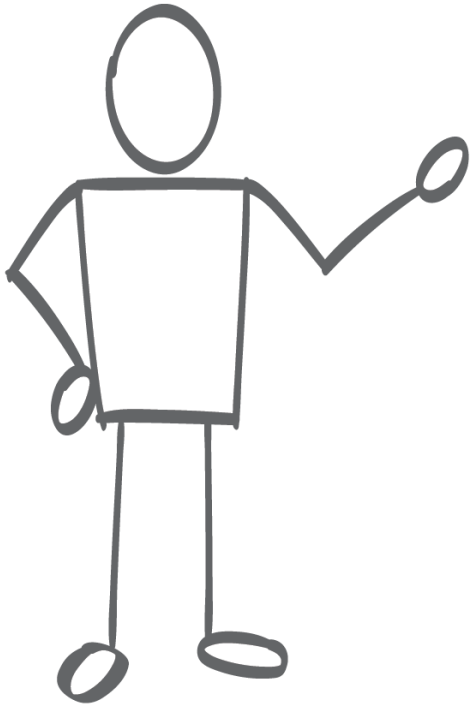
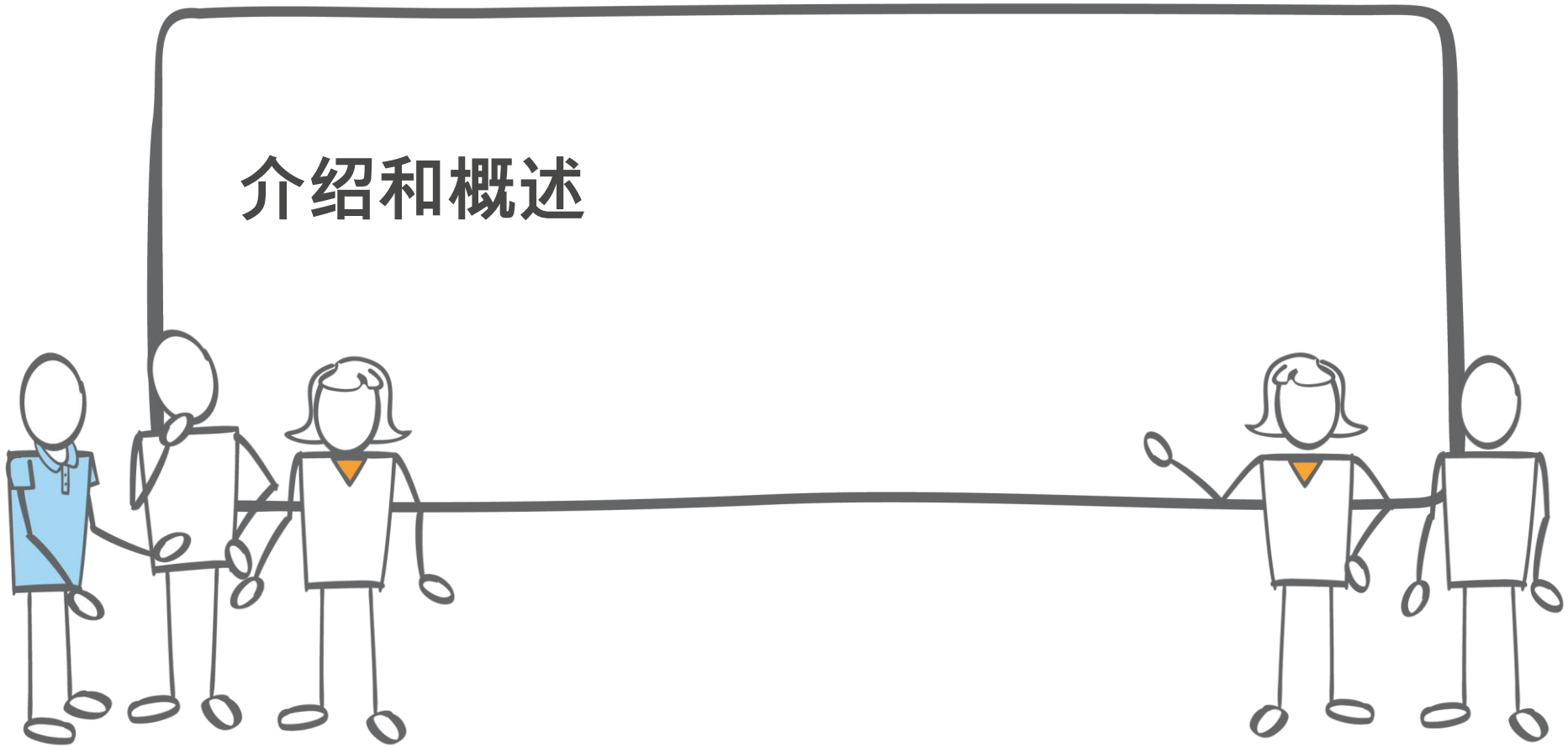


