

第七章云基础设施机制

§7.1 逻辑网络边界

§7.2 虚拟服务器

§7.3 云存储设备

§7.4 云使用监控

§7.5 资源复制

§7.6 已就绪环境



云机制

- 云基础设施机制
- 特殊云机制
- 云管理机制
- 云安全机制



§7.1逻辑网络边界

- 将一个网络环境与通信网络的其他部分隔离开来，形成了一个虚拟网络边界。
- 它包含并隔离了一组相关的基于云的IT资源（云服务角度）或者本地IT资源（云用户角度），这些资源在物理上可能是分布式。
- 逻辑网络边界可被用于将云中的IT资源与用户或非用户隔离，也可以将本地IT资源与其他网络环境进行隔离。
- 逻辑网络边界一般作为虚拟化IT环境进行部署，包括：
 - 虚拟防火墙（virtual firewall）
 - 虚拟网络（virtual network）



逻辑网络边界

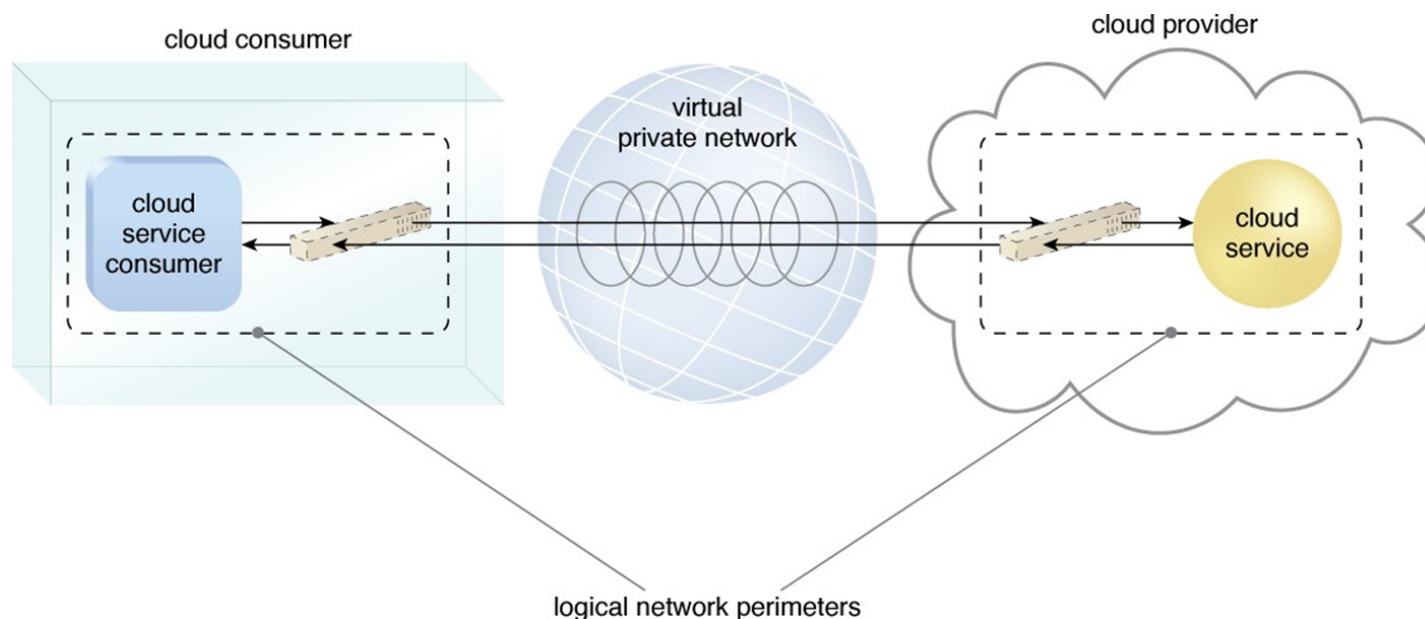


Figure7.3 — 包含云用户和云提供者环境的两个逻辑网络边界

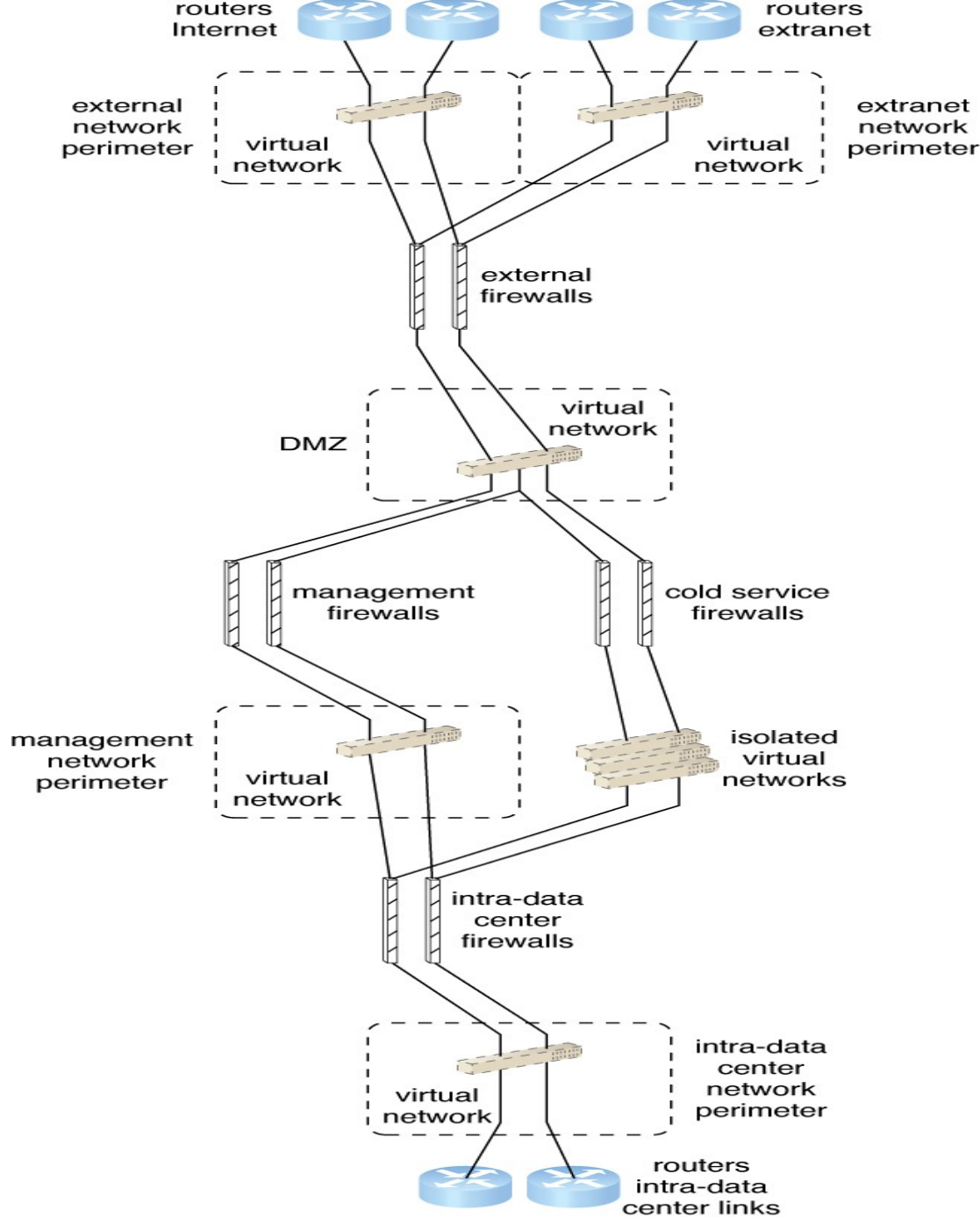
Two logical network perimeters:

- One contains a cloud consumer's on-premise environment,
- while another contains a cloud provider's cloud-based environment.

These perimeters are connected through a VPN that protects communications, since the VPN is typically implemented by point-to-point encryption of the data packets sent between the communicating endpoints.

案例研究

Figure 7.4 — 利用各种防火墙和虚拟网络，通过一组逻辑网络边界建立的逻辑网络布局



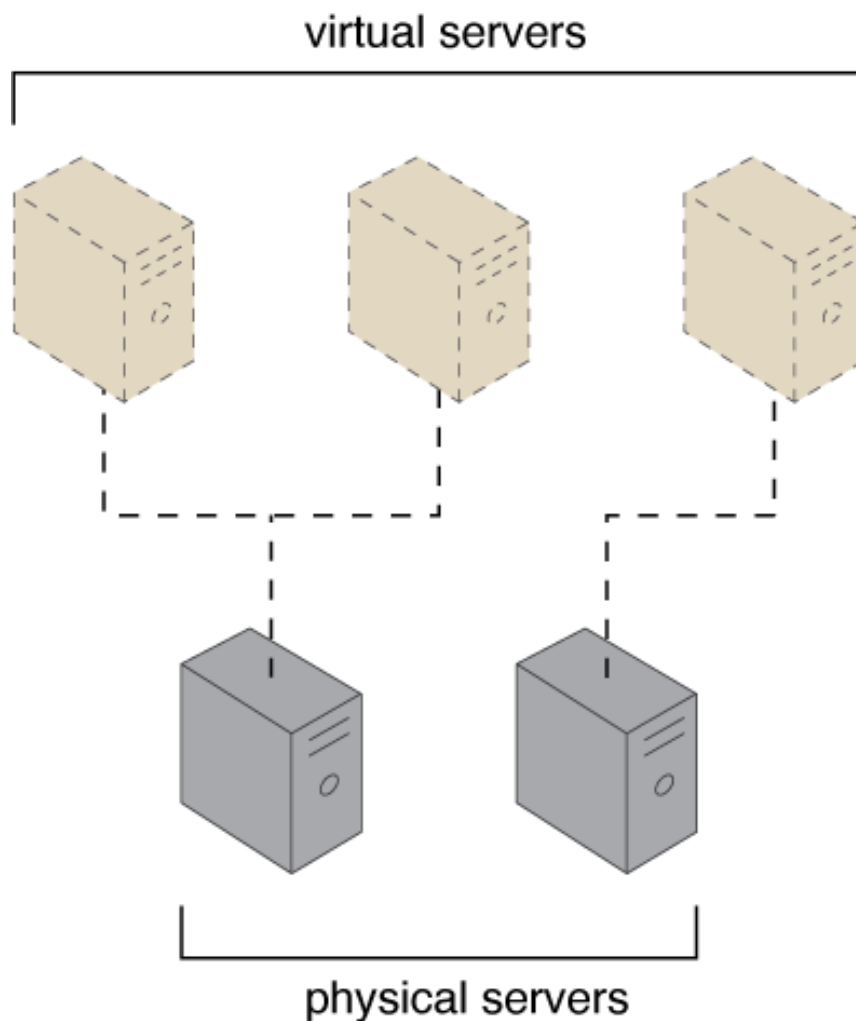
§7.2 虚拟服务器

- 虚拟服务器是一种模拟物理服务器的虚拟化软件。
- 虚拟服务器是最基本的云环境构建块。
- 虚拟服务器作为宿主，包括：
 1. 多个IT资源
 2. 基于云的解决方案
 3. 各种其他云计算机制
- 从映像文件进行虚拟服务器的实例化是一个可以快速且按需完成的资源分配过程。
- 通过安装或释放虚拟服务器，云用户可以定制自己的环境。
 - 这个环境独立于其他正在使用由同一底层物理服务器控制的虚拟服务器的云用户。



