N-tier Architecture in Azure

Overview
An N-tier architecture divides an application into logical layers and physical tiers to manage responsibilities and dependencies. Layers separate functionality, while tiers provide physical separation for scalability and resilience.

Logical and Physical Separation

Logical Layers:
- **Presentation Layer:** Handles user interface and user interaction.
- **Business Layer:** Contains business logic and processing.
- **Data Layer:** Manages data storage and retrieval.

Physical Tiers:
- **Web Tier:** Hosts the presentation layer, often using web servers.
- **Middle Tier:** Hosts the business logic, using application servers.
- **Database Tier:** Hosts the data storage, using database servers.

Communication Models
- **Strict Model:** Requests flow through adjacent tiers sequentially.
- **Relaxed Model:** Requests can skip tiers if necessary.

Direct vs. Asynchronous Communication
- **Direct:** Tiers call each other directly.
- **Asynchronous Messaging:** Uses message queues for communication, improving decoupling and scalability.

Closed vs. Open Layer Architecture
- **Closed Layer Architecture:** Each layer calls only the next immediate layer.
- **Open Layer Architecture:** Layers can call any lower layer, potentially increasing performance but also complexity.

When to Use N-tier Architecture
- Simple web applications.
- Starting point when architectural requirements are unclear.
- Migrating on-premises applications to Azure with minimal changes.
- Unified development of on-premises and cloud applications.

Benefits

- Portability between cloud and on-premises.
- Familiar to most developers.
- Cost-effective without major rearchitecture.
- Supports heterogeneous environments (Windows/Linux).

Challenges
- Potential for unnecessary latency.
- Monolithic design hinders independent deployment.
- More management effort compared to managed services.
- Complex network security management.
- Multi-tier user and data flows complicate testing and observability.

Best Practices
- **Autoscaling:** Use to handle load changes.
- **Asynchronous Messaging:** Decouple tiers for better scalability.
- **Caching:** Use for semistatic data to improve performance.
- **Database High Availability:** Configure using solutions like SQL Server Always On.
- **Web Application Firewall (WAF):** Protect the front end.
- **Subnet Isolation:** Use subnets for security boundaries.
- **Restrict Data Tier Access:** Allow requests only from the middle tier.

N-tier Architecture on Virtual Machines

Physical Setup
- **Availability Sets/Scale Sets:** Use multiple VMs for resilience and scaling.
- **Load Balancers:** Distribute requests across VMs in a tier.
- **Subnets:** Place each tier in its own subnet for network security.

Example Configuration
- **Web Tier:** Stateless, handling user requests.
- **Business Tier:** Stateless, managing business logic.
- **Data Tier:** Replicated database for high availability (e.g., SQL Server with Always On for Windows, Apache Cassandra for Linux).

Network Security
- **Network Security Groups (NSGs):** Restrict access to each tier.
- **Business Tier Labeling:** Use clear naming conventions for resources.
- **Layer-7 Routing:** For complex applications with multiple tiers.
- **DMZ for Security:** Use network virtual appliances (NVAs) for firewall and

packet inspection.
- **No Direct RDP/SSH:** Use a jumpbox or bastion host for secure access.

Additional Considerations
- **Managed Services:** Use where possible to reduce management overhead.
- **Hybrid Network Integration:** Extend virtual networks to on-premises using VPN or Azure ExpressRoute.
- **Active Directory Integration:** Extend AD for identity management.
- **High Availability Across Regions:** Replicate applications across regions and use Azure Traffic Manager for failover.

Next Steps
- Explore virtual network integration for Azure services.
- Understand how network security groups evaluate traffic.
- Learn through tutorials on creating and managing NSGs.
- Troubleshoot network security groups to resolve communication issues.
- Enable NSG flow logs for traffic analysis.

For further reading and detailed guidelines, refer to Azure's documentation on network security groups and N-tier architectures.