Step 8: Create and Manage Break-Glass Accounts

Objective

To create and configure emergency access (break-glass) accounts that allow secure entry into the environment during outages, misconfigurations, or PIM-related issues.

1. What is a Break-Glass Account?

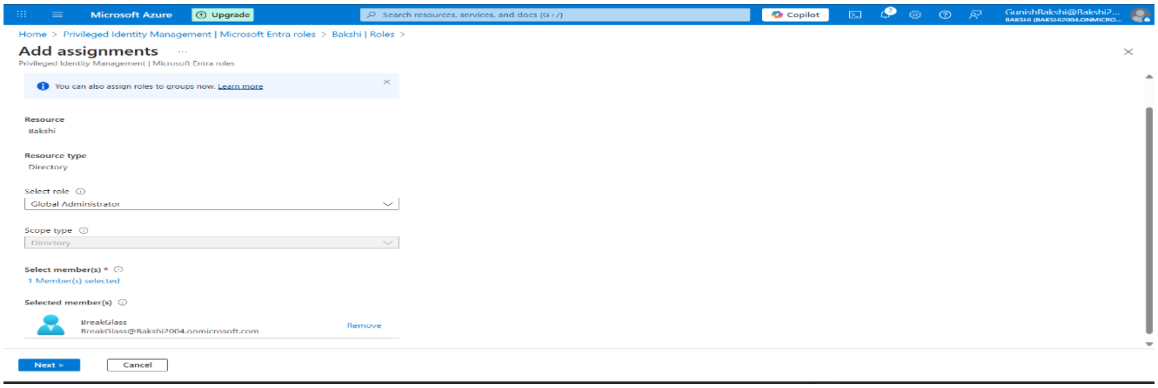
Break-glass accounts are **permanent Global Administrator accounts** that:

- Are **excluded** from conditional access policies
- Are used **only in emergencies**, like when PIM is unavailable or misconfigured

2. Create the Break-Glass Account

Steps:

1. Create a dedicated user:
   - Username: breakglass@Bakshi2004.onmicrosoft.com
   - Strong, complex password (stored securely in a password vault)
2. Assign **Global Administrator** role permanently



Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.ONMICRO...

Home > Privileged Identity Management | Microsoft Entra roles > Bakshi | Roles >

Add assignments

Privileged Identity Management | Microsoft Entra roles

You can also assign roles to groups now. Learn more

Resource
Bakshi

Resource type
Directory

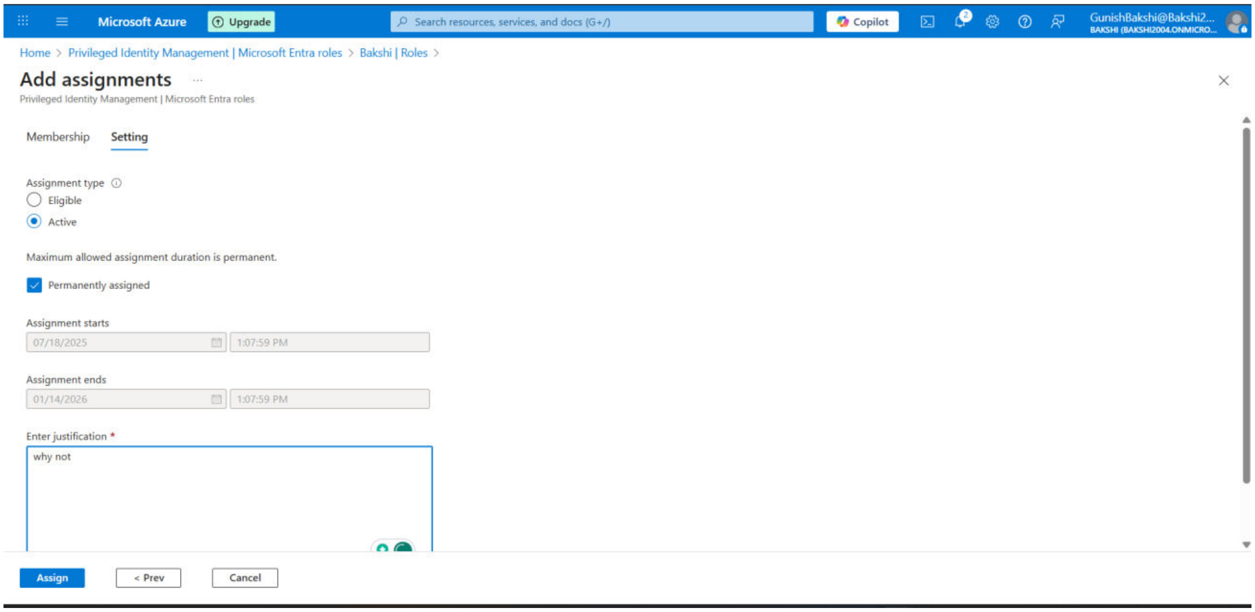
Select role
Global Administrator

Scope type
Directory

Select member(s) *
1 Member(s) selected

Selected member(s)
BreakGlass
BreakGlass@Bakshi2004.onmicrosoft.com
Remove

- Adding breakglass as a Global Admin


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.ONMICRO...
Home > Privileged Identity Management | Microsoft Entra roles > Bakshi | Roles >

Add assignments

Privileged Identity Management | Microsoft Entra roles

Assignment type
○ Eligible
● Active

Maximum allowed assignment duration is permanent.

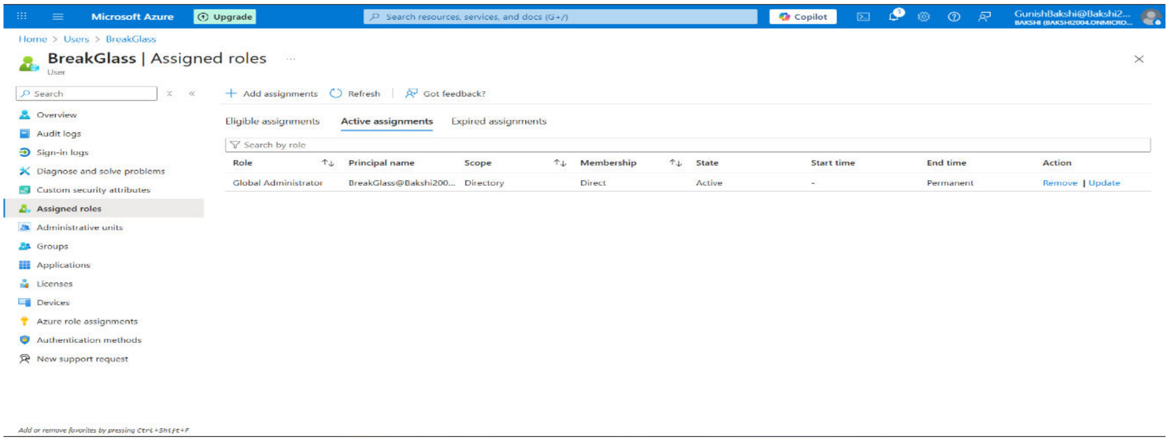
☑ Permanently assigned

Assignment starts: 07/18/2025 1:07:59 PM

Assignment ends: 01/14/2026 1:07:59 PM

Enter justification *: why not

- It will have active status as it has to bypass all reviews and JIT.



BreakGlass | Assigned roles

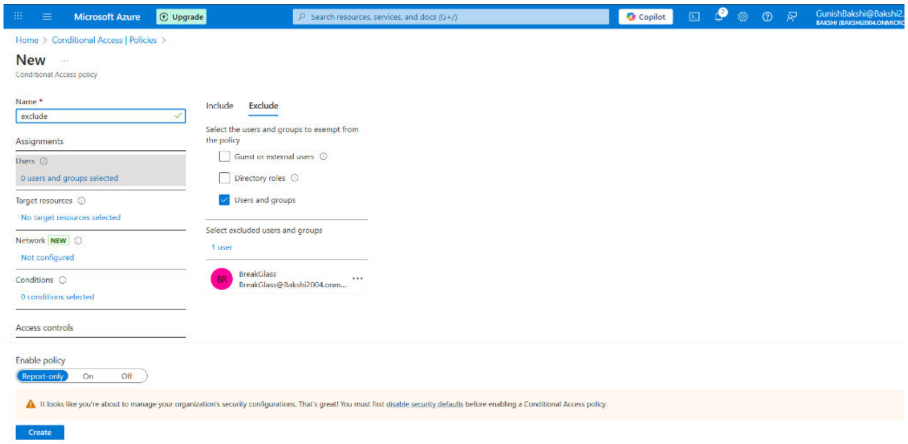
User

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Global Administrator	BreakGlass@Bakshi200...	Directory	Direct	Active	-	Permanent	Remove | Update

- Active Global Administrator account.

3. Secure the Break-Glass Account

Security Measure	Configuration
MFA	**Do not require MFA** (must be accessible even if MFA is down)
Conditional Access	**Exclude this account** from all Conditional Access policies
Password Vault	Store credentials in a **secure vault**, e.g., Azure Key Vault, 1Password, or Bitwarden
Usage Monitoring	Set up **alerting and logging** in case this account is used


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.ONMICRO...
Home > Conditional Access | Policies >

New

Conditional Access policy

Name * exclude

Assignments

Users: 0 users and groups selected

Target resources: No target resources selected

Network NEW: Not configured

Conditions: 0 conditions selected

Access controls

Include | Exclude

Select the users and groups to exempt from the policy

□ Guest or external users

□ Directory roles

☑ Users and groups

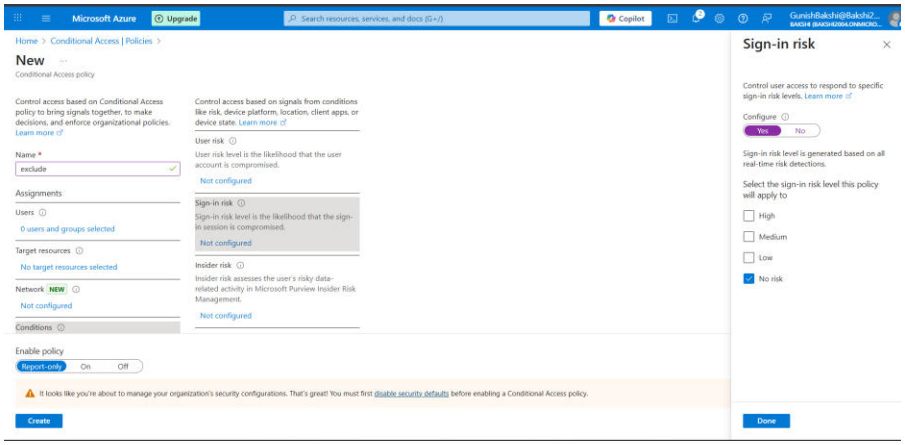
Select excluded users and groups

1 user

BR BreakGlass
BreakGlass@Bakshi2004.onm...

Enable policy: [✓ Report-only] On Off

It looks like you're about to manage your organization's security configurations. That's great! You must first disable security defaults before enabling a Conditional Access policy.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.ONMICRO...
Home > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name * exclude

Assignments

Users: 0 users and groups selected

Target resources: No target resources selected

Network NEW: Not configured

Conditions

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more

User risk: User risk level is the likelihood that the user account is compromised. Not configured

Sign-in risk: Sign-in risk level is the likelihood that the sign-in session is compromised. Not configured

Insider risk: Insider risk assesses the user's risky data-related activity in Microsoft Purview Insider Risk Management. Not configured

Enable policy: [✓ Report-only] On Off

It looks like you're about to manage your organization's security configurations. That's great! You must first disable security defaults before enabling a Conditional Access policy.

Sign-in risk

Control user access to respond to specific sign-in risk levels. Learn more

Configure: [✓ Yes] No

Sign-in risk level is generated based on all real-time risk detections.

Select the sign-in risk level this policy will apply to

□ High

□ Medium

□ Low

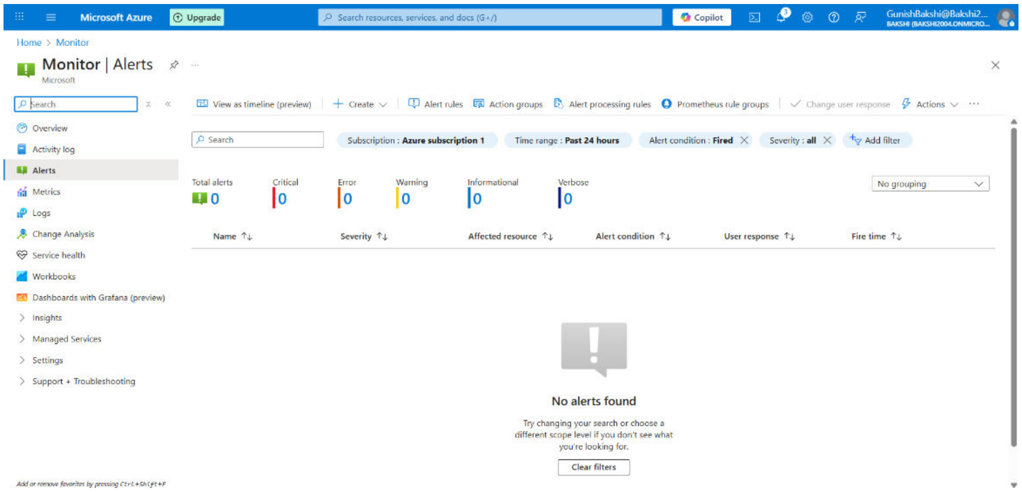
☑ No risk

- Conditional access

4. Monitor Break-Glass Usage

Break-glass accounts should never be used under normal circumstances. Set up:

- **Azure Monitor Alerts** to detect sign-ins
- **Log Analytics** queries to track usage patterns
- Regular review of sign-in logs for the account



Home > Monitor

Monitor | Alerts

Microsoft

Subscription : **Azure subscription 1** | Time range : **Past 24 hours** | Alert condition : **Fired** | Severity : **all**

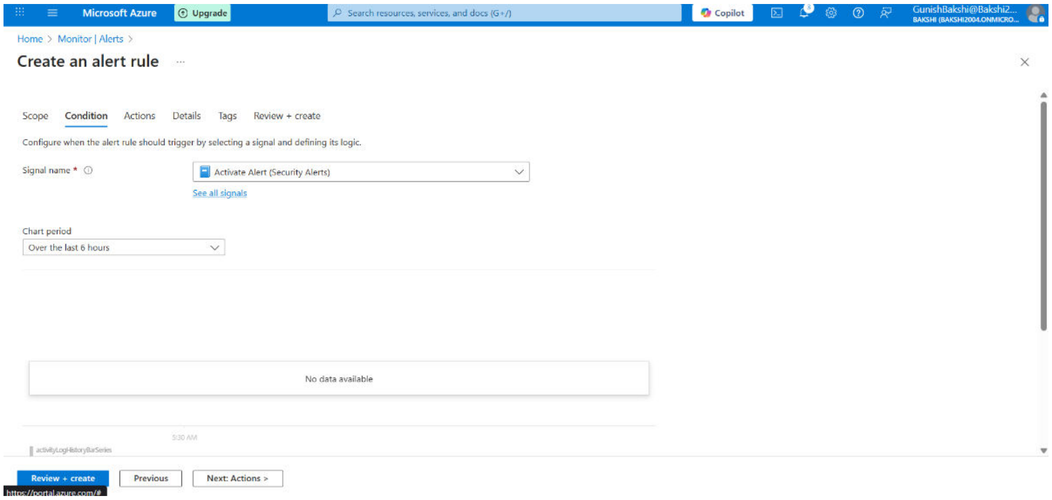
Total alerts	Critical	Error	Warning	Informational	Verbose
0	0	0	0	0	0

Name ↑↓	Severity ↑↓	Affected resource ↑↓	Alert condition ↑↓	User response ↑↓	Fire time ↑↓

No alerts found

Try changing your search or choose a different scope level if you don't see what you're looking for.

