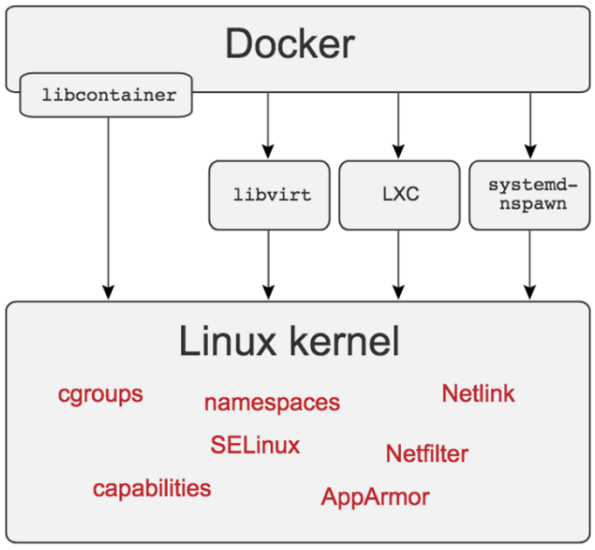
Introduction to Cloud Security with Microsoft Azure (Study Notes)

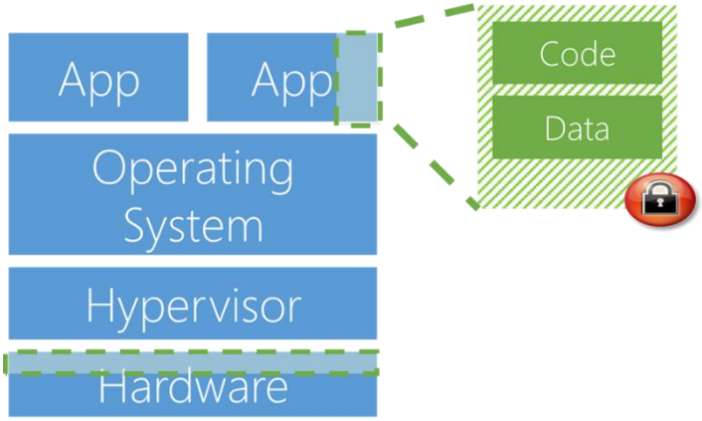
Basics of the Cloud

- **Cloud Computing**
  - **Benefits**
    - Increase Availability
    - Higher Resiliency
    - Unlimited Elasticity
  - **Virtualization**
    - Hypervisor
      - Specialized software used to emulate the physical components of a computer and controls access to the physical resources
      - Hypervisor Types
        - Type I (Bare Metal)
        - Type II (Hosted)
        - Always ensure that your hosting operating system is properly patched and secured
    - Container-based



    - Hyperconverged infrastructure allows for the full integration of storage, network, and servers without performing any hardware changes
    - VDI
      - Full desktop operating systems being delivered to the end user through a cloud-based service provider

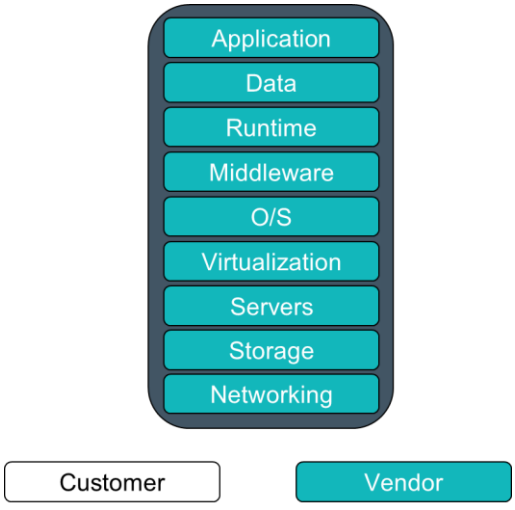
- **Secure Enclave**



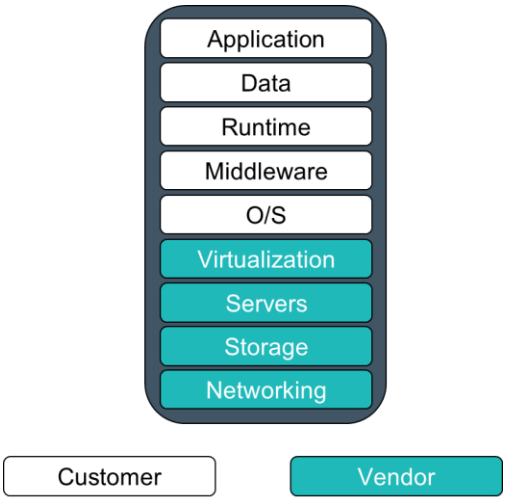
- **Secure Volumes**

- **On-premise vs Hosted Solutions**
  - **Hosting Options**
    - On-Premise
      - On-premise solution provides higher levels of confidentiality since you control logical and physical access to the servers.
    - Hosted Solution
      - Multi-tenancy solutions allow hardware to be store in a facility with a large number of other organizations

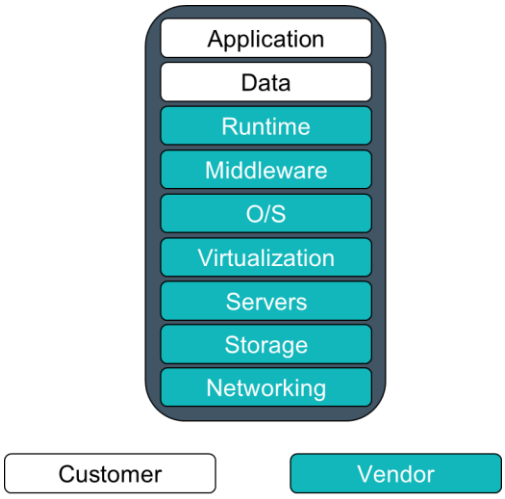
- **Cloud Service Models**
  - **Types of Service**
    - **SaaS (Software as a Service)**

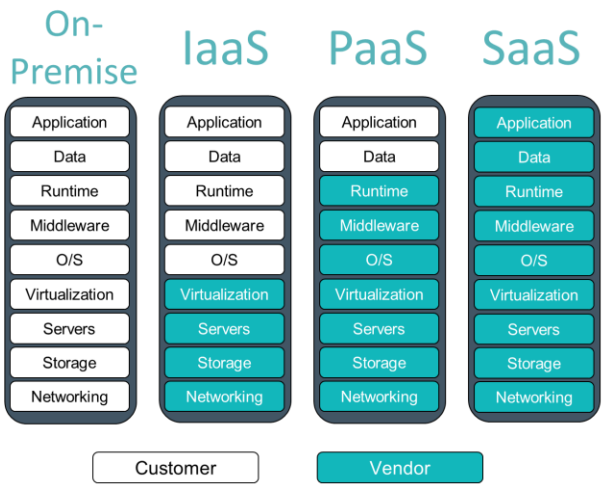


- **IaaS (Infrastructure as a Service)**

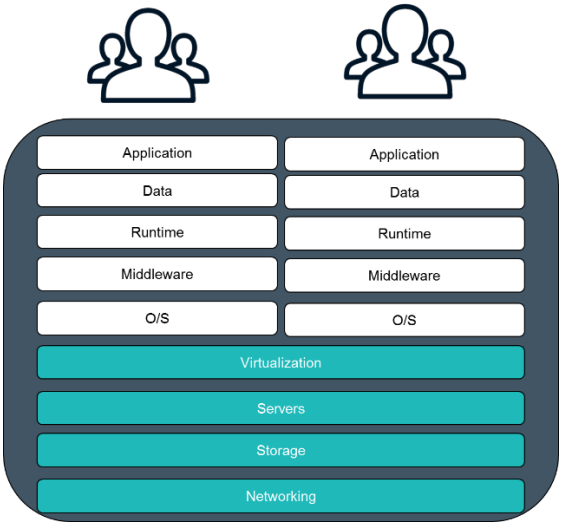


- **PaaS (Platform as a Service)**





- **Types of Clouds**
  - **Public**
    - Service provider makes resources available to end users over the Internet under a pay-for-service model
  - **Private**
    - Company creates its own cloud environment that only it can utilize
  - **Hybrid**
    - Hybrid clouds combine the benefits of public and private cloud architectures
  - **Community**
    - The resources and costs required are shared amongst multiple organizations with similar requirements
  - **Multi-tenancy**



- **Single tenancy**
  - Single tenancy models allow only a single organization to be assigned to an individual physical server

- **Augmenting Security with Cloud Services**
  - **Cloud anti-malware solutions require very little processing power and are always up-to-date**
    - Disadvantages
      - Requires always on connection
      - Only core files may be scanned
  - **Vulnerability Scanning**
    - Provides you with the option of conducting the scan from an attacker's perspective
    - Advantages
      - Lower cost
      - Efficient
      - Always up-to-date
    - Critical information about your vulnerabilities may be stored on the cloud provider's systems
  - **Cloud Security Brokers**
    - Simplify the offerings into a single solution for your organization
  - Security as a Service (SECaaS) provides organizations with the ability to outsource necessary security skills

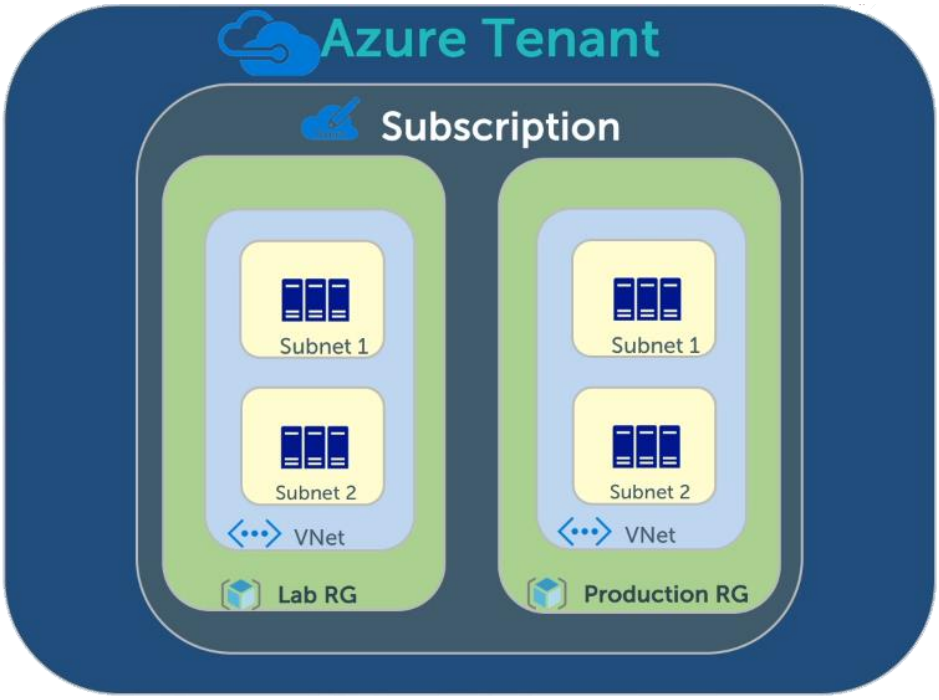
Basics of Azure

- **Azure's Terminology**
  - **Tenant**
    - Represents an organization
    - Where all the user identities live
  - **Subscription**
    - Unique ID
    - Grants access to Azure services
  - **Resource Group**
    - Container to store and group resources
    - Region-based
    - RBAC permissions

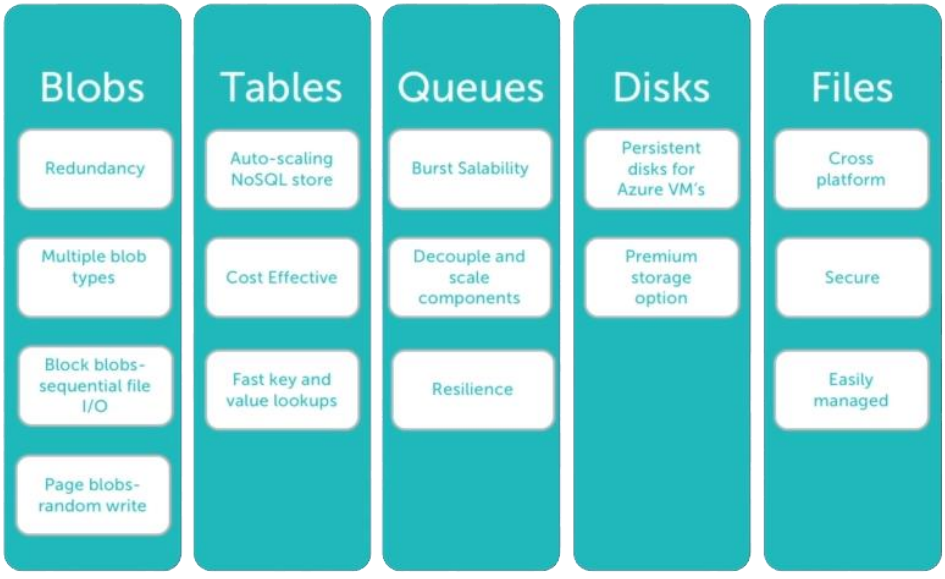
- **How much does it all cost?**
  - **Pricing calculator**
  - **Forecast feature**
  - **Cost analysis feature**

Virtualization

- **The Deployment Model**



- **How does storage work in Azure?**



- **Storage account**
  - General Purpose
    - Blobs
    - Files
    - Queues
    - Tables
    - Disks
  - Blob storage
    - Hot tier
    - Cool tier
    - Archive tier
- **Blobs**
  - Unstructured
  - Massively scalable
  - Block blobs – Media files
  - Append blobs – Log files
  - Page blobs – VHD files
  - Blobs Storage Tiers
    - Premium Tier – High performance hardware
    - Hot Tier – Accessed frequently
    - Cool Tier – Accessed infrequently
    - Archive Tier – Rarely accessed
- **Table Storage**
  - Structured data
  - NoSQL datastore
  - Fast
  - More cost-effective than traditional SQL
- **Queue Storage**
  - High throughput messaging system
  - Authenticated http/https calls
  - Scale independently
  - Rest API
- **Disk Storage**
  - Premium storage option
  - Intensive I/O workloads
  - Solid State Drives are used
- **File storage**
  - Network file share
  - HTTPS/SMB 3.0 supported
  - Cross platform

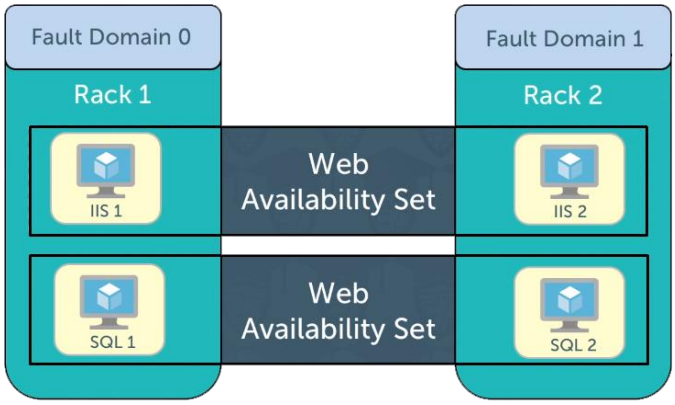
- **Virtual Machine Types**
  - **Available VM Series**
    - General purpose
    - Compute-optimized
    - Memory-optimized
    - Storage-optimized
    - GPU-optimized
    - Performance-optimized
  - **Planning**
    - Region
    - VNet/Subnet
    - Redundancy
    - Scalability
    - Storage

