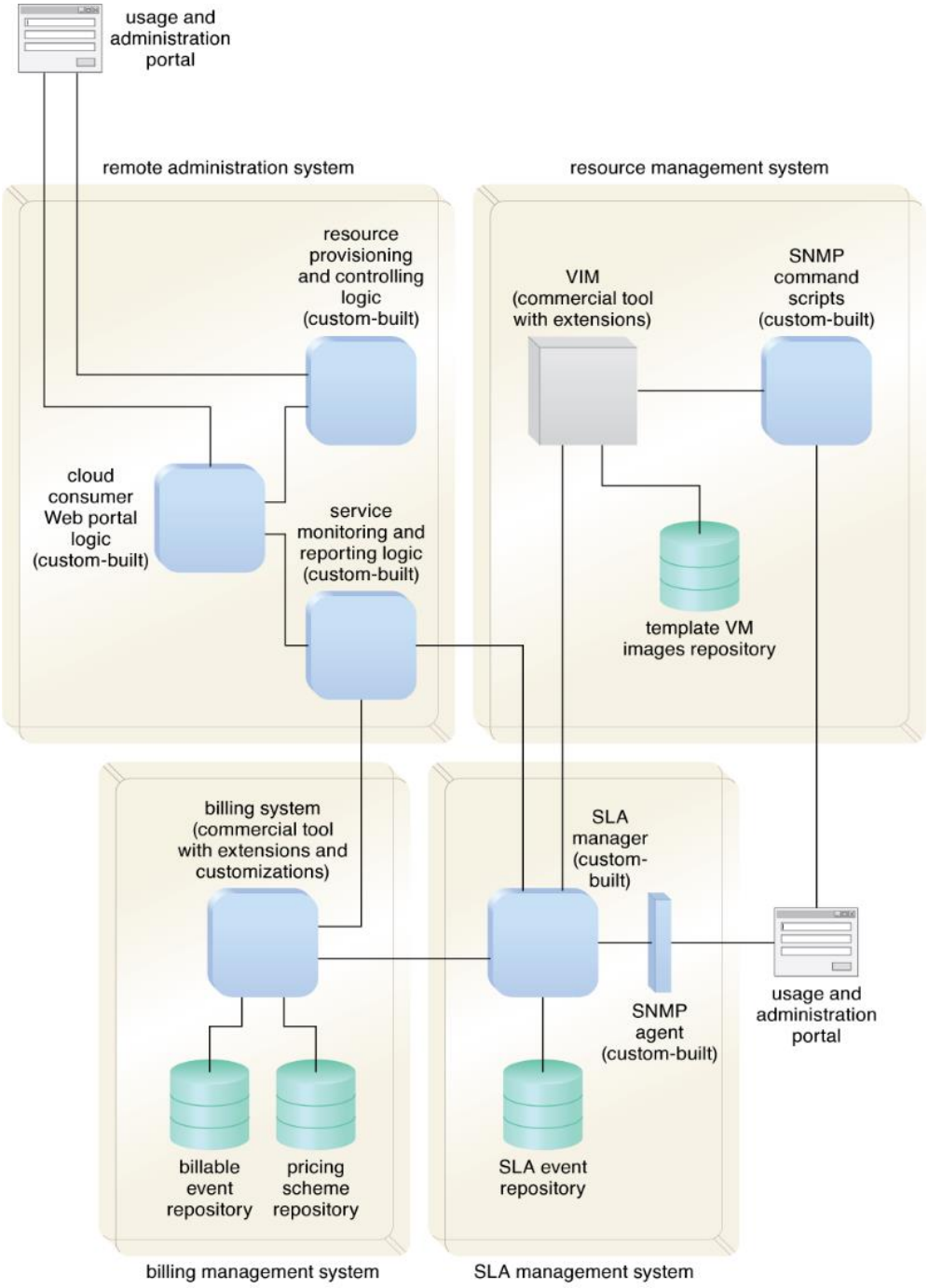
使用SaaS服务

- 基于SaaS的云服务一般都提供通用的API
  - 使得这些服务可以集成到其他系统和服务里。
  - 如Google 地图提供了全面综合的API，使得地图信息和影像可以被继承到Web站点和基于Web的应用里。

使用SaaS服务

- SaaS产品的用户自定义选项通常局限于对云服务实例的运行时使用控制。
- 例如：
  - 管理基于安全的配置
  - 管理对可用性和可靠性选项的选择
  - 管理使用成本
  - 管理用户账户、档案和访问授权
  - 选择和监控SLA
  - 设置手动和自动的可扩展性选择和限制

图14-5


usage and administration portal
remote administration system
resource management system
resource provisioning and controlling logic (custom-built)
VIM (commercial tool with extensions)
SNMP command scripts (custom-built)
cloud consumer Web portal logic (custom-built)
service monitoring and reporting logic (custom-built)
template VM images repository
billing system (commercial tool with extensions and customizations)
SLA manager (custom-built)
SNMP agent (custom-built)
usage and administration portal
billable event repository
pricing scheme repository
SLA event repository
billing management system
SLA management system

课后题

1、SaaS环境中IT 资源分割通常不发生在其基础设施层次上，为什么？