Windows Azure

在Windows Azure中部署活动目录

演讲者
职位
公司

为什么使用活动目录?

商业需求

其他应用或服务的支持需求
作为分公司/总部域控制器的替代或者故障恢复
为只有云的数据中心作为主要的认证

设计考虑

某些活动目录配置旋钮和部署拓扑结构比其他更适合云

把活动目录域主控服务器放在Windows Azure上等价于运行一个虚拟的域主控服务器

虚拟机管理程序提供或淡化一些技术，这些技术和许多分布式系统不匹配，包括Active Directory

考虑

虚拟化DC是否安全?

活动目录数据库(DIT)的位置

为流量和成本优化部署

只读的DC(RODC)或读写?

全局编录(Global Catalog)或不用？

信任或复制？

IP地址和名称解析

地理分布的云托管域控制器

虚拟化的DC是否安全?

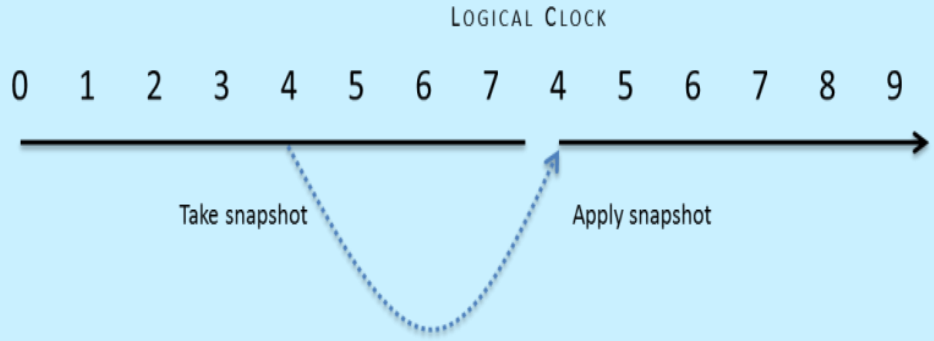
背景

通常的虚拟化操作，例如备份/恢复 虚拟机/VHD会导致虚拟DC的状态回滚

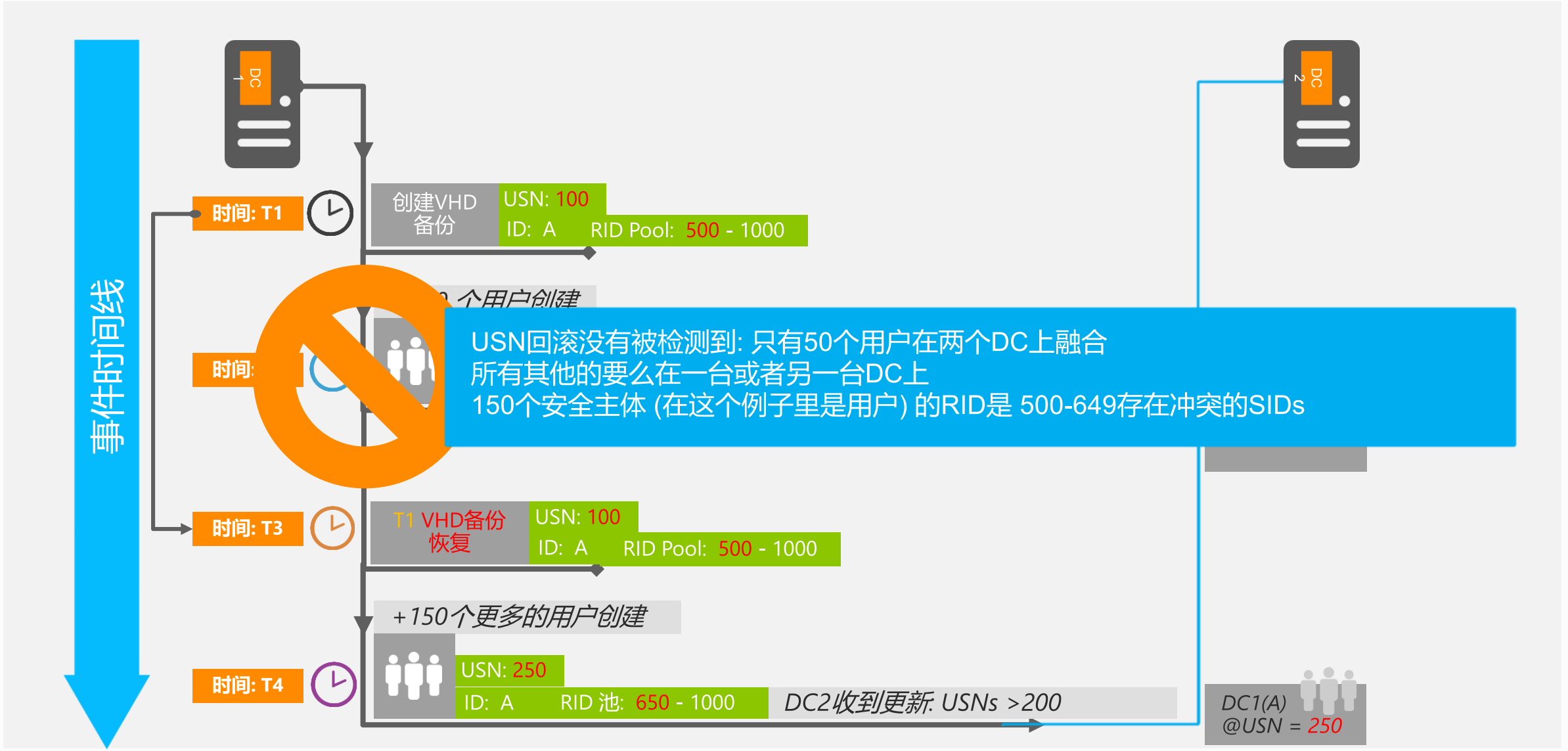
介绍USN 气泡导致的永久不同状态的后果：

- 过时对象(lingering objects)
- 不一致的密码
- 不一致的属性值
- 如果Schema FSMO回滚，那么会导致不匹配

安全性主体还潜在可能创建重复的SID



域控制器如何被影响？


事件时间线
DC 1
DC 2
时间: T1
创建VHD
备份
USN: 100
ID: A
RID Pool: 500 - 1000
个用户创建
时间:
