PragmaEdge

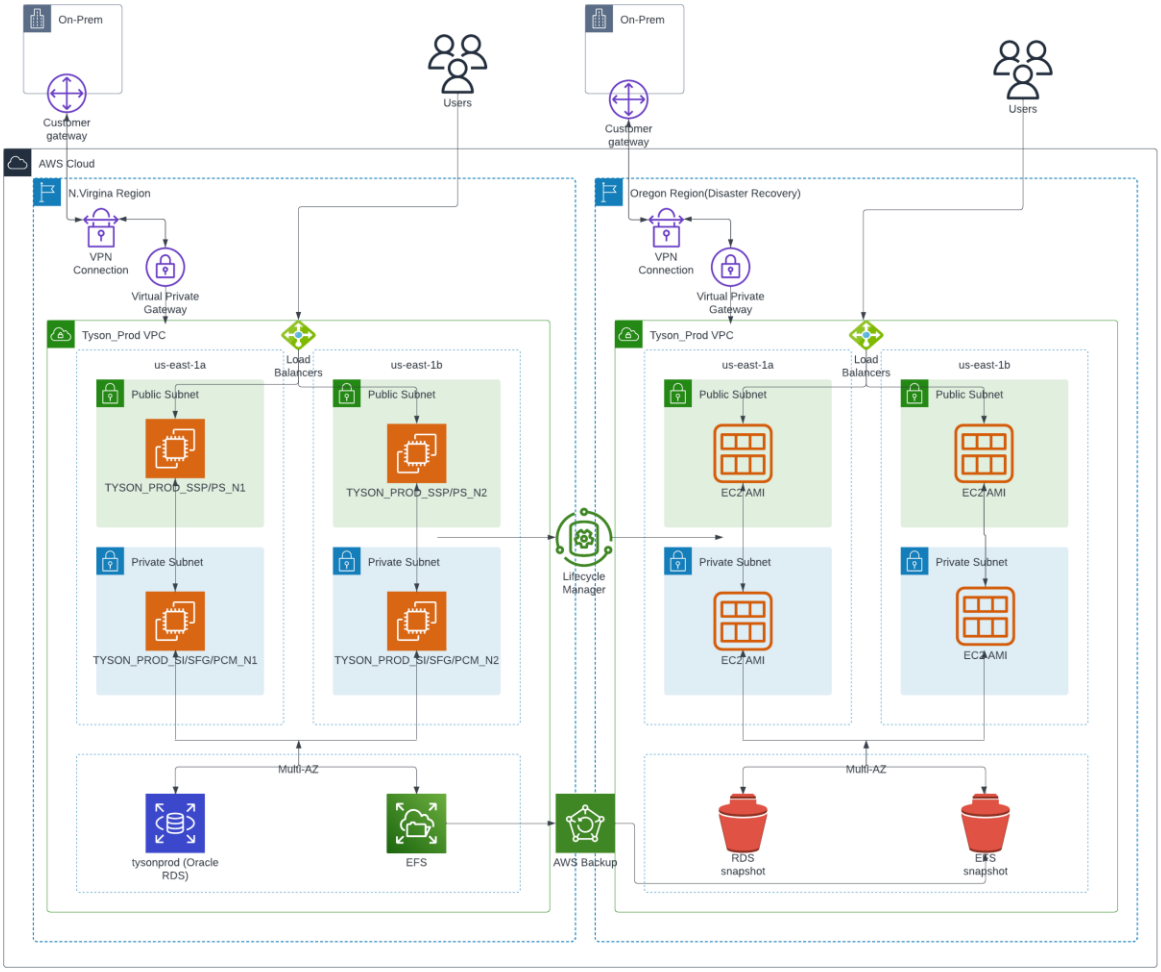
All Clients Disaster Recovery Architecture Documentation

PragmaEdge

Document Revision History

Revision	Date	Description (Changes Made)	Author
1.0	02/21/2024	Initial Version	Indu Dayanand

Tyson DR Architecture



The above architecture is for Tyson client and describes how we are prepared for disaster recovery.

For Tyson Client we are using a two-tier architecture.

As you can see in the above architecture, we have two nodes in different availability zones for high availability. We have servers in both public and private subnets.

The servers in public subnets are Perimeter servers used as proxies for external partners before they connect to our applications.

