The architecture you described for AWS can be mapped to Azure services as follows:

- \*\*Virtual Network (VNet)\*\*: Equivalent to AWS's VPC, a VNet in Azure is a dedicated network within the Azure cloud.

- \*\*Public Subnets\*\*: In Azure, these can be subnets within a VNet with a public IP address range.

- \*\*NAT Gateway\*\*: Azure NAT Gateway provides outbound internet connectivity for VMs in your private subnets.

- \*\*Azure Bastion\*\*: Serves a similar purpose to a Linux Bastion host in AWS, providing secure and seamless RDP/SSH access to virtual machines.

- \*\*Private Subnets\*\*: Subnets within a VNet designated for private resources.

- \*\*Azure Database for PostgreSQL\*\*: A managed database service that can be used in place of Aurora DB. It supports creating read replicas and automated backups.

- \*\*Azure Key Vault\*\*: Used for managing cryptographic keys and secrets, Azure Key Vault is comparable to AWS KMS.

- \*\*Azure Monitor\*\*: Functions similarly to Amazon CloudWatch, it is used to track performance metrics and operational data. Azure Monitor also has alerting capabilities akin to SNS notifications in AWS.