USN回滚没有被检测到: 只有50个用户在两个DC上融合
所有其他的要么在一台或者另一台DC上
150个安全主体 (在这个例子里是用户) 的RID是 500-649存在冲突的SIDs
时间: T3
T1 VHD备份
恢复
USN: 100
ID: A
RID Pool: 500 - 1000
+150个更多的用户创建
时间: T4
USN: 250
ID: A
RID 池: 650 - 1000
DC2收到更新: USNs >200
DC1(A)
@USN = 250

活动目录DIT的位置

活动目录DIT/sysvol应该被部署在数据磁盘

数据磁盘和操作系统磁盘时两个不同的Azure磁盘类型

- 他们展示了不同的行为（和不同的默认值）

不想OS磁盘，数据磁盘默认不缓存写操作

- 注意: 数据磁盘限制在1TB
- 1TB > 最大的已知活动目录数据库 == 不是问题

为什么这是个问题?

写后面的磁盘缓存使得DC的假设失效

- DC断言的FUA (强迫单元访问forced unit access) 且期待IO子系统遵守
- FUA期望保证敏感的写到耐用的媒体中。
- 在失败的情形下会引入USN气泡

虚拟化结论

Windows Azure虚拟机支持AD

(不是VM角色)

DC不支持捕获/镜像

部署一个新的虚拟机创建DC，然后执行DC Promo

为流量和成本优化你的部署

根据需求考虑成本和部署

入流量是免费的，出流量不是

应用标准的Azure出流量价格

对网关自己有公开的每小时价格

可以根据合适开始和停止
如果停止，虚拟机和公司网络断开

RODCs将可能被证明更具成本效益

为流量和成本优化你的部署(继续)

