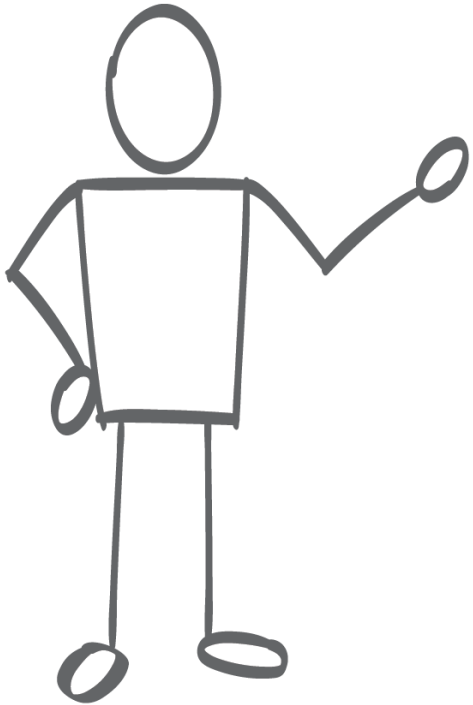


Mid-Curriculum Project

InnoMed Startup Company

Introduction and Overview

Introduction

- **InnoMed** is a startup software as a service (SaaS) company.
- It has built an online medical social networking and diagnosis assistance application for users in APAC, the US, and Europe.
- The application connects patients and doctors to allow online appointments, remote consultation, remote diagnosis, electronic prescription transfer, and payment services.
- The application allows customers to upload documents and images. Text is extracted from documents, and images are converted into multiple formats.
- The application has not yet been launched publically.

Overview – Current Environment

- InnoMed's development and test infrastructure is deployed with a server hosting company.
- InnoMed uses Microsoft Windows servers to host their web and application tiers with Microsoft SQL Server Standard Edition backend databases.
- The application launch date is coming soon and InnoMed expects many users to start using the application.
- InnoMed has decided to use cloud technologies to support its rapid growth.
- InnoMed has hired you to architect an infrastructure in AWS to meet their application needs.

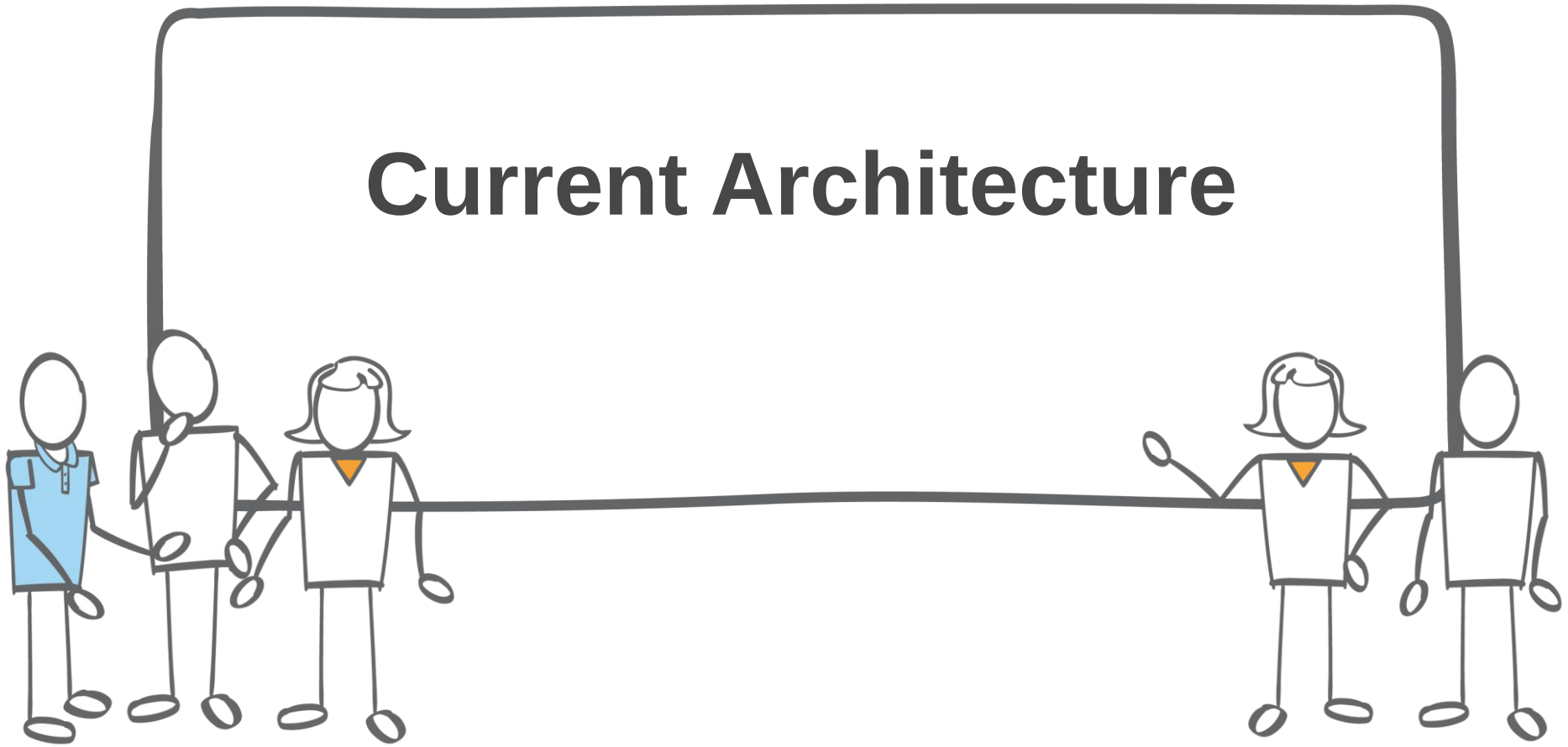
Overview – Requirements

InnoMed plans to move their application into AWS.

The plan includes:

- Configuring access permissions to conform with AWS best practices.
- Configuring auditing to track all user actions.
- Building networks that conform to AWS best practices while providing all the necessary network services to the applications in their different environments.
- Building an architecture that matches the current architecture at the server hosting company and that can handle doubling the number of servers.
- Ensuring that no code changes are required.

Current Architecture



Current Architecture

Web Tier

- Two physical servers (Two CPUs / 4-GB memory)
- Microsoft Windows 2016 Base with IIS
- HAProxy load balancer used to balance traffic between the web servers

