



# 搭建混合IT架构方法和案例

张侠 博士

AWS首席云企业顾问

2015年4月24日

# 日程

- 什么是混合IT架构
- AWS支持混合IT架构
- 混合IT架构及使用案例



## 什么是IT混合架构？

# 什么是混合架构？

“Hybrid IT is the result of combining **internal and external services**, usually from a combination of internal and public clouds, in support of a **business outcome**.”

“混合 IT架构是指结合**内部和外部的服务**， 通常通过结合公有云和私有云，来实现**业务结果**。”

**Gartner**

<http://www.gartner.com/technology/research/technical-professionals/hybrid-cloud.jsp>

# 混合IT架构的定义



# 云是新常态，为什么还要混合架构？

- 继续使用已经建设的设施
- 在投资CapEx和运营OpEx之间控制支出
- 合规或行业性要求
- 降低单个供应商风险
- 实现独特的功能性能
- 商业授权维护支持的限制
- 兼得私有云和公有云的好处

# 混合IT架构是近期的趋势

“Nearly half of large enterprises will have hybrid cloud deployments by the end of 2017.”

“到2017年底， 近半大企业都会采用混合云部署。”

**Gartner**

<http://www.gartner.com/newsroom/id/2599315> - October 1, 2013



# 混合IT架构是旅程，不是目的地

Hybrid IT is part of the Journey,  
not the Destination.

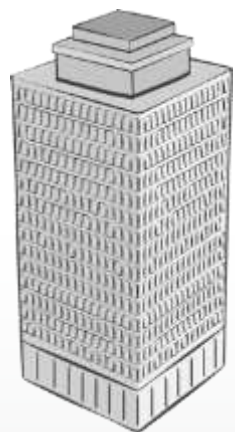






## 实现混合架构的关键

# AWS支持混合IT架构



Your Data Centers

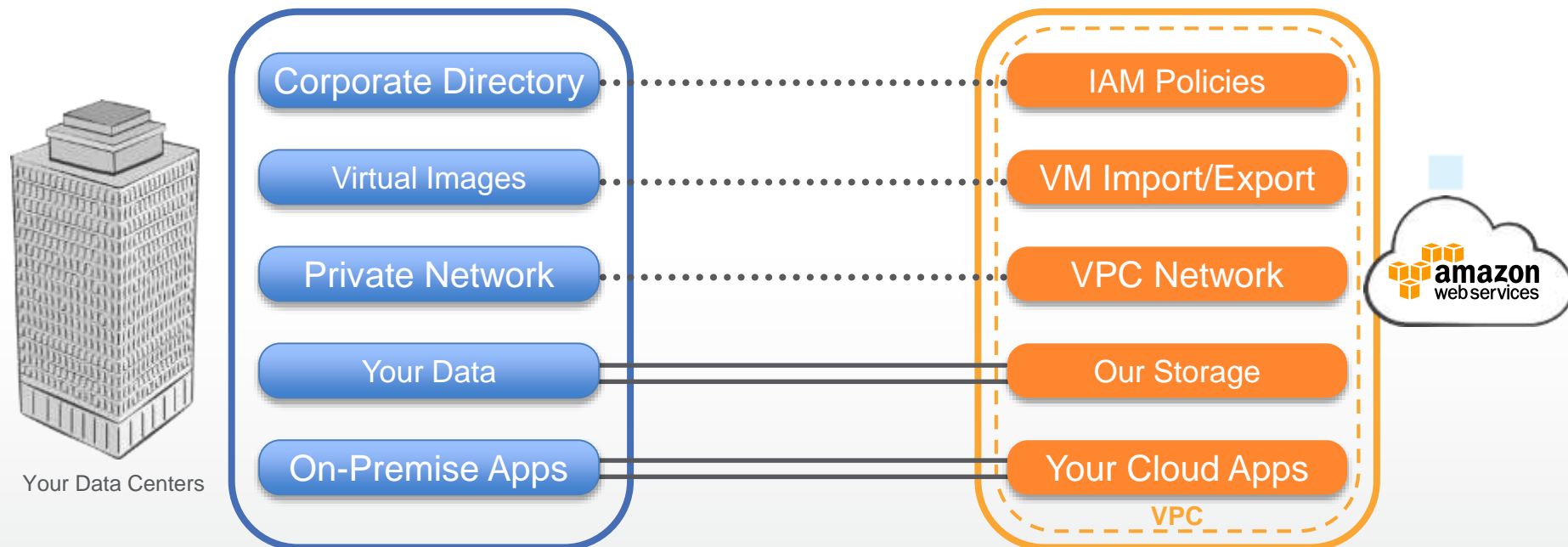
自有环境上的应用

私有连接  
工作负载与数据迁移  
访问控制集成  
与现有的管理工具  
一起使用

云应用



# 支持混合IT的工具



# 支持混合IT的云服务



Amazon Virtual  
Private Cloud



AWS Direct  
Connect



Virtual Private  
Network



Directory  
Services

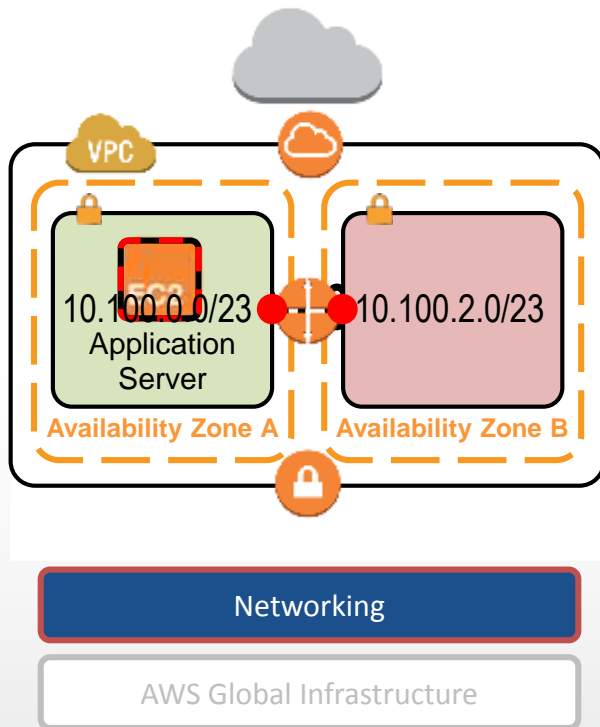


AWS  
Import/Export



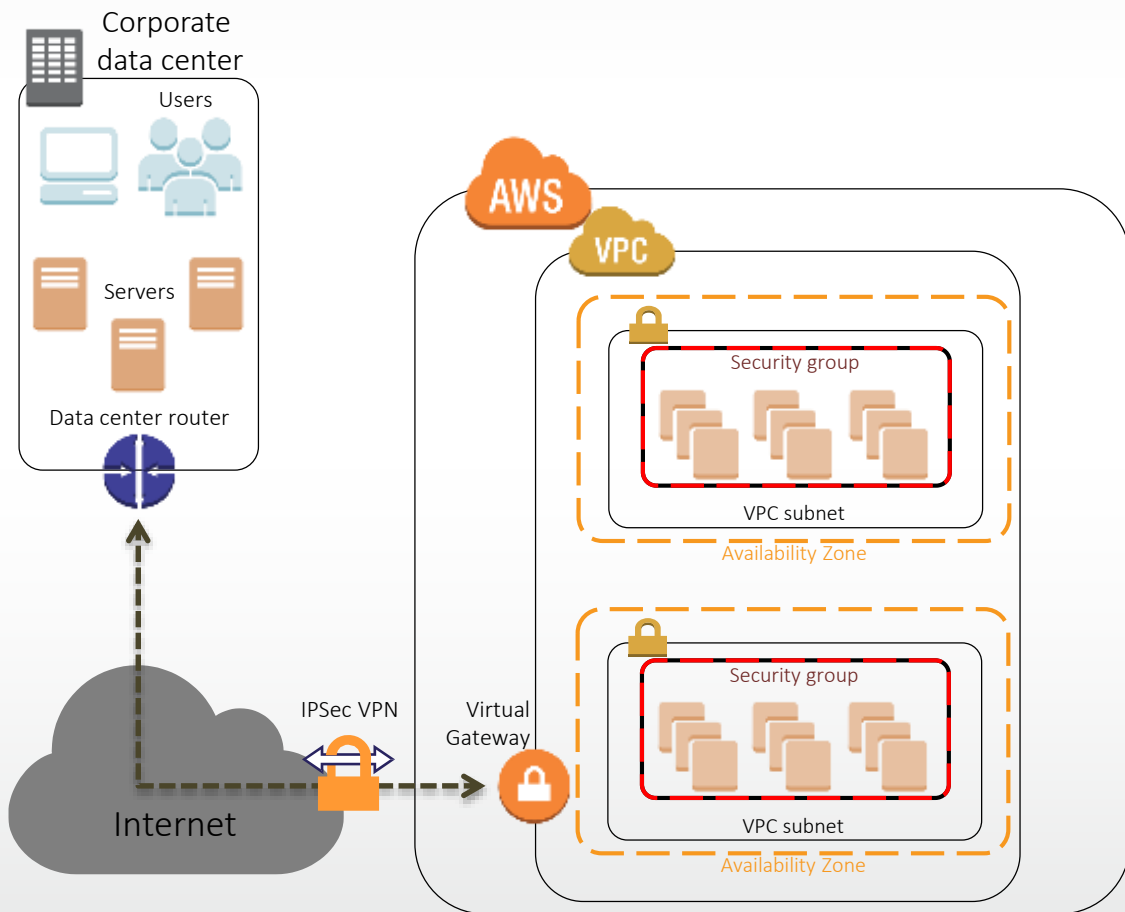
AWS Storage  
Gateway

# 服务: 网络: VPC



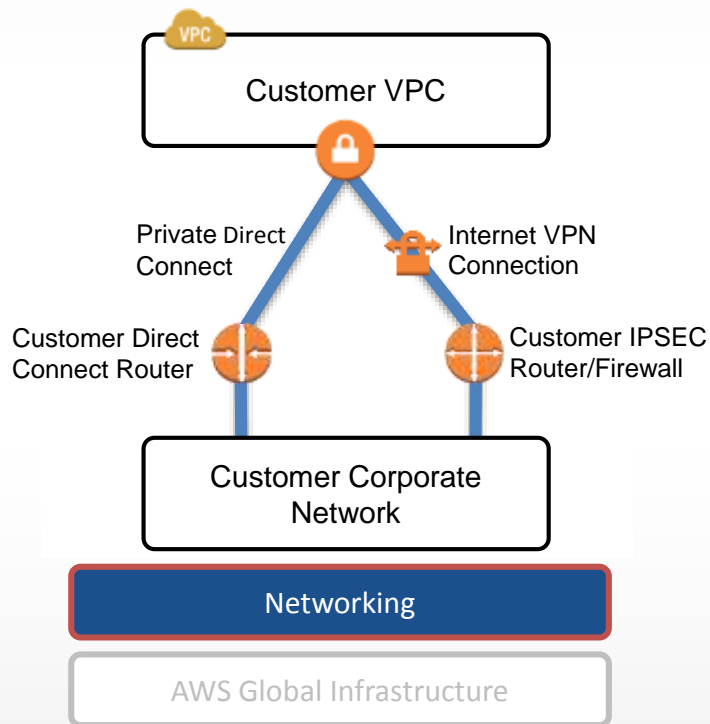
- 用户使用自己的网络地址段在AWS Cloud上创建逻辑上隔离的网络
- 企业拥有对虚拟网络环境完全的控制权，包括创建子网，定义IP地址，路由表和网关
- 在多个可用区AZ创建公有和私有子网
- 用户自己选择将EC2实例部署到哪个子网
- 用户使用NACL管理子网层面的网络安全
- 用户自己管理EC2实例的安全组，为每个EC2实例提供有状态的网络防火墙

# AWS IPSec VPN



- IPSec硬件 VPN 连接支持VPN专用设备
- 加密和验证
- 私密 RFC 1918 寻址
- 使用 BGP路由和失效备援
- VPN 服务提供管理的接入端

# 服务: 网络: Direct Connect

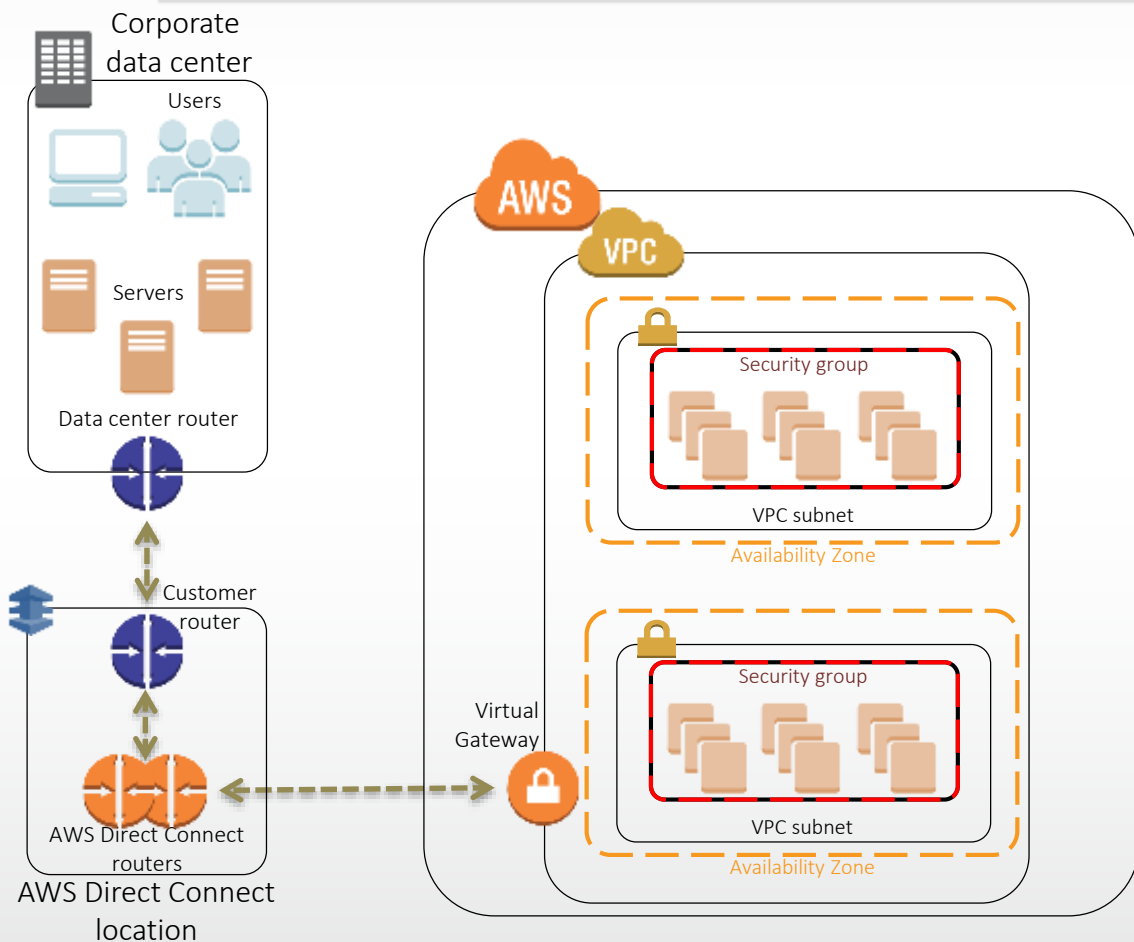


将用户网络接入VPC

- 通过标准的基于互联网的IPSec VPN tunnels, 或者通过私有线路, 或者两者结合连接到AWS直连驳接处
- 用户自己选择连接速度, 支持从50M to 10G
- 通过行业标准的VLANs和Layer 3路由
- 实现通过专线直连用户的VPC资源
- 可以在Direct Connect驳接处使用用户的网络设备, 如WAN优化装置

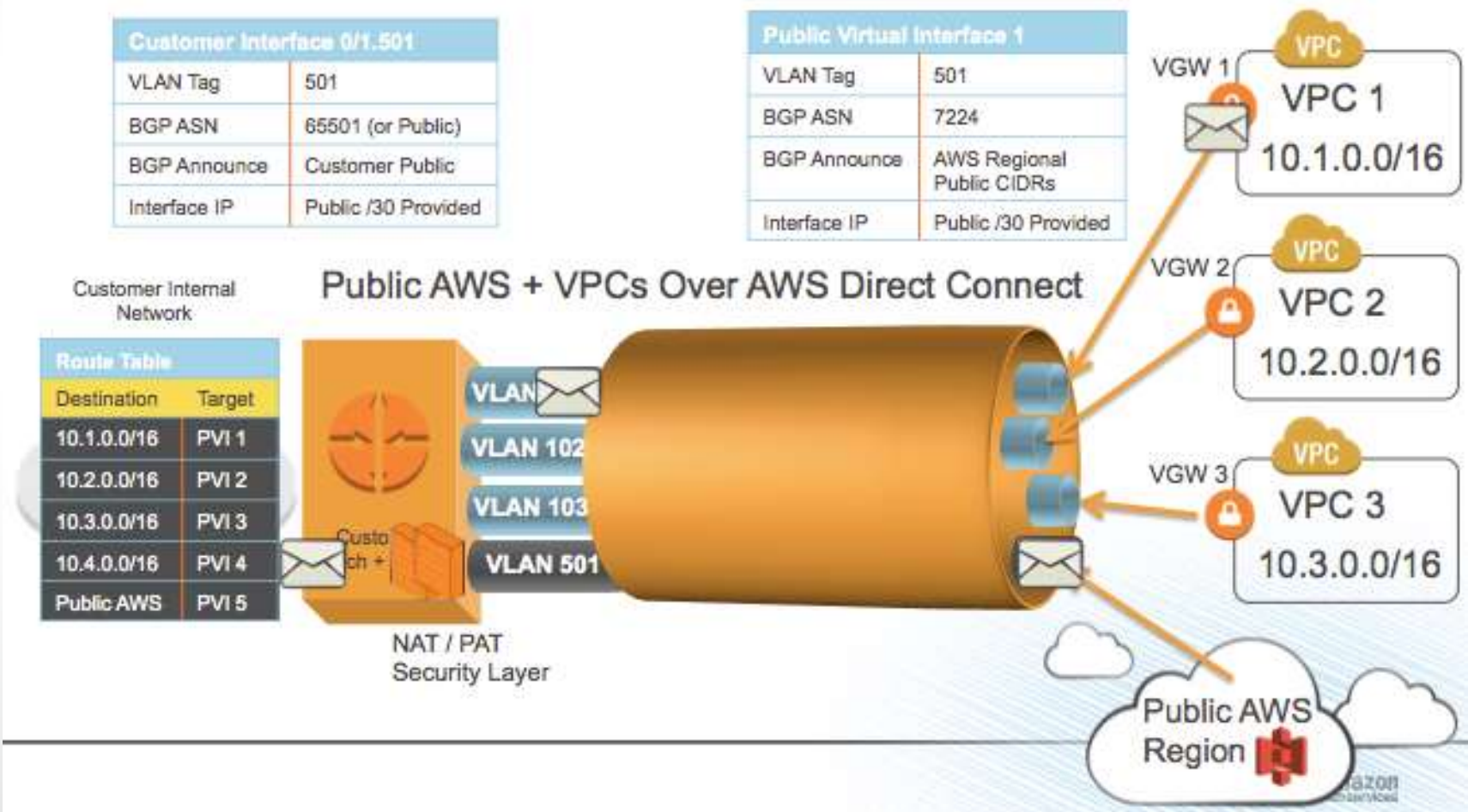


# AWS Direct Connect

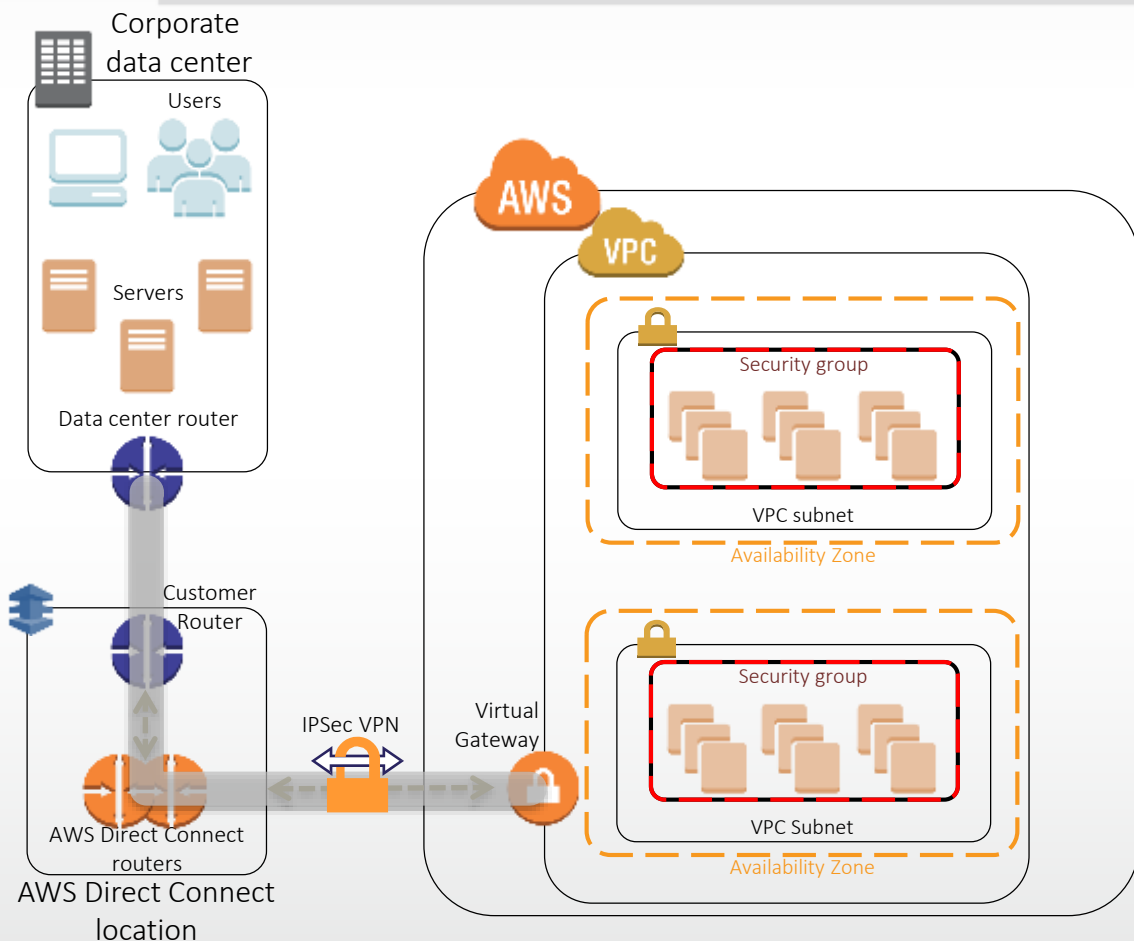


- 使用 Layer 2 单模光纤  
1000BASE-LX or 10GBASE-LR
- 利用 802.1Q VLANs 实现连接.
  - 标注 IP 流量
- 路由用BGP A/A or A/P multipath.
- 每条专线 DX 连接到单一的AWS Region

# AWS Direct Connect



# AWS Direct Connect + AWS VPN



- 专用网络路径以确保带宽
- 比基于互联网的IPSec VPN – 避免网络穿线
- 降低 IPSec 网络传输成本
- 额外网络安全保证

**Direct Connect**

**Datacenter**

**Cloud**

<https://secure.flickr.com/photos/squeaks2569/3700355978/in/photostream/>

**QCon**

Brought by **InfoQ**



**Direct Connect**

**Datacenter**

**Cloud**

<https://secure.flickr.com/photos/squeaks2569/3700355978/in/photostream/>

**QCon**

Brought by **InfoQ**

**Direct Connect**

**Datacenter**

**Cloud**

<https://secure.flickr.com/photos/squeaks2569/3700355978/in/photostream/>

**QCon**

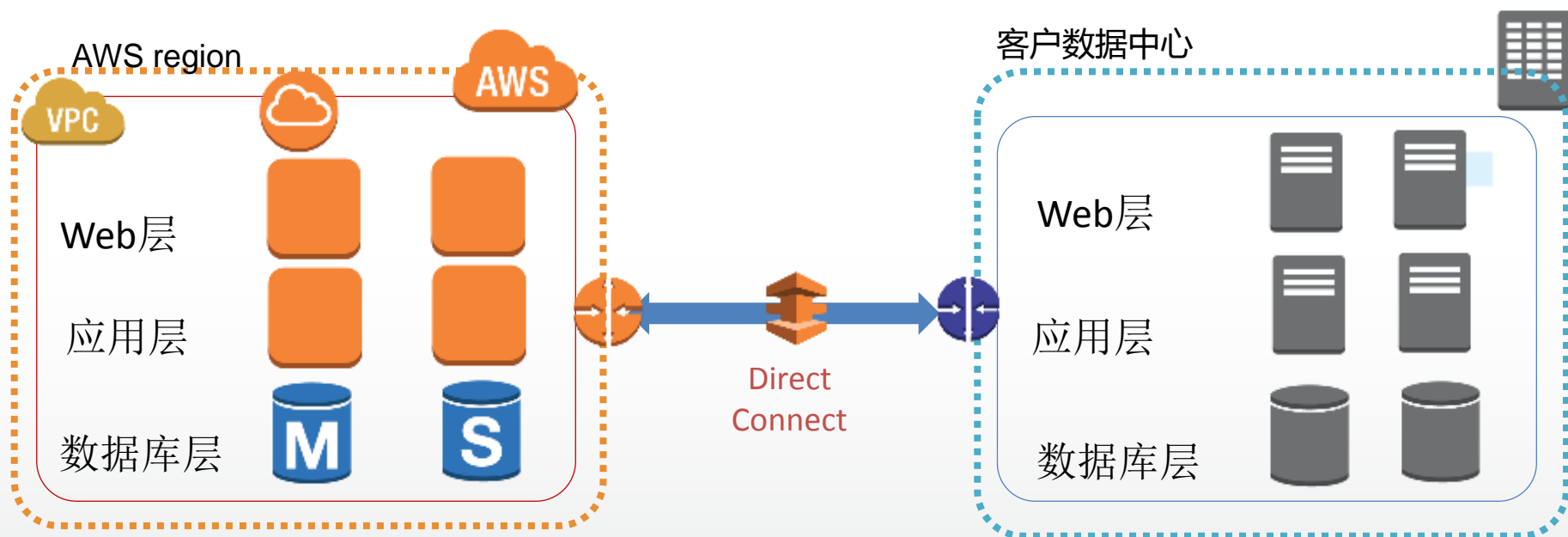
Brought by **InfoQ**



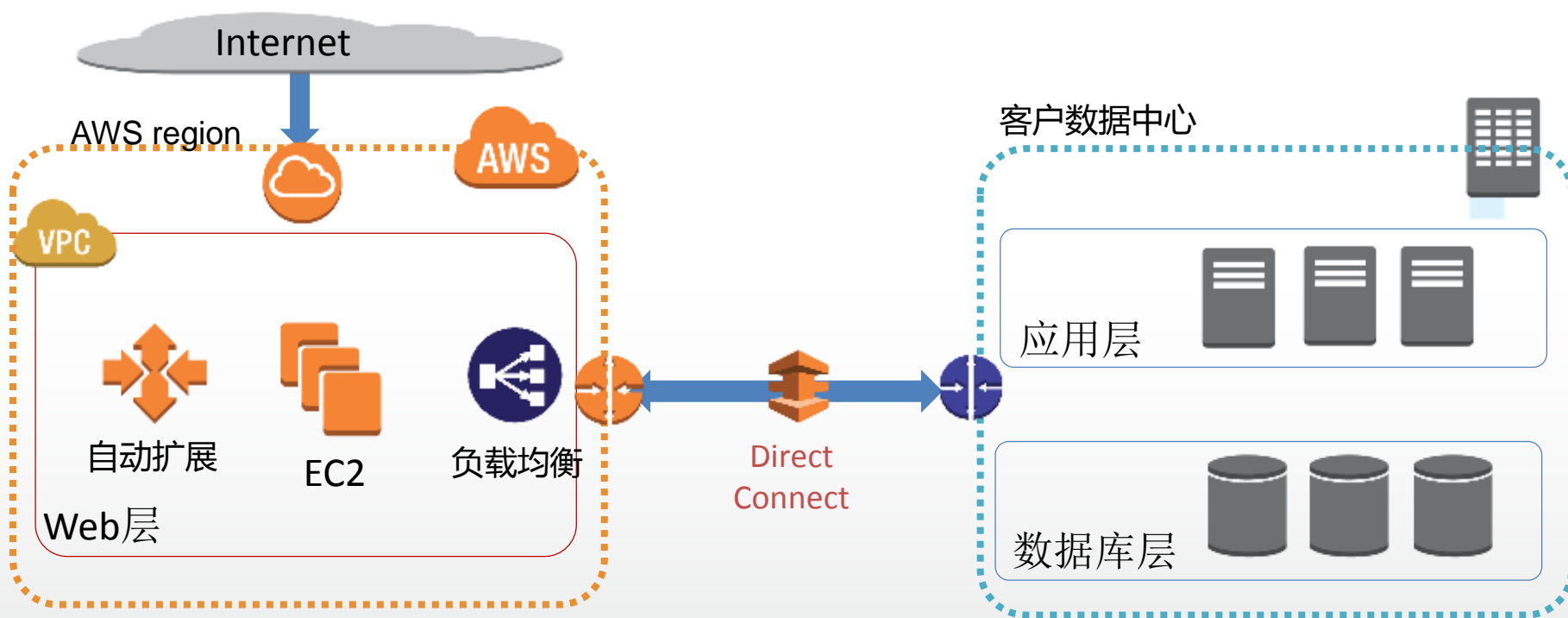


## 混合架构用法和案例

# 实现混合架构--专线直连

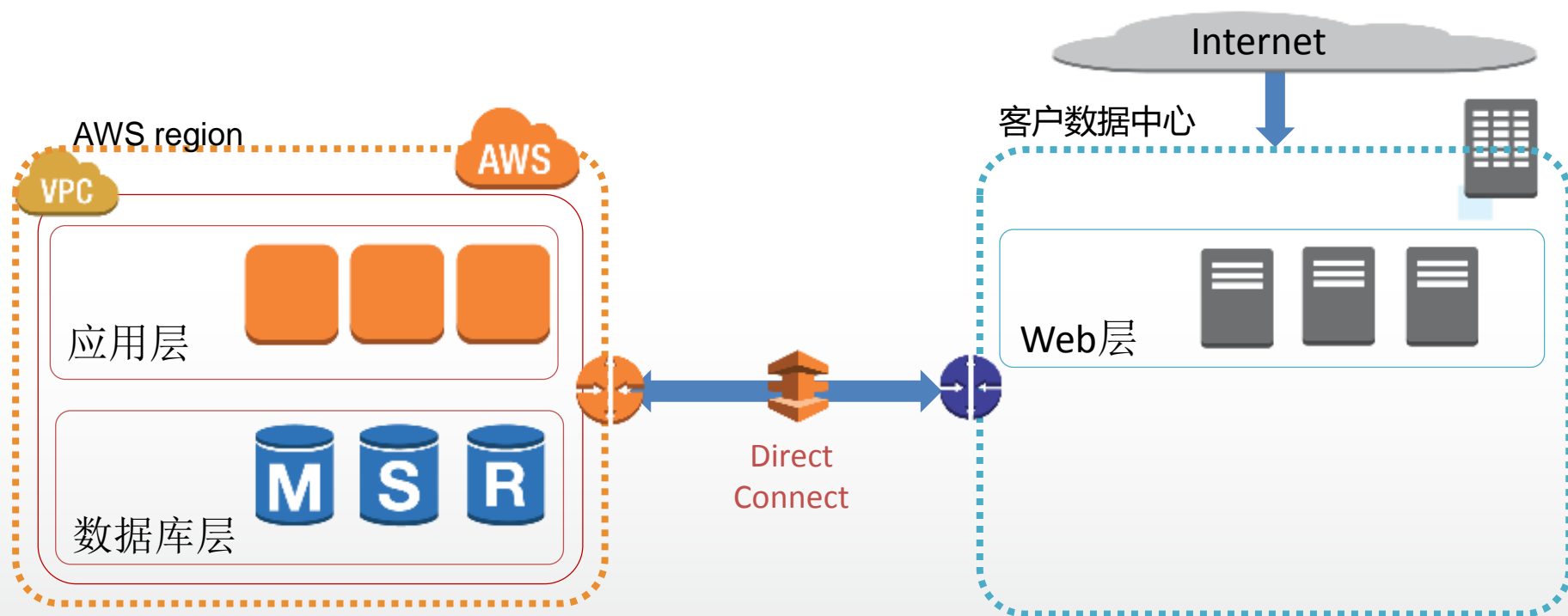


# 实例：Split Tier：AWS前端

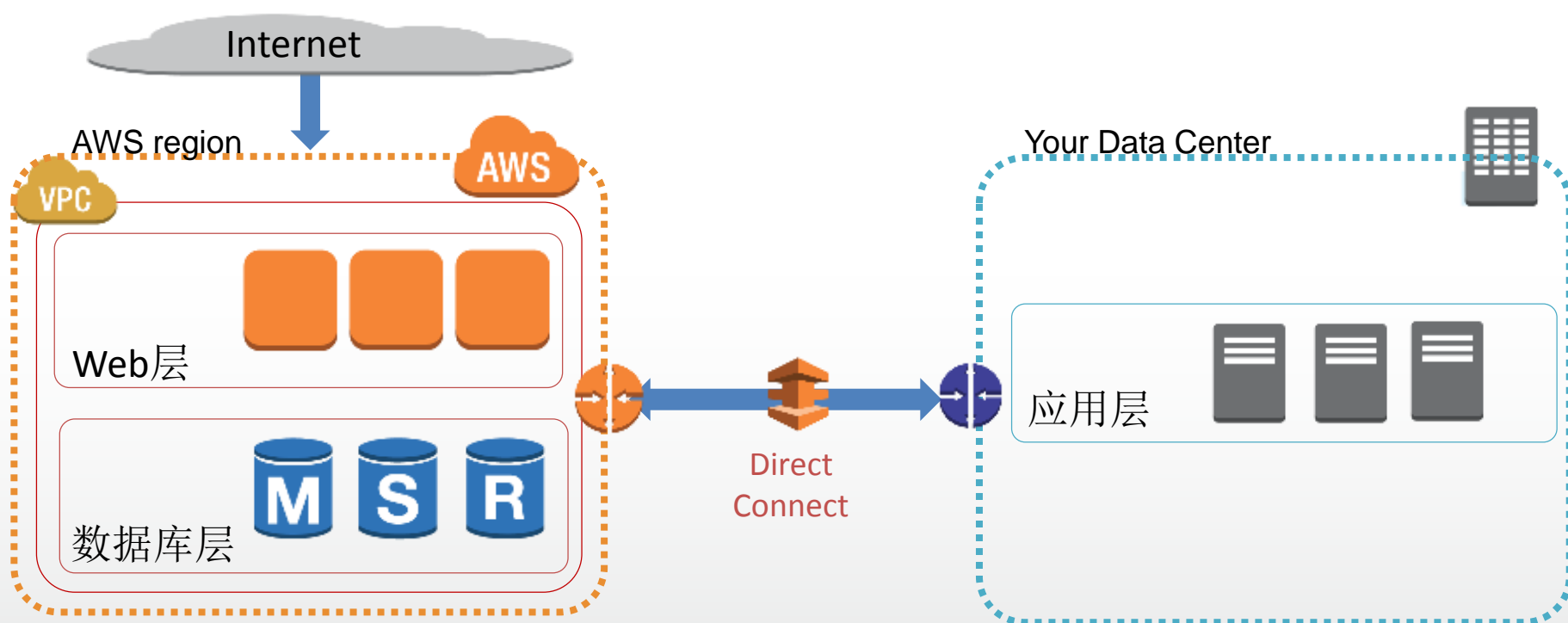




# 实例：Split Tier：本地DMZ 前端



# 实例：Split Tier：应用 Cloud Bursting



# 存储扩展

- 虚拟存储卷可以连接作为 iSCSI, NFS and CIFS 卷使用
- 通过本地缓存盘实现快速读取
- 网关前数据加密安全

## AWS Marketplace 合作伙伴



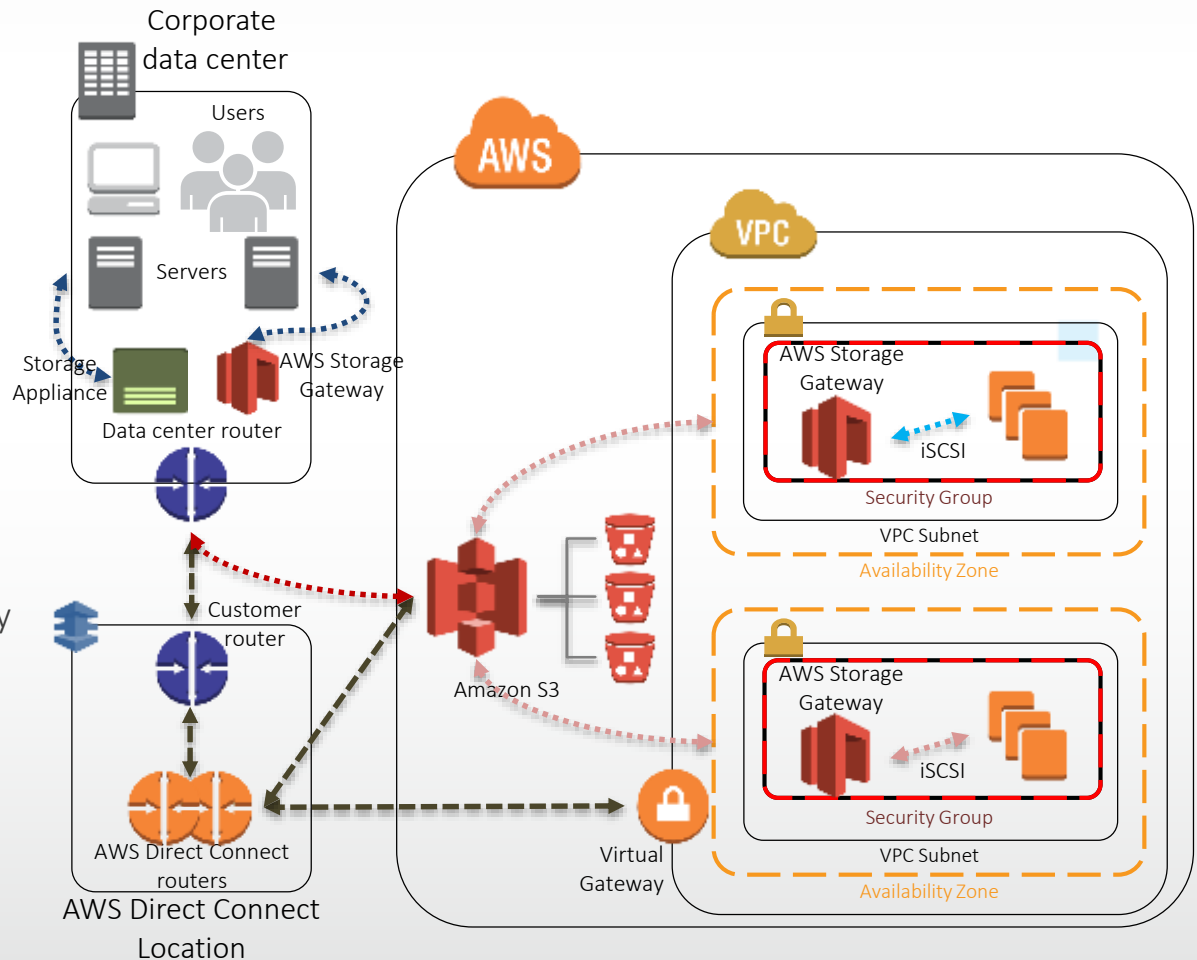
TwinStrata CloudArray



Panzura Global NAS



Cloud ONTAP Secure Cloud-Integrated Backup





# 备份和存档

- 备份网关与Amazon S3集成整合
  - 冷数据通过 Amazon S3 向 Amazon Glacier备份
- 从充分利用现有的投资和可供选择的解决方案
  - 去重
  - 压缩
  - WAN广域网加速

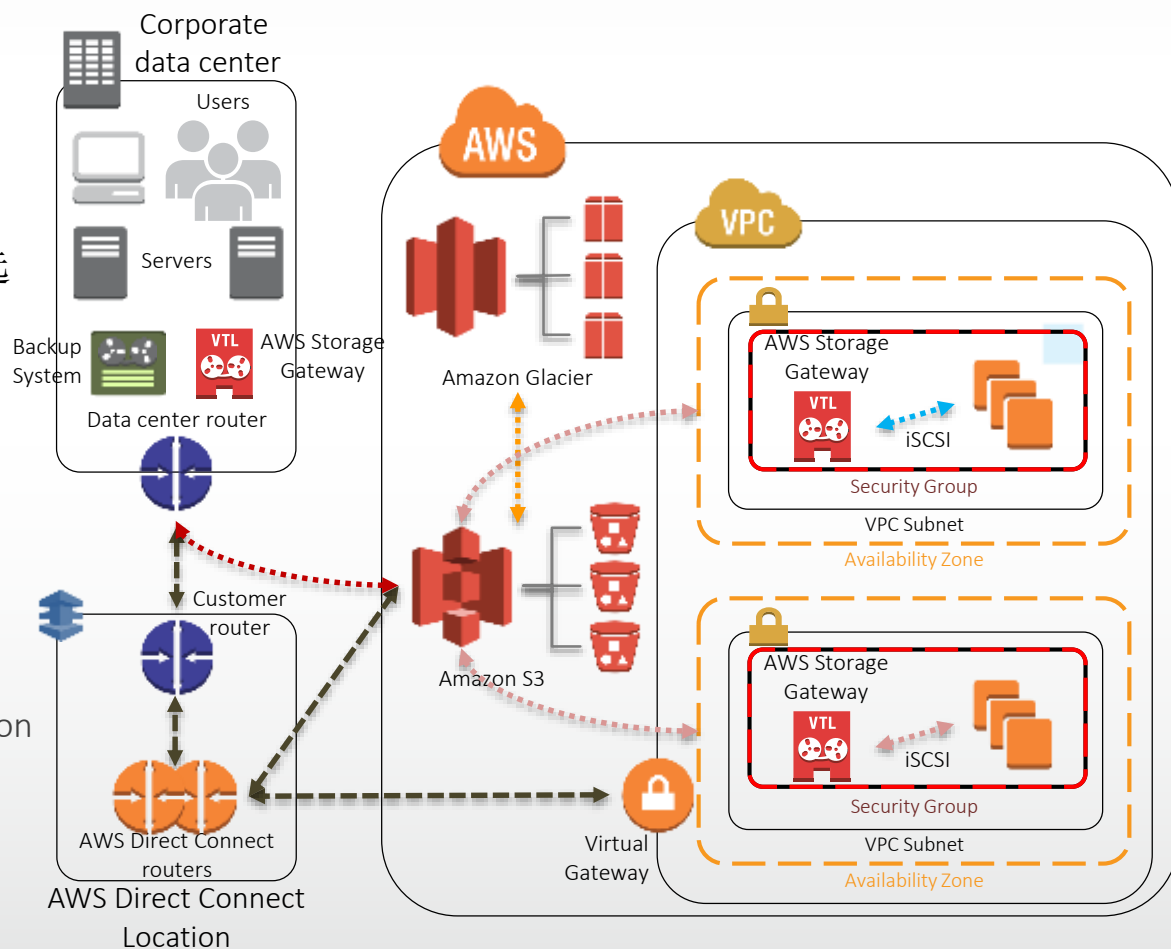
## AWS Marketplace合作伙伴

 Symantec Net Backup

 Veeam Backup & Replication

 Cloud ONTAP Secure Cloud-Integrated Backup

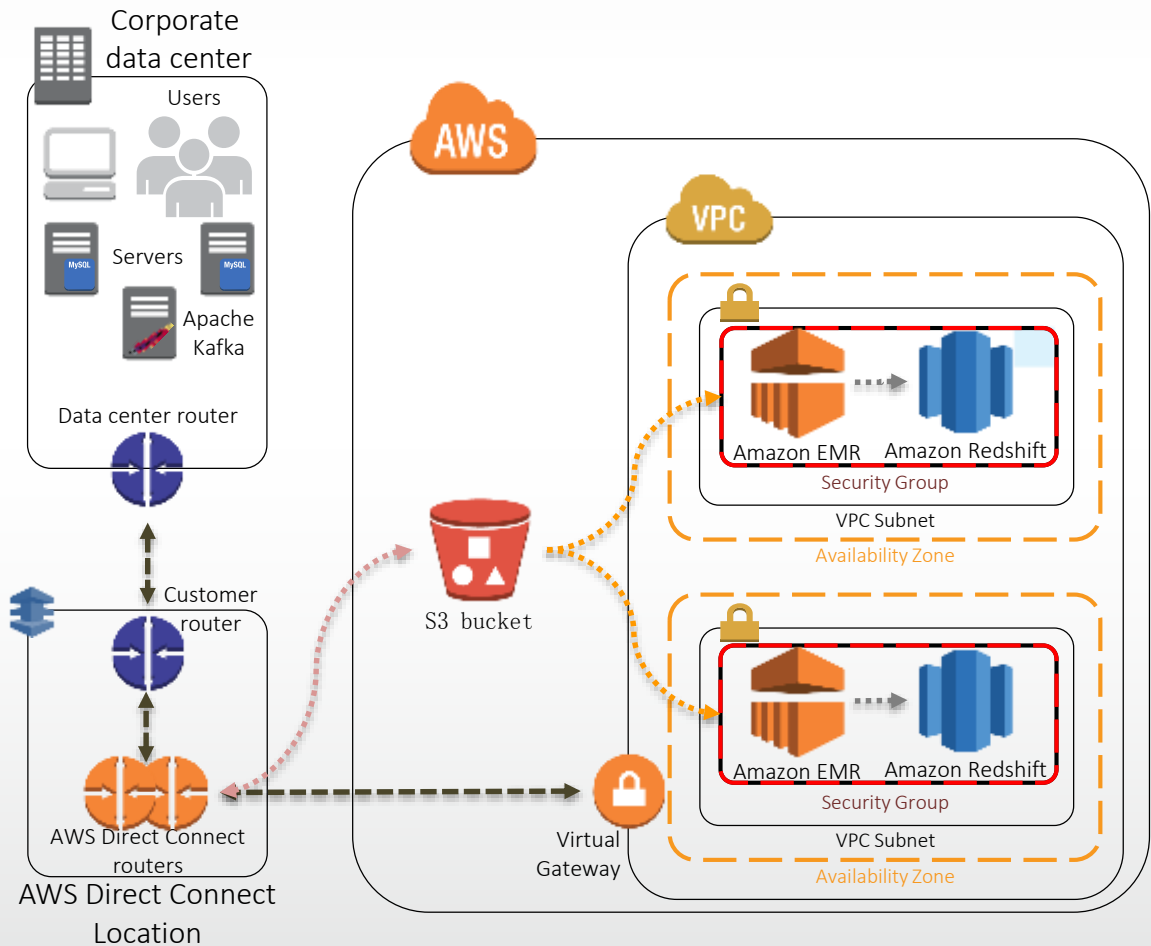




# 使用各托管的服务

## ○ 使用托管工具的好处

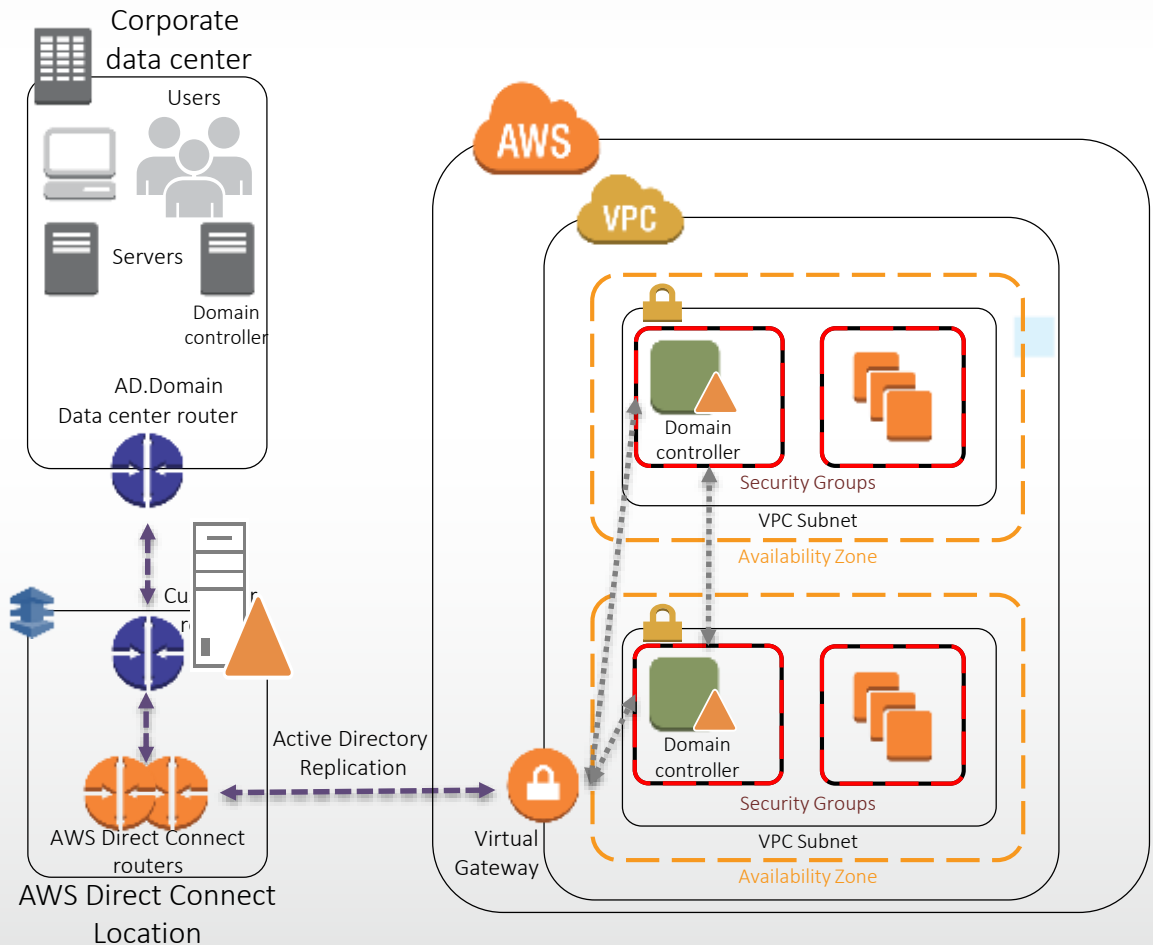
- 灵活快速
- 易于伸缩
- 安全可靠
- 自动维护升级



# Active Directory / LDAP

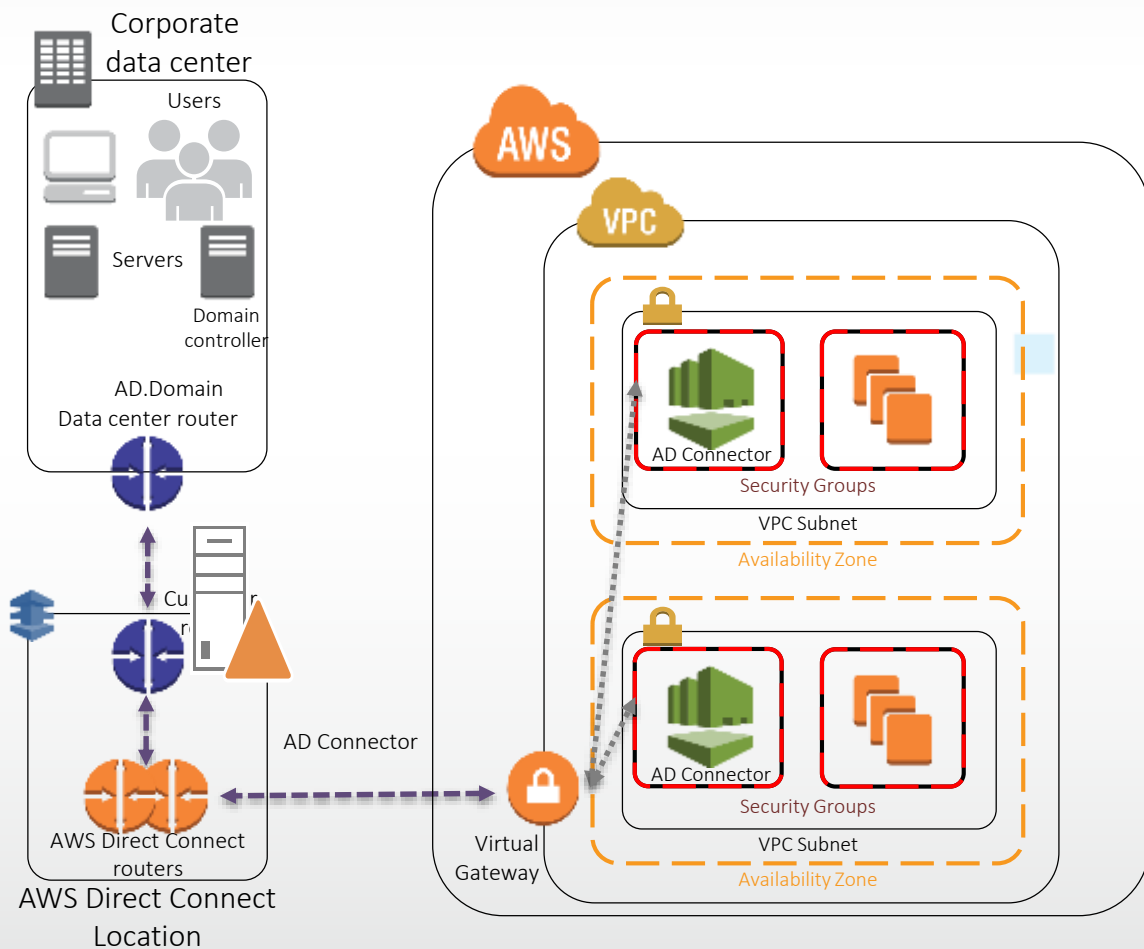
- 减少往返流量
- 减少认证延迟
- 增加韧性 Resiliency
- 使能:
  - Multi-Master Read/Write Domain Controllers
  - Read-only Domain Controllers (RODCs)
- ✧ 需要 IPsec VPN 或 Direct Connect 连接

Type	Port Number
TCP	54, 88, 135, 137, 139, 389, 445, 464, 636, 3268, 3269, 5722, 49152-65535
UDP	53, 67, 123, 138, 389, 445, 464, 2535, 5355, 49152-65535



# AWS Directory Service

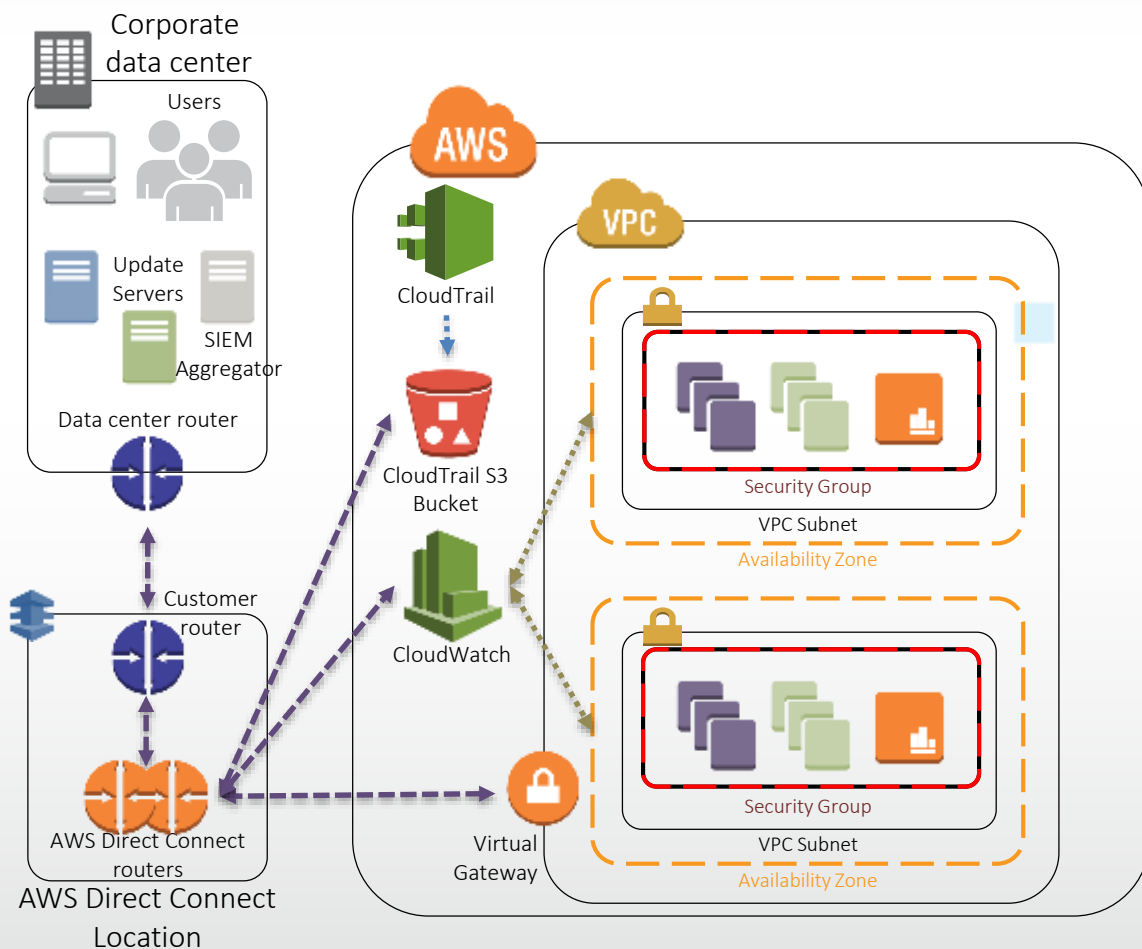
- 以下属两种模式部署
  - Directory Service Connect
  - Simple AD – 建在Samba 4 Active Directory 兼容服务器上
- 简化 IAM Federation
  - 避免部署基于 SAML的 federation架构的复杂性和额外成本
  - 作为代理服务器- 没有数据存放在AWS 架构上
  - 支持已有RADIUS-based MFA
- ✧ 需要IPSec VPN or Direct Connect 连接





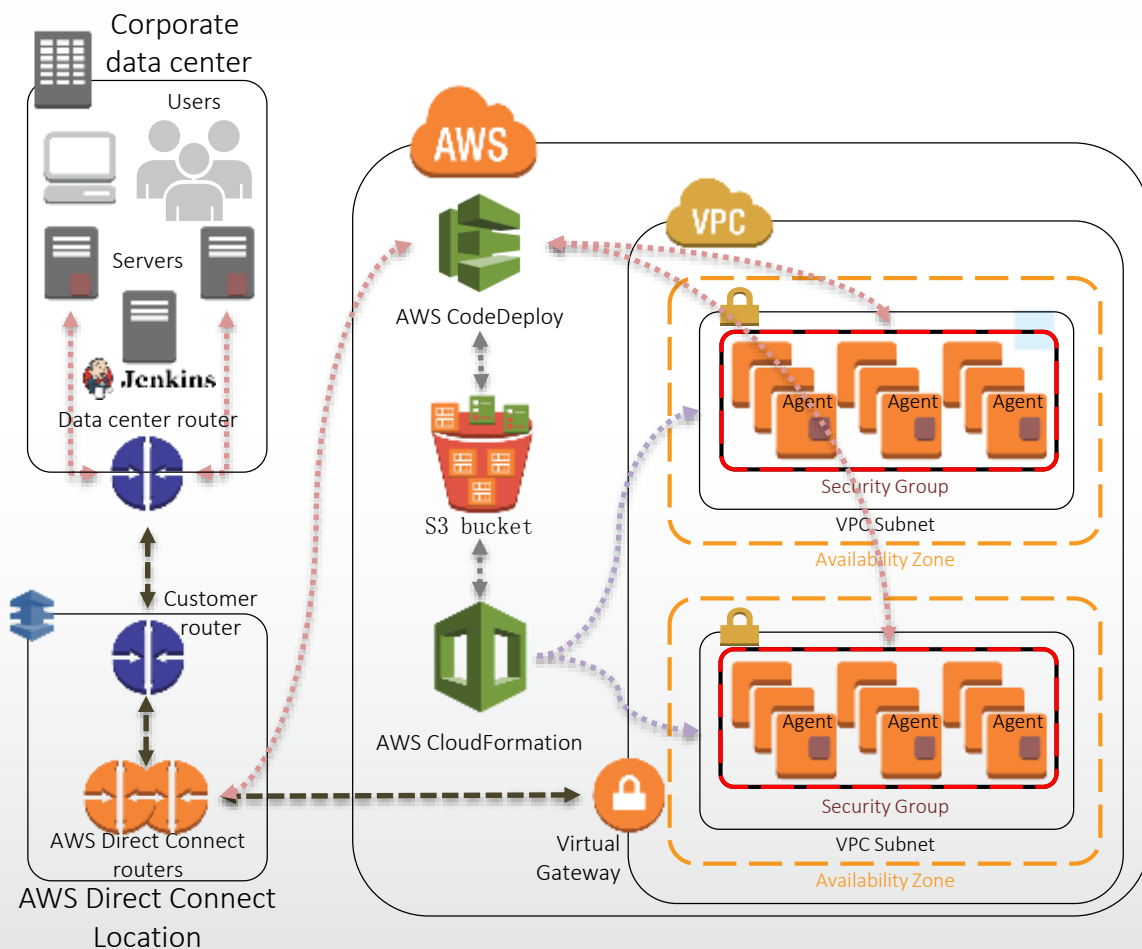
# 运营和监控工具

- 使用CloudTrail 和 SIEM  
Aggregator 对集成连接进行安全监控
- 通过CloudTrail 和 SNMP MIBs  
登录 SIEM Aggregator.
- 通过EC2 guest GEN agent将平台和应用健康信息放入SIEM Aggregator
- 通过本地部署的升级服务器做补丁和升级



# 持续集成，持续交付

- 利用CodeDeploy实现将应用灵活部署在企业安置或AWS EC2上
- 重复使用各种现有的脚本和工具
  - Bash, PowerShell, Chef, Puppet, anything...
- 与主要开发工具集成整合
  - GitHub, Jenkins, CloudBees, TravisCI, Eclipse...



# 常见混合云应用

存储扩展

开发，测试  
验证

关键  
业务应用

备份,存档

灾难恢复

大数据分析

# 实例介绍：云闪购和呼叫中心直连

呼叫中心专线直连

混合云实现云闪购

# 总结

- 混合架构是通向云的征程
- 连接性是实现混合架构的关键
- **AWS**帮助企业实现混合架构
- 大小企业都该早日踏上云的征程

谢谢！



网站

[www.amazonaws.cn](http://www.amazonaws.cn)

博客

[blog.csdn.net/awschina](http://blog.csdn.net/awschina)

微信

AWS中国



微博

[weibo.com/amazonaws](http://weibo.com/amazonaws)