虚拟服务器

Figure 7.5 — 第一个物理服务器控制2个虚拟服务器，第二个物理服务器控制1个虚拟服务器——一个物理服务器能够控制的虚拟服务器的最大个数取决于该物理服务器的性能。



Copyright © Arcitura Education



虚拟服务器

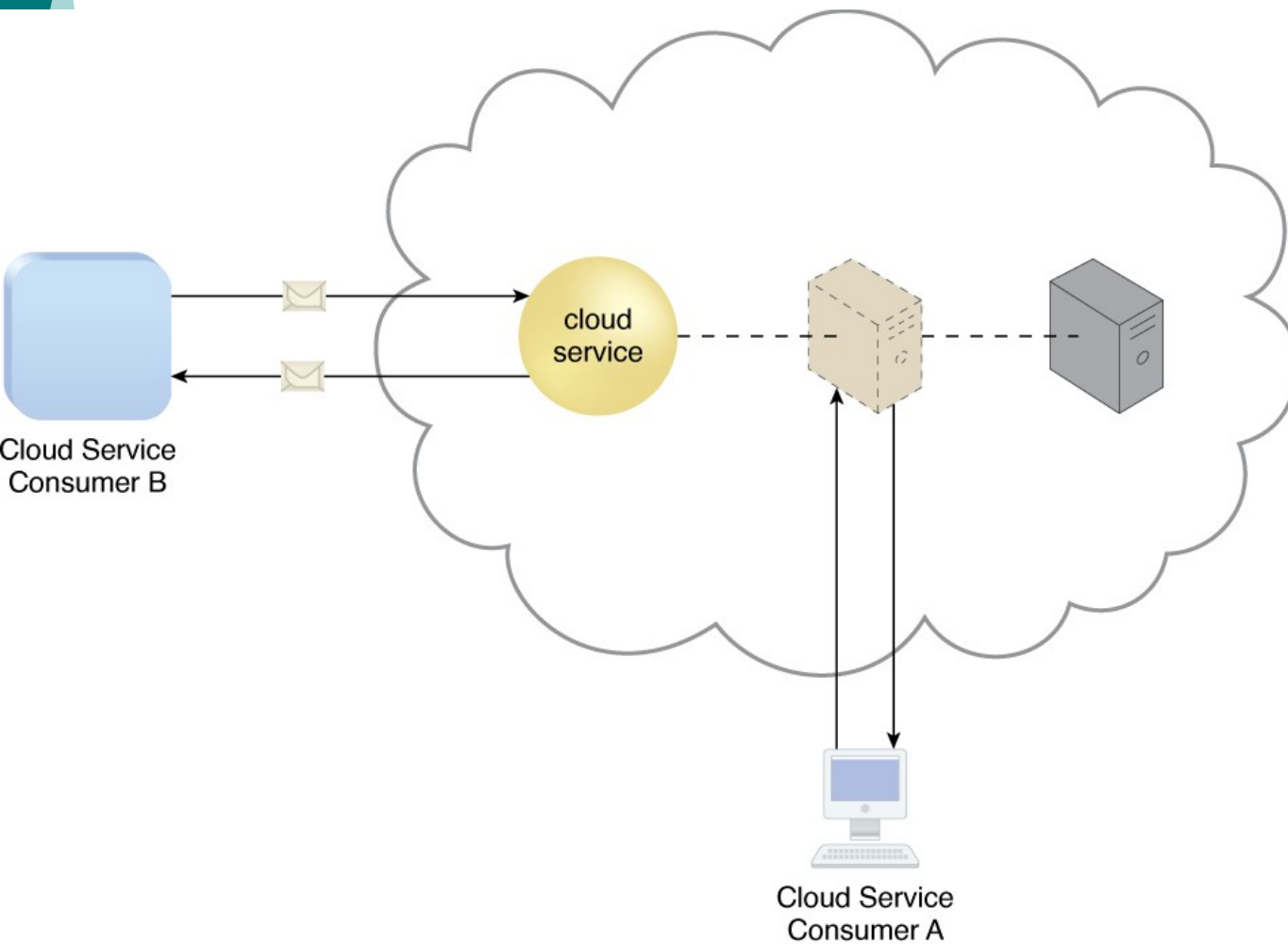
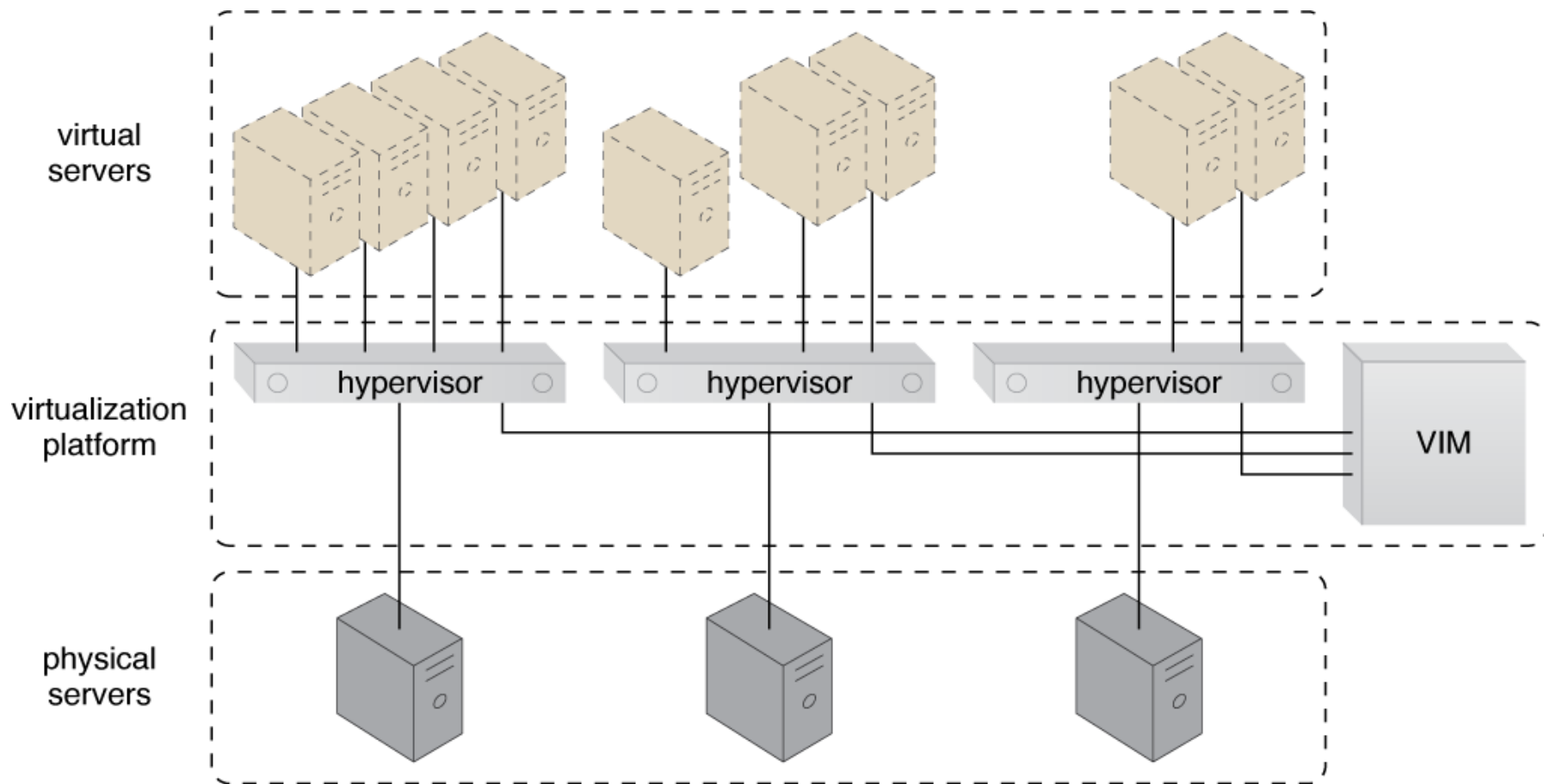


Figure7.6 — 一个虚拟服务器驻留着一个正在被使用的云服务，同时一个云用户以管理为目的对该服务器进行访问

案例研究



Copyright © Arcitura Education

Figure7.7 — 通过物理服务器的虚拟机监控器和中心VIM创建虚拟服务器



§7.3 云存储设备

- 云存储设备是指专门为基于云配置所设计的存储设备。
- 在支持按使用计费的机制时，云存储设备通常可以提供固定增幅的容量分配。
- 与云存储相关的主要问题是数据的安全性、完整性和保密性。



云存储设备

- 云存储设备机制提供常见的**数据存储逻辑单元**，例如：
 - 文件（**file**）——存放于文件夹中，可以不同大小、格式，通常直接被替换，更改
 - 块（**block**）——存储的最低等级，最接近硬件，可被独立访问的**最小数据单位**
 - 数据集（**dataset**）——基于**表格**的、以**分隔符**分隔的或以**记录**形式组织的**数据集合**
 - 对象（**object**）——将数据及其相关的元数据组织为基于**Web**的资源



云存储设备

- 根据不同的存储等级，有**三种**相关的技术接口：
 - 网络存储接口——文件或块
 - 对象存储接口——Web资源
 - 数据库存储接口——分为关系数据存储和非关系数据存储（NoSQL），即数据集



云存储设备---网络存储接口

Old network storage, e.g. files and blocks, most commonly falls under the category of network storage interfaces. It includes storage devices with industry standard protocols, such as

- 1 SCSI for storage blocks and the server message block (SMB)
- 2 common Internet file system (CIFS)
- 3 network file system (NFS) for file and network storage.



云存储设备---对象存储接口

- Various types of data can be referenced and stored as **Web resources**. This is referred to as **object storage**, which is based on technologies that can support a range of data and media types.
- Cloud Storage Device mechanisms that implement this interface can typically be accessed via **REST** or **Web service-based cloud services using HTTP** as the prime protocol.



云存储设备---数据库存储接口

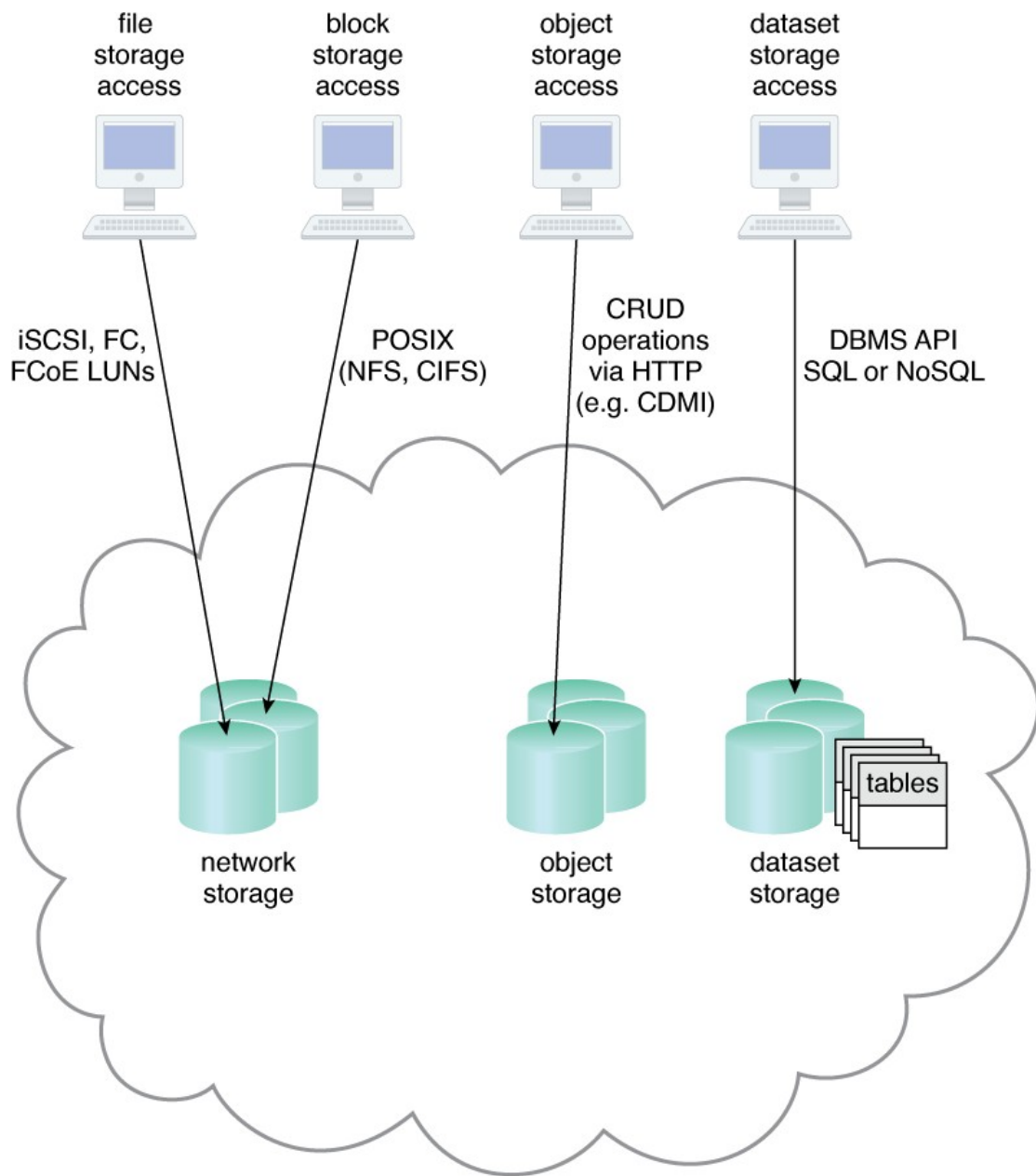
Cloud storage device mechanisms based on **database storage interfaces** typically support a **query language** in addition to basic storage operations.

Storage management is carried out using a **standard API** or an **administrative user-interface**.



云存储等级

Figure 7.9 — 不同的云服务用户使用不同的技术与虚拟化云存储设备相连接



案例研究

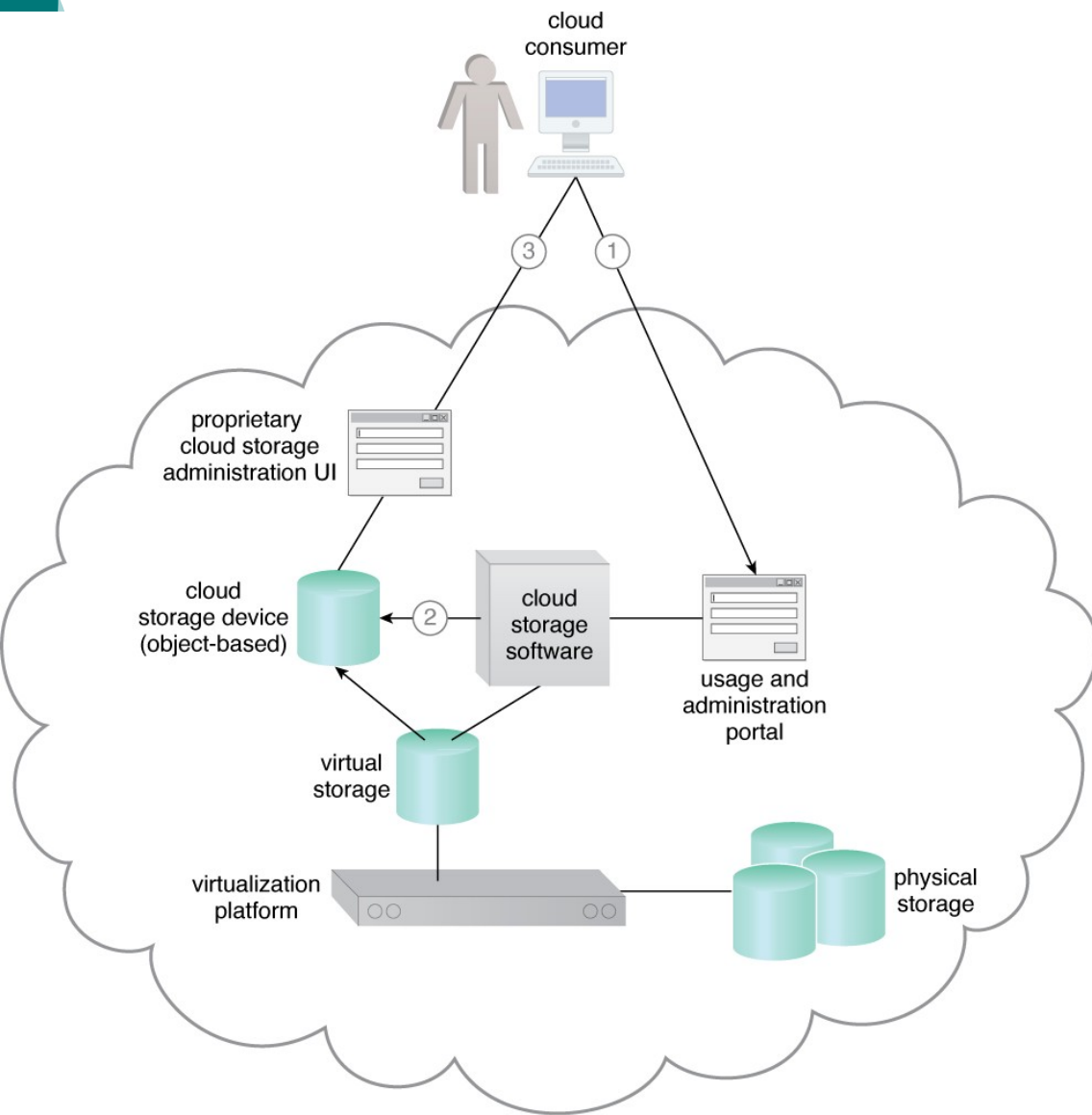


Figure7.10 — 云用户通过使用与管理入口进行交互，

(1) 创建一个云存储设备，并定义访问控制规则；

(2) 创建云存储设备实例，并对其数据对象实行请求访问策略。所有的数据对象都存入同一个虚拟存储卷。

(3) 云用户通过专有云存储设备界面直接与数据对象交互。

案例研究

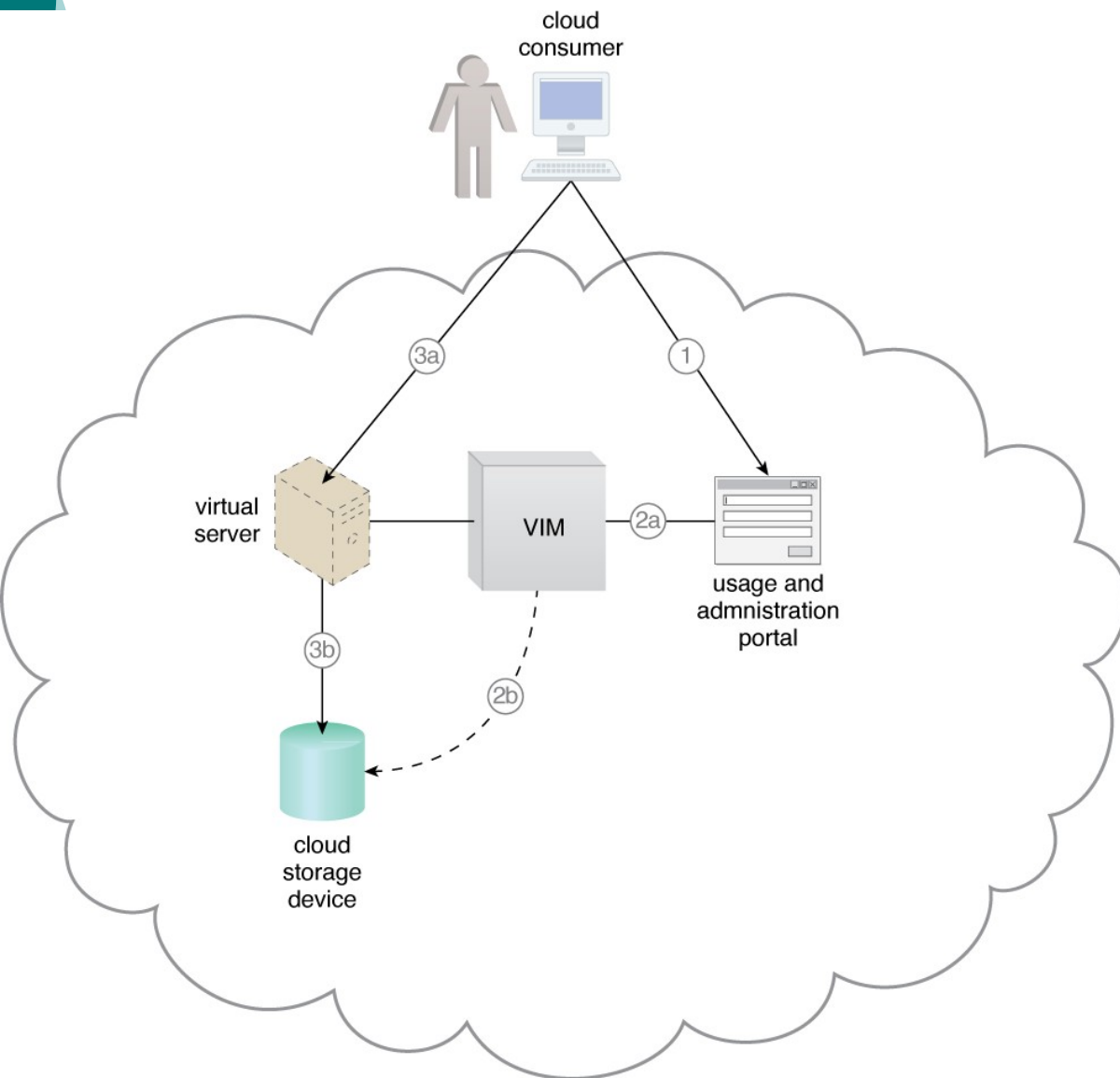


Figure 7.11 — 云用户通过使用与管理入口

(1) 为一个已有虚拟服务器创建并分配一个云存储设备（**基于文件的**），

(2a) 与VIM交互，

(2b) 创建并配置适当的**LUN**（**逻辑单元号**），每个云存储设备使用的是虚拟化平台控制下的独立**LUN**；

(3a) 云用户直接远程登录到虚拟服务器，

(3b) 访问云存储设备。

§7.4 云使用监控

- 云使用监控机制是一种轻量级的自治软件程序
- 用于收集和~~处理~~IT资源的使用数据
- 将使用数据发送到日志数据库，以便进行后续处理和报告。
- 三种常见的实现形式：（基于代理）
 - 监控代理（monitoring agent）
 - 资源代理（resource agent）
 - 轮询代理（polling agent）



云使用监控---监控代理

Definition

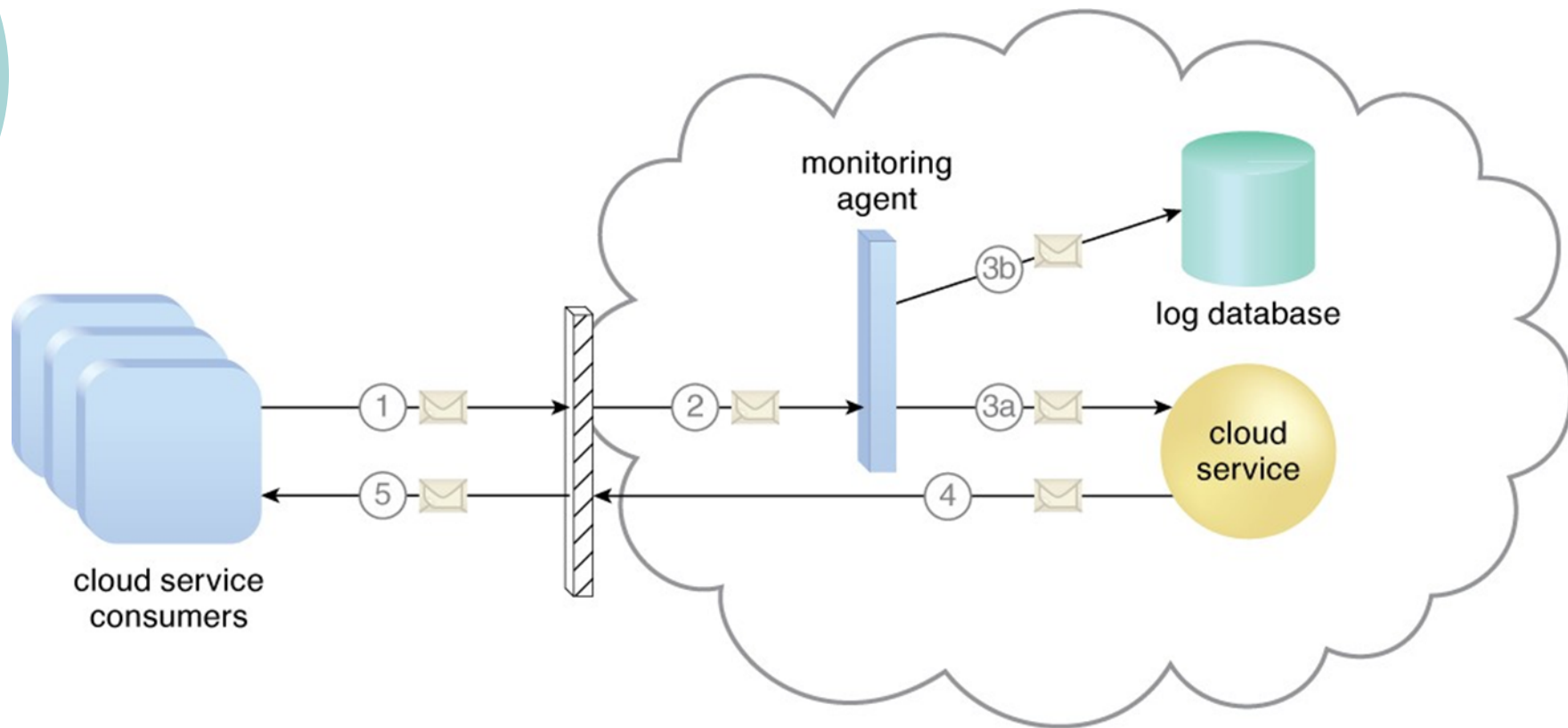
A monitoring agent is an intermediary, event-driven program that exists as a service agent and resides along existing communication paths to transparently monitor and analyze dataflows.

This type of cloud usage monitor is commonly used to measure network traffic and message metrics.

一个中间的事件驱动程序，对数据流进行透明的监控和分析



监控代理



Copyright © Arcitura Education

Figure7.12 — 云服务用户向云服务发送请求消息（1）监控代理拦截此消息，收集相关使用数据（2），然后将其继续发往云服务（3a）。监控代理将收集到的使用数据存入日志数据库（3b）。云服务产生应答消息（4），并将其发送回云服务用户，此时监控代理不会进行拦截（5）。



