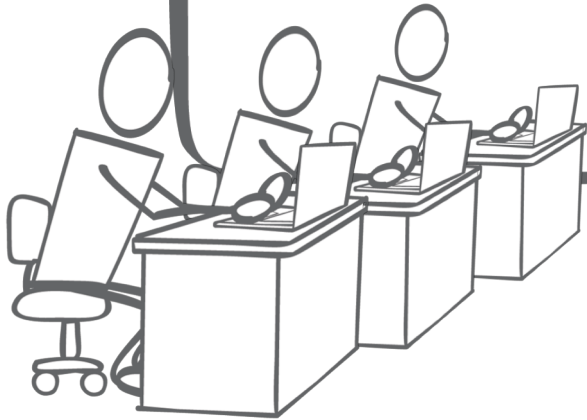


Mid-Curriculum Project

InnoMed Startup Company

Solution Template

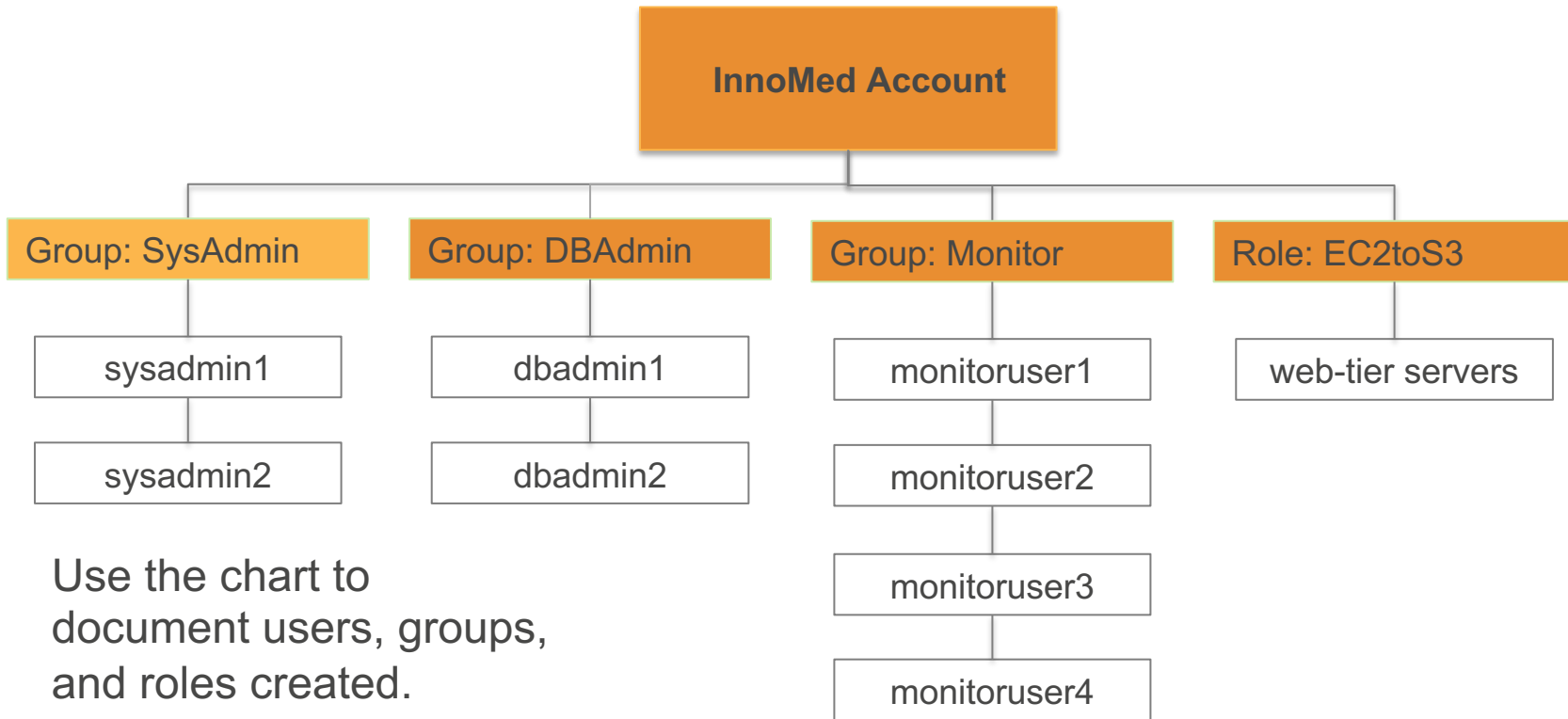
For Educator



Which Services Will You Use?