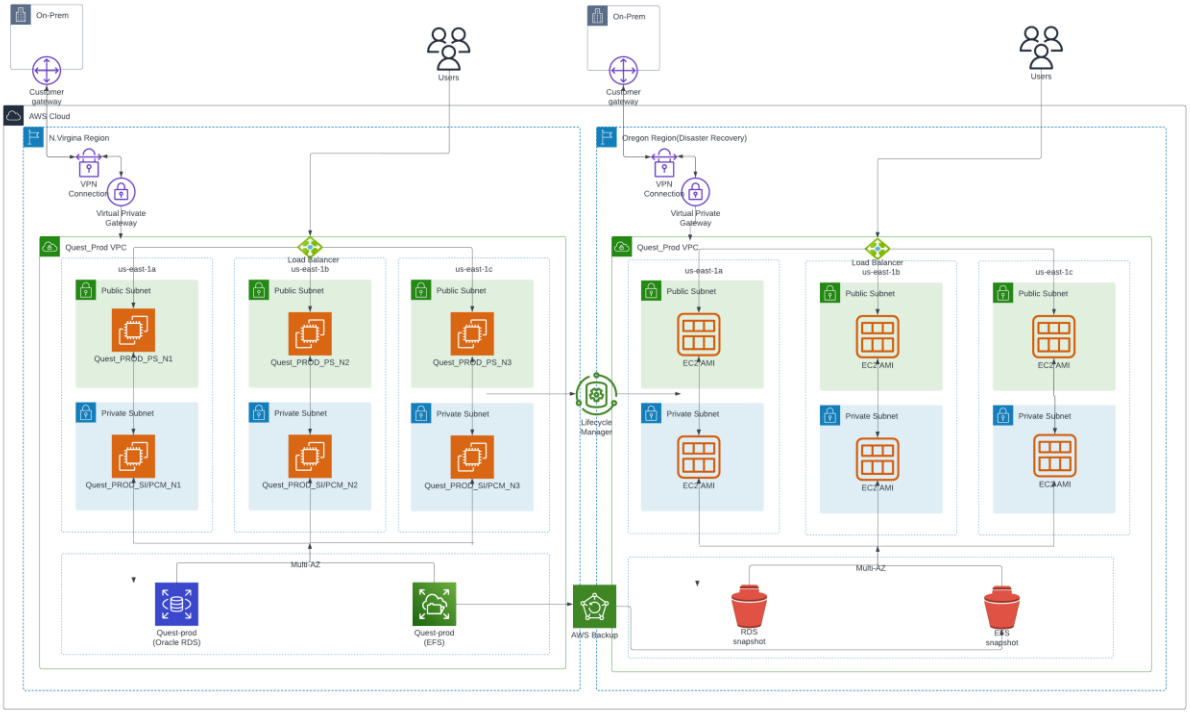
The servers in private subnets are SI/SFG/PCM servers used by our internal partners.

The external partners connect to applications in SSP/PS servers from load balancer through 20445 and 20543 ports.

The internal partners connect to applications in SI/SFG/PCM servers from VPN through 10445 and 10543 ports.

We have RDS and EFS in multi-AZ for high availability. The data is moved from EFS to S3 using AWS Backup policy for reducing the cost and replicating data in case of data loss. We have AWS Lifecycle Policy for backing up the EC2 as AMIs in cross region which is scheduled 1st and 16th of every month. We have 2 AMI backup retention per month. We also have AWS backup for cross region backup of EFS scheduled every day.

Quest DR Architecture



The above architecture is for Quest client and describes how we are prepared for disaster recovery.

For Quest Client we are using a two-tier architecture.

As you can see in the above architecture, we have three nodes in different availability zones for high availability. We have servers in both public and private subnets.

The servers in public subnets are Perimeter servers used as proxies for external partners before they connect to our applications.

