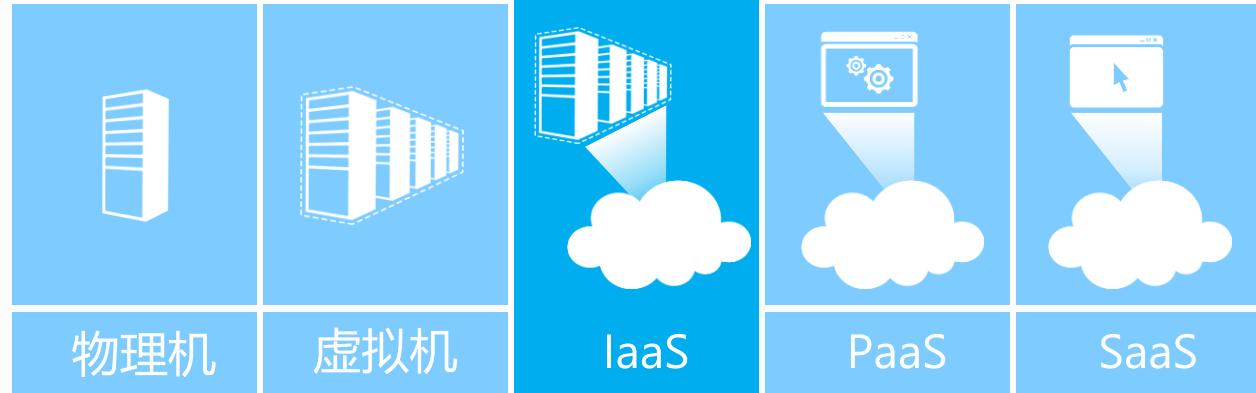


# Windows Azure 虚拟机

演讲者  
职位  
公司

# 从公有云到私有云



# Windows Azure 虚拟机

	支持关键的服务器应用
	简单的存储管理
	高可用性
	高级网络
	和计算PaaS集成

# IaaS 工作负载 – 一切关于应用

## 商业应用产品线

自定义的应用程序，CRM, CMS, ERP, 商业智能BI

## 应用程序基础设施

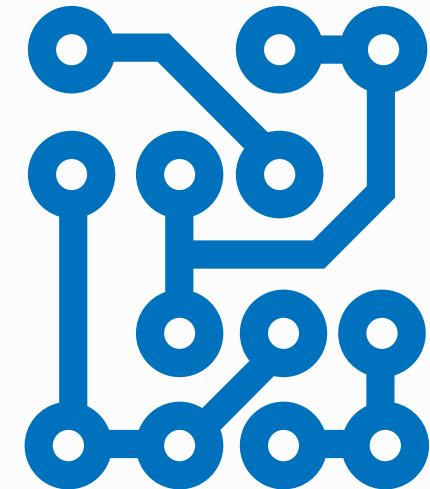
文件服务器，数据库，认证，源代码控制

## 开发，测试和部署环境

快速部署和移除整个环境

## 混合的应用程序

跨私有数据中心和云之间的应用程序



# 虚拟机 vs VM 角色

	VM Role	虚拟机
存储	非持久的存储	持久存储 简单增加额外存储
部署	线下创建VHD，上传到存储中	直接在云里创建VHD或者线下创建并上传
网络	Internal 或者 Input Endpoints 通过服务模型配置.	通过网站或者自动化方式配置Endpoint (PowerShell/Bash)
主要使用场景	将需要冗长复杂的安装的应用部署 到无状态的PaaS应用中	在Azure上运行需要持久化存储的应用程序

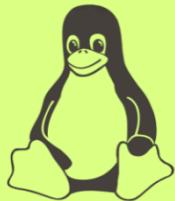
# 预览版中可用的镜像



Windows Server 2008 R2

Windows Server 2008 R2 with SQL Server 2012 Evaluation

Windows Server 2012



OpenSUSE 12.1

CentOS 6.2

Ubuntu 12.04

SUSE Linux Enterprise Server SP2

# 从虚拟机开始



# 云优先供应

开始



管理网站



脚本

(Windows, Linux 和 Mac)