DC定位器和ISTG/ISM (站点间拓扑生成器和消息发送器)

正确定义和连接活动目录子网和站点会影响你的底线

- 站点，站点链接和子网影响谁认证哪里以及DC的复制拓扑结构

确保在任何内部站点和云站点上的成本被合适地劝诫。

- 即，“下一个最近的站点”的概念（一个通常在活动目录里回退的概念）不应该得出云是下一个最近的结论。

确保复制是预定的（不是通知驱动的）

确保它被压缩（并且完成它-域控制器在复制流量的压缩上提供了激进的控制）

将复制日程和延迟容忍度保持一致

- DC 只复制最近的状态，如果有足够的更新，可以降低成本。

只读DCs (RODC)或可读可写？

在Azure中使用RODC想都不用想？真的吗？

这不是真的，当他们被设计为

- 设计为缓存DC用于物理不安全的分支站点
- 这是个信任问题... 你相信Azure数据中心吗？

但是HBI/PII是问题吗？

RODCs提供 ROFAS (一个过滤的属性集)，允许目标属性从RO复制中排除

但是RODC引入已知和位置的应用程序兼容性问题，增加了测试压力和相关的支持成本。

最后，RODC从不向外复制任何东西

他们需要生成可缓存的密钥，需要流量来作为用户/计算机认证来获取

考虑通过缺乏复制而节省向外流量来节约成本

全局编录(GC) 或不是?

对多域森林的认证GC是必须的

对云中的DC认证的工作负荷仍然会生成对外的认证流量

- 用于扩展通用组成员
- 由于他们托管每个域（一部分），和GC相关的成本比较难预测
- 如果工作量托管面向互联网的服务和对活动目录认证的用户，那么成本完全无法预测

可以利用 “通用组成员缓存”

主要是复制入站

- 出站复制有可能适合其他GC

信任或复制?

选择

在云中添加复制DC或者创建新的森林然后创建信任？

- Kerberos 或Federated

激励

安全性(可选择的认证功能)

合规/隐私(HBI/PII 问题)

成本

- 复制更多或者生成更多向外流量是验证和查询的结果

恢复能力/容错

- 如果链接断了，信任场景可能整个中断

IP 地址和名称解析

Azure虚拟机需要"DHCP租用地址"，但是租用从不过去或在虚拟机上移动

非静态的部分和最多活动目录管理员过去使用的是相反的

当一台Azure VM租用一个地址，在租用期间它可以路由

租用的时间长度直接登录服务的生命周期 → 所以这是好的 ☺

传统的域控制器的内部最佳实践不可用

不要考虑静态定义之前的租用地址作为解决方法

- 这一开始在剩下的租用时间看起来会工作，但是一旦当租用过期，虚拟机会丢失和网络的通讯 → 当它是域控制器时非常不好

名称解析

在域控制器上部署Windows Server DNS

- Windows Azure提供的DNS不能满足活动目录复杂的名称解析的需要 (DDNS, SRV 记录等等)