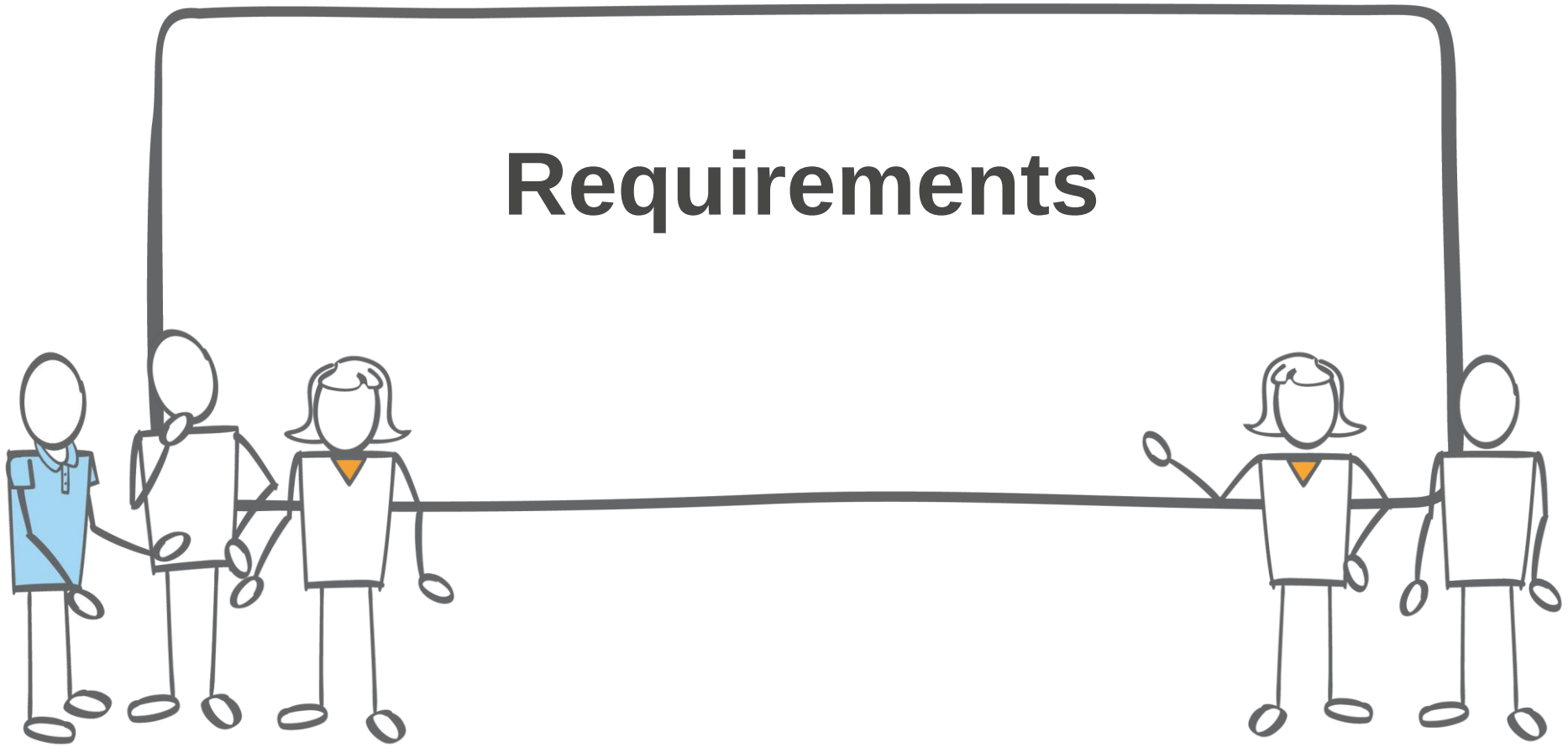
Application Tier

- Two physical servers (Four CPUs / 16-GB memory)
- Microsoft Windows 2016 Base with IIS
- HAProxy load balancer used to balance traffic between app servers

Database Tier

- One physical server (Eight CPUs / 32-GB memory / 5-TB storage)
- SQL Server Standard Edition – v12.xx
- Microsoft Windows 2016 Base
- DBAs access and manage the database, but no RDMBS or advanced configuration is required.

Requirements



Requirements – User Authentication (1 of 2)

- Users with access to AWS are in three groups:
  - System Administrator group: 2 users
  - Database Administrator group: 2 users
  - Monitor group: 4 users
    - Monitoring infrastructure resources for the application (EC2, S3, RDS)

- Follow AWS best practices for distributing permissions.
- The InnoMed application must read and write to S3 buckets.

Requirements – User Authentication (2 of 2)

- A password policy should enforce the following:
  - A password with at least 8 characters, 1 uppercase and 1 lowercase letter, 1 number, and 1 special character
  - Forced password change every 90 days
  - No re-use of the previous three passwords
- All administrators require programmatic access and AWS Management Console access.
  - When signing in to the console, each administrator is required to provide a user name, a password, and a random generated code provided by the Virtual MFA.
- All other users should only have AWS Management Console access, using a combination of user name and password.

