**Build Budgets and Alerts**

* Budgets show a simple view of current spending against resources
* This can be set to resource groups
* Can return budget analysis monthly, quarterly, or yearly
* Alerts can be set to send an email once cost threshold is met or exceeded
* Cost alert
* Budget alert
* Credit alert
* Department spending quota.

**Move azure resources to another resource group**

* Moving azure resources need to be done if you have resources in a resource group with both ‘production’ and ‘development’ resources.
* Some resources have limitations for moving to another resource group
* Like if you move a web app resource then you cant automatically move 3rd party ssl certificates
* VM’s have limitations as well

VM’s limitations

* Move a vm, all dependants must go with it
* Cant move with certificates in key vault subscriptions
* Cant move managed disks that are in availability zones in different regions

Resources that can be moved

* Azure storage accounts
* Azure virtual machines
* Azure virtual networks

Resources that cant be moved

* Active directory domain services
* Backup vaults
* Azure app service gateways

Test Move resources

* If done through powershell or azure CLI you use ‘REST API’.
* If move is done through azure portal then there’s no need to validate
* REST API is a programming interface used to call an HTTP request. Used in custom code from clients such as mobile apps.

For REST API move you must have

* Azure sub id
* Name of resource group holding your resource
* Resource id of resources in the group
* Resource id of the destination resource group
* Your access account token

**Move using Azure CLI**

1. Create a resource group.

* az group create --name <destination resource group name> --location <location name>

1. Get the resource.

* yourResource=$(az resource show --resource-group <resource group name> --name <resource name> --resource-type <resource type> --query id --output tsv)

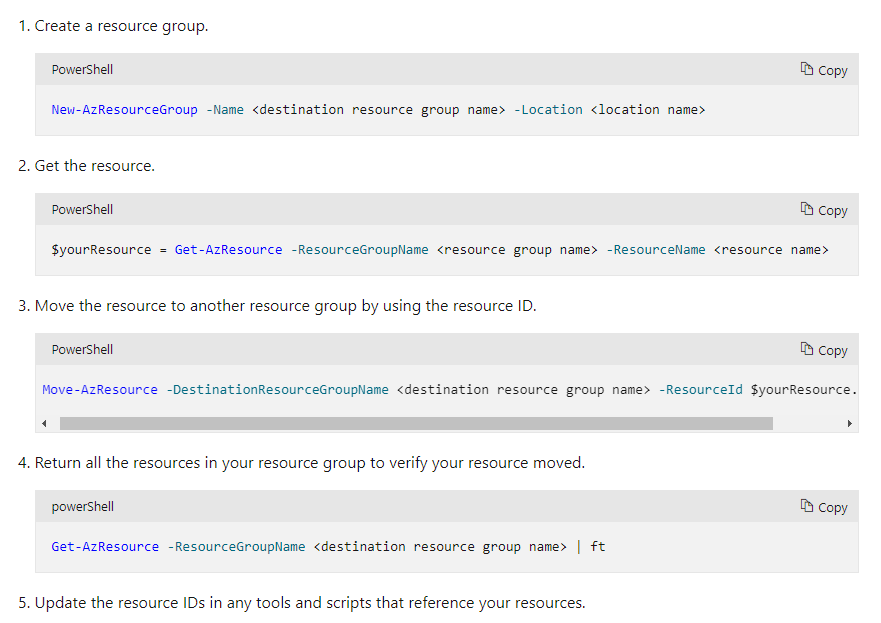
1. Move the resource to another resource group by using the resource ID.

* az resource move --destination-group <destination resource group name> --ids $yourResource

1. Return all the resources in your resource group to verify your resource moved.

* az resource list --resource-group <destination resource group name> --query [].type --output tsv | uniq

Move using Azure Powershell



**Manage device identity with Azure AD join and Enterprise State Roaming**

* Helps control devices that you add to your organizations Azure AD instance
* Helps control the data, resources, and assets that the devices can access