Add or remove favorites by pressing Ctrl+Shift+F



Home > Monitor | Alerts >

Create an alert rule

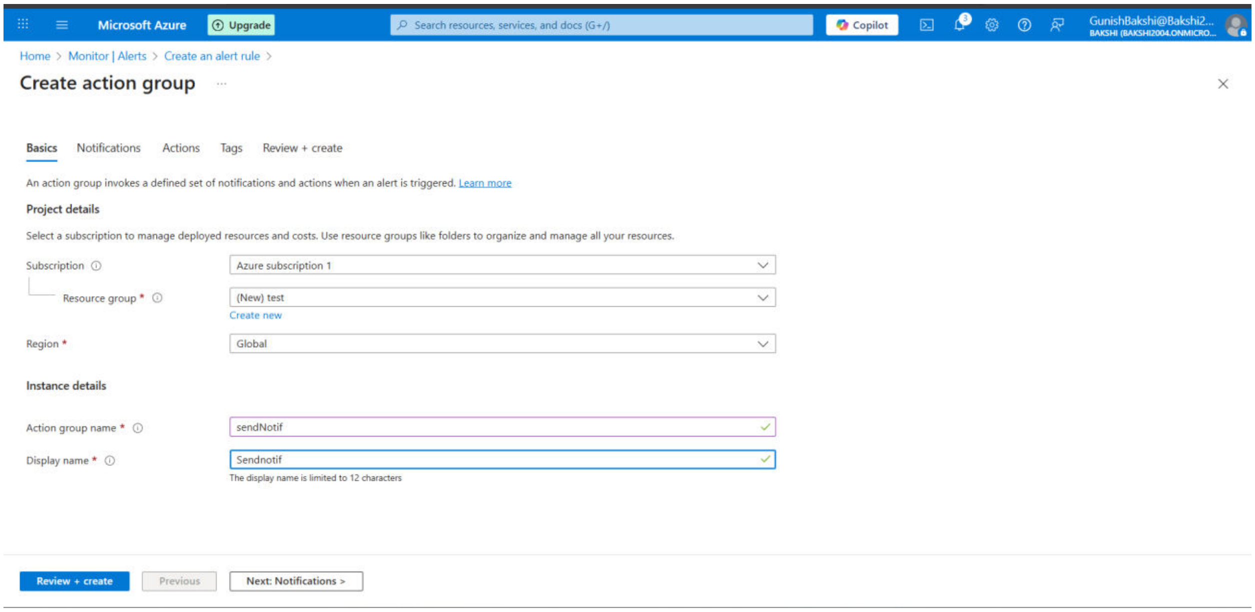
Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name *: Activate Alert (Security Alerts)

Chart period: Over the last 6 hours

No data available

- Azure alerts when anyone signs in



Create action group

Basics
Notifications
Actions
Tags
Review + create

An action group invokes a defined set of notifications and actions when an alert is triggered. Learn more

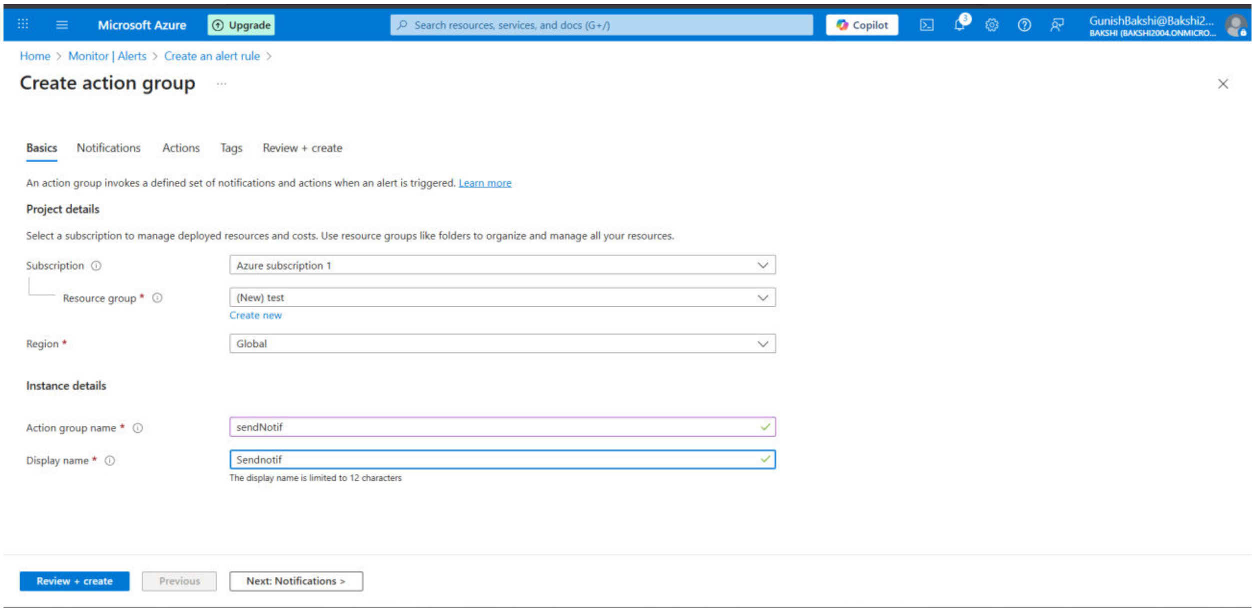
Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription	Azure subscription 1
Resource group *	(New) test Create new
Region *	Global