Requirements – Auditing

Administrators must be able to track every AWS action in the account, including:

- Every service or object that was created or configured.
- The user who created the object or configured the service.
- The interface used for each creation or configuration action.
  - For example: AWS Management Console or CLI
- The source of each creation or configuration action.
  - For example: IP address or DNS alias

Requirements – Network and Security (1 of 2)

The new architecture must conform to AWS best practices.

This includes:

- Achieve high availability for all tiers to reduce downtime.
- Control access to the applications and limit public entry points.
- Minimize IP address usage to reduce the attack surface.
- Maintain separate networks for InnoMed's development/testing environment and production environment.

Requirements – Network and Security (2 of 2)

The new architecture must conform to AWS best practices.

This includes:

- The web tier load balancer can receive requests from the Internet on port 80.
- Web tier servers can receive requests from the web tier load balancer only on port 80.
- The Application Load Balancer can receive requests from web tier servers only on port 8080.
- Application tier servers can receive requests from the application tier load balancer only on port 80.
- Database servers can receive requests from application servers only on port 1433.

Requirements – Web Tier and Application Tier

- All the instance names in the web tier should be tagged as Key = Name and value = web-tier.
- All the instance names the in application tier should be tagged as Key = Name and value = app-tier.
- All instances in the application tier must support EBS optimization.
- Load balancers for web tier and application tier must support HTTP, HTTPS, and TCP protocols.

Requirements – Business Continuity

The new architecture should be designed for business continuity.

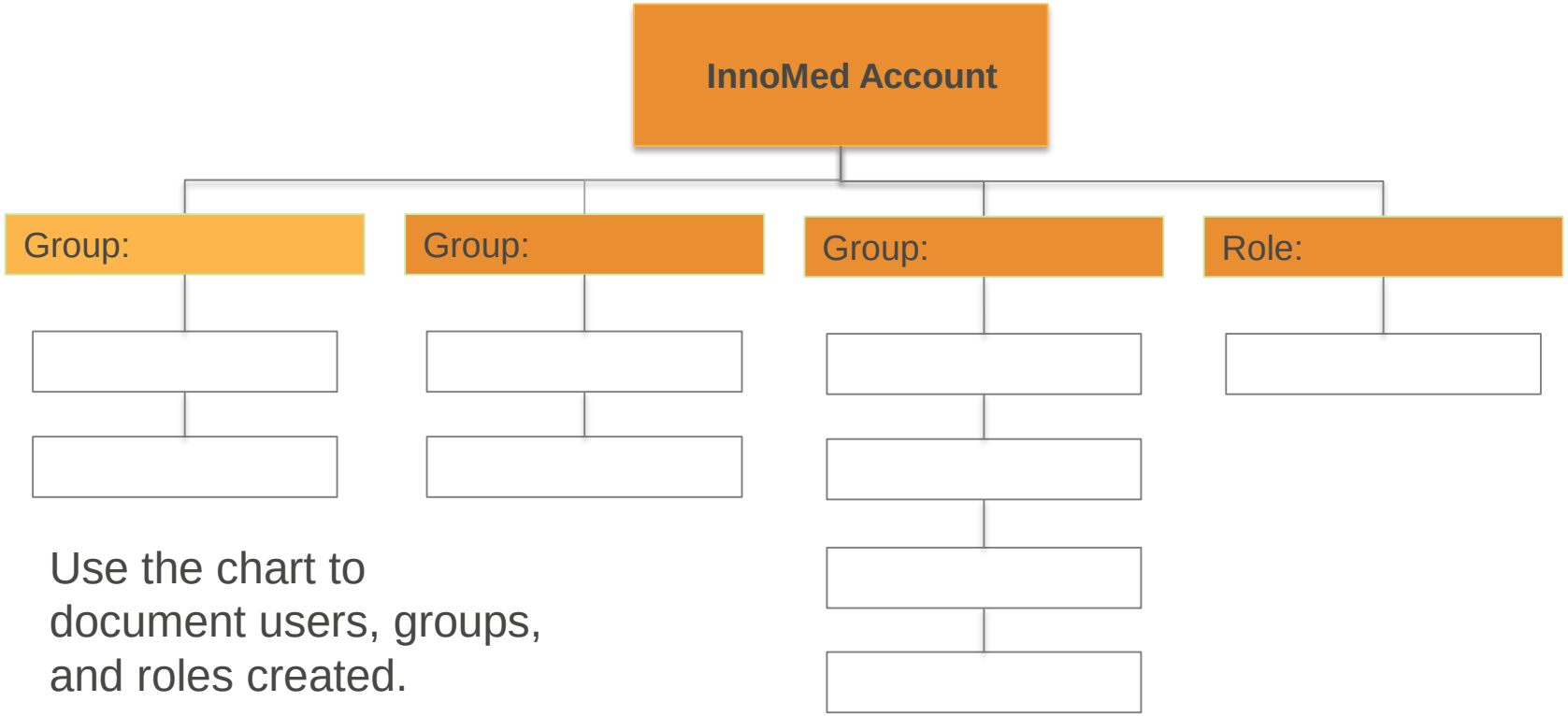
This includes:

- The web and application tiers should be self-healing.
  - If a server becomes unavailable it will be replaced by a new server.
  - A server is considered to be unavailable if the operating system or application fails to respond.
- The database tier should support Multi-AZ deployment.
- The architecture should handle doubling the number of servers to support its rapid growth.

Solution Template

Which Services Will You Use?

Users, Groups, and Roles



Use the chart to document users, groups, and roles created.

Users, Groups, and Roles

Group/Role #	Group/Role Name	Permissions
Group		
Group		
Group		
Role		

Password Policy

Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number.	
Change passwords every 90 days and ensure that the previous three passwords can’t be re-used.	
Administrator sign-in to the AWS Management Console requires the use of Virtual MFA.	
All administrators require programmatic access	

VPC Details

VPC	Region	Purpose	Subnets	AZs	CIDR range
1					
2					

Production Subnet Details

Subnet Name	VPC	Subnet type (Public/private)	AZ	Subnet Address
	#1			
	#1			
	#1			
	#1			
	#1			
	#1			
	#1			
	#1			

Test/Dev Subnet Details

Subnet Name	VPC	Subnet type (Public/private)	AZ	Subnet Address
	#2			
	#2			
	#2			
	#2			
	#2			
	#2			
	#2			
	#2			

Instance Details

Describe the type, size, and justification for the instances you will use for each tier.

Tier	Tag*	OS	Type	Size	Justification	# of instances	User Data?
Web	Key = Name Value = web-tier						
App	Key = Name Value = app-tier						
DB	Key = Name Value = db-tier						

* Tags must be configured as shown to meet the lab objectives

Load Balancer and Instance Security Group Details

Load Balancer	Name*	External /Internal	Subnets	SG Name*	Rule	Source
For Web Tier	web-elb			web-elb-sg		
For App Tier	app-elb			app-elb-sg		

Instance Tier	SG Name*	Rule	Source
Web Tier	web-tier-sg		
App Tier	app-tier-sg		
Database Tier	db-tier-sg		

* Names must be configured as shown to meet the lab objectives

Auto Scaling Launch Configuration

Tier	OS	Type	Size	Configuration Name*	Role	Security Group
Web				WebTier		
App				AppTier		

* Name must be configured as shown to meet the lab objectives

Auto Scaling Group

Tier	Launch Configuration*	Group Name*	Group Size	VPC	Subnets	ELB	Tags
Web	WebTier	WebTier					
App	AppTier	AppTier					

* Names must be configured as shown to meet the lab objectives

Auditing Options

Q. How do you configure an account to create an audit trail for all executed API calls?

_____

Q. Where do you save your logs?

_____

Errors or corrections? Email us at aws-course-feedback@amazon.com.
Other questions? Contact us at
https://aws.amazon.com/contact-us/aws-training/.