对域控制器和加入域的客户端有一个关键的配置项

- 必须能通过自己注册（DC）以及解析资源

由于静态地址不支持，这些设置必须在虚拟网络定义中设置

地理分布，云托管域控制器

Azure对域控制器的地理分布提供了一个激动人心的选项

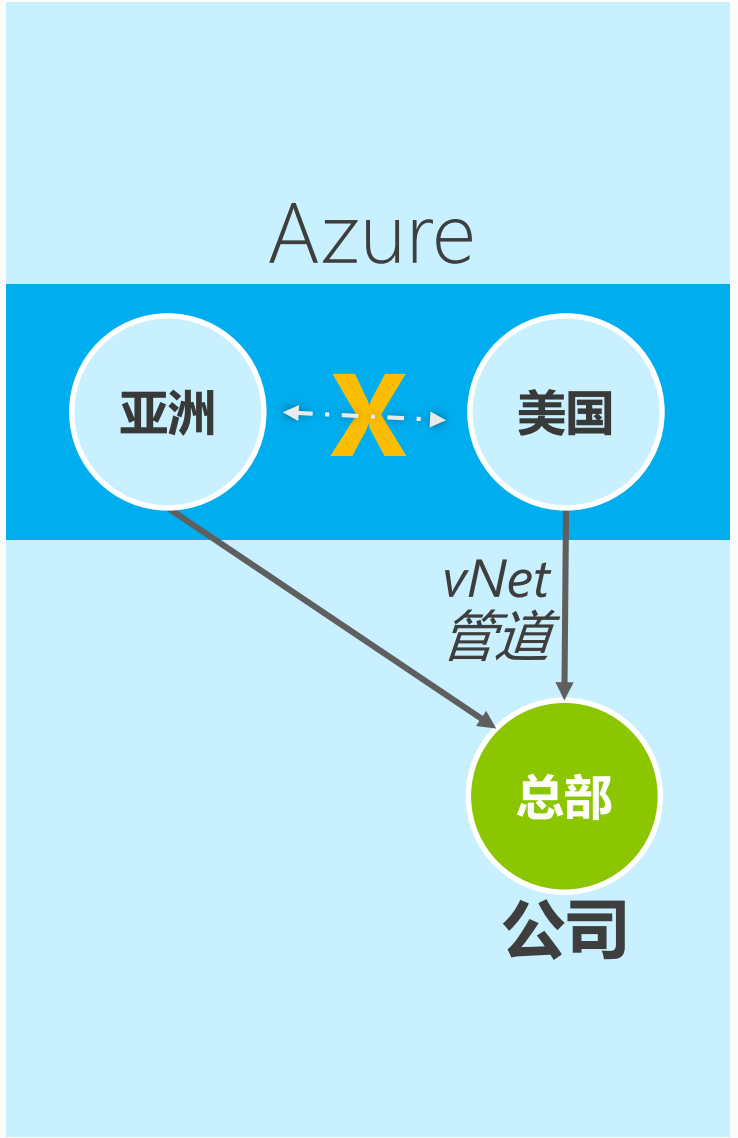
站外容错