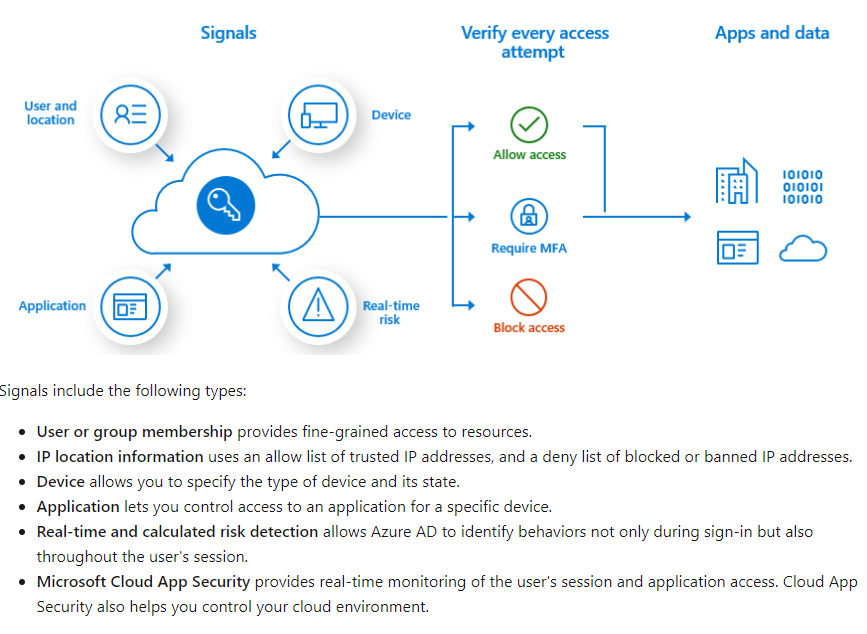
Device registration options

* Azure AD registered, bring your own device. Privately owned or they use a personal Microsoft account
* Azure AD Joined, owned by your organization. Users access cloud based using organization credentials
* Hybrid Azure, like Azure AD joined. Device identities exist in both on-premises and cloud

Conditional access

* Uses data from sources called ‘signals’
* Enable device identity management but is complex
* Use ‘if-then’ statements

Signal types



Common decisions

* Grant access
* Block access

The criteria can be one or more of

* Multifactor authentication
* Device marked as compliant
* Approved app
* Need for app protection policy
* Device that’s Azure hybrid

to make policies work you must configure

* Cloud apps, to enable you to control how authorized access to apps
* Users and groups,
* Access controls, if conditions are satisfied, policy assessor will know what to do

Considerations for identity management

* Using Hybrid or Azure AD limits to only using Windows based or Windows server based OS on the system
* Conditional access requires P1 tier license or a Microsoft 365 business license

What operating systems do Azure AD registered devices support?

Windows 10, iOS, Android, and macOS

What device security sign-in options does Azure AD join support?

An Azure AD work account with password or Windows Hello, and multifactor authentication

When is conditional access applied?

After first-factor authentication

**What is Azure AD join?**

* Allows to join Azure AD devices without the need to sync in an on premises active directory
* Recommended for an organization that is mostly cloud based but can operate in a hybrid environment
* Works with windows 10 or windows server 2019 devices

Identity infrastructure

* Managed environment, uses pass through authentication or password hash for single sign on
* Federated environment, needs use of identity provider.
* Smart cards and certificate based
* Manual user config, if users are manually created then you need to sync accounts using AD-Connect. If created in Azure Ad then no need

Device management

Azure AD uses mobile management platform to manage devices attached to Azure AD

* MDM only, managed exclusively through and MDM provider.
* Co-management, uses MDM provider and a locally installed system configuration center manager

Considerations for resources and apps

* Cloud based apps
* On premises web apps, custom made software hosted on premises can still be accessed through Azure AD join. Users must add app to their trusted sites or intranet zone. This allows windows integrated authentication without prompting user for sign in
* Other devices,
* Printer resources,

Provisioning options

* Self service
* Windows autopilot
* Bulk enrolment

Enterprise state roaming

* Allows users to sync settings and app data with their organizations cloud service
* Benefits include; better management, enhanced security, separation of corporate and consumer data
* Requires premium azure active directory subscription

Data that syncs and roams

* These are settings that are built on windows operating system. They’re mostly personalized settings like themes, passwords, language, ease of access etc.
* Application data when synced is done to an application folder. Any data written to the folder will automatically be synced.

Data storage

* Enterprise state roaming is usually stored in the region closest to you. Usually already determined during first setup but can be changed

Data retention

* All data deleted on the cloud service will temporarily stay there for 90 days before permanently deleted. After 90 days you cannot recover

Explicit data deletion

* User deletion
* Azure ad org deletion
* On request deletion

Stale data deletion

* Any enterprise data that has not been accessed during the past year is automatically treated as ‘stale data’. After 90 days it is then deleted

Data recovery

* After the 90-day retention period is done and data is deleted. It is not completely done. Next time your device connects the data will be restored.