REST API

选择镜像和虚拟机  
大小



Windows Server



Linux



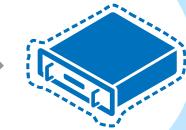
特小  
小  
中  
大  
特大

存储中新的持久化  
磁盘

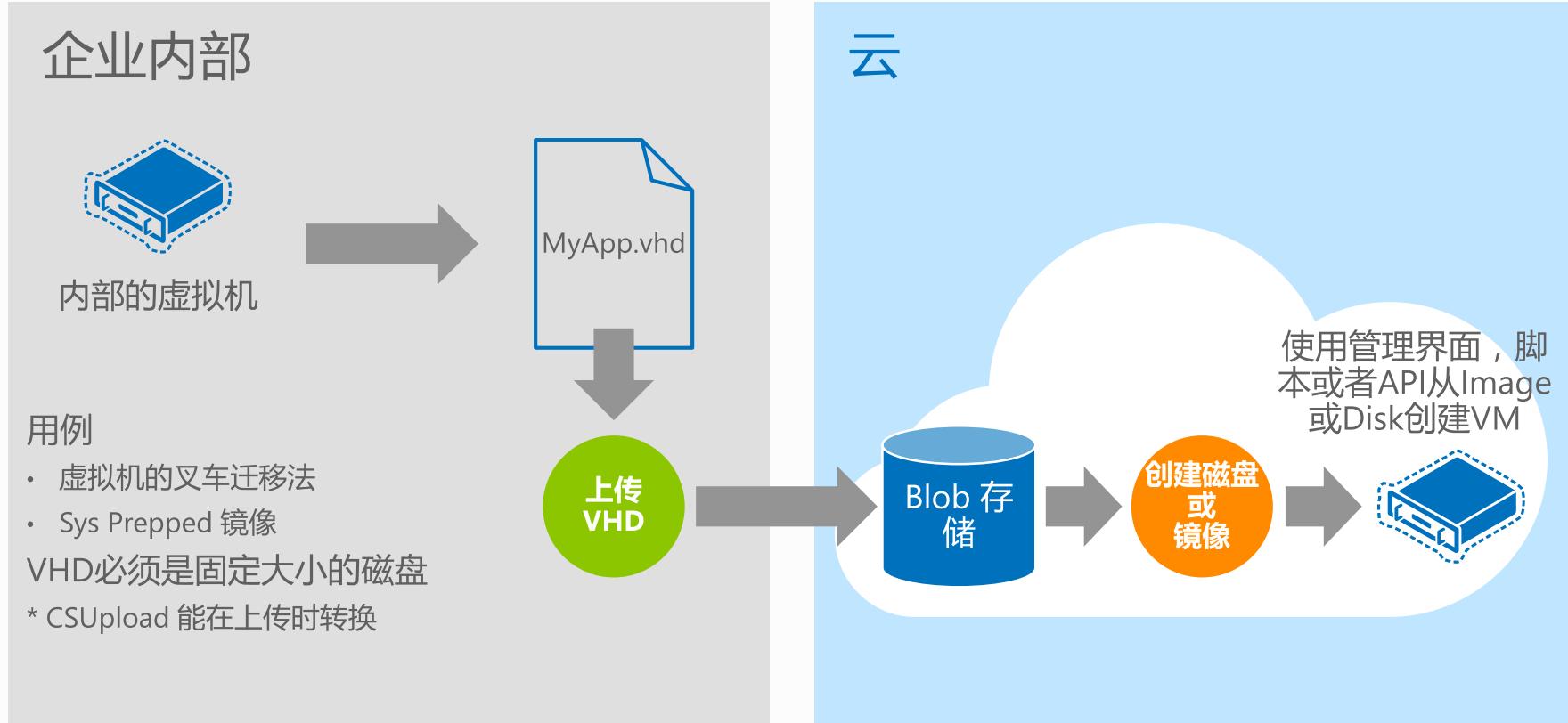
从新的磁盘启动虚拟机



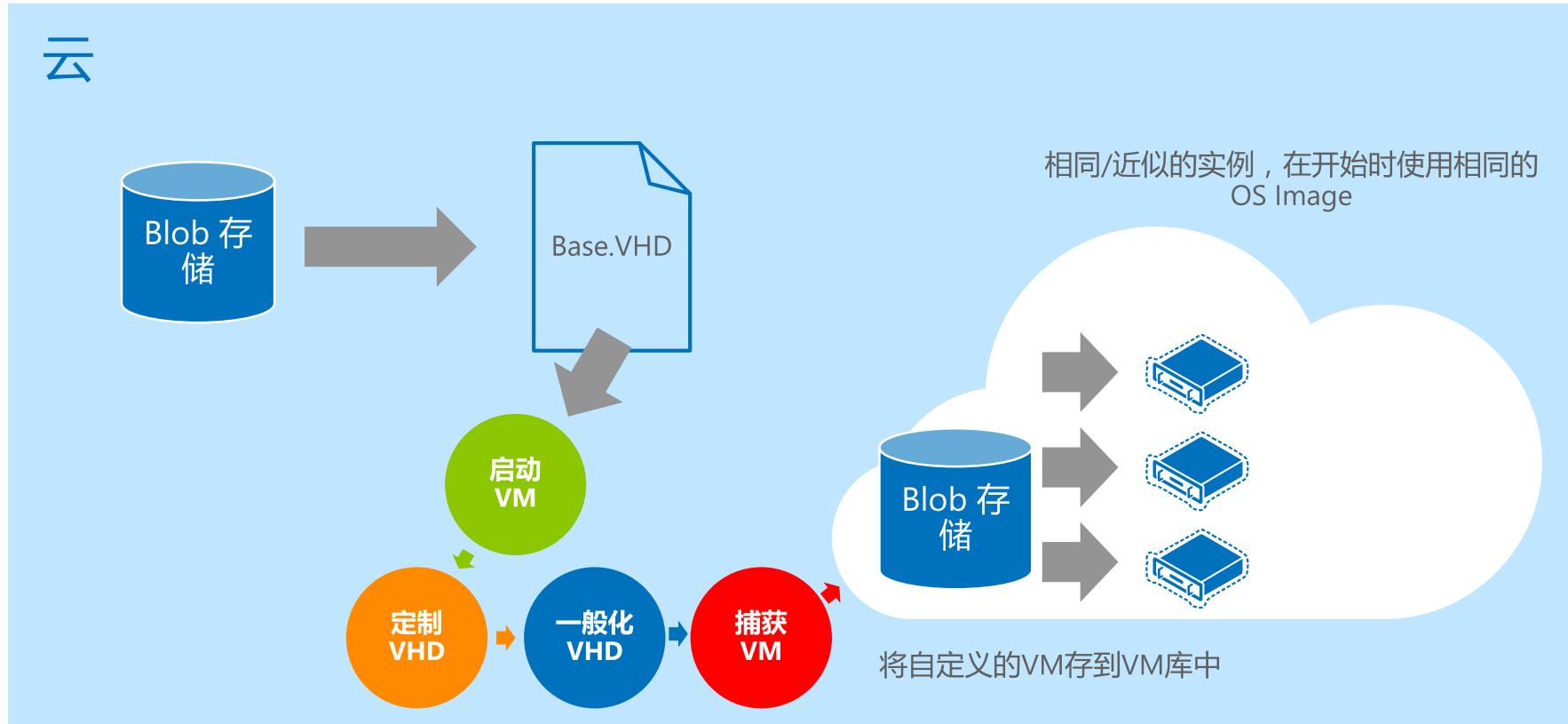
云



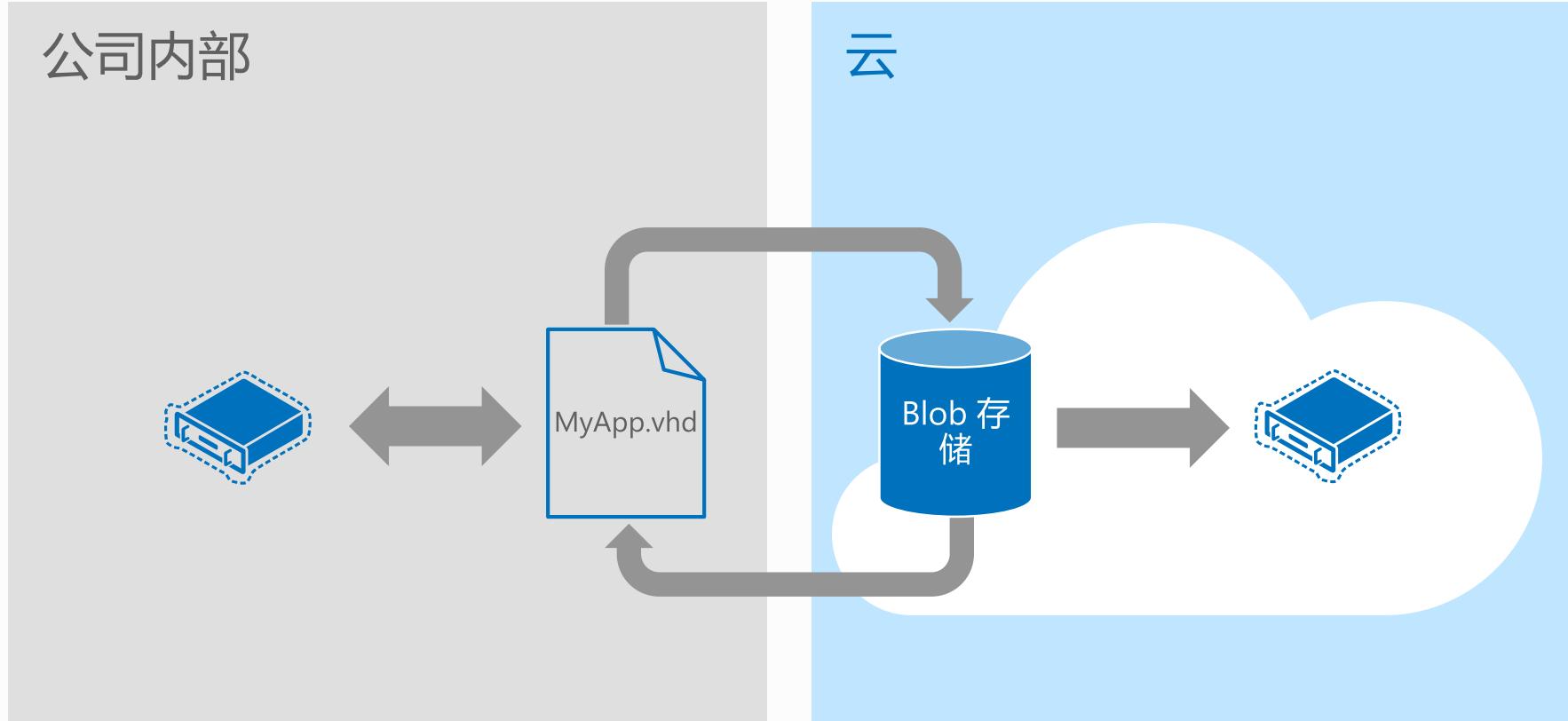
# 创建自己的服务器VHD



# 在云中创建镜像



# Image 可移动性



# 磁盘和镜像

## OS 镜像

- 微软
- 合作伙伴
- 用户



对新的虚拟机有基础OS镜像  
Sys-Prepped/一般化/只读  
通过上传或者捕获创建

## 磁盘

- OS 磁盘
- 数据磁盘



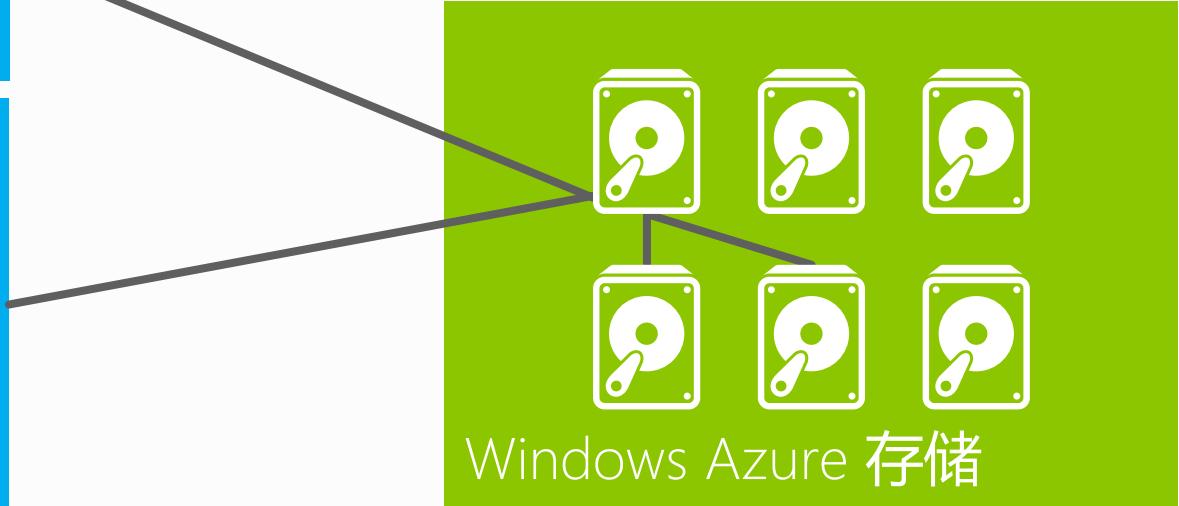
虚拟机的可写磁盘  
在虚拟机创建的时候创建或者上传存  
在的VHD

# 持久化磁盘管理

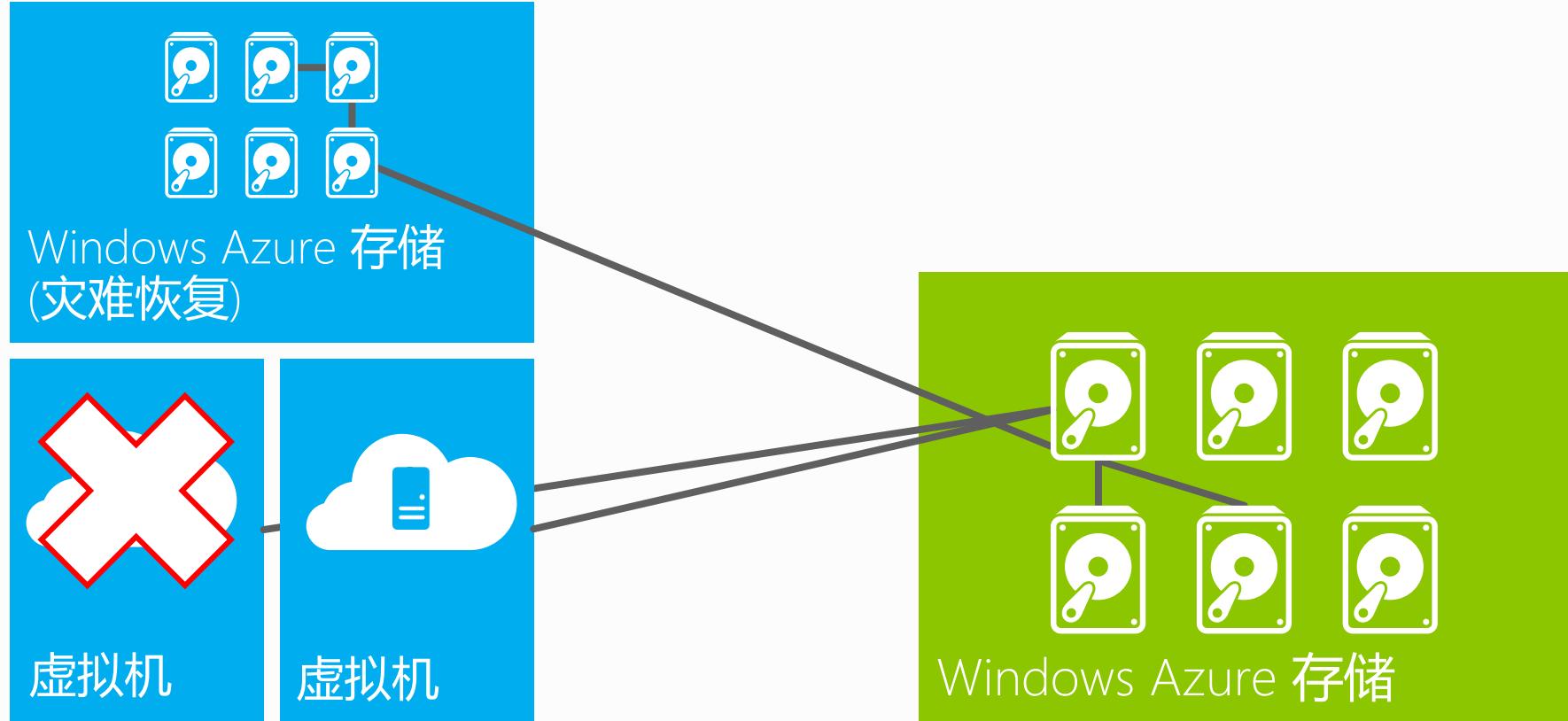
能力	OS 磁盘	数据磁盘
默认托管的缓存	读写	无
最大大小	127 GB	1 TB
可以变成镜像	是	否
热更新	缓存设置需要重启	修改缓存无需重启，添加/删除无需重启

- C:\ = OS 磁盘
- D:\ = 非持久化的缓存磁盘
- E:\ F:\. G:\ ... 数据磁盘

# 持久的磁盘和高耐用性



# 持久的磁盘和高耐用性



# 虚拟机大小

虚拟机大小	CPU 核数	内存	带宽	# 数据磁盘
特小	共享	768 MB	5 (Mbps)	1
小	1	1.75 GB	100 (Mbps)	2
中	2	3.5 GB	200 (Mbps)	4
大	4	7 GB	400 (Mbps)	8
特大	8	14 GB	800 (Mbps)	16

每个持久化的数据磁盘能最高达到1TB

# 磁盘缓存

磁盘类型	默认	支持
OS 磁盘	读写	只读和读写
数据磁盘	无	无，只读和读写

使用Set-AzureOSDisk或者Set-AzureDataDisk来修改

# 虚拟机管理和自动化

活动目录组策略 ( Active Directory Group Policy )

Windows 远程管理 (WinRM)

SCOM 2012 对管理虚拟机的支持

完整的编程自动化和管理的 REST API 接口

Windows Azure PowerShell Cmdlets

跨平台脚本 (Linux, Mac 和 Windows)

Windows Azure 管理服务(在路线图上)



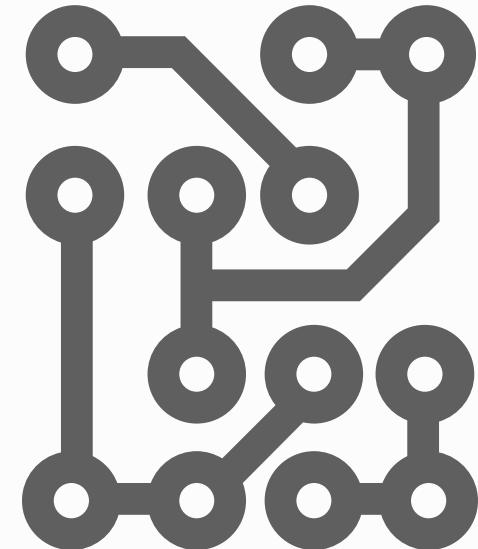
# 脚本能力

## IaaS完全支持

- Windows Azure PowerShell Cmdlets
- 基于node.js的跨平台脚本支持

## 能力

- 创建，删除
- 重启，启动
- 导入和导出虚拟机设置
- 支持Windows and Linux VMs
- 创建时支持Windows加入域
- 完全自定义的数据磁盘和端点配置
- 自动虚拟网络设置



演示

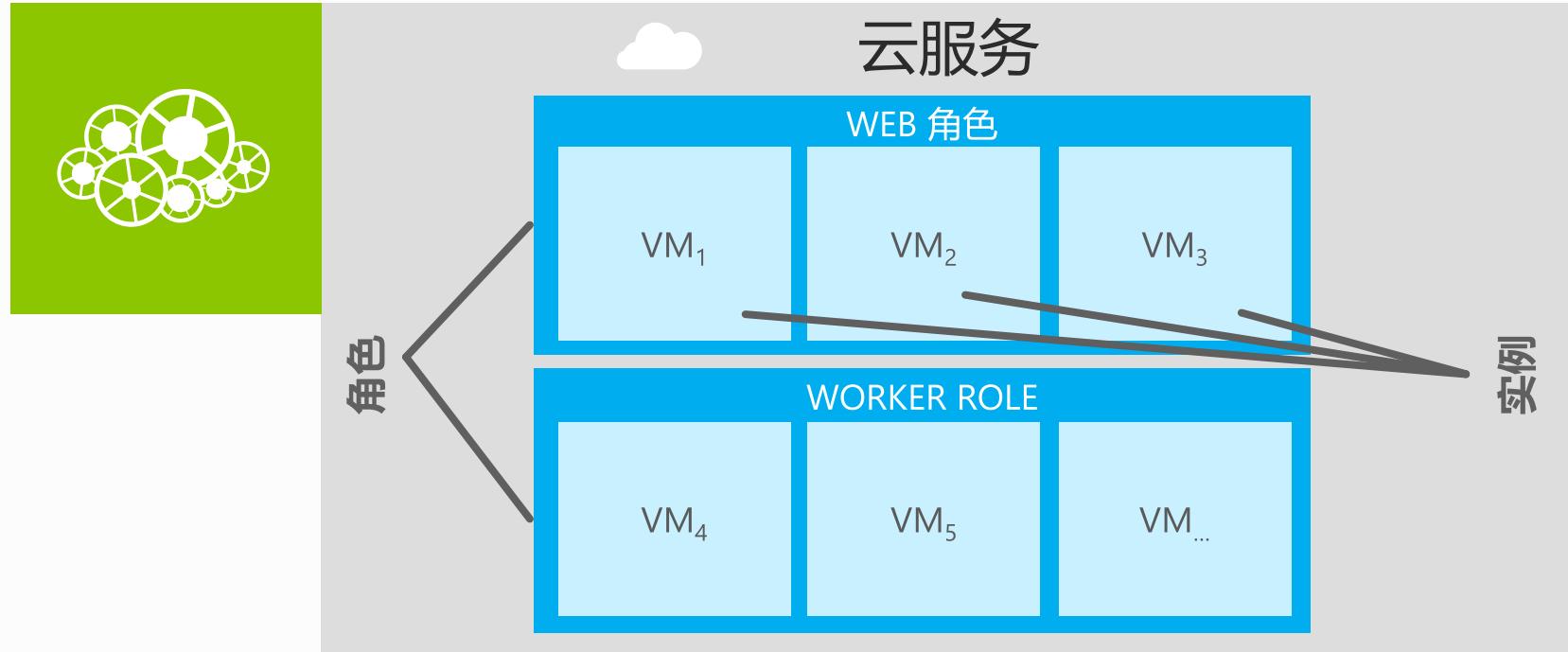
从虚机开始



# 虚拟机和云服务

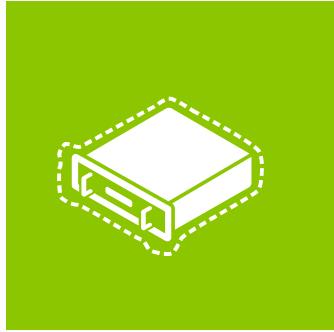
# 云服务，角色和实例

云服务是一个管理，配置，安全，网络和服务模型的边界



# 虚拟机

虚拟机是只有一个实例的角色



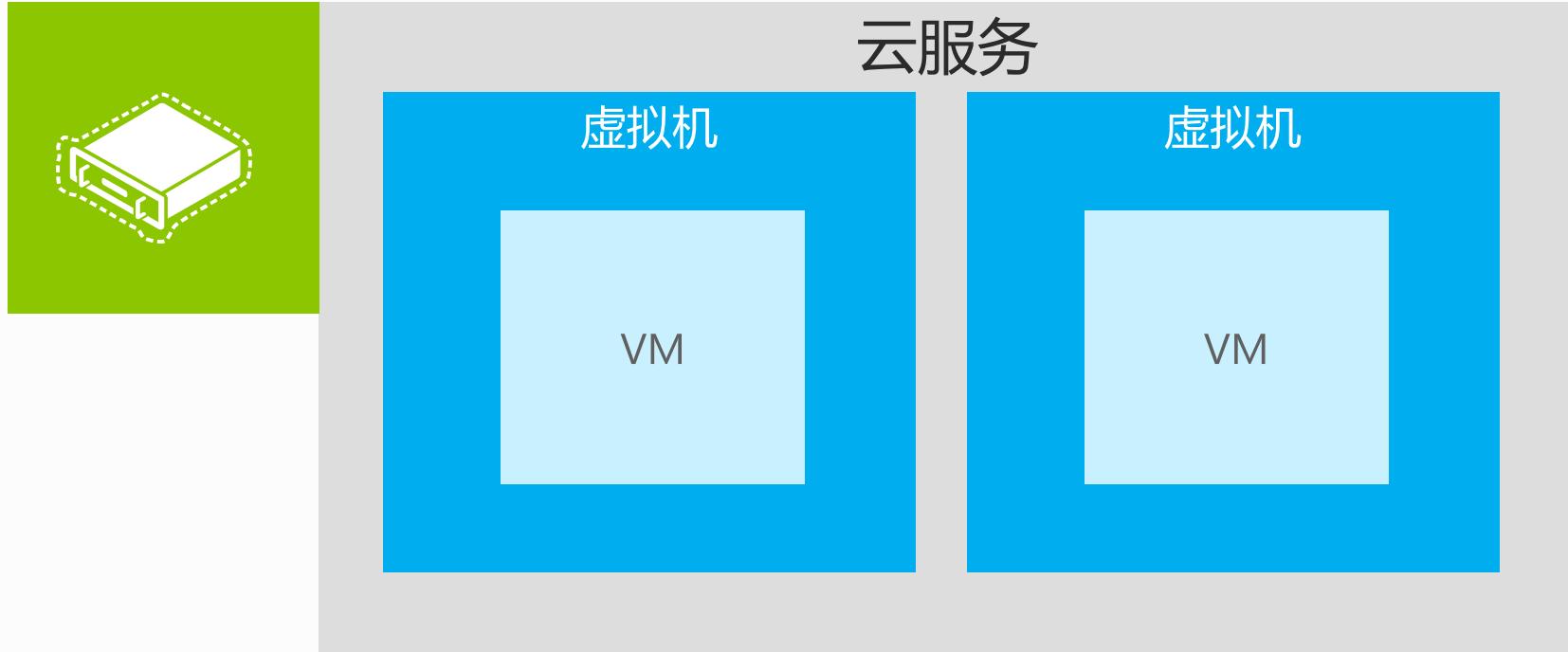
默认的云服务

虚拟机

VM

# 虚拟机

多个虚拟机可以在同一个云服务中寄存



# 虚拟机网络

# 虚拟机名称和DNS

通过机器名完全控制

Windows Azure提供DNS

在相同的云服务中通过名字解析  
机器名在DNS服务中明确地确定并注册

自己的DNS服务器

使用您自己内部的DNS服务器  
在Windows Azure中部署一个DNS服务器  
使用公共DNS服务

# 协议和端点

## 支持UDP通讯

对内的通讯支持负载均衡，允许对外通讯

## 支持所有基于IP的协议 (VM to VM)

实例到实例的通讯

TCP, UDP 和ICMP, 动态端口

## 端口转发端点Port Forwarded Endpoints

在相同的云应用中直接到多个VM的通讯

## 自定义的负载均衡健康情况探测

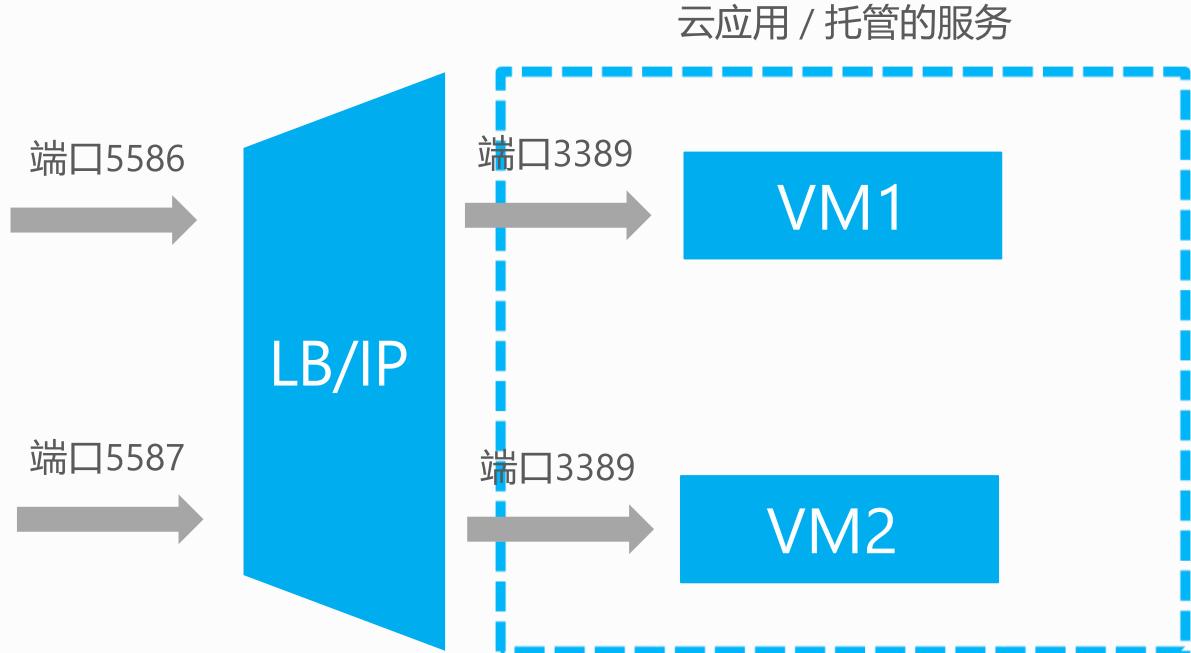
含有超时的健康状态检查

基于HTTP的探测，允许小块的健康检查控制

# 端口转发端点

## 端点集合

公共端口  
本地端口  
协议 (TCP/UDP)  
名称

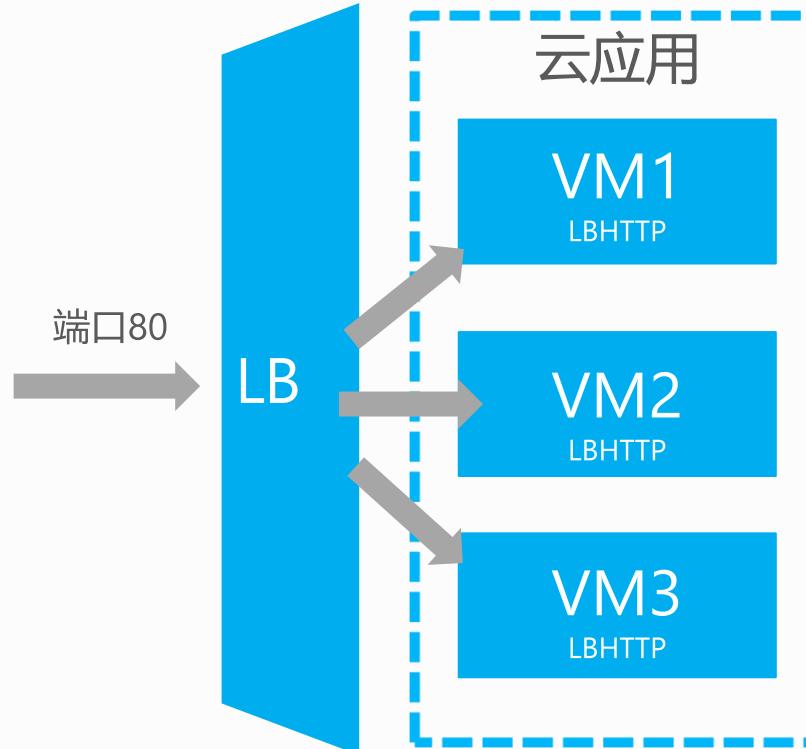


每个云服务只有一个公共IP

# 负载平衡集合

## 端点集合

公开端口  
本地端口  
协议(TCP/UDP)  
名称



# 自定义负载均衡探测

负载均衡器嗅探

名称

探测协议 (HTTP/TCP)

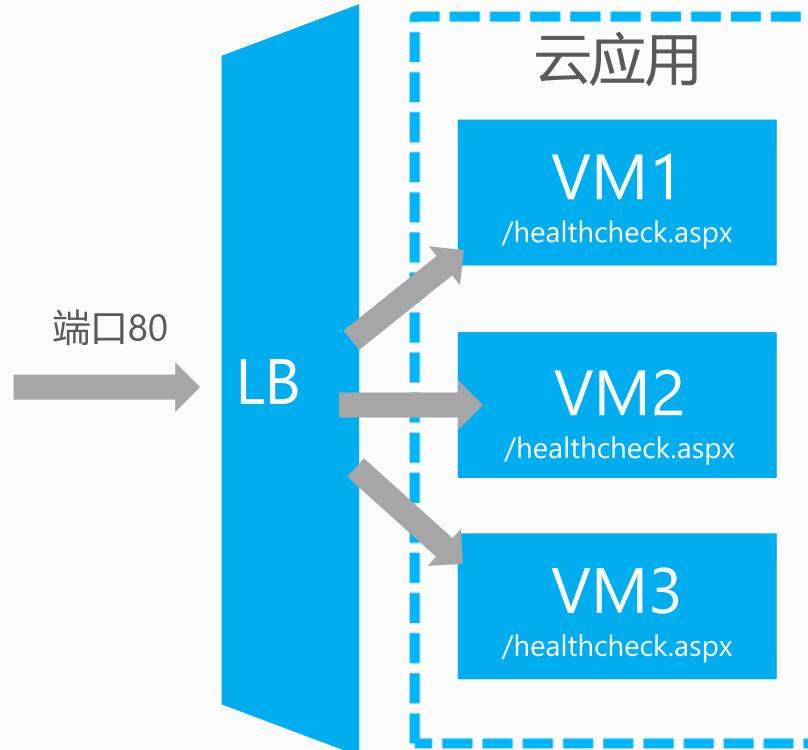
探测端口

探测路径

(/healthcheck.aspx)

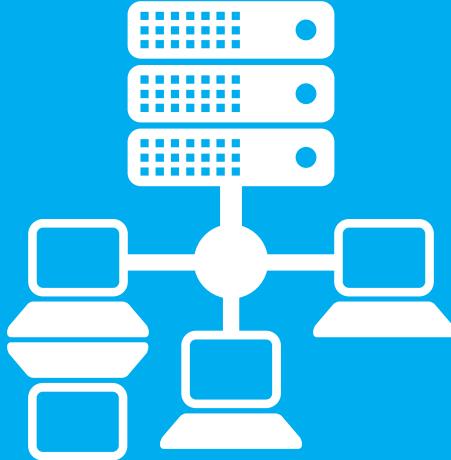
寻找HTTP 200

(对TCP省略嗅探路径)



# 虚拟机可用性

# Service Level Agreements



**多个实例99.95%**  
每年4.38小时下线时间

**单个实例99.9%**  
每年8.75小时下线时间

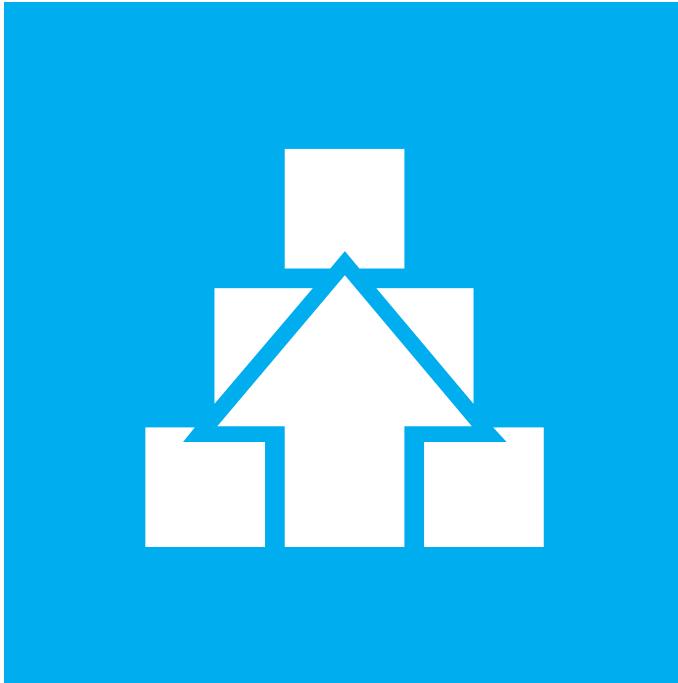
## 包括

计算机硬件失效 (磁盘 , CPU , 内存)  
数据中心失效 - 网络 , 电源  
硬件升级 , 软件维护 - 操作系统升级  
计划内 - 6天通知 , 6小时窗口 , 25分钟down

## 不包括

第三方软件 , 客户操作系统导致的VM崩溃

# 故障和更新域



## 故障域 Fault Domains

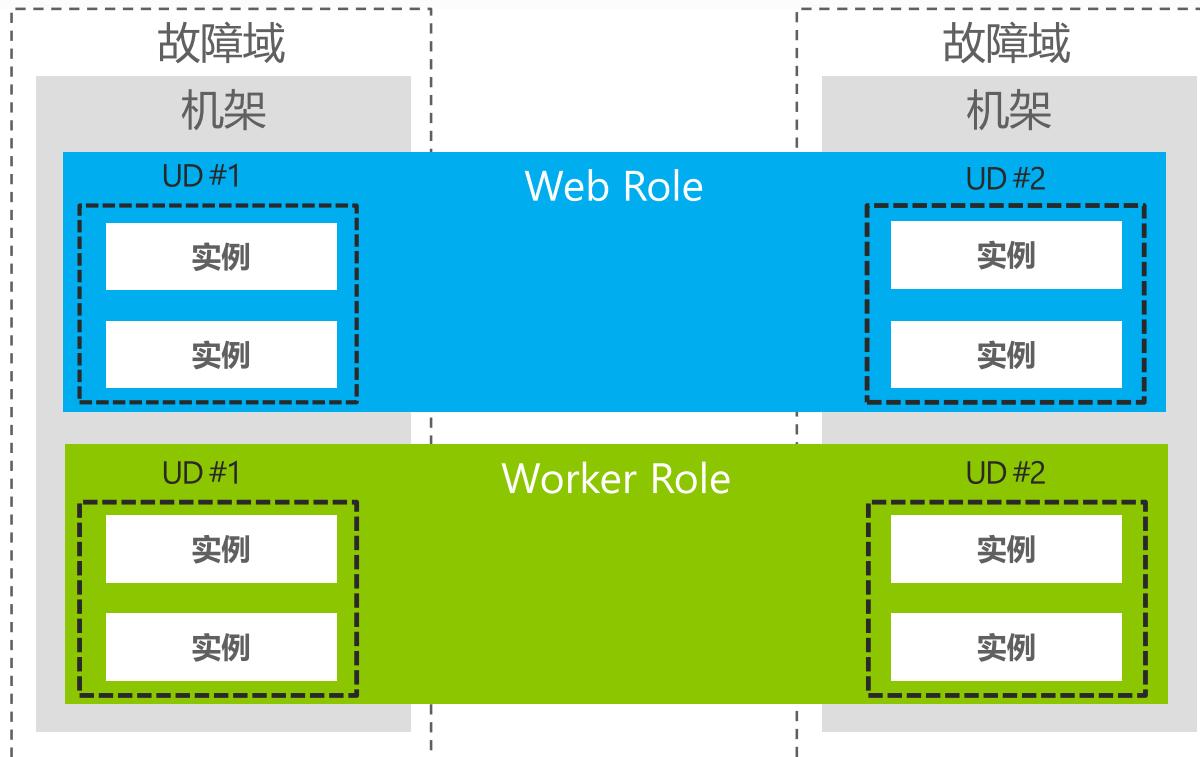
代表一组一起失效的资源  
即. 相同的机架，相同的服务器  
Fabric将实例分布在至少2个故障域中

## 更新域 Update Domains

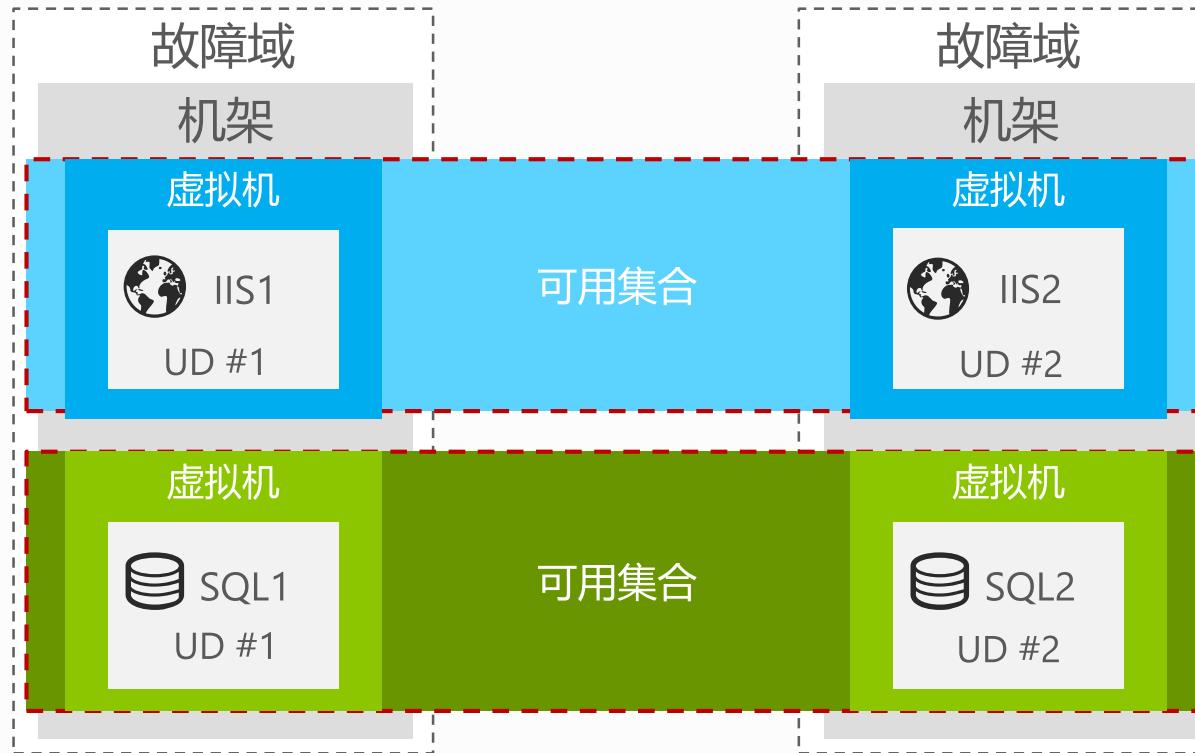
代表一组一起更新的的资源  
更新时依次更新每个域  
在服务定义中确定  
默认5个(最多20个)

Fabric将实例分布在更新域和故障域中

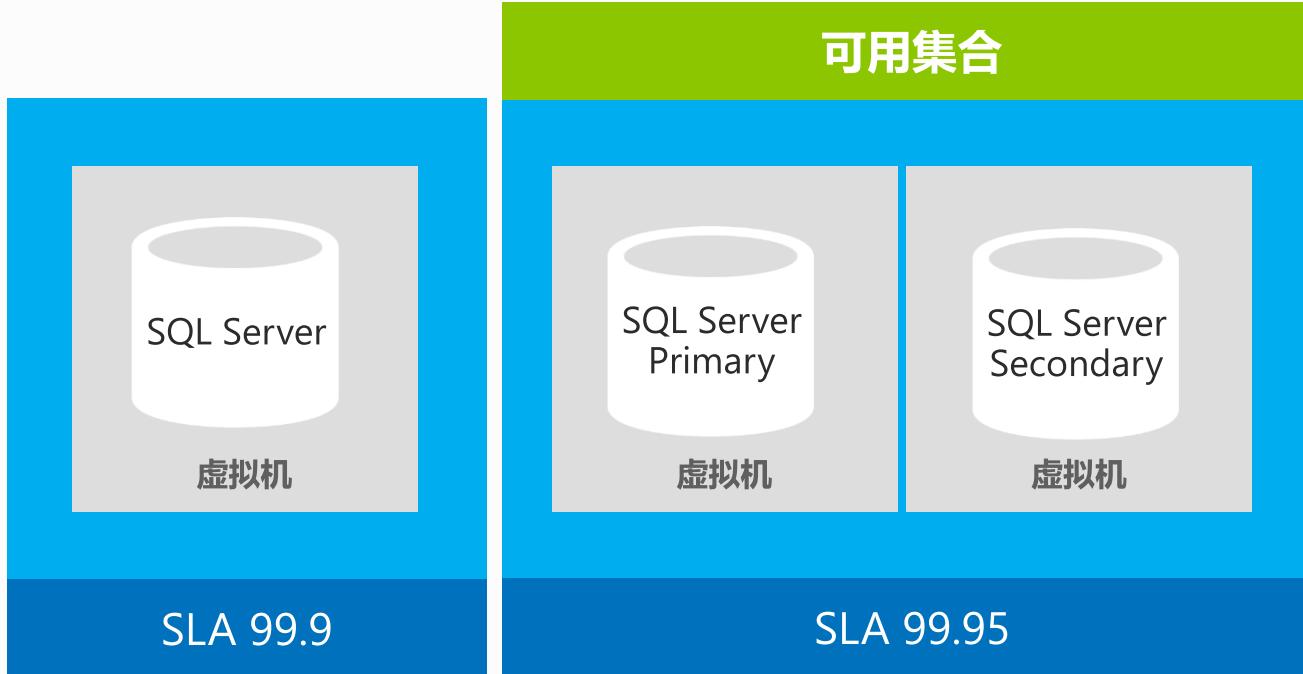
# 故障和更新域



# 虚拟机的可用集合

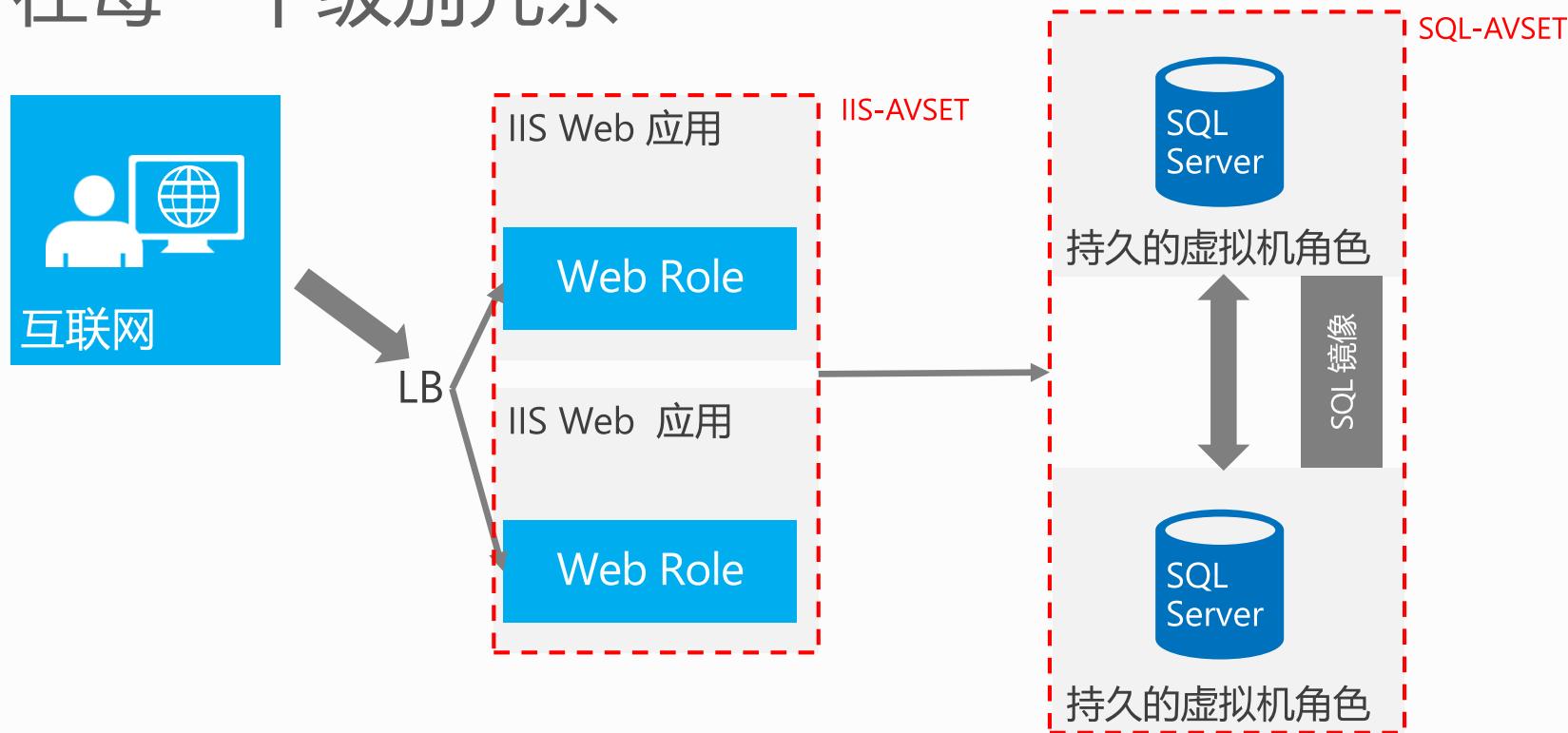


# 和SLA的关系



# 端对端的高可用性解决方案

在每一个级别冗余



备注

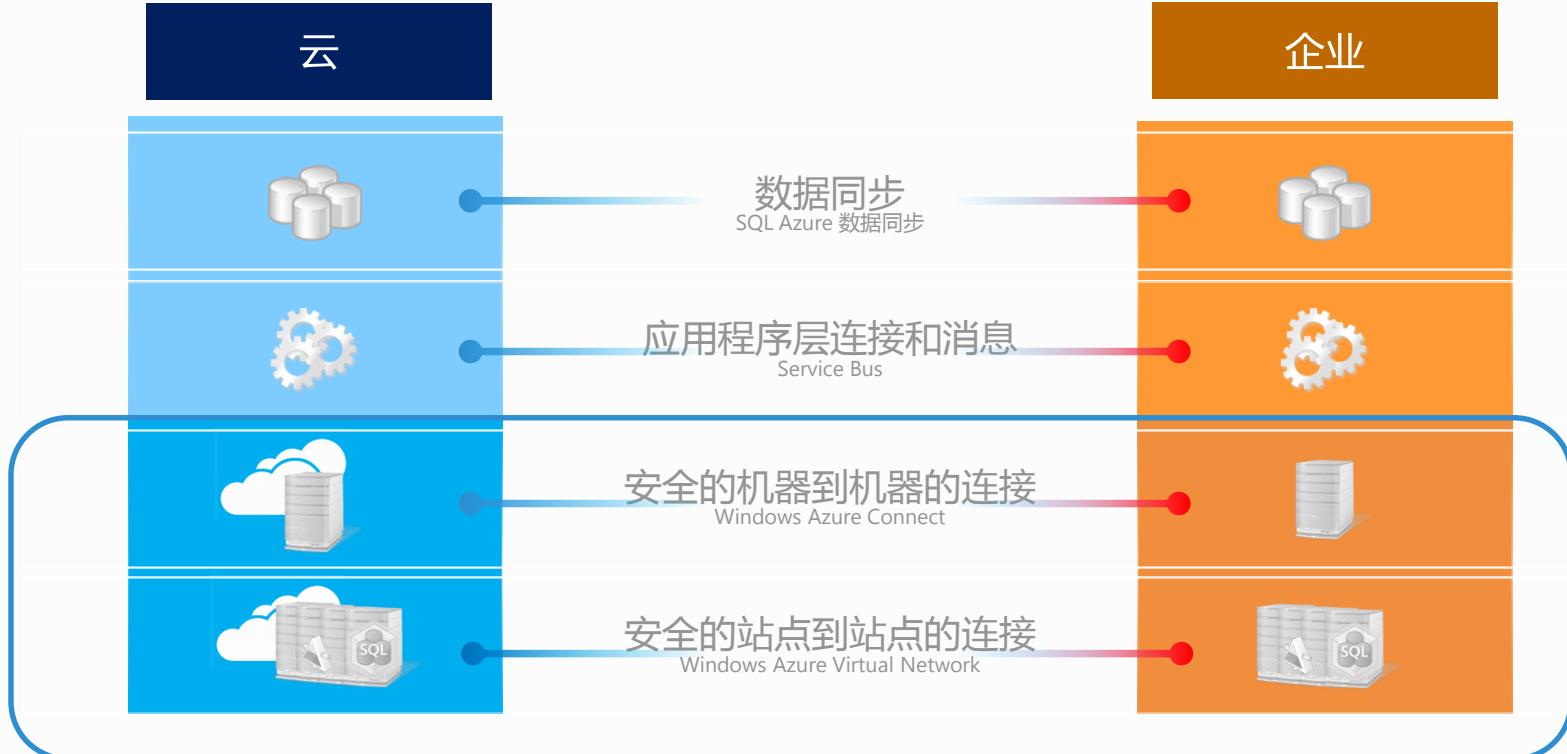
配置负载均衡和可用集合



# Windows Azure 虚拟网络



# 跨内部连接



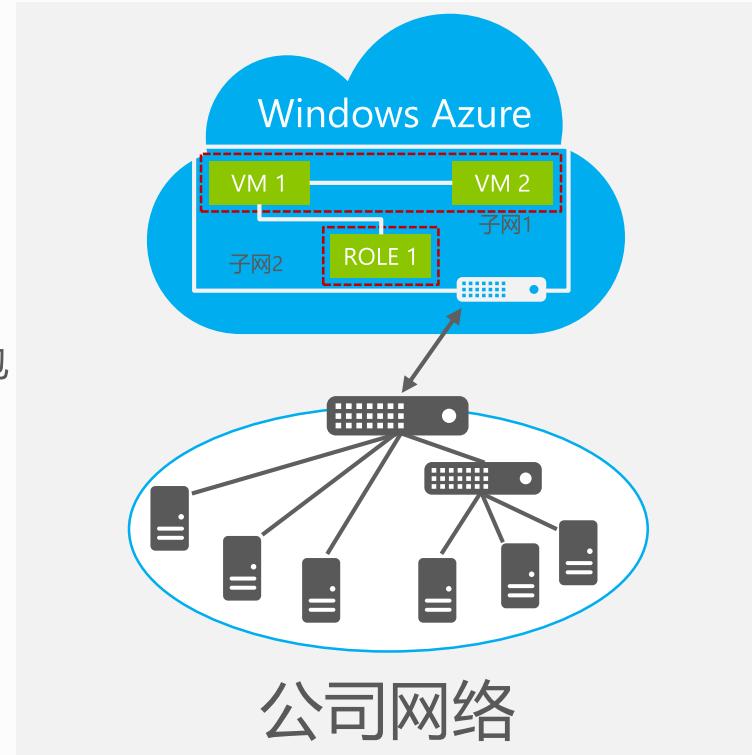
# Windows Azure 虚拟网络

## 在云中虚拟数据中心

将企业网罗扩展入Windows Azure  
将现有的应用和服务通过网络迁移到云  
允许跨云和内部的混合应用

## 云中被保护的虚拟网络

允许创建安全私有的IPV4网络，完全被Windows Azure地址所包含  
服务内DIP-to-DIP通讯



# 虚拟网络场景

## 混合的共有/私有云

在Windows Azure中的企业应用需要连接到内部的资源

## 企业的认证和访问控制

使用内部的资源（内部AD）管理认证和访问控制

## 监控和管理

对在Windows Azure中的资源进行远程监控和故障排除

## 高级连接需求

云部署需要固定IP和直接的跨服务的连接



# 你的应用需要虚拟网络吗？

## 持久的IP地址需求

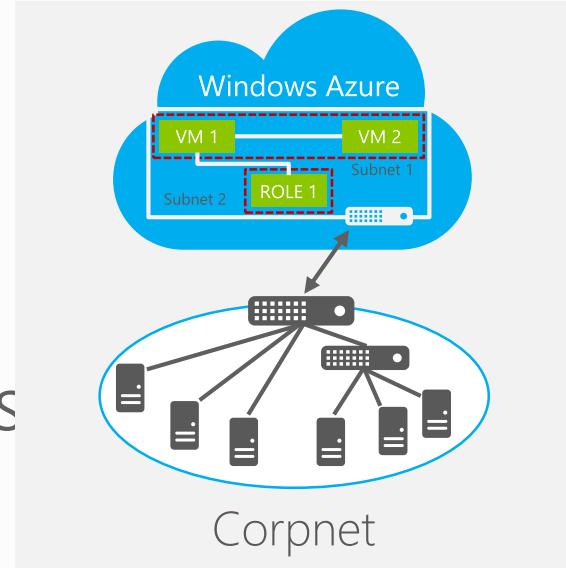
在虚拟网络中的虚拟机拥有无限的DHCP租用

## 混合的内部云应用

需要您的数据中心和共有云之间的连接

## 在云服务之间的连接

在云中部署活动目录或者将一个PaaS服务连接到IaaS服务



# 支持的VPN设备

Cisco

平台	操作系统	例子
ASA 5500 系列(Adaptive Security Appliances)	ASA Software 8.4+	5505, 5550
ASR 1000 系列 Aggregation Services Routers	IOS XE 2.1+	1002
ISR Series Integrated Services Routers	IOS 12.2+	2801, 2901, 2911

Juniper

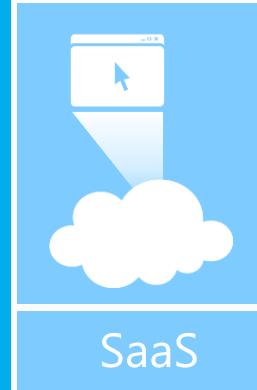
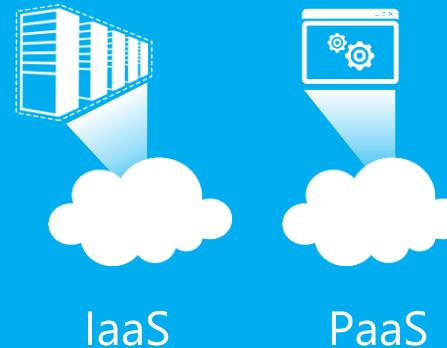
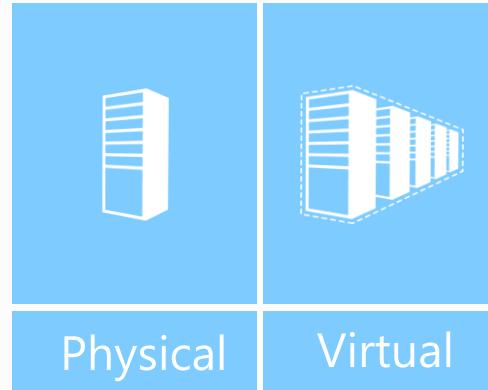
平台	操作系统	例子
SRX Series Routers	JunOS 10.2+	210, 650
J Series Routers	JunOS 9.4+	4350
ISG Series Routers	ScreenOS 6.2+	SX2
SSG Series Routers	ScreenOS 6.2+	550

## 一般的VPN设备必须支持

- IKE v1
- AES 128, 256
- SHA1, SHA2



# IaaS 和 PaaS — 协同工作



# PaaS的好处



## PaaS 更迅速

原因: 开发人员的工作更少

好处: 应用程序能够更快地从想像变为现实



## PaaS 更便宜

原因: 更少的管理工作

好处: 组织花费更少



## PaaS 风险更小

原因: 平台做了更多, 错误的机会更少

好处: 获得更大的稳定性

# IaaS 和 PaaS



## 通过虚拟IP连接云应用

通过连接公共端点简单创建服务



## 通过虚拟网络直接连接

为了高级的连接场景，例如活动目录或者DCOM

# 连接应用程序和虚拟机

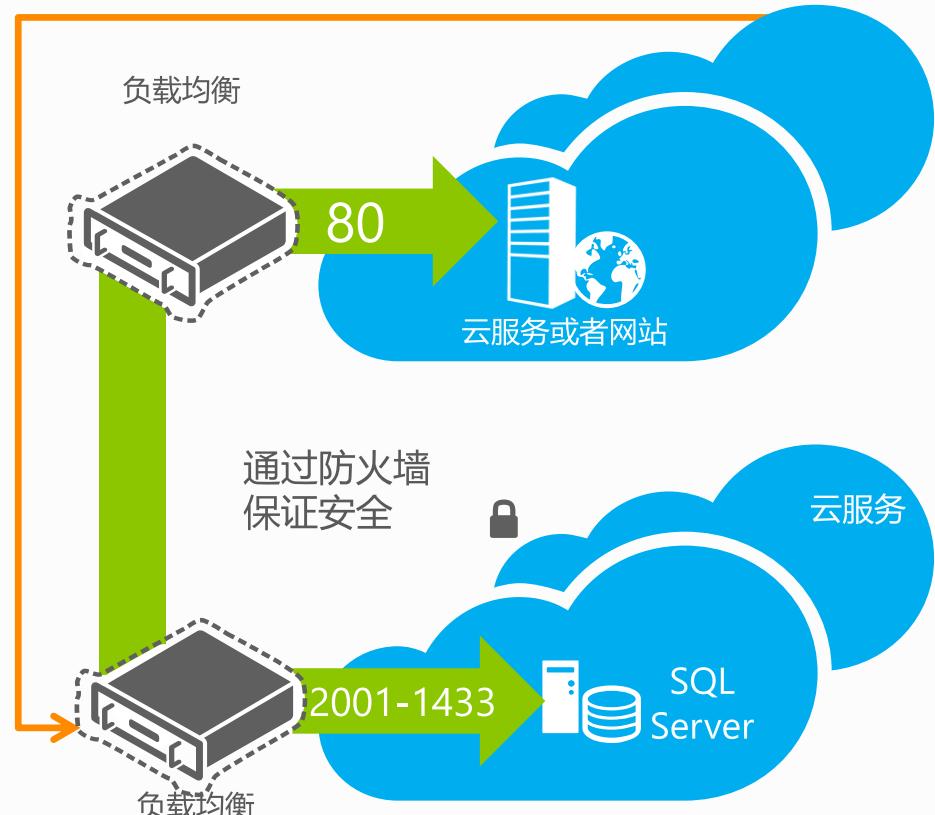
## 优势

简单  
用户自治  
虚拟IP交换(云服务)  
简单的本地开发/测试

通过公共端点进行SQL数据访问

## 缺点

高延迟  
安全性降低  
更多管理和部署



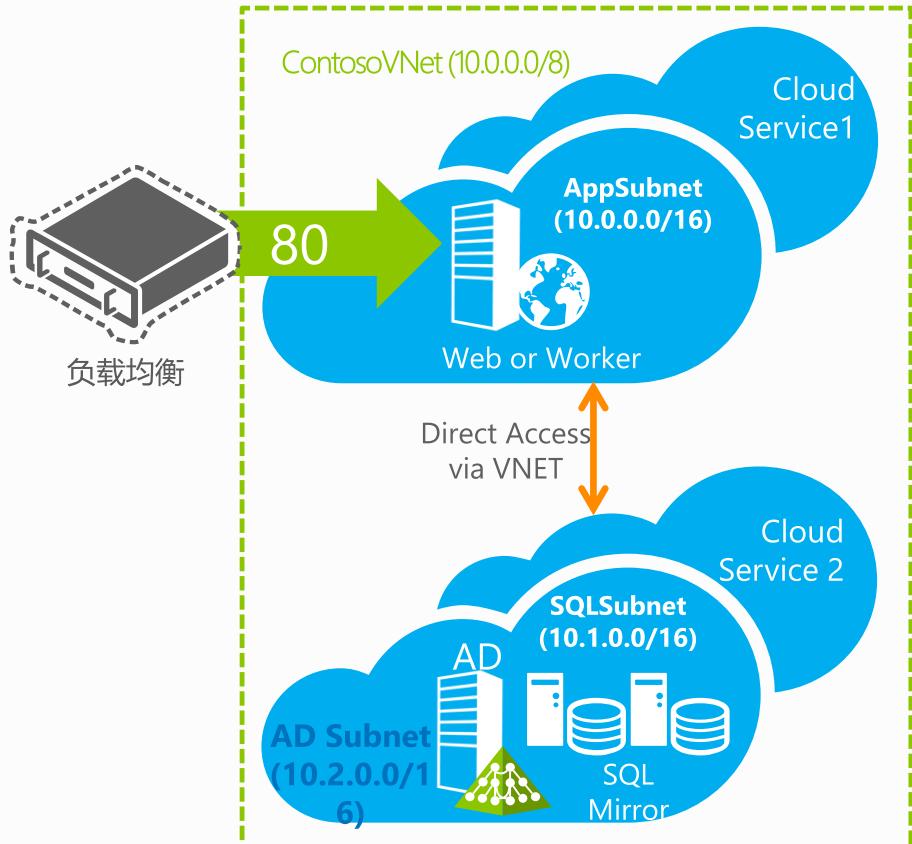
# 通过虚拟网络连接云服务

## 优势

从开放的互联网保护虚拟机  
降低延迟  
虚拟IP交换(web/worker roles)  
高级连接的需求

## 缺点

虚拟网络的复杂性  
Windows Azure提供的DNS不能跨云服务



Demo

连接云服务



# 总结



支持关键的服务器应用



简单的存储管理



高可用性



高级网络



和PaaS集成



© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.  
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.  
Translated to Chinese Simplified Version by Shanghai Yungoal Info Tech Co., Ltd [YunGoal](#)