Azure Identity and governence

Saturday, November 27, 2021

4:06 PM

Subscription:

* Is form of billing of resources on how much you consume on monthly/quarterly/yearly basis
* Subscription name can be like pay- as- you-go and such names can be renamed to user friendly name
* Multiple subscriptions can be created if has to be differentiated for diff departments or if billing has to be differentiated.
* It also helps in controlling resources separately

Types:

Pay-as-you-go

Developer

Pro-direct

Standard support

Different types of roles:

There are different sets of roles:

Azure AD

Subscription

RBAC -- fine grain level of access to resources and resource groups in azure

Azure Active Directory:

Is identity provider available in azure platform

In AAD you can define 3 entities that will have access to resources:

User

Group

Service principle

* Whenever an azure account is created there is a AAD directory that is created.
* All the azure resources are part of azure subscription and subscription has trust with AAD
* (if a user want to authenticate and when a user can authenticate himself it informs subscription and he will be able to access resources)
* More precise access is given using RBAC
* AD has other features like MFA, service principle instead of users authenticating for access apps can authenticate using service principle

AAD licensing tiers:

Free

Office 365

Prem P1, premium P2

AAD -- licensing -- activate free prem

User has to be part of custom domain to purchase licenses

AAD --> user --> **+user can add user to groups, add roles and this user has no access to resources need to explicitly give access to resources using RBAC**

Group is collection of users. Instead of giving access to one by one can create group so that roles will be inherited.

Dynamic groups: Need to have premium licenses

If users need to add to group automatically based on attributes then use dynamic groups.

This can be used to users, devices

One dynamic group cannot be for both devices and user it has to be separate.

Values are not case sensitive

Azure subscriptions:

Pay as you go

Visual studio yearly sub - monthly azure credits

Add Azure to your EA

Work with Microsoft Partner

Permissions for user who can access Azure subscription:

Classic Roles:

Account administrator: one per account

Manage all subscriptions in an account

Create new subs

Cancel subs

Change the billing for a sub

Change service admin

Service administrator:

Manages all resources in portal

Can assign users to co-admin role

These roles are diff from AD and RBAC

Management group: group of azure subscriptions together

IAM, policies can be applied to management group level instead at sub level

Now after creating management group. We now can add rules at 4 levels:

Management group level

Subscription level

Resource group level

Resource level

Azure AD

When a Azure account is created by default an instance is created called AD

Azure AD is identity an access management in Azure

Using this users/groups can be created and can be given access to resources

When a azure account is created an instance of AAD is created known as Azure AD tenant

Azure AD tenant has default directory:

[AZ-104 Microsoft Azure Administrator Certification 2021 (udemy.com)](https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/23598016#announcements)

Default directry (AAD directory) : Each Azure tenant has a dedicated and trusted AD directory that includes tenant's users, groups and apps and is performing identity and access management

New directory can be created. (Why? Orgnizations may have diff companies and can create directories)

At any point in time, each subscription can trust only one directory and the users of that directory can be given access to only that specific subscription

Azure AD roles:

These are specific for Azure Ad resources

Global admin:

Manage access to all administrative features in AAD

Assign admin roles to others

Reset pwd for any user and all admins

User admin

Create and manage all aspects of users and groups

Manage SR, monitors service health

Change pwd for users, helpdesk admin and all other admins

Billing admin:

Make purchase

Manage subscriptions

Manage SR, monitors service health

Custom domain:

Why: user while creating user name is appended @default directory as domain name

It can be created with custom domain name

Custom domain name has to be registered with azure AD

Need to verify from Azure AD --> Custom domain (add DNS record at domain provider and then verify from portal)

AAD Join | Device:

Connect o m/c : access work or school --> join aad -->

Control panel -->system and security --> system --> remote settings (uncheck allow users from computers running remo) apply

And can login with domain creds

Edit rdp file

[AZ-104 Microsoft Azure Administrator Certification 2021 (udemy.com)](https://deloittedevelopment.udemy.com/course/microsoft-certified-azure-administrator/learn/lecture/25667648#announcements)

Self service pwd reset: is a feature where a user can reset pwd on his own when it is enabled for a specific set of users from portal.

Azure AD --> Password reset -->properties --> select specific group enable

Define authentication methods

Need to have P1/P2

To enable this login to myapps.microsoft.com and verify email

Important points:

**Built in roles RBAC \*\*\***

**Diff between owner and contri \*\*\***

**Resources/Resource group --> IAM --> Add custom role**

**All the active directory roles are managing different aspects of active directory and nothing to do with resources**

**RBAC are for the resources that are defined as part of azure subscription**

Inviting guest user:

AAD --> All users --> +New guest user or

while creating user selct invite user

AAD --> User setting --> Collaboration external settings --> can limit who can invite guest user

Azure Monitor:

Monitoring service that is available in Azure

Many aspects like:

Can view Metrics for Azure resources like CPU usage, disk metrics and network stats and alerts can be configured based on these

Activity logs, can configure alerts

Log analytics workspace

App insights: perf mngmt sys for live apps. App performance can be analysed using this

Log Analytics work space:

Central solution for all logs.

Kusto query language can be used

Market solutions are available to visualize data that is available

Not region specific. If it is in different region transfer cost is also incurred.

Log analytics work space --> VMs --> shows all the VMs that are in Azure select and connect

After connecting an extension is added to the VM

LAW --> Agents mngmnt --> download agent for windows/linux

Download RDP file in same folder edit --> local resources -->more --> driver --> c connect

Choose the type of data:

LAW --> Agents config --> windows event logs/ perf counters

LAW --> Logs --> will have tables with data

Queries:

*Event | search "demovm"*

*Event | take 5 ( This is taken in no specific order )*

*Event | top 10 by TimeGenerated*

*Event | where EventLevel == 4*

*Event | where TimeGenerated > ago(5m)*

*Event | where TimeGenerated > ago(5m) | project EventLog, Computer*

*Perf | where TimeGenerated > ago(5m) | summarize count() by ObjectName, CounterName*

*Perf | where TimeGenerated > ago(5m) | summarize avg(CounterValue) by Computer*

Alerts:

Alerts can be created based on queries and action can be defined to a group like notifying over email.

Monitor --> Activity log --> can visualize data - diagnostic settings select the log type and destination

Dest: storage account, event hub, LAW

Logs:

Admin

Service health

Resource health

Alerts

Autoscale

Recommendations

Seccurity

Policy

Demo: event hub - create

Stream analytics - create

Monitor - activity log - diagnostic setting - select log and dest

Stream analytics jobs - + Add stream inp

Monitor - metrics --> new chart (select resources)pin to dashboard (shared) can be edited and published and can add multiple metrics to this dashboard

Azure Monitor pricing:

LAW - Data ingetion and retention

AppInsights: Data ingetion and retention

Metrics:

Std- unlimited

Custom - 150 MB per month

Metric queries

Alerts: price is diff if based on metrics, logs, activity logs

And based on notifications as well, emails, web hooks, sms voice calls

Azure backup reports:

Can get reports on all backupitems, vaults, subsc and region

For enabling backup need to have LAW

You need to configure diagnostic settings on backup and recovery vault.

Recovery service vault -->diagnostic setting --> +Add setting.. Select law, select logs

**Applicantion Insights:**

Create app insight, --> setting take connection string

VM --> extenstions --> app insights --> mention connection string here and say OK

So that VM can connect to app insight

App insight --> Live metrics --> can see the data

App insight --> Performance --> can see avg duration of response time

can use app insights on web apps as well

**Tags:**

Name : value

To organize billing of resources dept wise

Subscription --> cost analysis

**Cost - Azure**

Cost analysis as part of Azure subs:

**Overview:**

Current spending, spending per resource, spending history, spending based on resource tags, resource types

Azure Advisor: is a tool that gives lot of recommendations on billing aspect

Cost mngmt +billing : gives cost, resources

but this doesn’t give the forecast

Good to understand if can go beyond budget m gives usage based on limits

Cost analysis - gices cost history

Azure advisor: gives recommendations from cost perspective

**Moving Azure resources:**

Tenant ID has to be same.

Few resources cannot be moves: ADDS, container service

Limitations for VMs:

VMs with certificate stored in KV can be moved to new RG but not new subs

VMs with backup

Vnets:

All resources within Vnet has to be moved

If peering is enabled that has to be removed first

Classic deployments:

Vnets cant be moved

VMs has to be moved along with cloud service

Azure policies:

Security policy for governance aspect for azure resources

Ex: Company has restriced size of VM with cost perspective

Antimalware is installed on all windows VM

All RGs have resource tags in place

Lot of inbuilt available and create custom policies

Azure policy --> select category (ex: compute) --> u'll get in built policy --> select and assign

and while assigning it can be at managemnet group level, sub or RG

Exclusion: ex: policy to all the subscription except a RG - can be used

It takes around 30 mins for policy to reflect

This shows all the resources that are non-complaint it is user responsibility to take necessary action

Lab example: policy --> definition --> deploy anti-virus malware extension

Select create a remediation task so that it deploys and make complaint

Management groups:

Group of subs:

Use: can manage easily like policies

Subscription:

-----------------

Service admin - 1 who and highest privilage

Co- admin- max 200 per sub

Owner

Contri

Reader

<https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles>

Co-administrator: 200 per subs

Same as service admin but can't change association of subsc to azure directories

Assign users to co admin role, but cannot change service admin

Security reader: