GET2CLOUD

GROUP 1
HONESTY DOGUNRO
TITILAYO OYELAKIN
JESSE EDWARD
SUSAN UDEGO
MACFRANKLIN IFEANYI

Get2cloud Cohort 2 Project

Implementing Role-Based Access Control (RBAC) With Privileged Identity Management (PIM) in Azure

GET2CLOUD

Project Overview

Implementing and managing RBAC and PIM within Azure to enhance security and control.

Objective

Implement and manage PIM and RBAC.

Key Goals

- Define user roles and responsibilities.
- Configure just-in-time access with time limits.
- Simulate real-world scenarios to assess security effectiveness.

GET2CLOUD

Company Background

Our fictitious company is a growing tech firm with a diverse set of cloud needs.

Company

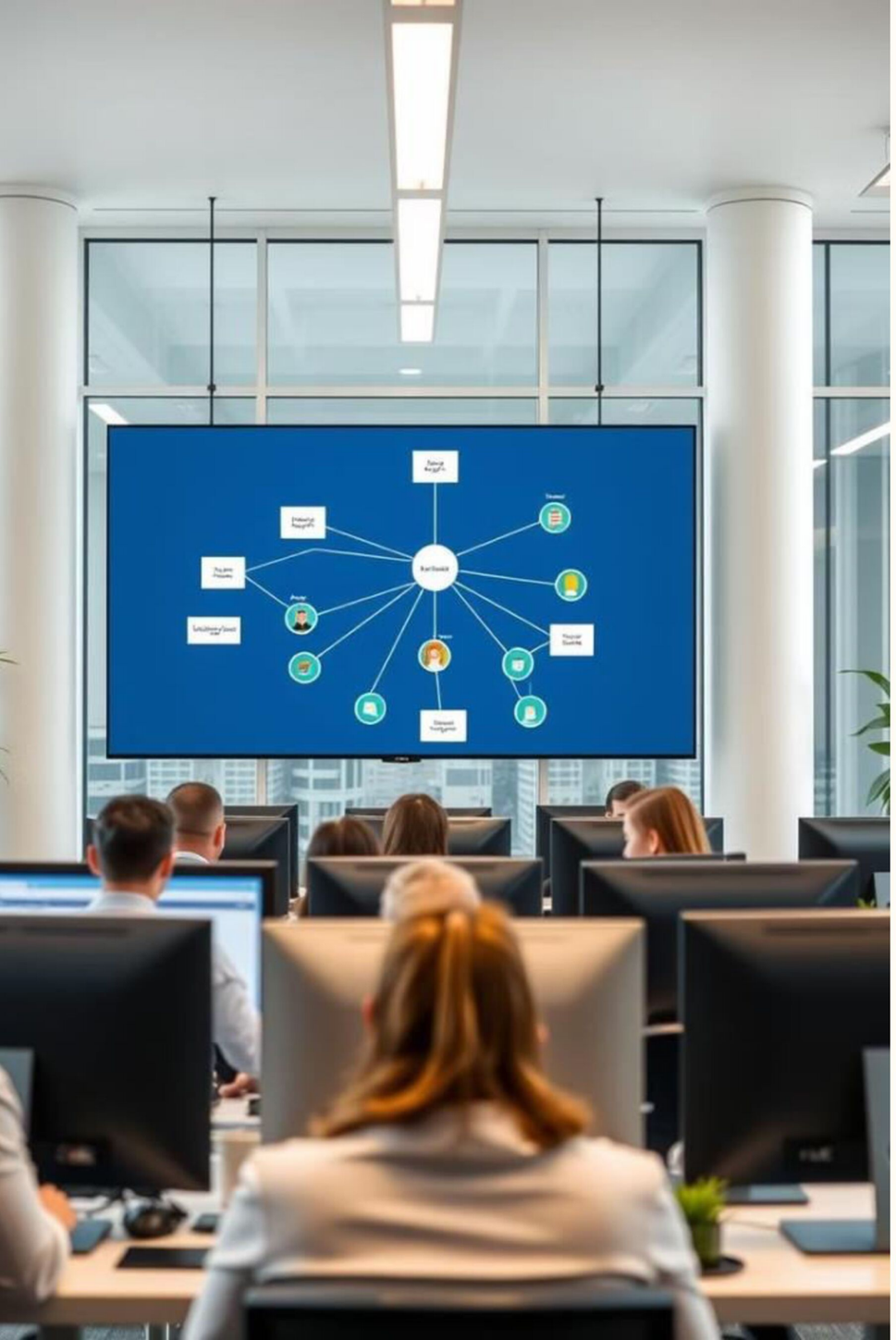
Growing tech firm with expertise in software development and IT services.