Instance details

Action group name *	sendNotif
Display name *	Sendnotif The display name is limited to 12 characters


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
GunishBakshi@Bakshi2...
BAKSHI (BAKSHI2004.ONMICRO...
Home > Monitor | Alerts > Create an alert rule >

Create action group

Basics
Notifications
Actions
Tags
Review + create

An action group invokes a defined set of notifications and actions when an alert is triggered. Learn more

Project details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription: Azure subscription 1
Resource group *: (New) test
Create new
Region *: Global

Instance details

Action group name *: sendNotif
Display name *: Sendnotif
The display name is limited to 12 characters

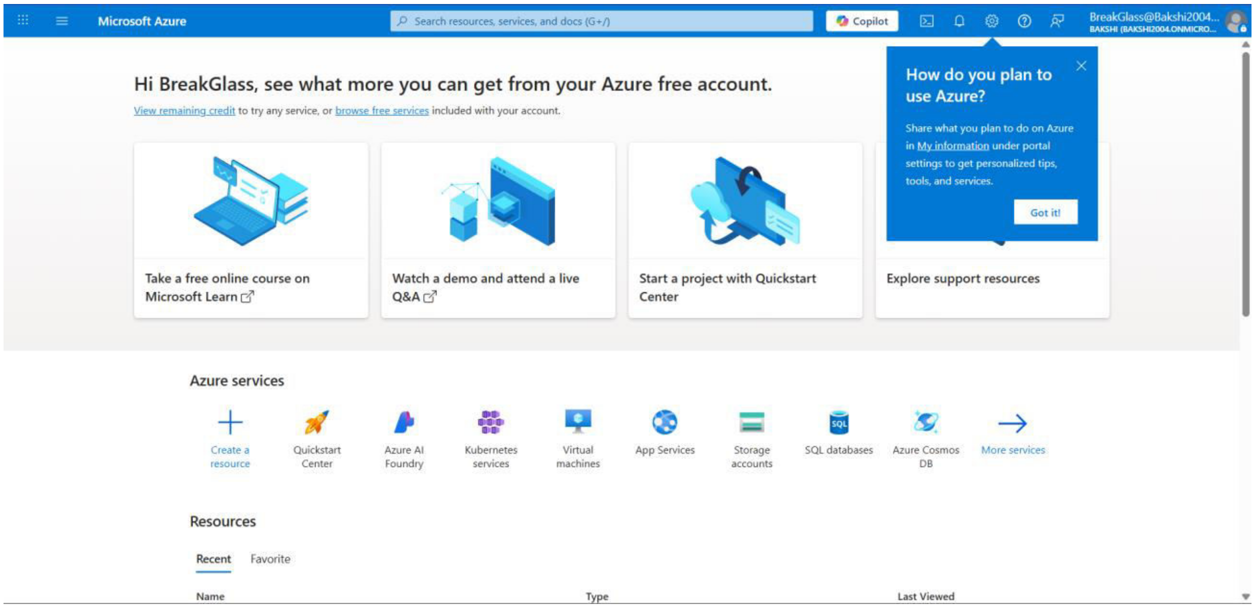
Review + create
Previous
Next: Notifications >

- Email rules are created to notify anytime access occurs.

5. Test the Break-Glass Account

Steps to test:

1. Sign in using breakglass@Bakshi2004.onmicrosoft.com
2. Verify access to Microsoft Entra and Azure roles
3. Confirm that:
   - PIM access is bypassed
   - You can perform administrative actions



Hi BreakGlass, see what more you can get from your Azure free account.

View remaining credit to try any service, or browse free services included with your account.

How do you plan to use Azure?

Share what you plan to do on Azure in My information under portal settings to get personalized tips, tools, and services.

Summary of This Step

- Emergency access account (breakglass@Bakshi2004.onmicrosoft.com) created
- Role assigned outside of PIM
- Secured, excluded from CA/MFA
- Logging and alerting set up
- Successfully tested login functionality