和分公司物理上更近（低延迟）

但是没有直接的虚拟网络到虚拟网络的通讯存在

需要一个隧道从每个虚拟网络回到内部的公司网络

所有的复制会通过公司域控制器路由或弹回

可能生成大量的向外流量

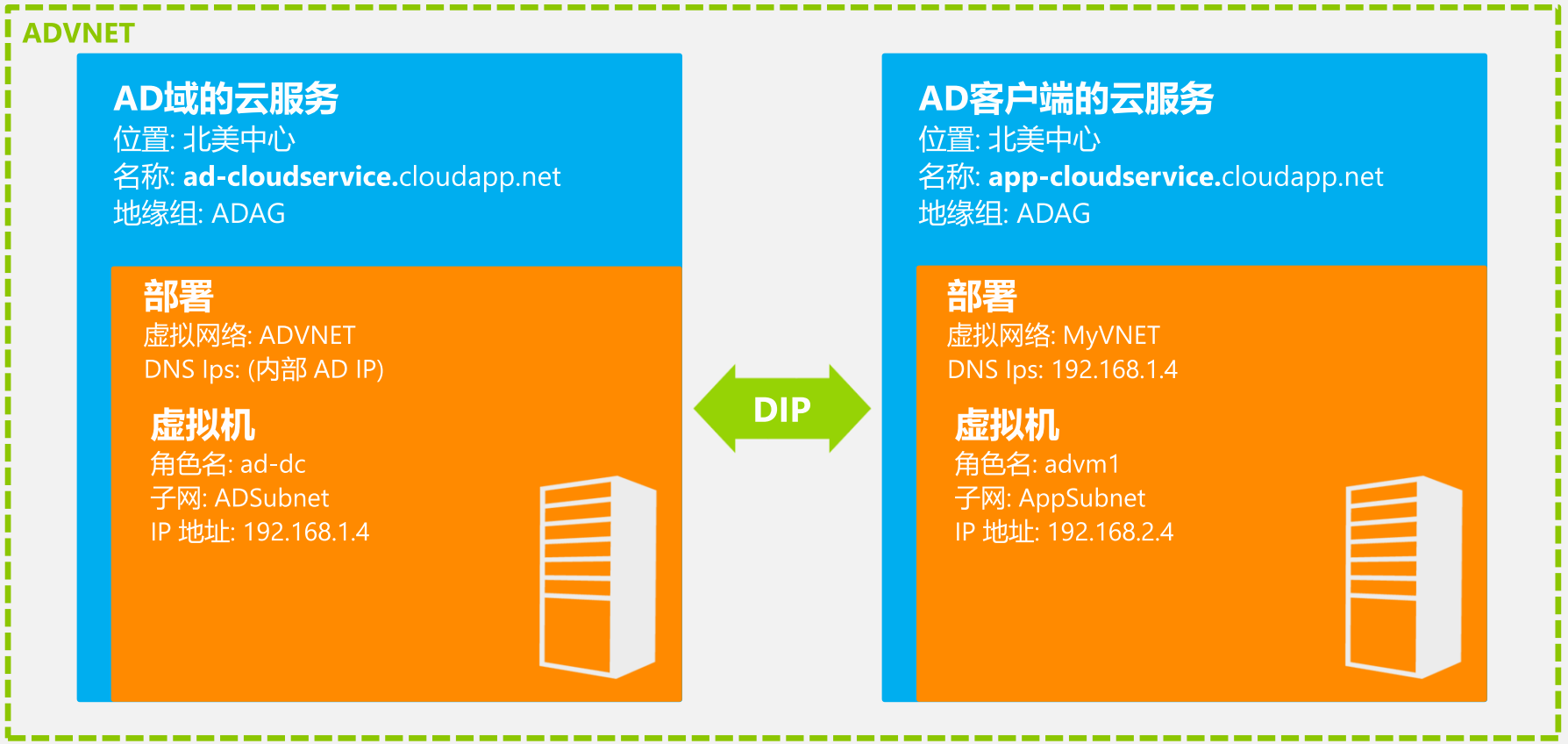


Azure AD 架构选项