云使用监控---资源代理

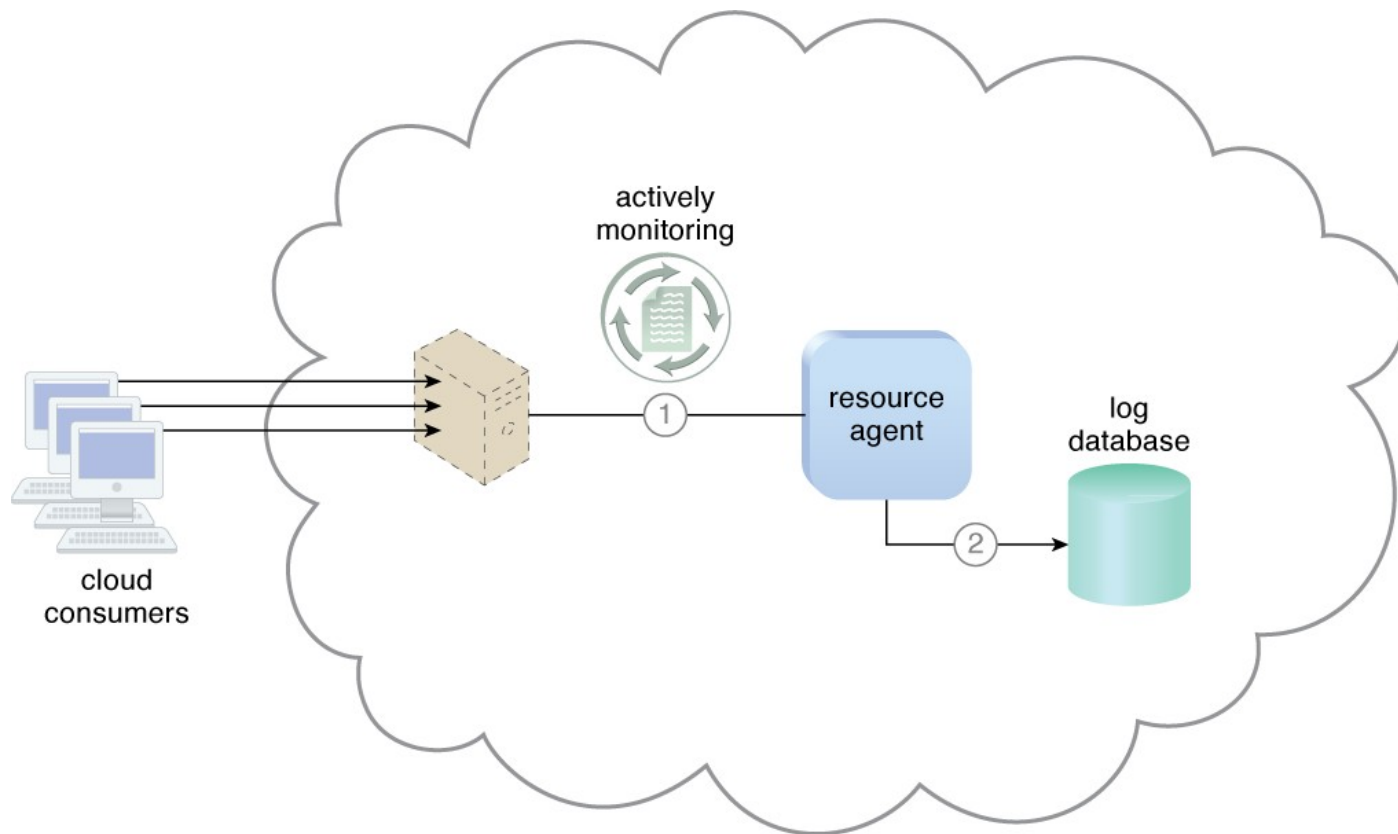
Definition

A **resource agent** is a **processing** module that collects **usage data** by having **event-driven interactions** with specialized resource software.

This module is used to **monitor usage metrics** based on pre-defined, observable events at the **resource software level**, such as

- initiating
- suspending
- resuming
- vertical scaling.

资源代理



Copyright © Arcitura Education

Figure7.13 — 资源代理主动监控虚拟服务器，并检测到使用的增加（1）。资源代理从底层资源管理程序收到通知，虚拟服务器正在进行扩展，按照其监控指标，资源代理将收集的使用数据存入日志数据库（2）。



云使用监控---轮询代理

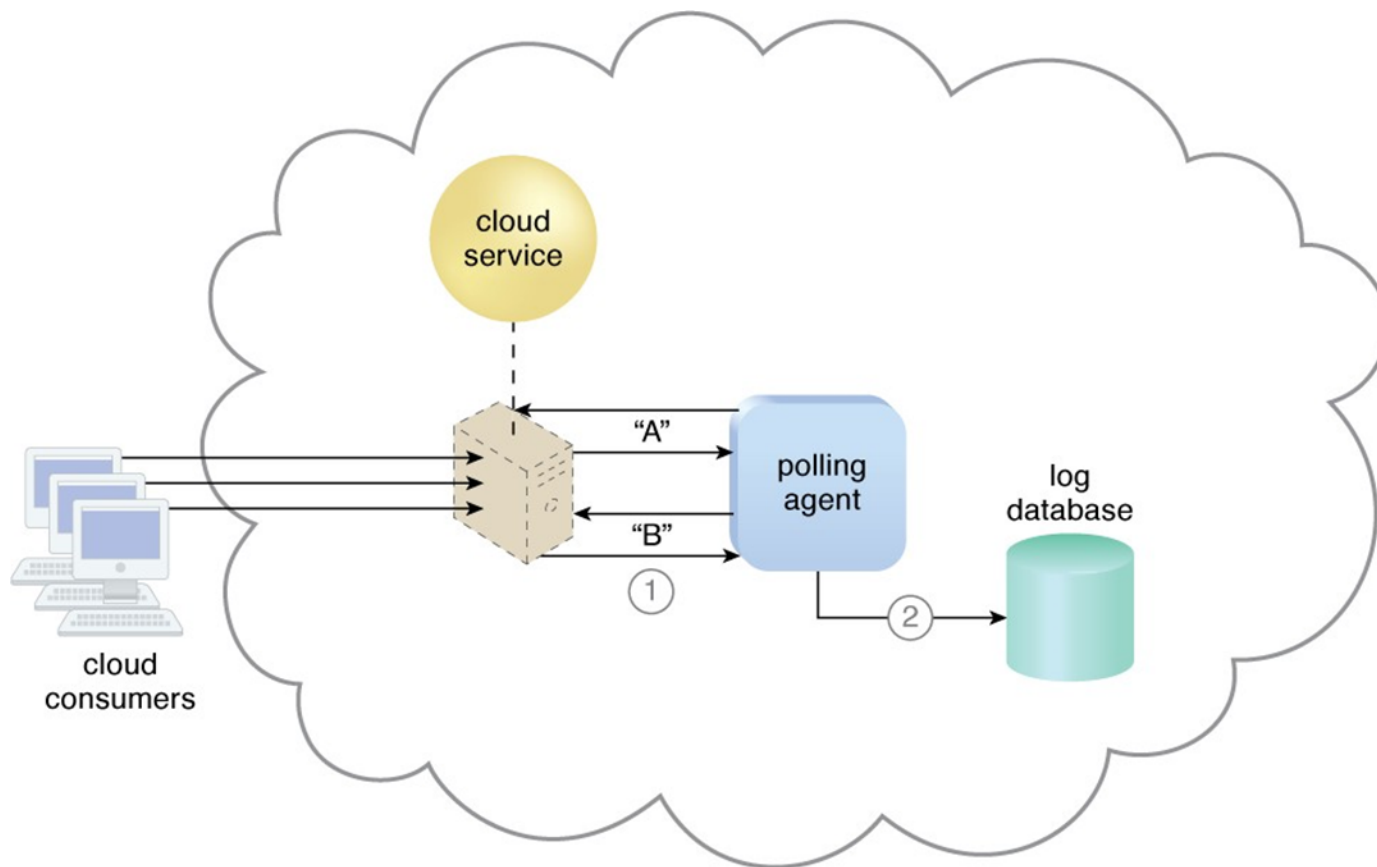
Definition

A **polling agent** is a **processing** module that collects **cloud service usage data** by polling IT resources.

This type of cloud service monitor is commonly used to periodically **monitor IT resource status**, such as uptime and downtime.



轮询代理



Copyright © Arcitura Education

Figure7.14 — 轮询代理监控虚拟服务器上的云服务状态，它周期性地发送轮询消息，并在数个轮询周期后接收到使用状态为“A”的轮询响应消息。当代理接收到使用状态为“B”时（1），轮询代理就将新的使用状态记录到日志数据库中（2）。



案例研究

Figure 7.15 【1/2】 — 云用户（CS_ID=CS1）请求创建虚拟服务器（VM_ID=VM1），配置大小为type1（VM_TYPE=type1）（1）。

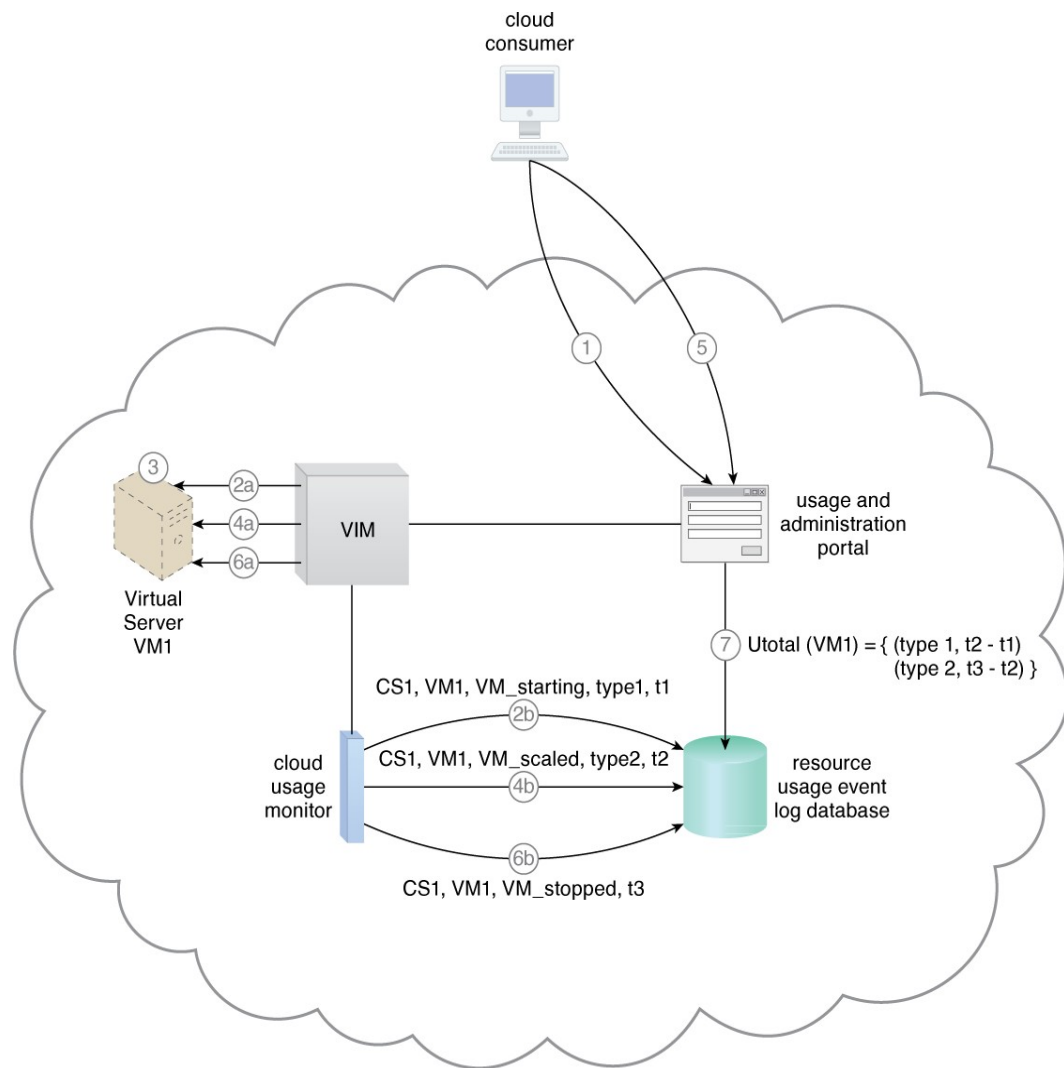
VIM创建虚拟服务器（2a）。

VIM事件驱动API生成时间戳为t1的资源使用时间，云使用资源监控软件将其捕捉记录在资源使用事件日志数据库中（2b）。

虚拟服务器使用增加并达到自动扩展的阈值（3）。

VIM将VM1的配置从type1扩展到type2（VM_TYPE=type2）（4a）。

VIM事件驱动API生成时间戳为t2的资源使用事件，云使用资源监控软件代理将其捕捉并记录在资源使用事件日志数据库中（4b）。

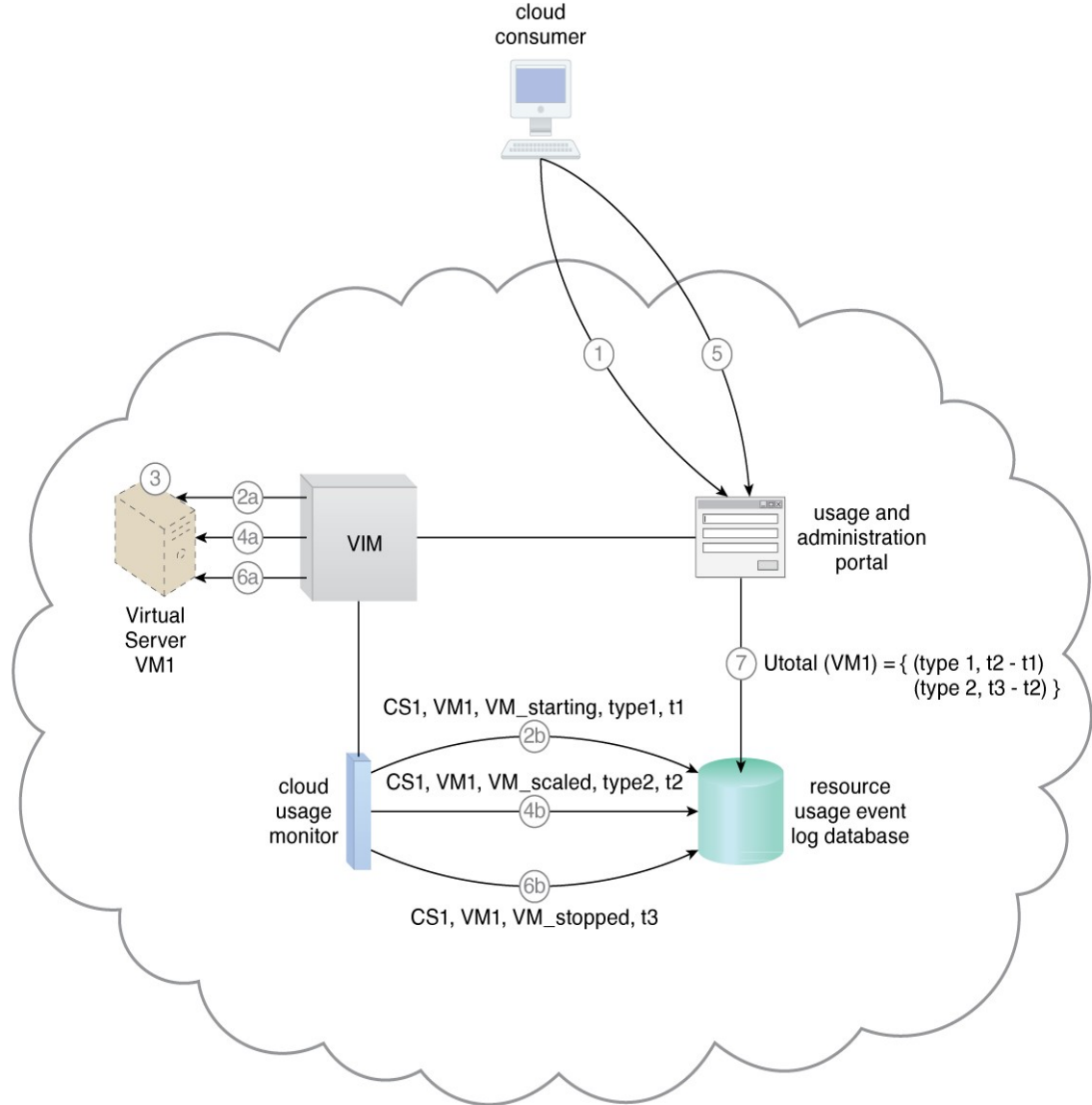


Copyright © Arcitura Education



案例研究

Figure 7.15 【2/2】 —云用户关闭虚拟服务器（5）。VIM停止VM1（6a）。其事件驱动API生成时间戳为t3的资源使用事件，云使用监控软件轮询代理将其捕捉并记录在资源使用时间日志数据库中（6b）。使用与管理入口访问日志数据库，计算虚拟服务器的使用总量Utotal VM1（7）。