Departments

IT, Development, HR, each with specific access requirements.

Challenge

Ensure secure and controlled access to Azure resources.



GET2CLOUD

Roles and Responsibilities

Defining user roles and their respective access levels for Azure resources.

1 IT Admin

Manages Azure infrastructure, networks, and databases.

2 Developer

Accesses development environments, code repositories, and testing resources.

3 HR Manager

Manages employee data and payroll information securely.

GET2CLOUD

Setting Up PIM

Configuring PIM for just-in-time access and granular privilege control.

PIM Configuration

Define specific roles: IT Admins, Developers, HR Managers.

Just-in-Time Access

Implement approval-based privileges with set time limits.

GET2CLOUD

Simulating Real-World Scenarios

Testing the security effectiveness of RBAC and PIM with real-world scenarios.

1

Scenario 1

Developer requests access to the production environment.

2

Scenario 2

HR Manager activates access for payroll processing.

3

Scenario 3

IT Admin requests elevated privileges for server maintenance.

Privileged Identity Management | Quick start

Privileged Identity Management

Quick start
Tasks
Manage
Microsoft Entra roles
Groups
Azure resources
Activity
Troubleshooting + Support

Azure Active Directory is becoming Microsoft Entra ID. Learn more

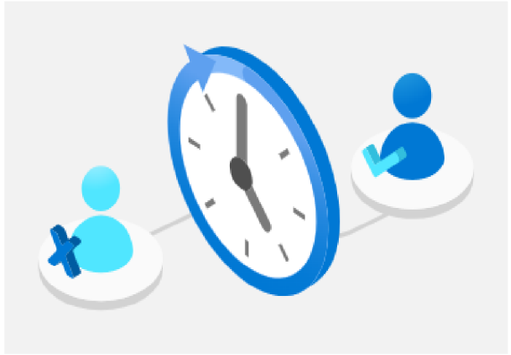
What's new | Get started

Manage your privileged access

Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. Learn more

Manage access

Users with excessive access are vulnerable in the event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extending



Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical

Discover and monitor

It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your

Privileged Identity Management | Azure resources

Privileged Identity Management

Quick start
Tasks
Manage
Microsoft Entra roles
Groups
Azure resources
Activity
Troubleshooting + Support

Activate role

Scope defines a set of resources. Select a scope below to manage an Azure resource.
Learn more

You can only view and manage resources to which you have permissions. Check your access. Learn more

Search by management group id or subscription id

Management groups
Select the management group

Subscriptions
Microsoft Azure Sponsorship

Resource groups
GROUP1-Get2cloudRG

Resources
Select the resource

Current selection

Name	GROUP1-Get2cloudRG
Resource Id	/subscriptions/ee7cf281-2a95-4bdb-ae0f-

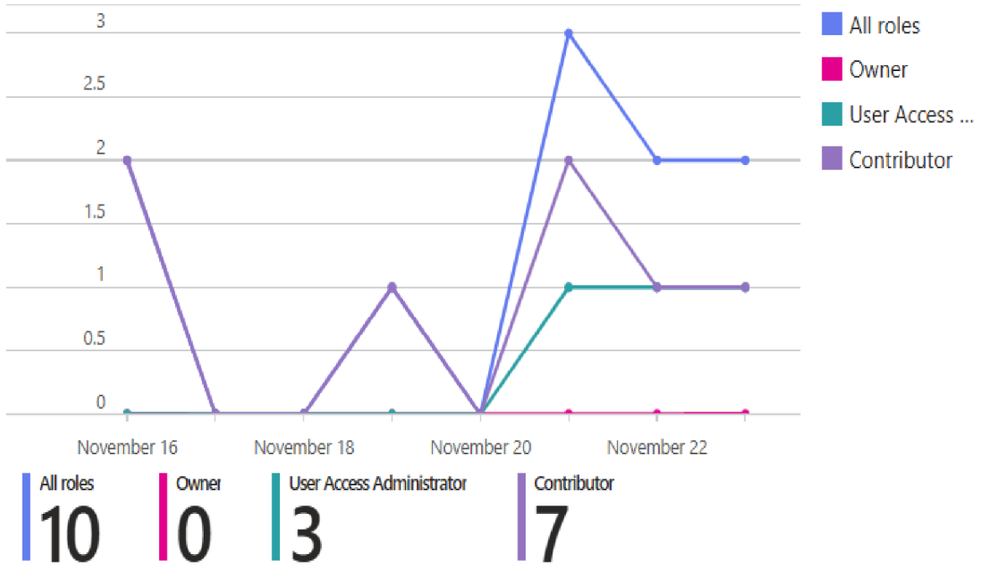
GROUP1-Get2cloudRG | Overview

Privileged Identity Management | Azure resources

Overview
Tasks
Manage
Roles
Assignments
Settings
Activity

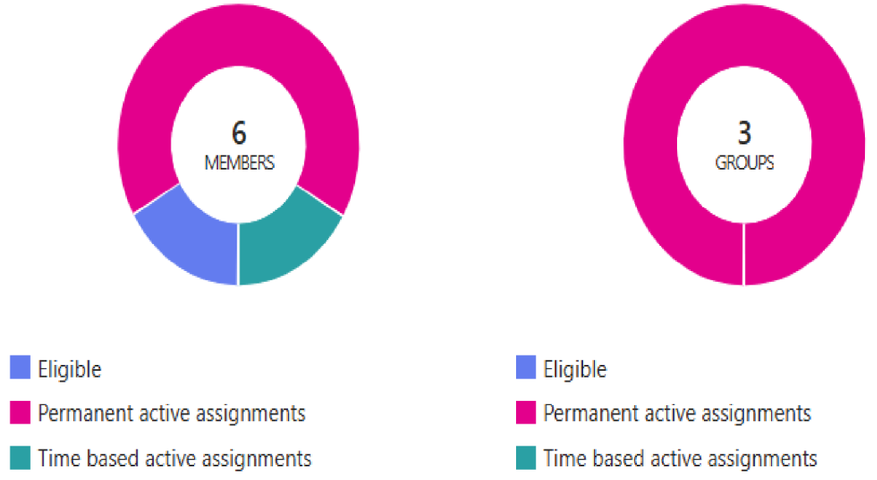
Admin view | My view

Role activations in last 7 days



All roles	Owner	User Access Administrator	Contributor
10	0	3	7

Role assignment distribution



PIM Activities in last 30 days

Title	Count
Members with new eligible assignments	15
Members assigned as active	3

Roles by assignment (descending)

Role	Member
Contributor	4
User Access Administrator	2

GROUP1-Get2cloudRG | Roles

Privileged Identity Management | Azure resources

Overview
Tasks
Manage
Roles
Assignments
Settings
Activity

Add assignments | Refresh | Got feedback?

Search by role name

Role	Active	Eligible
AcrPush	0	0
API Management Service Contributor	0	0
AcrPull	0	0
AcrImageSigner	0	0
AcrDelete	0	0
AcrQuarantineReader	0	0
AcrQuarantineWriter	0	0
API Management Service Operator Role	0	0
API Management Service Reader Role	0	0
Application Insights Component Contributor	0	0
Application Insights Snapshot Debugger	0	0
Attestation Reader	0	0
Automation Job Operator	0	0
Automation Runbook Operator	0	0
Automation Operator	0	0
Avere Contributor	0	0

Contributor

Privileged Identity Management | Azure resources

+ Add assignments | Review | Settings | Refresh | Export | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by member name