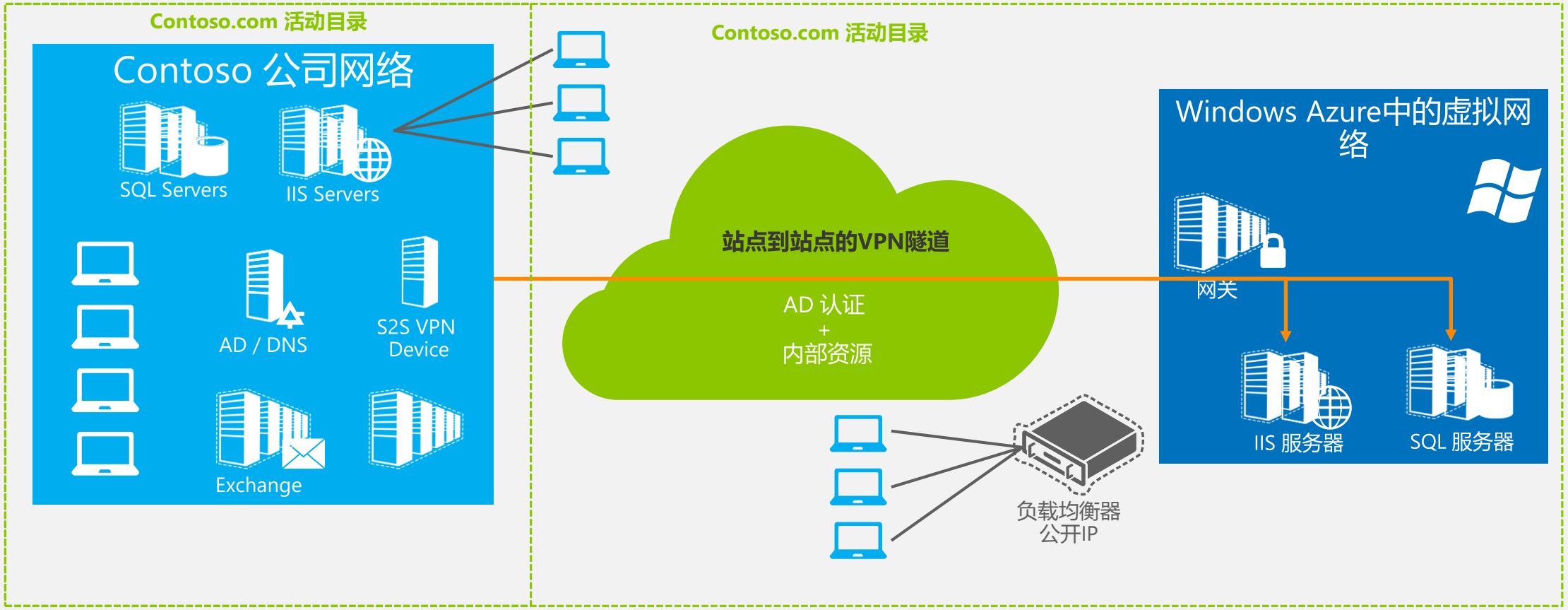
Windows Azure™

AD的云服务配置

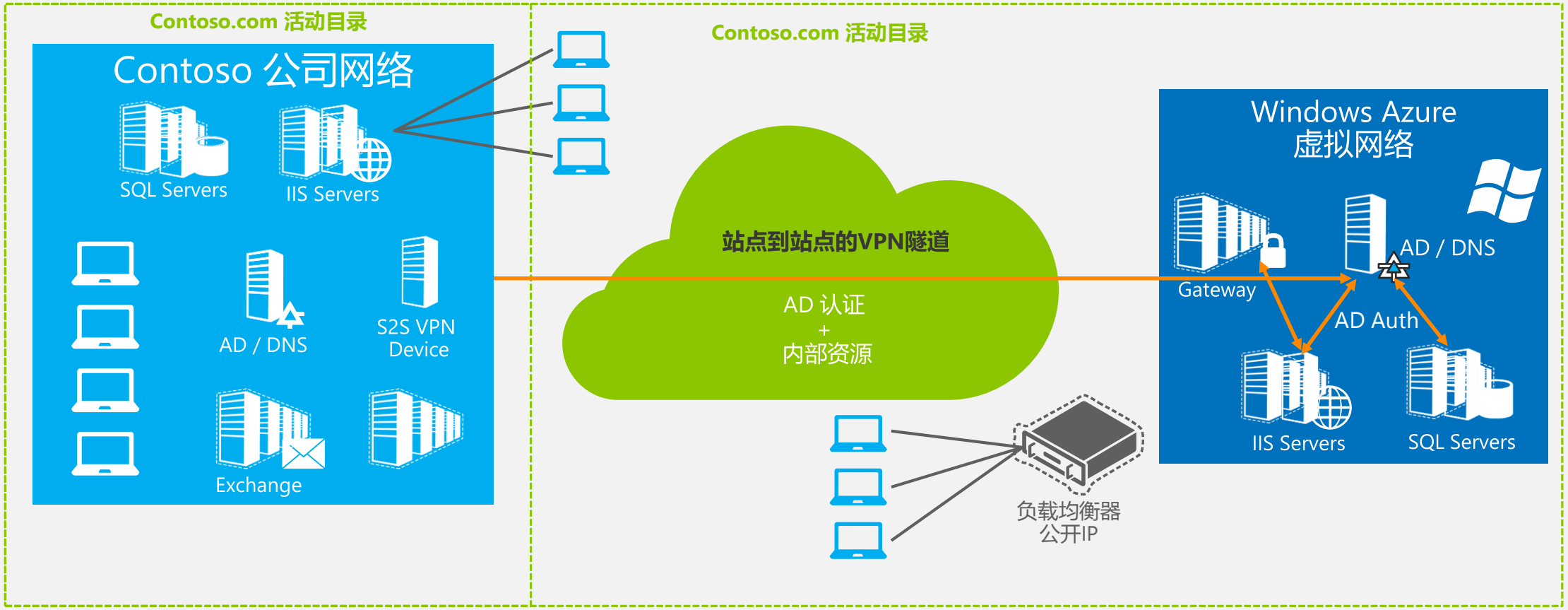
在一个单独的云服务中部署DC



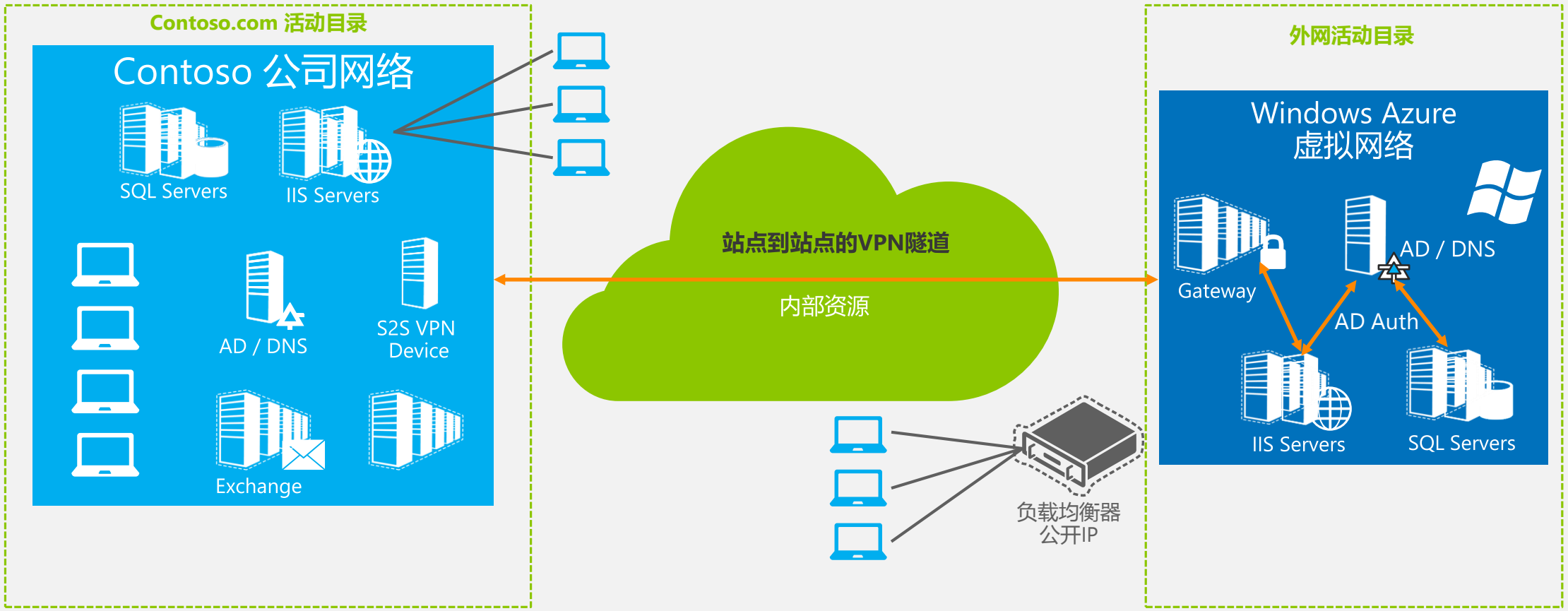
内部的域控制器


Contoso.com 活动目录
Contoso 公司网络
SQL Servers
IIS Servers
AD / DNS
S2S VPN Device
Exchange
Contoso.com 活动目录
站点到站点的VPN隧道
AD 认证
+
内部资源
负载均衡器
公开IP
Windows Azure中的虚拟网络
网关
IIS 服务器
SQL 服务器

云中的域控制器


Contoso.com 活动目录
Contoso 公司网络
SQL Servers
IIS Servers
AD / DNS
S2S VPN Device
Exchange
Contoso.com 活动目录
站点到站点的VPN隧道
AD 认证
+
内部资源
负载均衡器
公开IP
Windows Azure
虚拟网络
Gateway
AD / DNS
AD Auth
IIS Servers
SQL Servers

只有云的AD


Contoso.com 活动目录
Contoso 公司网络
SQL Servers
IIS Servers
AD / DNS
S2S VPN Device
Exchange
站点到站点的VPN隧道
内部资源
负载均衡器
公开IP
外网活动目录
Windows Azure
虚拟网络
Gateway
AD / DNS
AD Auth
IIS Servers
SQL Servers

AD 云部署模式

Windows Azure™

为一台DC部署虚拟机 – 新的森林

```
## 创建域控制器
## 不定义AD设置，因为你会使用DC Promo来创建新的森林
## 在这个例子里OS磁盘托管缓存被设为只读缓存
## 默认OS磁盘时可读可写，对数据库不安全

$dc1 = New-AzureVMConfig -Name 'MYDC1' -ImageName $imgname -InstanceSize Small |
       Add-AzureProvisioningConfig -Windows -Password $pwd |
       Set-AzureOSDisk -HostCaching ReadOnly |
       Set-AzureSubnet 'DNSSubnet'

New-AzureVM -ServiceName $cloudsvc -AffinityGroup $ag -VNetName $vnet -VMs $dc1 `
            –Location $location
```

加入活动目录的域变量

```
# 域设置
$domain = 'contoso'
$joindom = 'contoso.com'
$domuser = 'administrator'
$dompwd = 'dompassword'
$advmou = 'OU=AzureVMs,DC=contoso,DC=com' # create OU first
$vnetname = 'ADVNET'
$vmsubnet = 'FrontEndSubnet'
```

为一台DC部署虚拟机 – 现有森林

```
## 创建域控制器
## 设置活动目录加入域设置和内部DNS
$dc1 = New-AzureVMConfig -Name 'MYDC1' -ImageName $imgname -InstanceSize Small |
       Add-AzureProvisioningConfig -WindowsDomain -Password $dompwd -Domain $domain `
       -DomainUserName $domuser -DomainPassword $dompwd -MachineObjectOU $advmou `
       -JoinDomain $joindom |
       Add-AzureDataDisk -CreateNew -DiskSizeInGB 15 -DiskLabel 'dc1-datadisk' -LUN 0 |
       Set-AzureSubnet 'DNSSubnet'

## 把新的云服务指向内部的DNS/AD服务器来进行名称解析
$dns = New-AzureDns -Name 'OnPremiseAD' -IPAddress '192.168.1.9'

## 在数据中心中创建虚拟机，定义内部DNS
New-AzureVM -ServiceName $cloudsvc -AffinityGroup $ag -VNetName $vnetname `
            -DnsSettings $dns -VMs $dc1 –Location $location
```

部署一台虚机来加入域

```
## 创建VM1
## 定义活动目录加入信息
## DNS信息可以要么是云中的DC，要么是本地DC
$vm1 = New-AzureVMConfig -Name 'myvm1' -ImageName $myimage -InstanceSize Medium |
    Add-AzureProvisioningConfig -WindowsDomain -Password $dompwd -Domain $domain `
        -DomainUserName $domuser -DomainPassword $dompwd -MachineObjectOU $advmou `
        -JoinDomain $joindom |
    Set-AzureSubnet $vmsubnet

## 域控制器的IP 地址（内部或者云部署的）
$dns1 = New-AzureDns -Name 'dns1' -IPAddress '10.1.2.4'

New-AzureVM -ServiceName $cloudsvc -AffinityGroup $ag -VNetName $vnetname `
            -DnsSettings $dns1 -VMs $vm1 –Location $location
```