- IAM – for users, groups, roles management
- VPC – for networks
- EC2 – for web tier, application tier
 - Classic ELB – for traffic balancing
 - Auto Scaling
- S3 – for object storage
- RDS – for database tier
- CloudTrail – for auditing purposes

Users, Groups, and Roles



Users, Groups, and Roles

Group/Role #	Group/Role Name	Permissions
Group	SysAdmin	AdministratorAccess
Group	DBAdmin	AmazonRDSFullAccess
Group	Monitor	AmazonEC2ReadOnlyAccess, AmazonS3ReadOnlyAccess, AmazonRDSReadOnlyAccess
Role	EC2toS3	s3:Get*, s3:List*, s3:Put*

Password Policy

Requirement	Solution
Should be at least 8 characters and have 1 uppercase, 1 lowercase, 1 special character, and a number.	E.g. Inno@Med101
Change passwords every 90 days and ensure that the previous three passwords can't be re-used.	In IAM "Account Setting," configure password policy
Administrator sign-in to the AWS Management Console requires the use of Virtual MFA.	Use Virtual MFA device
All administrators require programmatic access	Create access key/secret key pairs to admin accounts

VPC Details

VPC	Region	Purpose	Subnets	AZs	CIDR range
1	Any region that supports Amazon RDS Multi-AZ with Mirroring for SQL Server	Prod	8	2	10.0.0.0/16
2	Same as above	Test/Dev	8	2	10.0.0.0/16

Production Subnet Details

Subnet Name	VPC	Subnet type (Public/private)	AZ	Subnet Address
Public1	#1	Public	a	10.0.0.0/27
Public2	#1	Public	b	10.0.1.0/27
WebPrivate1	#1	Private	a	10.0.10.0/24
WebPrivate2	#1	Private	b	10.0.11.0/24
AppPrivate1	#1	Private	a	10.0.20.0/24
AppPrivate2	#1	Private	b	10.0.21.0/24
DBPrivate1	#1	Private	a	10.0.30.0/24
DBPrivate2	#1	Private	b	10.0.31.0/24

Test/Dev Subnet Details

Subnet Name	VPC	Subnet type (Public/private)	AZ	Subnet Address
Public1	#2	Public	a	10.0.0.0/27
Public2	#2	Public	b	10.0.1.0/27
WebPrivate1	#2	Private	a	10.0.10.0/24
WebPrivate2	#2	Private	b	10.0.11.0/24
AppPrivate1	#2	Private	a	10.0.20.0/24
AppPrivate2	#2	Private	b	10.0.21.0/24
DBPrivate1	#2	Private	a	10.0.30.0/24
DBPrivate2	#2	Private	b	10.0.31.0/24

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	Windows Server 2016 Base	t2	medium	Two physical servers (Two CPUs/4-GB memory)	2	Yes
App	Key = Name Value = app-tier	Windows Server 2016 Base	m4	xlarge	Two physical servers (Four CPUs/16-GB memory)	2	Yes
DB	Key = Name Value = db-tier	RDS (SQL Server SE)	db.m4	2xlarge	Multi-AZ deployment	N/A	N/A

* 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	External	Public1/Public2	web-elb-sg	Allow HTTP (80)	All traffic
For App Tier	app-elb	Internal	AppPrivate1/AppPrivate2	app-elb-sg	Allow 8080	web-tier-sg

Instance Tier	SG Name*	Rule	Source
Web Tier	web-tier-sg	Allow HTTP (80)	web-elb-sg
App Tier	app-tier-sg	Allow 80	app-elb-sg
Database Tier	db-tier-sg	Allow 1433	app-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	Windows Server 2016 Base	t2	medium	WebTier	EC2toS3	web-tier-sg
App	Windows Server 2016 Base	m4	xlarge	AppTier	none	app-tier-sg

* 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	2-4	#1	WebPrivate1 WebPrivate2	web-elb	Key = Name Value = web-tier
App	AppTier	AppTier	2-4	#1	AppPrivate1 AppPrivate2	app-elb	Key = Name Value = app-tier

* 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?

© 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.

This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

Errors or corrections? Email us at aws-course-feedback@amazon.com.

Other questions? Contact us at
<https://aws.amazon.com/contact-us/aws-training/>.

All trademarks are the property of their owners.