😊 Dynamic Groups

Dynamic groups in Azure AD are special types of groups whose membership is automatically managed based on rules or criteria defined by administrators. Unlike traditional groups where membership is manually added or removed, dynamic groups dynamically update their membership as users or objects within Azure AD match or no longer match the defined criteria.

Here's a summary of dynamic groups in Azure AD:

1. **Automated Membership:** Dynamic groups automatically add or remove members based on predefined rules or attributes. This eliminates the need for manual management of group membership.
2. **Rule-Based Membership:** Administrators can define rules or criteria based on user attributes such as department, job title, location, or other custom attributes. Objects that meet these criteria are dynamically added to the group.
3. **Real-Time Updates:** Membership in dynamic groups is continuously evaluated and updated in real-time as changes occur in Azure AD, such as user attribute updates or object creations.
4. **Scalability and Efficiency:** Dynamic groups offer scalability and efficiency by automating the process of managing group membership, particularly in large or dynamic environments with frequent user attribute changes.
5. **Use Cases:** Dynamic groups are commonly used for scenarios such as role-based access control (RBAC), application assignment, license assignment, and targeted policy enforcement based on user attributes.
6. **Integration with Conditional Access:** Dynamic groups can be integrated with Azure AD Conditional Access policies to apply access controls or security policies based on group membership dynamically.

Overall, dynamic groups in Azure AD provide a powerful mechanism for automating group membership management, improving operational efficiency, and ensuring that access controls and policies remain up-to-date in dynamic IT environments.

In this lab, we're setting up a dynamic group in Azure AD and configuring it to automatically manage its membership based on predefined criteria, such as user attributes like city. The end goal is to demonstrate how dynamic groups can automate the process of adding and removing members, improving operational efficiency, and ensuring that access controls remain up-to-date in Azure AD. This allows organizations to dynamically manage group membership without manual intervention, enhancing scalability and reducing administrative overhead.

😄 To begin with the Lab:

1. The prerequisite for this lab is that you should have a Microsoft Entra ID P2 license.

Search your tenant

Basic information

Name	CloudFreeks		Users	3
Tenant ID	bc45c375-f8b5-420b-9bae-325d48b59d33		Groups	1
Primary domain	CloudFreeks.onmicrosoft.com		Applications	0
License	Microsoft Entra ID P2		Devices	0

2. For this lab you should have two users in Azure AD.
3. Now go to groups in Azure AD and click on New Group.

Home >

Groups | All groups
CloudFreeks

«   New group   ↓ Download groups   ↻ Refresh

All groups

Deleted groups   ⓘ Azure Active Directory is now Microsoft Entra ID. L

✗ Diagnose and solve problems   🔍 Search

4. Now while creating a group you need to give it a name and then choose the membership type as Dynamic User. This option will allow Azure AD to add user itself to the group based on the query.
5. Now click on add dynamic query.

New Group ...

 Got feedback?

Group type * ⓘ

Security	⌄

Group name * ⓘ

GroupA	✓

Group description ⓘ

Just a demo group.	✓

Microsoft Entra roles can be assigned to the group ⓘ

Yes	No

Membership type * ⓘ

Dynamic User	⌄

Owners

No owners selected

Dynamic user members * ⓘ

Add dynamic query

6. Then in your query first you need to click on add expression then choose the property type, after that choose the operator then the value as you can see down below. Choose save.

Dynamic membership rules ...

🖫 Save   ✕ Discard | Got feedback?

Configure Rules   Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. ⓘ Learn more

And/Or	Property	Operator	Value
	<Choose a Property>	<Choose an Operator>	Add a value
And ⌄	city	Match ⌄	"New"

+ Add expression + Get custom extension properties ⓘ

Rule syntax

```
(user.city -match "New")
```

7. After that create your group. Then after some time you will be able to see your group.

🔍 Search   ▽ Add filter

Search mode 🔵 Contains

1 group found

	Name ↑	Object Id	Group type	Membership type	Email
☐	**G** GroupA	9117f37b-69a9-454a-b047-202c234fdfff	Security	Dynamic	

8. Once this is done then come back to default directory and go to users.
9. Open your User A, click on edit properties.

UserA ···
User

🔍 Search   «

   ✏ Edit properties   🗑 Delete   ↻ Refresh   🔑 Reset password   ⊘ Revoke sessions   ⚙ Manage view   🗨 Got feedback?

👤 Overview

📱 Audit logs

➡ Sign-in logs

Overview   Monitoring   Properties

Basic info

10. Then go to contact information and in the city type the city of your choices which has a word new in it.

UserA ···
Properties

Refresh | Got feedback?

All   Identity   Job Information   **Contact Information**   Parental controls   Settings   On-premises

This view only contains properties that can be updated. Learn more ↗

🔍 Search "Contact Informati..."

Showing 11 results under "Contact Information"

Street address	
City	New Delhi
State or province	
ZIP or postal code	
Country or region	
Business phone	
Mobile phone	
Email	
Other emails	+ Add or edit other emails

Save   Cancel

11. After that you need to do the same for User B also.

UserB ...
Properties

Refresh | Got feedback?

All | Identity | Job Information | **Contact Information** | Parental controls | Settings | On-premises

This view only contains properties that can be updated. Learn more ☒

🔍 Search "Contact Informati..."

Showing 11 results under "Contact Information"

Street address	
City	new delhi
State or province	
ZIP or postal code	
Country or region	
Business phone	
Mobile phone	
Email	
Other emails	+ Add or edit other emails

Save | Cancel

12. Now you have to wait for some time. Then go to your group and open it. Here you can see the basic information about it like it is a dynamic group.

GroupA

Membership type	Dynamic
Source	Cloud
Type	Security
Object Id	9117f37b-69a9-454a-b047-202c234fdfff
Created at	6/5/2024, 5:30:52 pm
Last membership change ⓘ	6/5/2024, 5:36:26 pm

For more recent activity, visit Audit logs

Dynamic rule processing status ⓘ	Succeeded

For more recent activity, visit Audit logs

Pause processing ⓘ   ⬤ No

13. Now from the left pane, go to members and you will see that both of the users has been added to it based on the properties we defined.

GroupA | Members
Group

- ⓘ Overview
- 🔧 Diagnose and solve problems

Manage
- ⬛ Properties
- 👥 Members
- 👥 Owners
- 👥 Roles and administrators
- 🖼️ Administrative units
- ⚙️ Group memberships

+ Add members   ✕ Remove   ↻ Refresh | 📄 Bulk operations ⌄ | ☰ Columns   🗨 Got feedback?

Direct members   All members

🔍 Search by name   +🔽 Add filters

Name	↑↓	Type	Email	User type
☐ Ⓤ UserA		User		Member
☐ Ⓤ UserB		User		Member