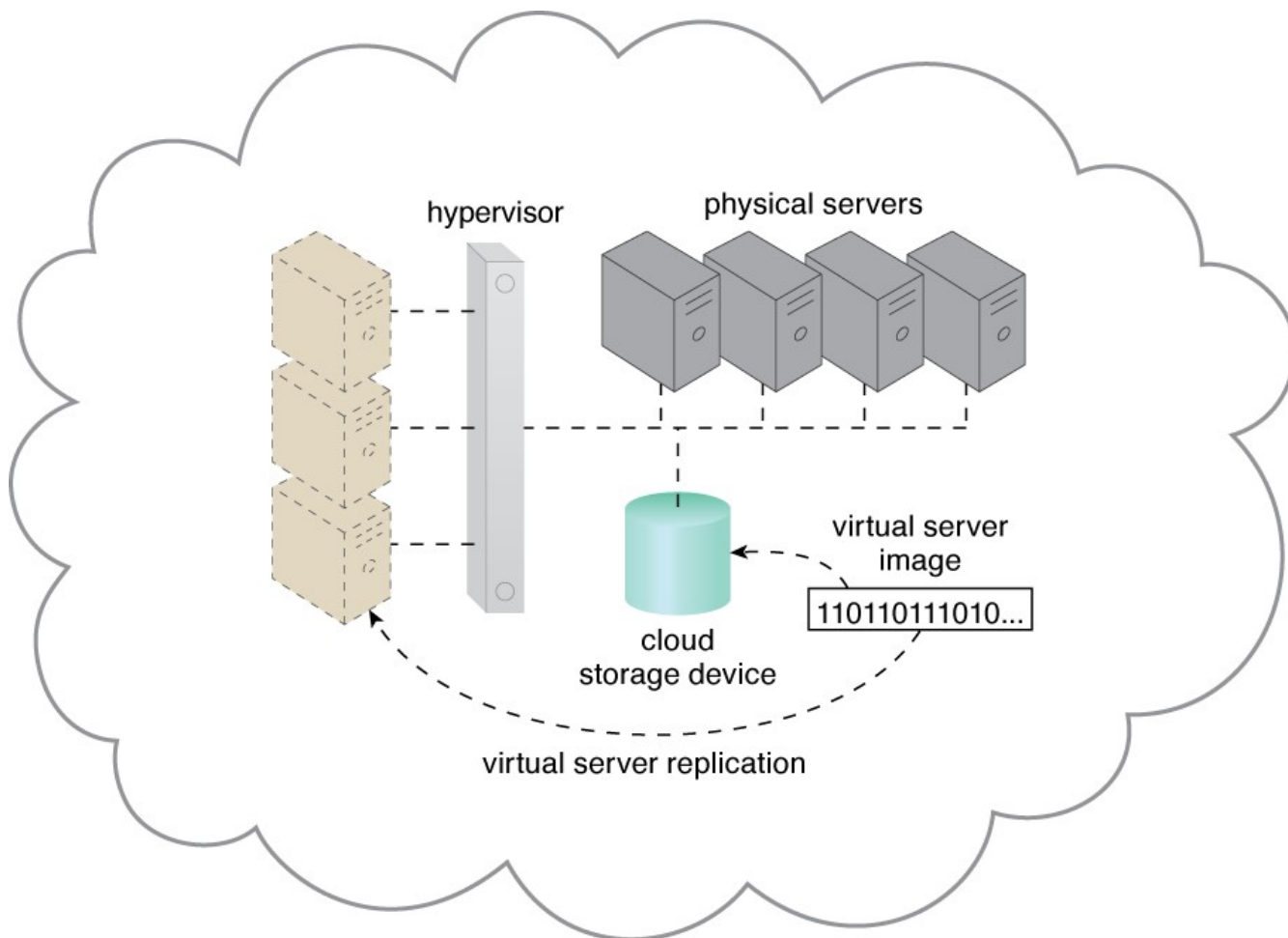


§7.5 资源复制

- 资源复制定义为对同一个IT资源创建多个实例，通常在需要加强IT资源的可用性和性能时执行。
- 资源复制机制使用虚拟化技术来复制基于云的IT资源。



资源复制



Copyright © Arcitura Education

Figure7.16 — 虚拟机监控器利用已存储的**虚拟服务器映像**复制了该虚拟服务器的多个实例

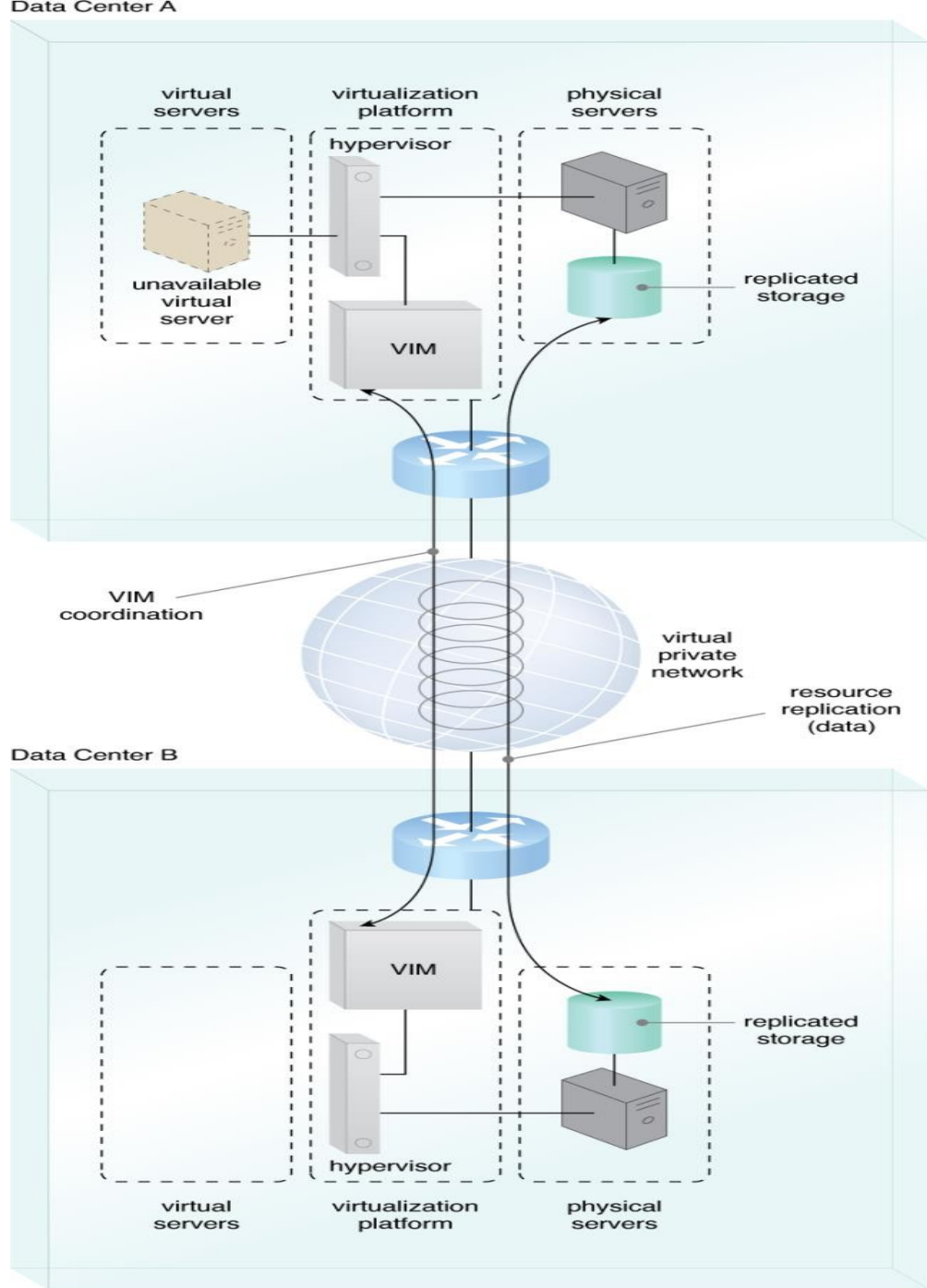


案例研究

Figure 7.17 — 一个高可用性
虚拟服务器运行在数据中
心A。

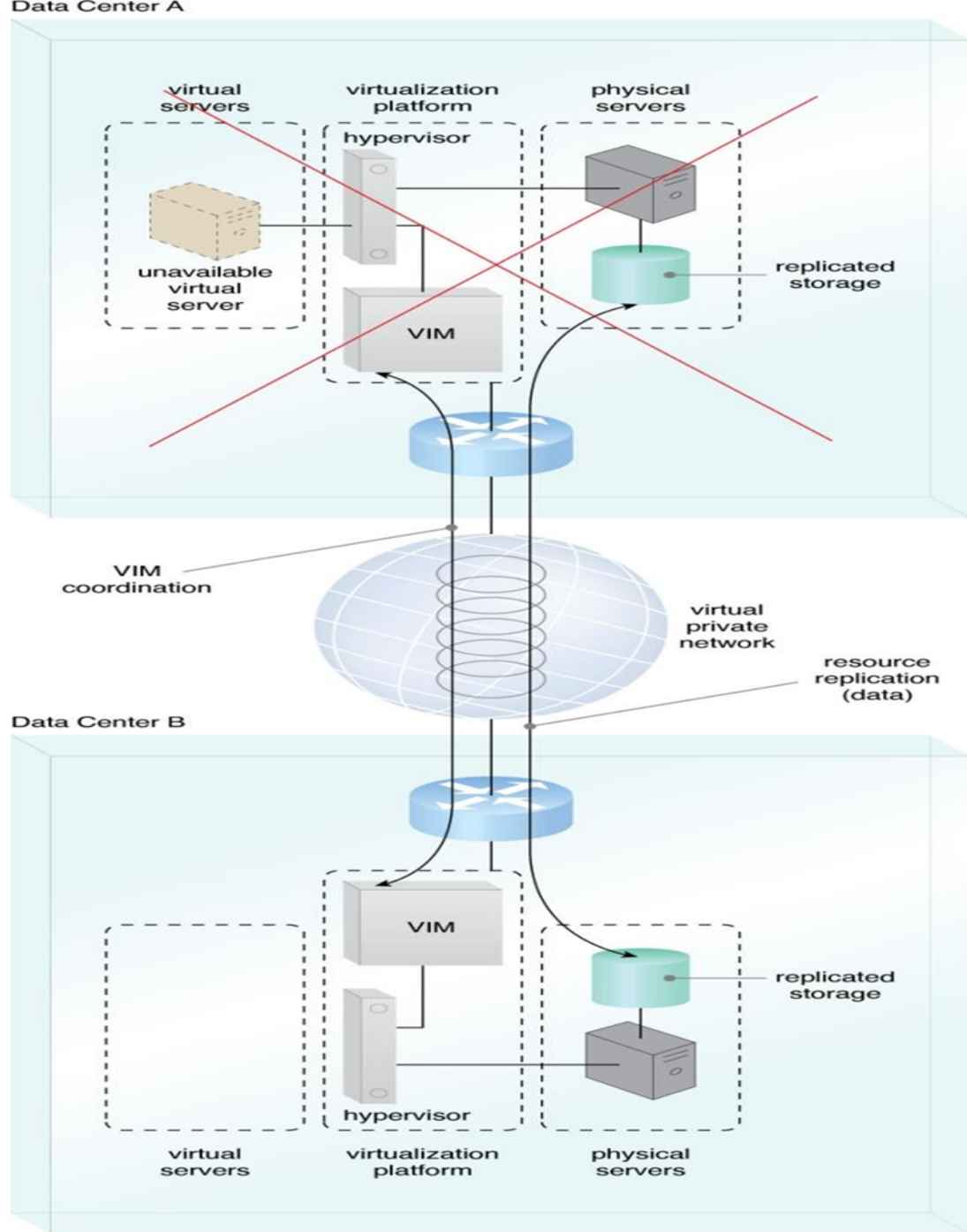
数据中心A和B中的**VIM**实例
执行协调功能，以便检测故
障情况。

高可用性架构的结果是已存
储的**VM**映像在数据中心之间
进行复制



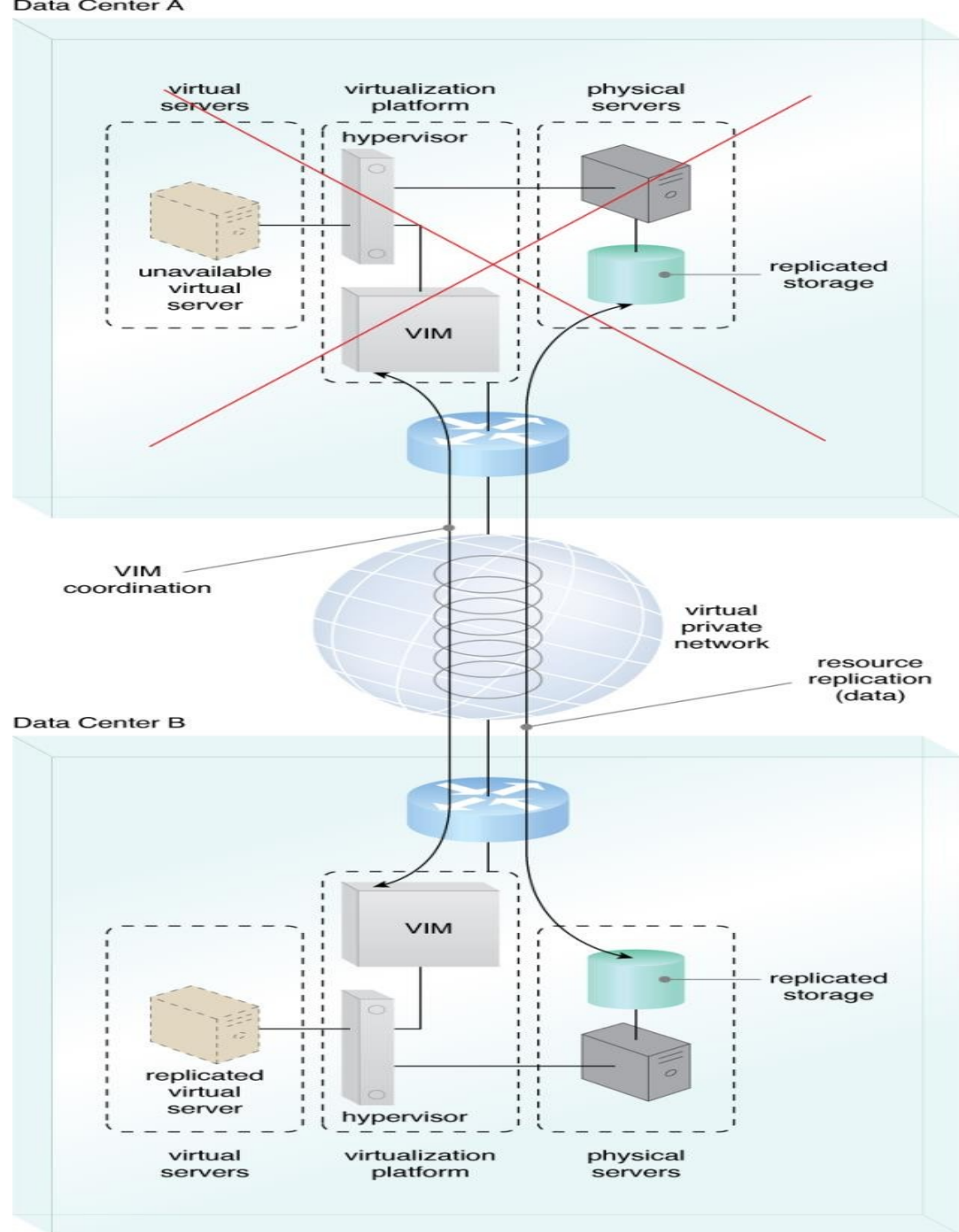
案例研究

Figure 7.18 — 数据中心A的虚拟服务器变得不可用。数据中心B的VIM检测到该故障情况，开始将数据中心A的高可用服务器重定位到B。



案例研究

Figure 7.19 — 在数据中心B创建了一个新的虚拟服务器实例，该实例为可用状态。

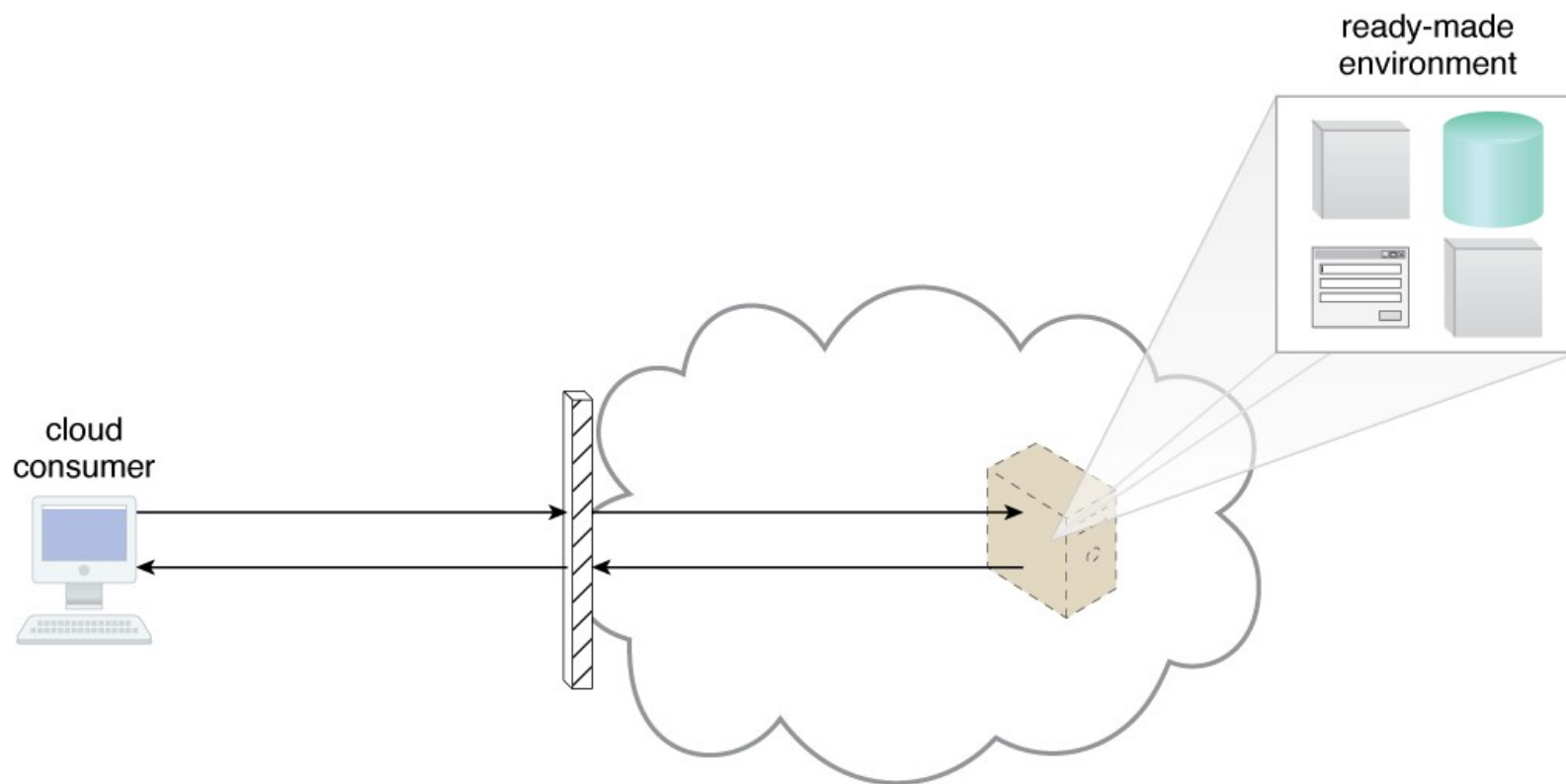


§7.6 已就绪环境

- 已就绪环境机制是PaaS云交付模型的定义组件，代表的是预定义的基于云的平台，该平台由一组已安装的IT资源组成，可以被云用户使用和定制。
- 已就绪环境被云用户用来在云内远程开发和配置自身的服务与应用程序，其通常配备了一套完整的软件开发工具包（SDK）。
- 典型的已就绪环境包括预安装的IT资源，如数据库、中间件、开发工具和管理工具。



访问已就绪环境

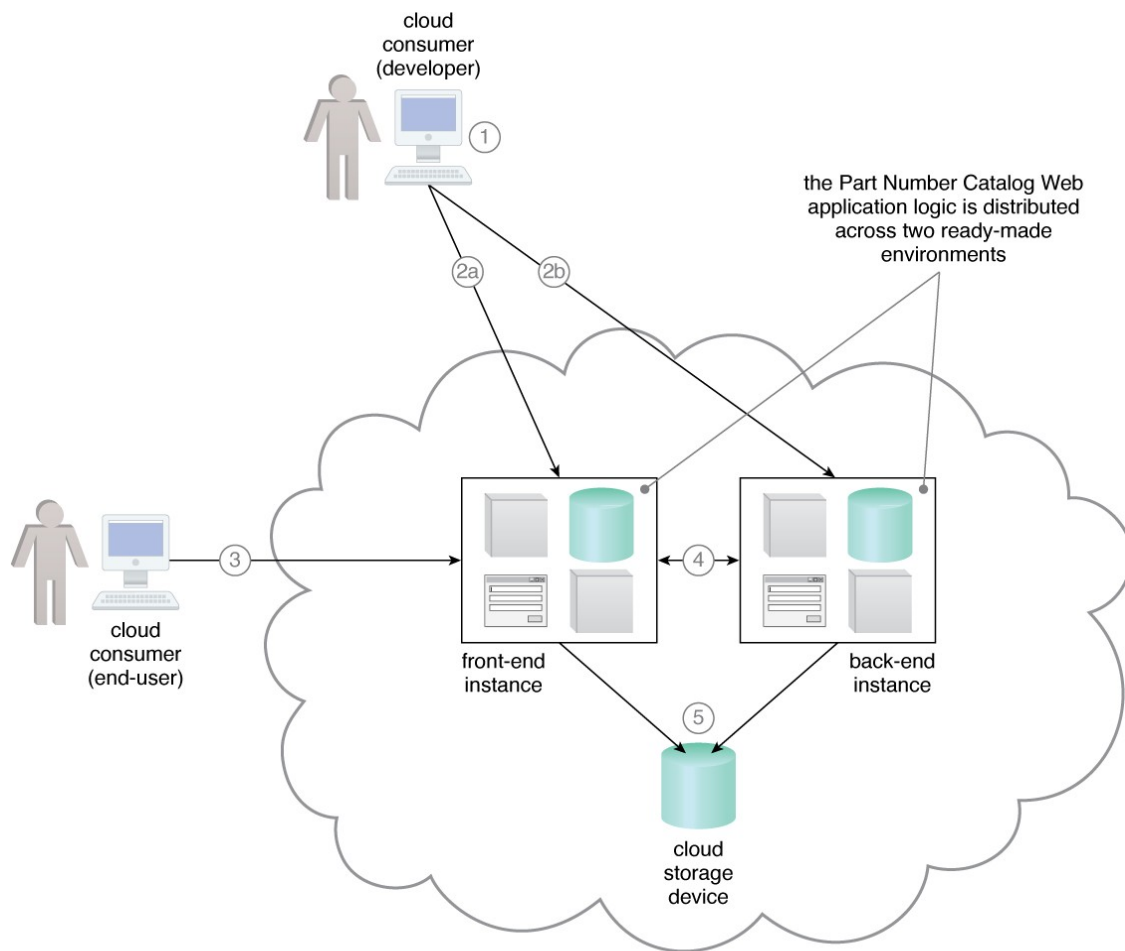


Copyright © Arcitura Education

Figure7.20 — 一个云用户访问位于虚拟服务器上的已就绪环境

案例研究

Figure 7.21 — 开发人员使用环境提供的SDK来开发Web应用 **(1)**。应用软件部署在由两个已就绪环境建立的Web平台上，这两个环节分别称为前端实例 **(2a)** 和后端实例 **(2b)**。一个终端用户可以访问其前端实例 **(3)**。运行在前端实例上的软件调用位于后端实例的长线任务，该任务对应于终端用户请求的处理 **(4)**。部署在前端和后端实例中的应用软件在云存储设备中进行备份，该备份提供了应用数据的持久性存储 **(5)**。



Copyright © Arcitura Education



本章小结

- 对云的基本机制进行了概念性介绍
- 主要是相关的系统资源管理机制
 - 虚拟服务器机制
 - 云存储机制
 - 使用监控机制
 - 资源复制



课后题

- 1、说说你对虚拟服务器的理解，以及这种机制的作用。
- 2、分析讨论每个云存储等级以及对应的云存储设备和相关的技术接口。
- 3、分析讨论云使用监控的3种实现形式。