Name	Principal name	Type	Membership	Condition	Start time	End time	Action
No results							

Add assignments

Privileged Identity Management | Azure resources

Membership | Setting

Resource

GROUP1-Get2cloudRG

Resource type

Resource group

Select role

Contributor

Select member(s) *

No member selected

Add assignments

Privileged Identity Management | Azure resources

Membership | Setting

Resource
GROUP1-Get2cloudRG

Resource type
Resource group

Select role
Contributor

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

Selected member(s)
Honesty
Honesty@janetnjokucgmail.onmicrosoft.com

Next > | Cancel

Select a member or group

Privileged Identity Management | Azure resources

Try changing or adding filters if you don't see what you're looking for.

Search

40 results found

All | Users | Groups

Name	Type	Details
Adebusayo	User	adebusayo@janetnjokucgmail.onmicrosoft.(
GROUP 1-Get2cloud	Group	
Anita	User	Anita@janetnjokucgmail.onmicrosoft.com
GROUP 2-Get2cloud	Group	
Annis	User	annis@janetnjokucgmail.onmicrosoft.com
GROUP 3-Get2cloud	Group	

Selected (1)

Reset

Honesty

Select

Add assignments

Privileged Identity Management | Azure resources

Membership Setting

Assignment type

- (•) Eligible
- ( ) Active

Maximum allowed eligible duration is 1 year(s).

Assignment starts *

11/23/2024 9:44:09 AM

Assignment ends *

11/23/2024 10:44:09 AM

Assign < Prev Cancel

GET2CLOUD

Role Activation Process

Defining the step-by-step process for activating privileged roles within Azure.

1

Request Activation

Users request activation for specific privileged roles.

2

Approval Workflow

An approval chain with defined time limits for access.

3

Role Expiry

Automatic revocation of privileges after the specified time period.

Privileged Identity Management | Quick start

Privileged Identity Management

Quick start
Tasks
Manage
Microsoft Entra roles
Groups
Azure resources
Activity
Troubleshooting + Support

Azure Active Directory is becoming Microsoft Entra ID. Learn more

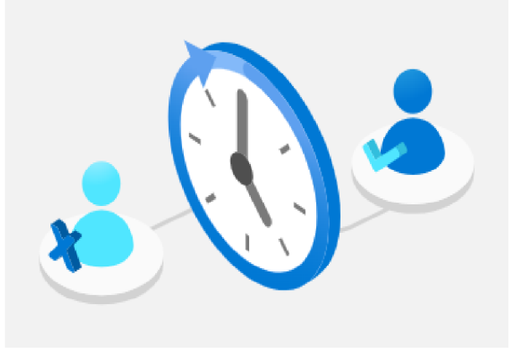
What's new | Get started

Manage your privileged access

Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. Learn more

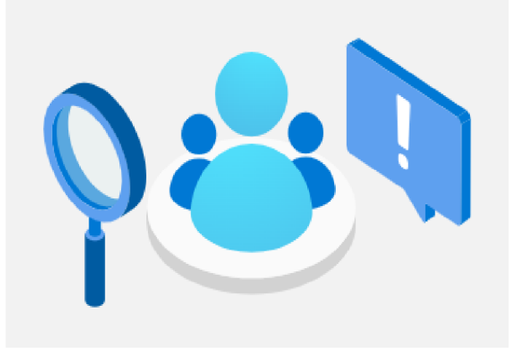
Manage access

Users with excessive access are vulnerable in the event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extending



Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical



Discover and monitor

It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your

My roles | Azure resources

Privileged Identity Management | My roles

Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support

Refresh | Open in mobile | Got feedback?

Eligible assignments | Active assignments | Expired assignments

Search by role or resource

Role	Resource	Resource type	Membership	Condition	End time	Action
Contributor	GROUP1-Get2cloudRG	Resource group	Direct	None	11/23/2024, 10:50:09 AM	Activate | Extend

My roles | Azure resources

Privileged Identity Management | My roles

Refresh | Open in mobile | Got feedback?

