



---

# AWS Summit

AWS技术峰会 2015 · 上海

---





# 创建你的虚拟数据中心

VPC 基础

AWS 技术销售部 陈耀炜

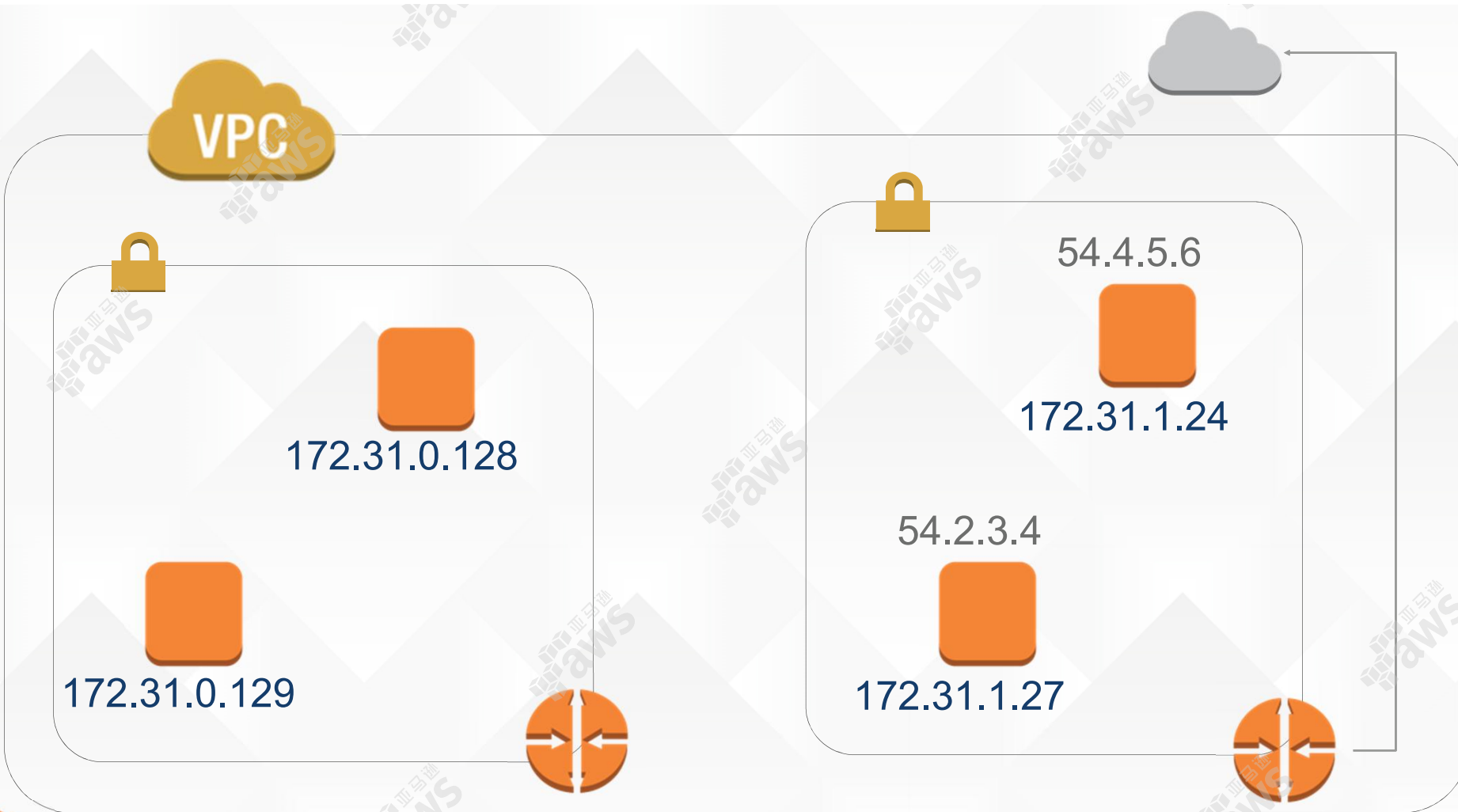
2015-12-17





EC2 虚机





VPC



# 我们会涵盖的内容

- 熟悉VPC的概念
- 建立一个基本VPC的流程

# 流程:建立一个互联网联通的VPC

# 建立一个互联网联通的VPC：步骤



选择一个地址段



在一个可用区内建立子网



创建一条指向互联网的路由



对进出VPC的流量进行控制



选择一个地址段



# CIDR 命名规则

- CIDR 段举例:

- 172.31.0.0/16

- 1010 1100 0001 1111 0000 0000 0000 0000



# 为你的VPC选择一个IP地址段



VPC

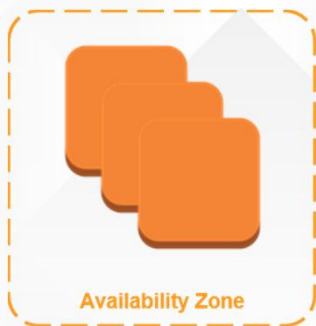


请注意一定要避免和你将要联  
通的网络地址段冲突重复

172.31.0.0/16

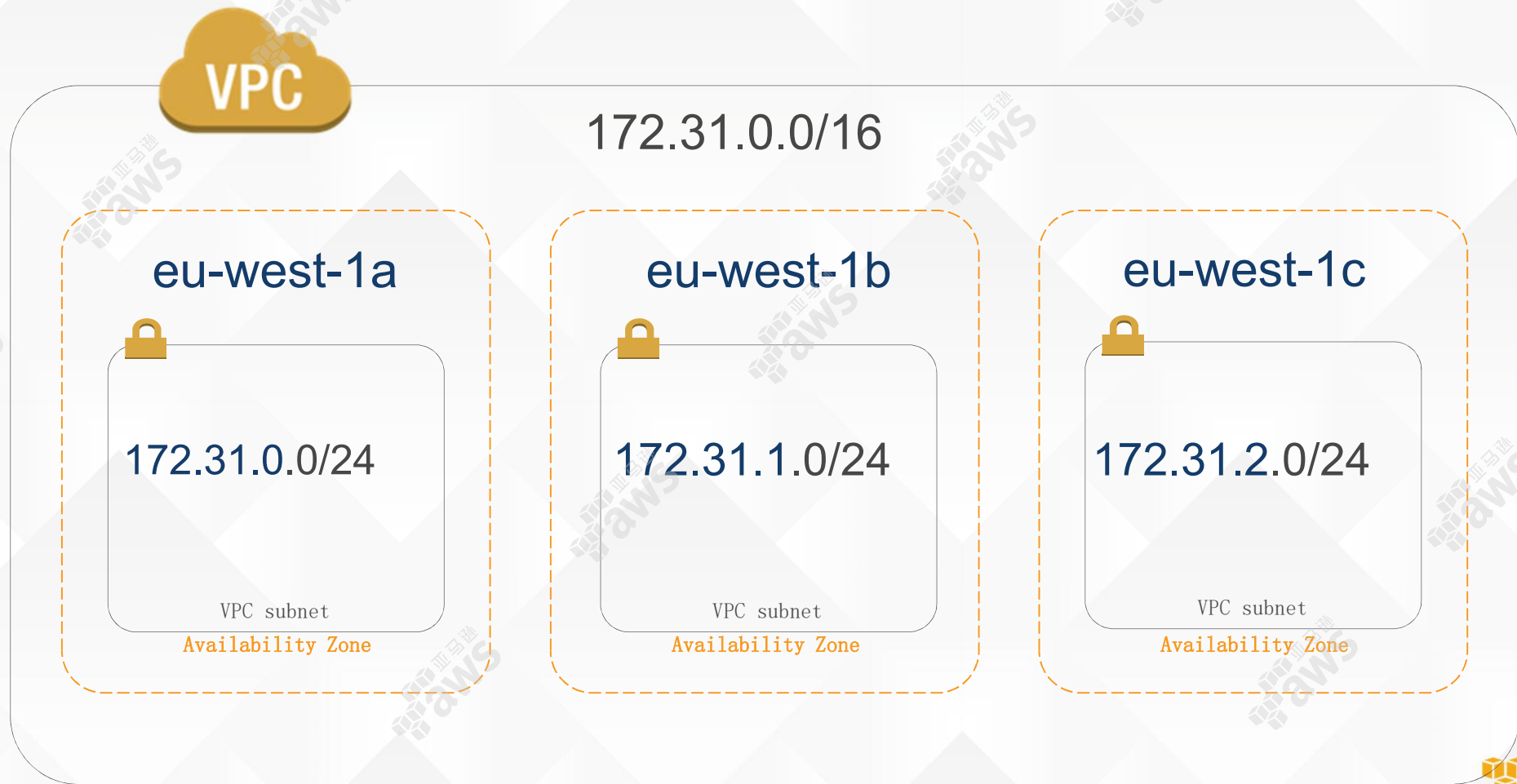
建议: RFC1918 range

建议:  
/16  
(64K addresses)



## 建立子网

# 为你的子网选择IP地址段



Create Subnet

Subnet Actions

Search Subnets and their properties

Name

subnet-a

subnet-b

subnet-c

subnet-849dcbe

Summary

Modify Auto

自动分配公网地址:  
所有的实例都会自动获得一个公网地址

Enable auto-assign this subnet.

☒ Enable auto-assign Public IP

Note: You can override the auto-assign public IP setting for each individual instance at launch time. Regardless of how you've configured the auto-assign public IP feature, you can assign a public IP address to an instance that has a single, new network interface with a device index of eth0.

Cancel

Save

State: available

Network ACL: acl-5cc5b539

## 关于子网更多的建议

- 适合于大多数客户的建议:
  - /16 VPC (64K addresses)
  - /24 subnets (251 addresses)
  - 每个可用区一个子网
- 这是还有什么需要做的呢





## 创建一条通向互联网的路由

# 你的VPC的路由

- 路由表保存了你的数据包会去哪里的规则
- 你的VPC有一个默认的路由表
- ... 但是你可以分配不同的路由表到不同的子网

172.16.0.0  
172.16.1.0  
172.16.2.0



Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associat	Main	VPC
	rtb-04304e61	0 Subnets	Yes	vpc-327d1857 (172.31.0.0/16)   ...

rtb-04304e61

Summary Tags

Cancel

Destination	Target	Status
172.31.0.0/16	local	Active

172.31.0.0/16 local Active No

Add another route

我的VPC的数据包的目的地

# Internet gateway

Create Internet Gateway Delete Attach to VPC Detach from VPC

Search Internet Gateways and X

« < 1 to 1 »

<input type="checkbox"/>	Name	ID	State	
<input checked="" type="checkbox"/>		igw-3376c756	attached	vpc-327d1857 (172.31.0.0/16)   ...

igw-3376c756

Summary Tags

ID: igw-3376c756

State: attached

Attached VPC ID: vpc-327d1857 (172.31.0.0/16) | Demo VPC

Attachment state: available

如果你希望你的数据包到达互联网请把  
他们导向这里

Create Route Table

Delete Route Table

Set As Main Table

Search Route Tables and their X

VPC可以到达互联网

rtb-04304e

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit

Destination

172.31.0.0/16 local Active No

0.0.0.0/0 igw-3376c756 Active No

172.31.0.0/16 local Active No

0.0.0.0/0 igw-3376c756 Active No



# 控制流量： 网络访问控制列表 安全组

# 网络访问控制列表 = 无状态防火墙规则

可以附加于最少一个子网

允许所有的流量进入

Search Network ACLs and the					
<input type="checkbox"/>	Name	Network ACL ID	Ass		
<input checked="" type="checkbox"/>		acl-5cc5b539	3 Subnets	Yes	vpc-327d1857 (172
acl-5cc5b539					
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

# 安全组遵循你应用的构架



# 安全组= 有状态防火墙

Create Security GroupDelete Security Group

Filter VPC security groups

Search Security Groups and tr X

<< 1 to 3

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input checked="" type="checkbox"/>	MyWebServers	sg-82ba7ee6	MyWebServers	vpc-327d1857	Allows all traffic from the Internet
<input type="checkbox"/>	MyBackends	sg-8fba7eeb	MyBackends	vpc-327d1857	Allows only traffic from MyWebServers
<input type="checkbox"/>		sg-07996163	default		

sg-82ba7ee6 | MyW

SummaryEdit

Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0

HTTP (80) TCP (6) 80 0.0.0.0/0

这个可以从80端口 (HTTP)被访问



# 安全组= 有状态防火墙

Create Security GroupDelete Security Group

Filter VPC security groups 🔍 Search Security Groups and t... X << 1 to 3 of

<input type="checkbox"/>	Name tag	Group ID	Group Name	VPC	Description
<input type="checkbox"/>	MyWebServers	sg-82ba7ee6	MyWebServers	vpc-327d1857	Allows all traffic from the Internet
<input checked="" type="checkbox"/>	MyBackends	sg-8fba7eeb	MyBackends		
<input type="checkbox"/>		sg-07996163	default		

只有位于MyWebServers 安全组的实例才能访问这个安全组的实例

sg-8fba7eeb | MyBackends

SummaryEdit

Type	Protocol	Port Range	Source
Custom TCP Rule	TCP (6)	2345	sg-82ba7ee6

Custom TCP Rule TCP (6) 2345 sg-82ba7ee6



# VPC中安全组：附加的注意点



- VPC允许创立进出两个方向的安全组规则
- 最佳实践：只要可能，通过指定的规则允许流量联通
- 很多的应用构架通过安全组（谁可以联通我）和IAM 角色（我可以做什么）定义1对1的互相访问规则（谁可以联通我）





Thank You