中秋节课程项目

InnoMed初创公司

介绍和概述



介绍

- **InnoMed** 是启动软件即服务（SaaS）的公司。
- 它已经建立了一个在线医疗社交网络和诊断援助在亚太地区，美国和欧洲用户的应用程序。
- 应用程序连接病人和医生允许网上预约，远程会诊，远程诊断，电子处方传递，和支付服务。

- 该应用程序允许用户上传文档和图像。文本被从文档中提取的，并且图像被转换为多种格式。

- 该应用程序还没有被公开发布。

概述 - 当前环境

- InnoMed的开发和测试基础设施部署了服务器托管公司。
- InnoMed使用Microsoft Windows服务器托管与Microsoft SQL Server标准版的后台数据库，他们的网络层和应用层。
- 申请上市日期即将到来，并InnoMed预计许多用户开始使用应用程序。
- InnoMed决定使用云技术，以支持其快速增长。
- InnoMed已聘请你到建筑师AWS的基础设施，以满足其应用需求。

概述 - 要求

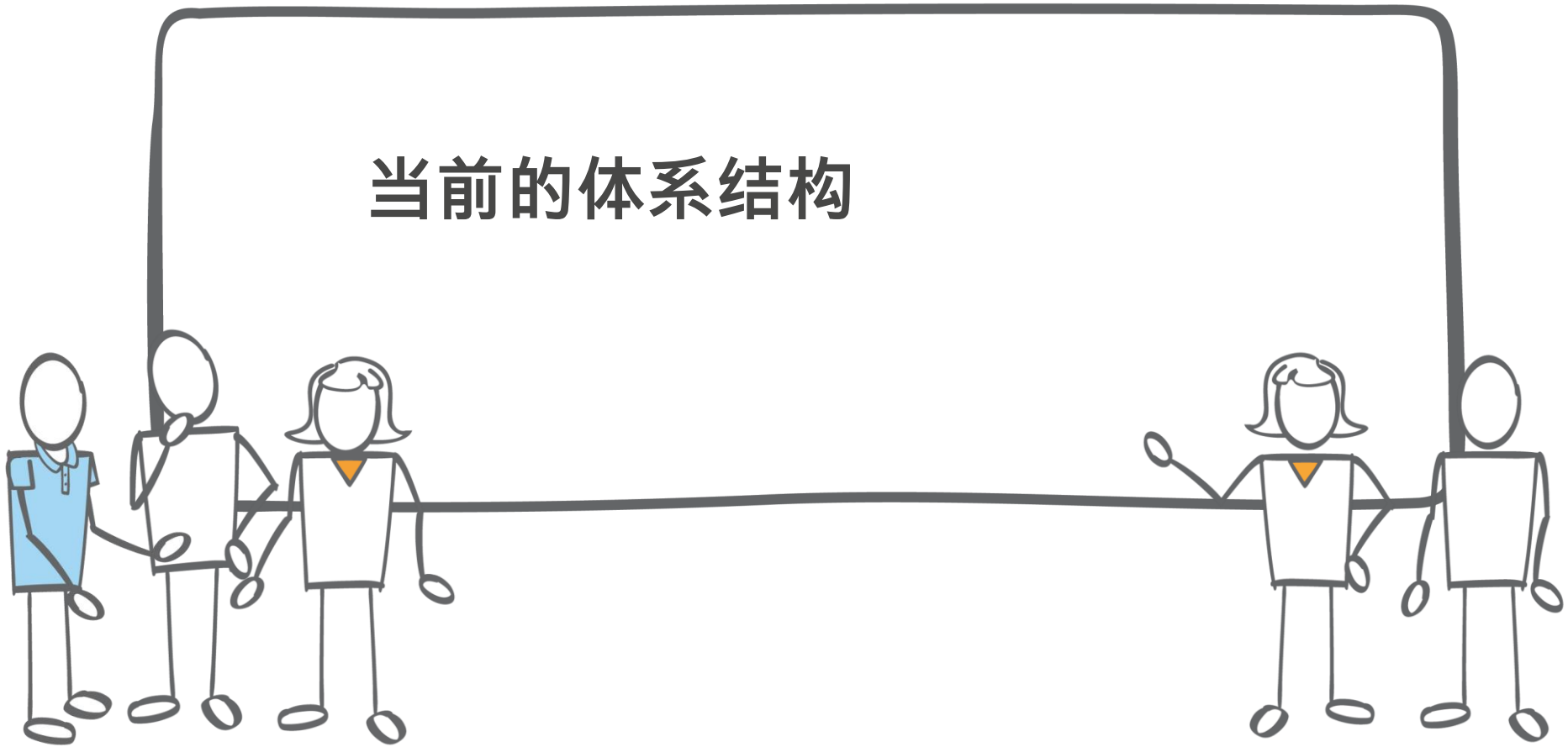
InnoMed计划将他们的应用程序移动到AWS。该计划包括：

- 配置访问权限与AWS的最佳做法接轨。
- 配置审核来跟踪所有用户操作。
- 建立网络符合AWS最佳实践，同时提供所有的应用程序所需的网络服务，在各自不同的环境。

- 建立，目前的体系结构在服务器托管公司相匹配，并且能够处理增加一倍的服务器数量的架构。

- 确保无需更改代码。

当前的体系结构



当前的体系结构

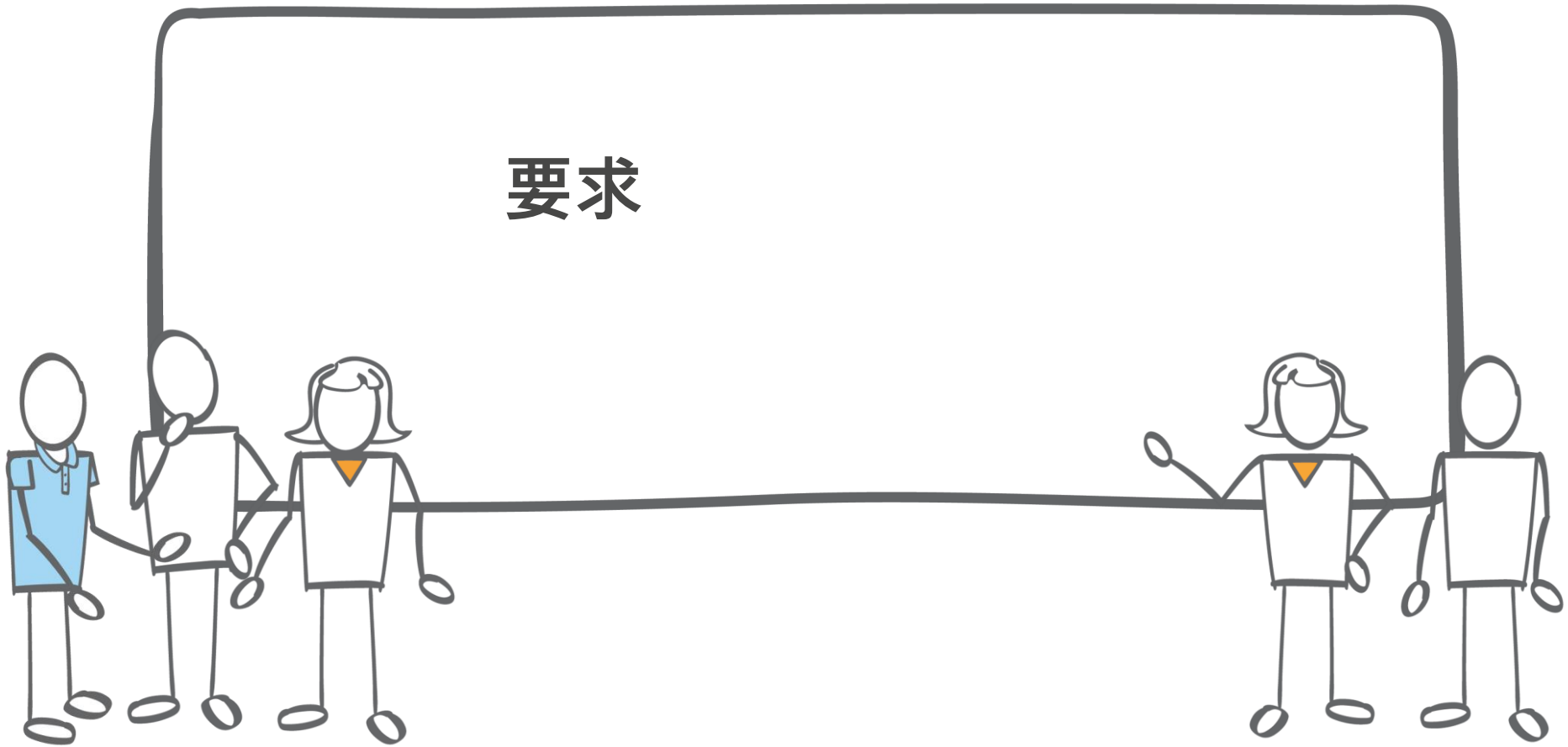
Web层

- 两个物理服务器（两个CPU / 4-GB存储器）
- 微软的Windows 2016基础与IIS
- HAProxy的负载平衡器使用的Web服务器应用程序层之间平衡流量

- 两台物理服务器（四个CPU / 16-GB内存）
- 微软的Windows 2016基础与IIS
- HAProxy的负载均衡器用于应用服务器数据库层之间平衡流量

- 一个物理服务器（八个CPU / 32-GB存储器/ 5-TB存储）
- SQL Server标准版 - v12.xx
- 微软的Windows 2016基础
- 数据库管理员访问和管理数据库，但没有RDMBS或高级配置是必需的。

要求



要求 - 用户认证（12）

- 能够访问AWS用户在三组：
  - 系统管理员组：　　2个用户
  - 数据库管理员组：　　2个用户
  - 摩立特集团：　　4个用户
    - 监测基础设施资源，为应用程序（EC2，S3，RDS）

- 按照分发权限AWS最佳实践。
- 该InnoMed应用程序必须读取和写入S3桶。

要求 - 用户认证（2/2）

- 密码策略应执行以下操作：
  - 具有至少8个字符，1个大写和1个小写字母，数字1，和一个特殊字符密码
  - 强制更改密码每90天
  - 没有再使用前三个密码
- 所有管理员需要进行编程访问和AWS管理控制台访问。
  - 当登录到控制台，每个管理员需要提供用户名，密码，并通过虚拟MFA提供了一个随机生成的代码。
- 所有其他用户应该只有AWS管理控制台访问，使用的用户名和密码的组合。

要求 - 审计

管理员必须能够跟踪账户每一个AWS行动，包括：

- 每个服务或者创建或配置的对象。
- 谁创造了对象或配置的服务用户。
- 用于每个建立或配置操作的接口。
  - 例如：AWS管理控制台或CLI
- 每个创建或配置操作的源。
  - 例如：IP地址或DNS别名

要求 - 网络与安全（12）

新的架构必须符合AWS最佳实践。这包括：

- **实现 高可用性 所有层，以减少停机时间。**
- 该应用程序，并限制公众进入点控制访问。
- 最大限度地减少IP地址的使用，以减少攻击面。
- 保持InnoMed的开发/测试环境和生产环境的独立的网络。

要求 - 网络与安全（2/2）

新的架构必须符合AWS最佳实践。这包括：

- Web层负载均衡器可以从端口互联网接收请求
  80。
- Web层服务器只能在80端口接收来自Web层负载均衡请求。
- 应用负载平衡器只能在端口8080上接收来自Web层服务器的请求。
- 应用层服务器只能在端口80上接收来自所述应用程序层负载平衡器请求。
- 数据库服务器只能在端口1433接收来自应用服务器的请求。

要求 - 网络层和应用层

- 在Web层的所有实例名应该被标记为重点=名称和值= Web层。
- 所有实例名称在应用层应该被标记为重点=名称和值=应用层。
- 在应用程序层的所有实例都必须支持EBS优化。
- 对于网络层和应用层负载均衡器必须支持HTTP，HTTPS和TCP协议。

要求 - 业务连续性

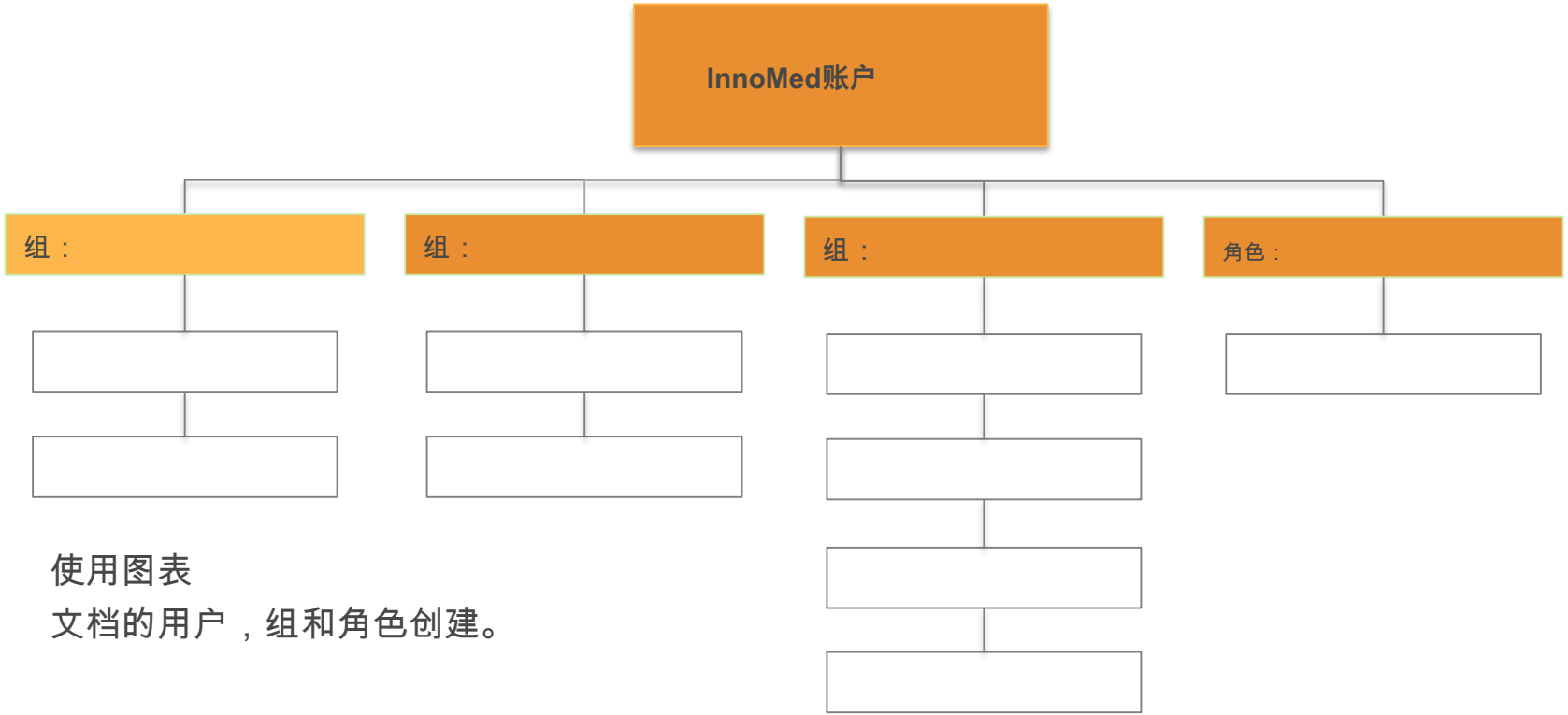
新架构的设计应实现业务连续性。这包括：

- 网络层和应用层应该是自愈。
  - 如果一台服务器不可用时也将被新服务器替换。
  - 服务器被认为是如果操作系统或应用程序无法响应不可用。
- 数据库层应该支持Multi-AZ部署。
- 架构应该加倍处理服务器的数量 以支持其快速增长。

解决方案模板

哪些服务您使用？

用户，组和角色



使用图表
文档的用户，组和角色创建。

用户，组和角色

组/角色 #	组/角色名称	权限
组		
组		
组		
角色		

密码策略

需求	解
至少应为8个字符，并有1个大写，小写1，特殊字符和数字。	
更改密码每90天，并确保前三个密码不能被重新使用。	
管理员登录到AWS管理控制台需要使用虚拟MFA的。	
所有管理员需要进行编程访问	

VPC详细

VPC	区域	目的	子网	AZS	CIDR范围
1					
2					

生产子网详细

子网名称	VPC	子网类型（公/私）	AZ	子网地址
	#1			
	#1			
	#1			
	#1			
	#1			
	#1			
	#1			
	#1			

测试/开发子网详细信息

子网名称	VPC	子网类型（公/私）	AZ	子网地址
	#2			
	#2			
	#2			
	#2			
	#2			
	#2			
	#2			
	#2			

实例详细信息

描述的类型，大小，以及你将用于每一层的实例理由。

一级	标签*	OS	类型	尺寸	理由	实例 #	用户数据？
卷筒纸	重点=名称值= Web层						
应用	重点=名称值=应用层						
D B	重点=名称值= DB 层						

* 如图所示，以满足实验室的目标标签必须配置

负载平衡器和实例安全组详细信息

负载均衡	名称*外部 /内部	子网	SG名称*	规则	资源
对于Web层	网络ELB		网络ELB-SG		
对于应用层	APP-ELB		APP-ELB-SG		

实例层	SG名称*	规则	资源
Web层	Web层-SG		
应用层	应用层-SG		
数据库层	DB层-SG		

* 如图所示，以满足实验室的目标名称必须配置

自动缩放启动配置

一级	OS	类型	尺寸	组态 名称*	角色	安全组
卷筒纸				WebTier		
应用				AppTier		

* 如图所示，以满足实验室的目标名称必须配置

自动伸缩群

一级	启动配置*	团队名字*	组大小	VPC	子网	ELB	标签
网络WebTier		WebTier					
应用	AppTier	AppTier					

* 如图所示，以满足实验室的目标名称必须配置

审计选项

Q. 你如何配置帐户创建所有的审计线索
执行API调用？

_____

Q. 你在哪里保存你的日志？

_____

错误或修正？请发送电子邮件至 aws-course-feedback@amazon.com 。
其他问题？联系我们在
https://aws.amazon.com/contact-us/aws-training/ 。