Activate
- Microsoft Entra roles
- Groups
- Azure resources

Troubleshooting + Support

Eligible assignments | Active assignments | Expired assignments

Search by role or resource

Role	Resource	Resource type	Membership
Contributor	GROUP1-Get2cloudRG	Resource group	Direct

Activate - Contribut

Privileged Identity Management | Azure r

Activating role

Scope: GROUP1-Get2cloudRG (Resource group)
Member: Honesty Role: Contributor

Roles | Activate | Scope | Status

Stage 1
Processing your request and activating your role.

Stage 2
Validating that your activation is successful.

Stage 3
Activation completed successfully.

When the final stage completes your browser will automatically refresh. You do not have to sign-out and back in again.

Refresh in 5 second(s) Cancel

Activate | Cancel

My roles | Azure resources

Privileged Identity Management | My roles

Activate
Microsoft Entra roles
Groups
Azure resources
Troubleshooting + Support

Refresh | Open in mobile | Got feedback?

Eligible assignments | **Active assignments** | Expired assignments

Search by role or resource

Role	Resource	Resource type	Membership	Condition	State	End time	Action
Contributor	GROUP1-Get2cloudRG	Resource group	Direct	None	Activated	11/23/2024, 10:50:24 A...	Deactivate
Reader	GROUP1-Get2cloudRG	Resource group	Group	None	Assigned	Permanent	Deactivate

DEVTEST1

Virtual machine

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
  - Insights
  - Alerts
  - Metrics
  - Diagnostic settings
  - Logs

Failed to stop virtual machine

Failed to stop the virtual machine 'DEVTEST1'. Error: The client 'Honesty@janetnjokucgmail.onmicrosoft.com' with object id '73a0dd3d-7560-460a-acb3-f962d3d05ff3' does not have authorization to perform action 'Microsoft.Compute/virtualMachines/deallocate/action' over scope 'GROUP1-Get2cloudRG/providers/Microsoft.Compute/virtualMac... or the scope is invalid. If access was recently granted, please refresh your credentials.

Help me troubleshoot

Advisor (1 of 9): Windows virtual machines should enable Azure Disk Encryption or EncryptionAtHost. →

Help me copy this VM in any region

Connect | Start | Restart | Stop | Hibernate | Capture | Delete | Refresh | Open in mobile | Feedback

Essentials

Resource group (move)	: GROUP1-Get2cloudRG	Operating system	: Windows (Windows 10 Pro)
Status	: Running	Size	: Standard D2s v3 (2 vcpus, 8 GiB memory)
Location	: East US (Zone 1)	Public IP address	: 172.208.105.31
Subscription (move)	: Microsoft Azure Sponsorship	Virtual network/subnet	: sample1-vnet/default
Subscription ID	: ee7cf281-2a95-4bdb-ae0f-9ea2c2165278	DNS name	: Not configured
Availability zone	: 1	Health state	: -
		Time created	: 11/16/2024, 11:55 AM UTC

Tags (edit) : Add tags

Properties | Monitoring | Capabilities (8) | Recommendations (9) | Tutorials

Virtual machine

Computer name	DEVTEST1
Operating system	Windows (Windows 10 Pro)
VM generation	V2

Networking

Public IP address	172.208.105.31 (Network interface devtest1505_z1)
Public IP address (IPv6)	-
Private IP address	10.0.0.5