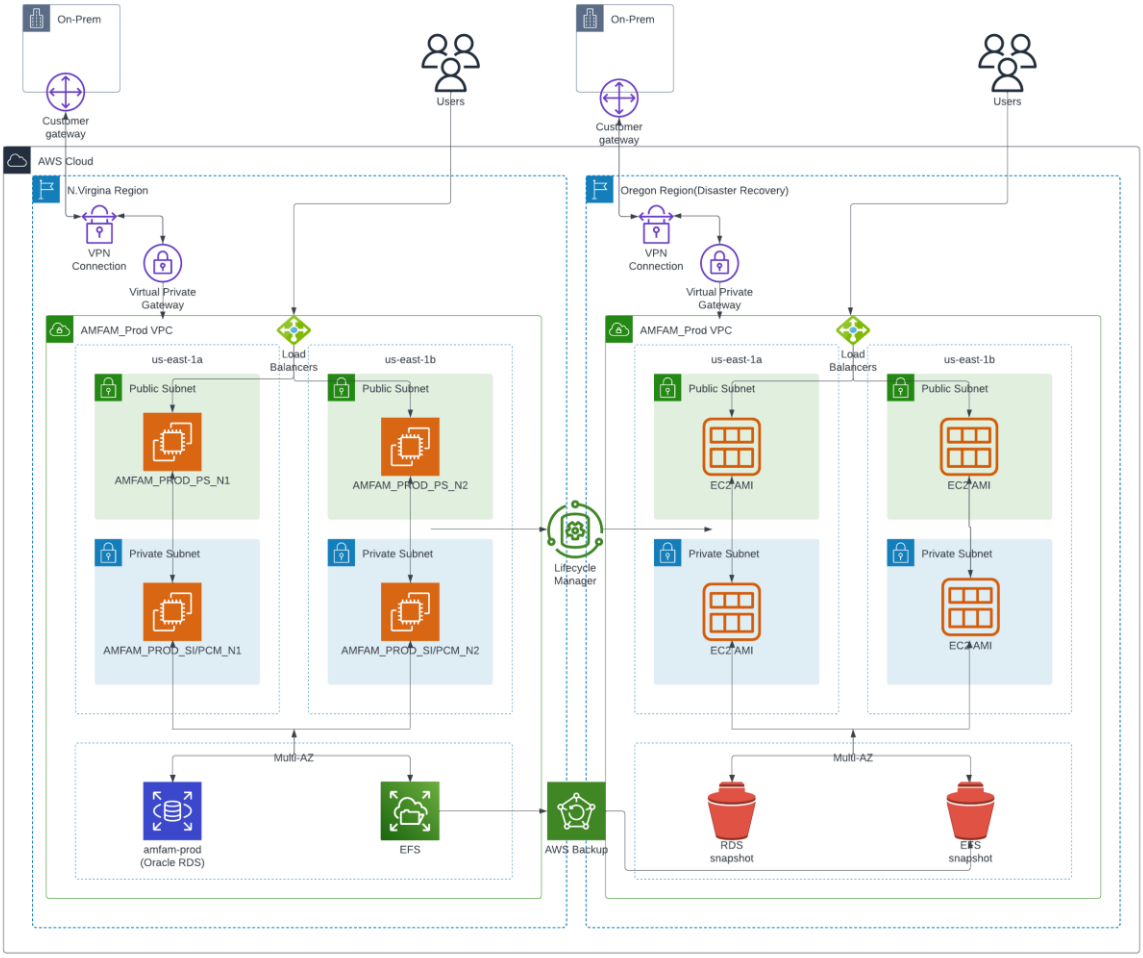
The servers in private subnets are SI/PCM servers used by our internal partners.

The external partners connect to applications in PS servers from load balancer through 11022 port.

The internal partners connect to applications in SI/PCM servers from VPN through 10022 port.

We have RDS and EFS in multi-AZ for high availability. The data is moved from EFS to S3 using AWS Backup policy for reducing the cost and replicating data in case of data loss. We have AWS Lifecycle Policy for backing up the EC2 as AMIs in cross region which is scheduled 1st and 16th of every month. We have 2 AMI backup retention per month. We also have AWS backup for cross region backup of EFS scheduled every day.

AMFAM DR Architecture



The above architecture is for AMFAM client and describes how we are prepared for disaster recovery.

For AMFAM Client we are using a two-tier architecture.

As you can see in the above architecture, we have two nodes in different availability zones for high availability. We have servers in both public and private subnets.

The servers in public subnets are Perimeter servers used as proxies for external partners before they connect to our applications.

The servers in private subnets are SI/PCM servers used by our internal partners.

The external partners connect to applications in PS servers from load balancer through xxxxx port.

The internal partners connect to applications in SI/PCM servers from VPN through xxxxx port.

We have RDS and EFS in multi-AZ for high availability. The data is moved from EFS to S3 using AWS Backup policy for reducing the cost and replicating data in case of data loss. We have AWS Lifecycle Policy for backing up the EC2 as AMIs in cross region which is scheduled 1st and 16th of every month. We have 2 AMI backup retention per month. We also have AWS backup for cross region backup of EFS scheduled every day.