- **Virtual Network capabilities**
  - **Purpose**
    - Resource communication
    - Secured by NSG
    - VNet peering
    - Hybrid solution via VPN
    - Different subnets traffic flow by default
    - Local IP address best practices still apply

Redundancy

- **Backups**
  - **Purpose**
    - Hybrid workloads supported
    - Cost-effective and secure
    - Recovery vault required
    - Variety of backup options
  - **Mars Agent**
    - Supports hybrid workloads
    - Limited to Windows OS's
  - **SC DPM**
    - Supports hybrid workloads
    - Both Windows and Linux supported
  - **Backup server**
    - Supports hybrid workloads
    - On-premises VM backup not supported
  - **Benefits of Azure backup**
    - Unlimited scaling
    - Geo-redundant options
    - Data encryption
    - Long-term retention

- **High Availability**
  - **Options**
    - Availability Sets
      - Based on fault & update domains



      - VM-based
      - Needs to be configured when creating VM
    - Availability Zones
      - Protects against entire data center failures

        - Zone-redundant services
        - 99.99% SLA-backed
    - Regional pairs
        - Provides data residency
        - Physical isolation
        - Platform-provided replication

- **Disaster Recovery**
    - **Azure Site Recovery**
        - Ease of management
        - Hybrid workloads supported
        - Simulated DR setting for compliance

Security

- **IaaS Security**
  - **Controls**
    - Layered defense
    - Web Application Firewalls
    - VPNs
    - Endpoint protection
    - OS and application patching
    - SIEM onboarding
    - User education

- **Virtual Private Network (VPN)**
  - **Types**
    - **Site-to-Site VPN**
      - Connect branches with each other
      - Hardware required
      - Configured on the router level
    - **Point-to-Site VPN**
      - Remote users
      - VPN software
      - Used on a case by case basis

- **Azure Security Center (ASC) Dashboard**
  - **Azure Security Center**
    - Built-in tool
    - Unified security management
    - Advanced threat protection
    - Hybrid workloads
    - Security hygiene
  - **ASC Features**
    - Centralized policy management
    - Continuous security assessments
    - Actionable recommendations
    - Prioritized security & alerts
    - Advanced cloud defenses
    - Integration supported

- **Data Security Considerations**
  - **Migration to the cloud can introduce some vulnerabilities to our systems and networks**
  - **Precautions**
    - Configure
    - Manage
    - Audit
  - **Minimize your risk by ensuring failover, redundancy, and elasticity are configured properly**
  - **Homogeneous Networks**
    - Occurs when every server is running the same underlying hardware and software
    - Most organizations choose to mitigate higher operation and training costs by utilizing the same hardware and software

- **Security Threats**
  - **Security Threats**
    - VM Escape
      - Type of attack where a hacker attempts to break out of an isolated virtual machine
      - Always ensure your hosting operating system is patched and updated to prevent attempted VM Escapes
    - Privilege Escalation
    - Live VM Migration
      - A virtual machine is copied from one server to another over the network while it is still in operation
    - Data Remnants
      - Data left on a cloud provider's storage devices when a server has been deprovisioned from use

Active Directory

- **Active Directory in Azure**
  - **AAD Benefits**
    - Management of identities
    - Directory services
    - RBAC for applications
    - Active Directory Domain Services supported
  - **AAD**
    - Sync cloud and local identities
    - Multi-factor Authentication
    - Self-service Reset Portal
    - Single Sign-On (SSO)
  - **AAD Editions**
    - Free
    - Basic
    - Premium P1
    - Premium P2

- **Azure Active Directory Business to Business (B2B) and B2C**
  - **B2B**
    - Used to collaborate with partners
    - Securely share resources
    - External identity management solution
    - Decreased IT overhead
  - **B2C**
    - Used for customer-facing applications
    - Supports all platforms
    - MFS-supported
    - Backed by SLA

- **How to Sync your on-premises and cloud identity**
  - **Directory Sync**
    - Merge cloud and on-premises identities
    - Simple to configure tool
    - Linked to on-premises AD OU's