GET2CLOUD

Monitoring and Auditing

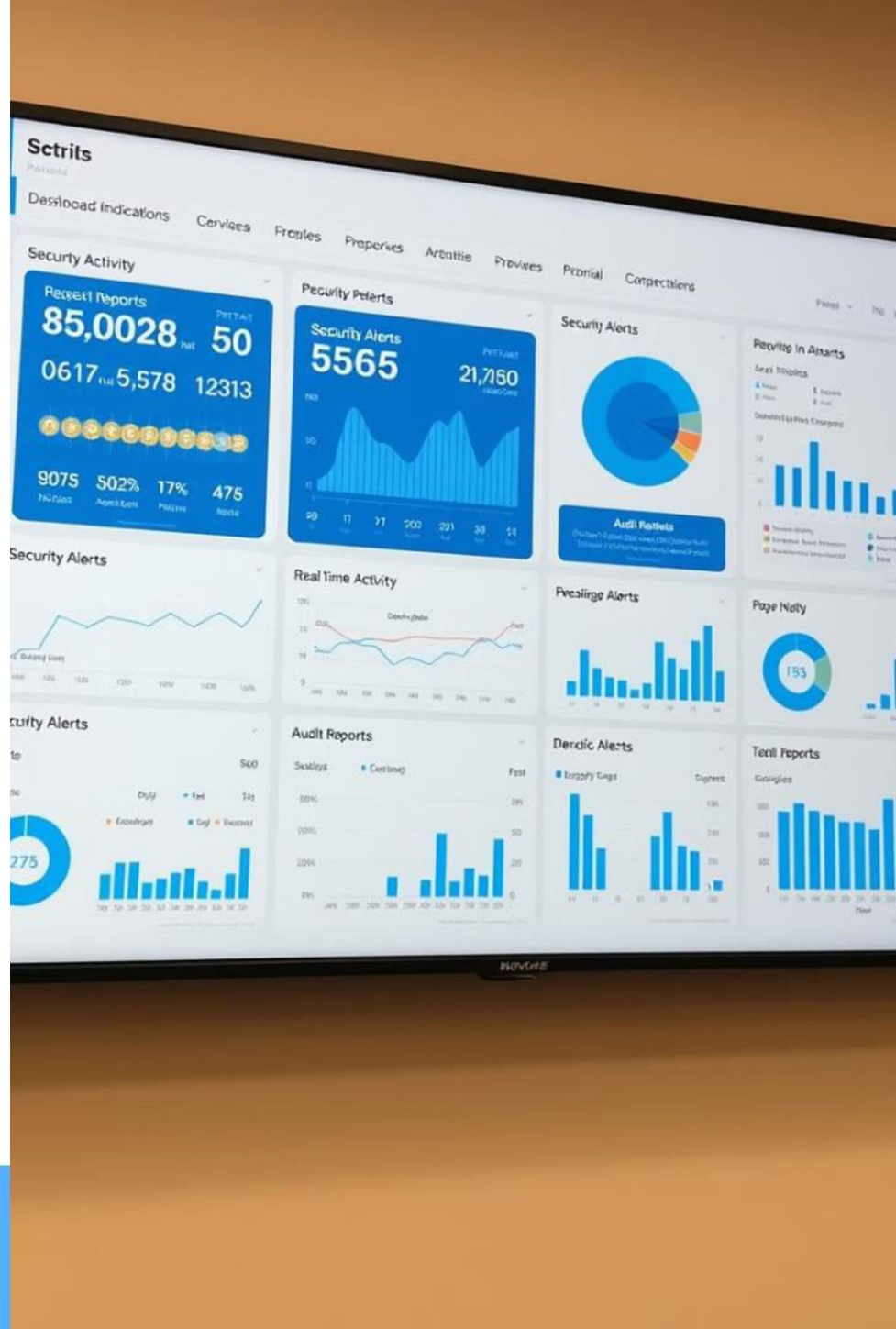
Ensuring ongoing security visibility and accountability through continuous monitoring.

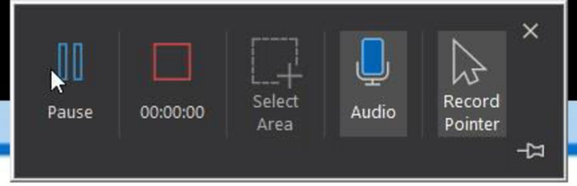
Logs and Alerts

Set up alerts for unusual activity and review logs regularly.

Reports

Generate audit reports for privileged role usage and access patterns.





Microsoft Azure

Search resources, services, and docs (G+/)

mfaesting@gmail.com
MRT

Home >

mrt | Overview

Azure Active Directory

- Create a resource
- Home
- Dashboard
- All services

FAVORITES

- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Microsoft Defender for Cloud
- Cost Management + Billing
- Help + support

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes (Preview)
- Licenses
- Azure AD Connect

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview

GET2CLOUD