Identity, governance, privacy and compliance

Azure active directory

Microsoft's cloud based identity and access management service.

Can detect unauth logins from strange locations or at strange times

It provides:

Authentication

SSO

Application management via MyApps portal

Device management via Microsoft intune

You can connect windows AD with Azure AD using Azure AD connect

* Azure AD connect
  + Synchronises user identities between on prem AD and azure AD
* Azure AD MFA
  + Enables azure AD mfa for admins with global admin access.
  + **AD premium** allows for more granular azure AD mfa configuration
* Conditional access
  + Access control to resources depending on identity signals - who the user is, where the user is, and what device the user is requesting access from --> More granular MFA
* AZURE PREMIUN: for on prem resources, and self password resets

Azure RBAC

* Applied to a scope, which is a resource or set of resources that the access applies to. It can be a management group, subscription, resource group, or resource
* Types of accounts: Observers, Users managing resources, Admins, and Automated processes
* Types of roles: Owner, reader, contributor
* It is enforced via resource manager
* It uses an allow model - which implicitly denies all other actions apart from the ones being allowed.
* Azure RBAC is managed on the access control (IAM) pane in azure portal

* **Resource lock:** prevents resources from being accidentally deleted or changed by applying either CanNotDelete or ReadOnly permissions
* **Azure Blueprints:** define the set of standard Azure resources that your organization requires. Can also define resource locks

Azure tags

Help organise Azure resources by providing 'metadata'. This helps with:

* Resource management:
* Cost management
* Operations management: tagging according to criticality
* Security, e.g. public or confidential
* Governance and compliance: identify resources that align with governance or regulatory compliance
* Workload optimisation: visualise resources in complex deployments

* You can manage tags in azure policy, and also specify tagging rules and conventions

Azure policy

Enables you to create, assign, and manage policies (initiatives) that control or audit your resources. For example, you can define a policy that allows only a certain SKU (stock-keeping unit) size for the virtual machines (VMs) to be used in your environment. It can then flag resources that arent compliant and auto remediate

1. Create a policy definition
2. Assign definition to resources within a scope
3. Review the evaluation results

A group of policies is called an initiative. You can define initiatives in azure portal or using CLI tools

Azure blueprints

Scale configuration of one environment to other subscriptions.

It can be used to scale:

* Role assignments
* Policy assignments
* Azure Resource Manager templates
* Resource groups

1. Create an Azure blueprint.
2. Assign the blueprint.
3. Track the blueprint assignments.

Azure creates a record that associates a resource with the blueprint that defines it. This connection helps you track and audit your deployments.

* **Blueprint artifacts:**
  + Each component in the blueprint definition is known as an artifact, e.g. employ threat detection on SQL server
  + Artifacts also have parameters that can be configured, such as allowed locations

Cloud adoption framework

Cloud Adoption Framework consists of tools, documentation, and proven practices. The Cloud Adoption Framework includes these stages:

Define your strategy - why are you moving to cloud?

Make a plan - Map goals to specific actions

Ready your organization: Start creating a landing zone environment on Azure

Adopt the cloud: Migrate and innovate existing deployments

Govern and manage your cloud environments: Benchmark current state and then make iterative changes

Subscription governance strategy

* Billing: You can create one billing report per subscription - so you could have one subscription per department
* Access control: every subscription is associated with an azure AD tenant, and is a deployment boundary. You could consider separate subscriptions to keep resources separate and isolated.
* Subscription limits: you can implement resource limits. They cannot be changed and if you need to change them, you have to create a new sub.

Microsoft's commitment to privacy

* Microsoft privacy statement: What data MS collects and how they use it
* Online services terms: legal agreement between MS and customer, about how data is used
* Data protection addendum: Defines data processing and security terms including compliance, processed data

Microsoft trust centre

In-depth information about security, privacy, compliance offerings, policies, features, and practices across Microsoft cloud products.

Azure government

Addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers. Azure Government offers physical isolation from non-US government deployments and provides screened US personnel.

To provide the highest level of security and compliance, Azure Government uses physically isolated datacenters and networks located only in the US

Azure China 21Vianet

Operated by 21Vianet. It's a physically separated instance of cloud services located in China.

According to the China Telecommunication Regulation, providers of cloud services, infrastructure as a service (IaaS) and platform as a service (PaaS), must have value-added telecom permits. Only locally registered companies with less than 50 percent foreign investment qualify for these permits. To comply with this regulation, the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft.