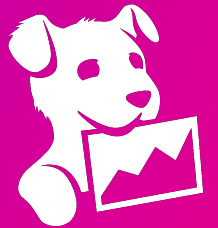


# Hidden in Plain Sight: (Ab)using Entra's AUs

Katie Knowles



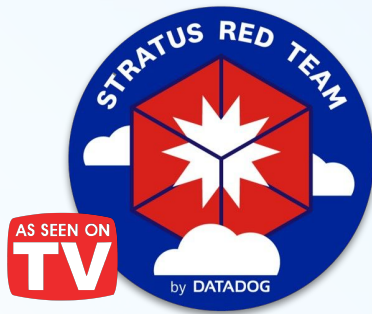
DATADOG



# Katie Knowles

Cloud Security Researcher, Datadog

# Agenda



---

**01** Administrative Units 101

---

**02** Restricted + HiddenMembership AUs

---

**03 Persistence:** Restricted Backdoor Account

---

**04 Persistence:** Hidden Permissions on Users

---

**05** Detection & Remediation

---

# DISCLAIMER

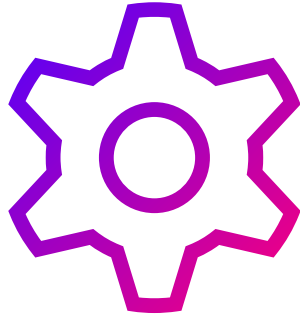
This talk describes usage of AU features "as designed", and **does not** contain vulnerability disclosure. Many useful features can cause damage with malicious intent or misuse. The focus of this talk is to document these possible methods of misuse and prepare an organization to defend against them.



# Administrative Unit **features**

# Review: Azure Roles

## Azure RBAC Roles

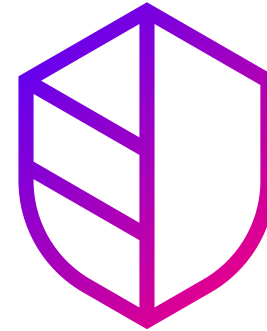


Permissions over Azure resources:  
VMs, storage, networking, etc.

### Examples

*Owner, Reader,  
Virtual Machine Contributor*

## Entra ID Roles



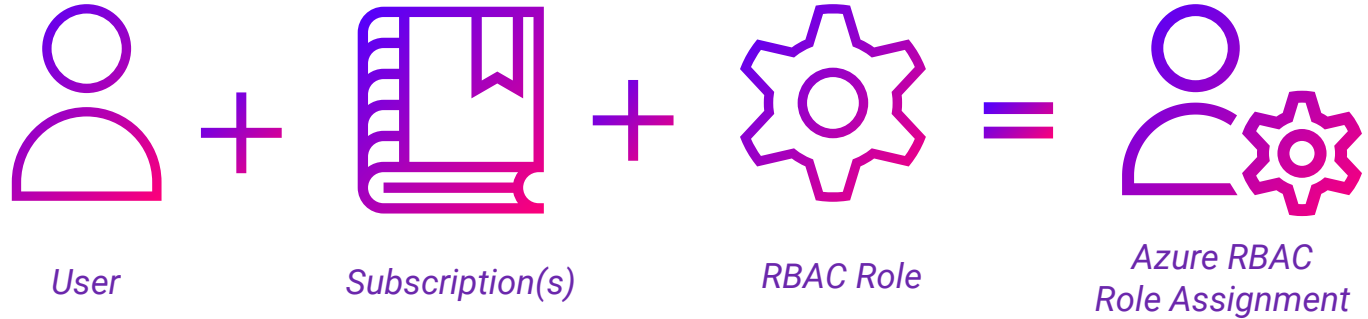
Permissions within Entra ID (Azure AD):  
Users, devices, tenant settings, etc.

### Examples

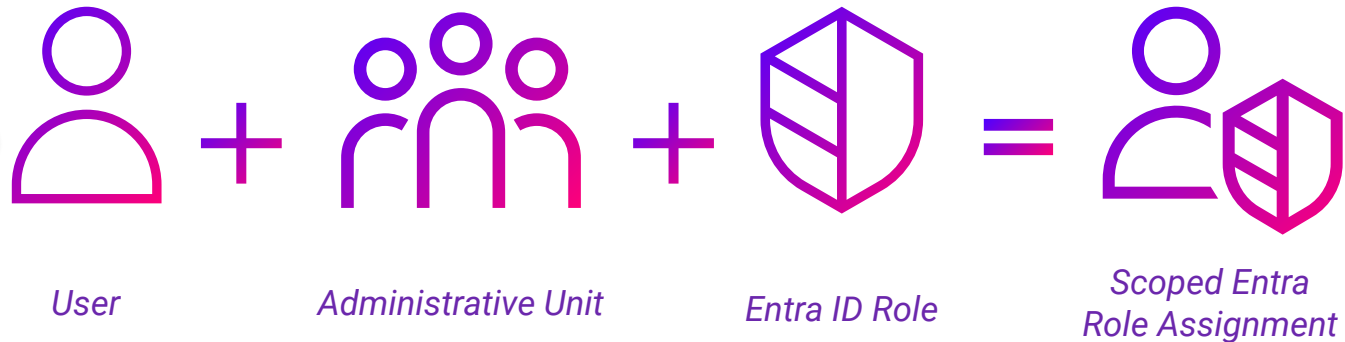
*Global Administrator,  
Directory Reader, Auth. Administrator*

# What are AUs?

## RBAC Role Assignment:

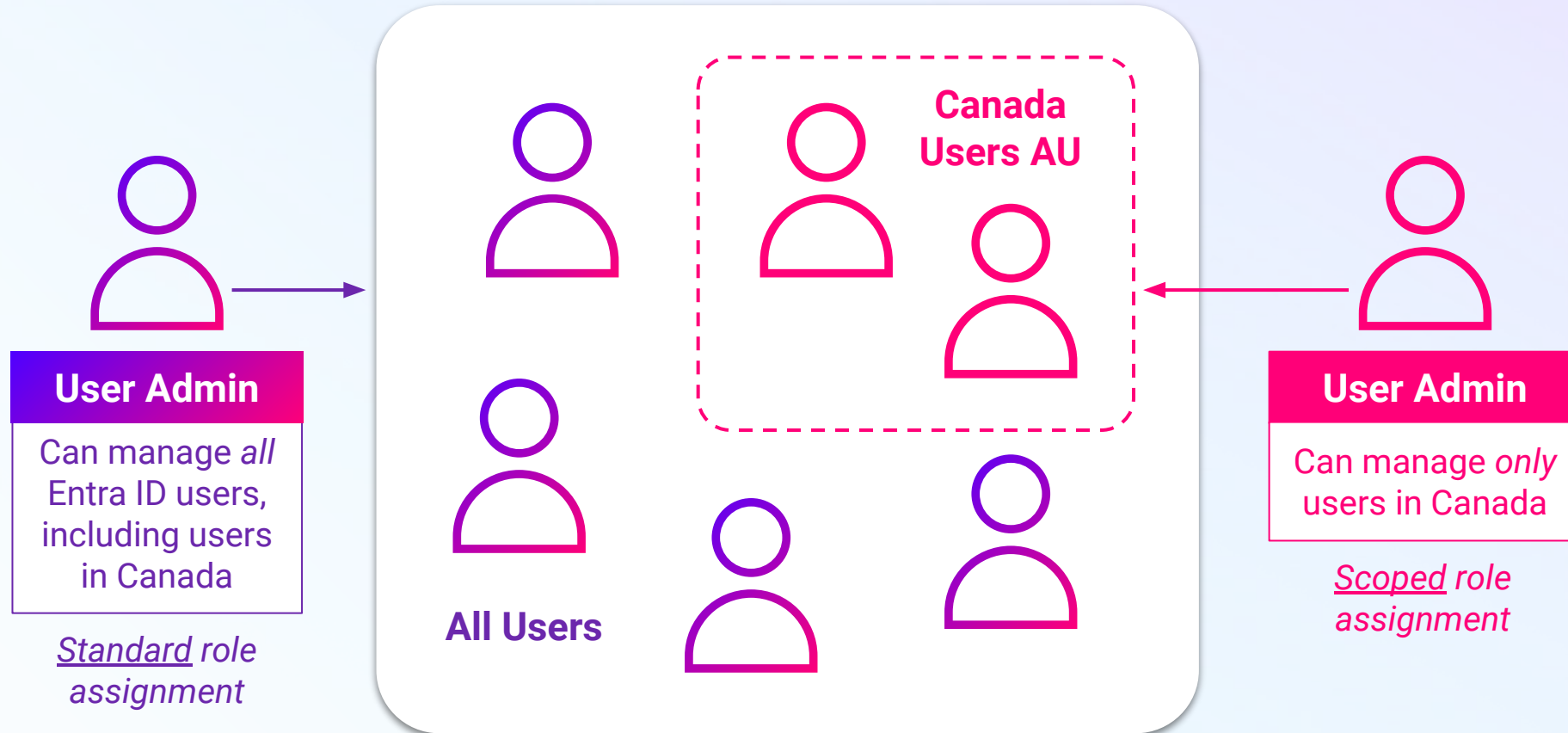


## Entra ID Role Assignment:



*Equivalent  
to...*

# 101: Administrative Units





# 101: Administrative Units

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

Administrative units > Dynamic Administrative Unit | Properties (Preview)

## Dynamic membership rules

Save Discard

### Configure Rules

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
<input type="text"/>	country	Starts With	"Canada"

+ Add expression + Get custom extension properties

### Rule syntax

(user.country -startsWith "Canada")

Edit

Microsoft Azure Copilot

Home > Administrative units

## Add administrative unit

Got feedback?

Properties Assign roles Review + create

Properties

Name  
Canadian Helpdesk

Description

Assignments

Password Administrator  
Katie Knowles

Create Previous

# Reading the docs...

The screenshot shows the Microsoft Entra ID documentation page for "Restricted management administrative units in Microsoft Entra ID (Preview)". The title "Restricted management administrative units in Microsoft Entra ID (Preview)" is circled in red. Below the title, the text "hmm..." is written in red. The page includes a sidebar with navigation links, a main content area with an "Important" note stating that these units are in preview, and a list of related articles.

Filter by title

Microsoft Entra roles documentation

- > Overview
- > Concepts
  - Understand Microsoft Entra roles
  - > Compare roles
  - Use groups to manage role assignments
- > Administrative units
  - Administrative units
  - Restricted management**
  - Best practices
- > Security
- > How-to guides
- > Reference

## Restricted management administrative units in Microsoft Entra ID (Preview)

Article • 06/13/2024 • 6 contributors [Feedback](#)

*hmm...*

### In this article

- [Why use restricted management administrative units?](#)
- [What objects can be members?](#)
- [What types of operations are blocked?](#)
- [Who can modify objects?](#)
- [Show 4 more](#)

**Important**

Restricted management administrative units are currently in PREVIEW. See the [Product Terms](#) for legal terms that apply to features that are in beta, preview, or otherwise not yet released into general availability.

*Restricted Management*

The screenshot shows the PowerShell documentation page for Microsoft Graph PowerShell. The title "PowerShell" is at the top. The page includes a sidebar with navigation links, a main content area with instructions on how to use the Connect-MgGraph command, and a code block showing the command to create a new administrative unit. The code block is circled in red, and the text "HiddenMembership" is circled in red. The text "hmm..." is written in red.

Filter by title

Microsoft Graph PowerShell Azure AD PowerShell

Use the [Connect-MgGraph](#) command to sign in to your tenant and consent to the required permissions.

```
PowerShell Copy
Connect-MgGraph -Scopes "AdministrativeUnit.ReadWrite.All"
```

Use the [New-MgDirectoryAdministrativeUnit](#) command to create a new administrative unit.

```
PowerShell Copy
$params = @{
    DisplayName = "Seattle District Technical Schools"
    Description = "Seattle District technical schools admini"
    Visibility = "HiddenMembership"
}
$adminUnitObj = New-MgDirectoryAdministrativeUnit -BodyParam
```

*hmm...*

*HiddenMembership*

# Restricted Management

**Restricted AU members** cannot be modified by tenant scoped roles (e.g. Global Admin)

**Scoped role assignment** is required to manage restricted AU members

**Restricted management** AUs are recommended for protecting sensitive users, e.g. CEO or VIPs



# Restricted Management AU Creation

**Request**

1 POST /beta/administrativeUnits HTTP/2  
2 Host: graph.microsoft.com  
3 User-Agent: []  
4 Accept: \*/\*  
5 Content-Language: en  
6 Content-Encoding: gzip, deflate, br  
7 Content-Type: application/json  
8 Content-Length: 105  
9 Referer: https://portal.azure.com/  
10 X-Ms-Command-Name: AdminUnit%20-%20CreateAdminUnit  
11 X-Ms-Effective-Locale: en.en-us  
12 []  
13 Origin: https://portal.azure.com  
14 Sec-Fetch-Dest: empty  
15 Sec-Fetch-Mode: cors  
16 Sec-Fetch-Site: cross-site  
17 Authorization: Bearer []  
18 Te: trailers  
19 {  
20 "displayName": "Test AU",  
"description": "[]",  
"isMemberManagementRestricted": true  
}

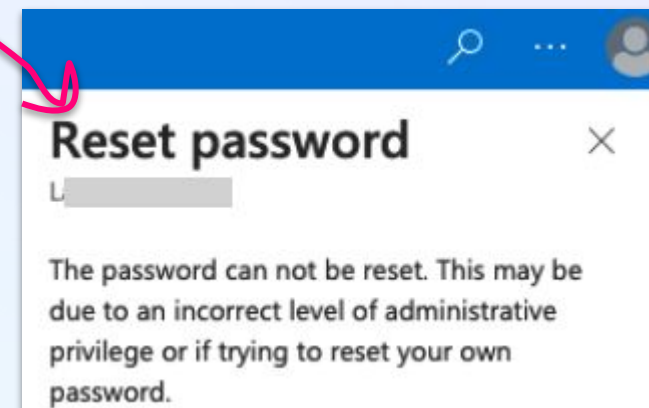
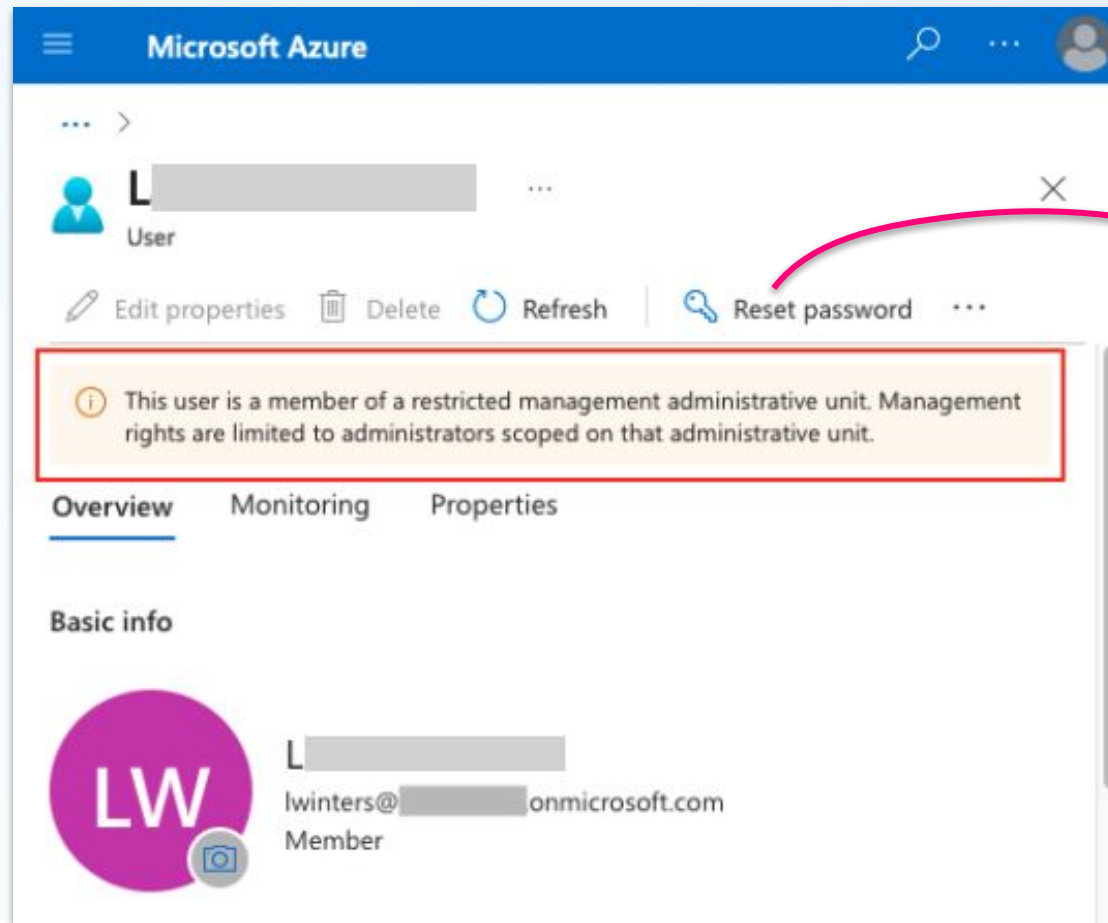
Restricted management administrative unit ①  
Yes No

**Response**

1 HTTP/2 201 Created  
2 Cache-Control: no-cache  
3 Content-Type: application/json;odata.metadata=minimal;odata.streaming=true;IEEE754Compatible=false;charset=utf-8  
4 Location: https://graph.microsoft.com/v2/[redacted]/directoryObjects/93dad08e-9413-4f09-8a51-04a84ca24fcb/Microsoft.DirectoryServices.AdministrativeUnit  
5 []  
6 X-Ms-Resource-Unit: 1  
7 Odata-Version: 4.0  
8 Date: Fri, 14 Jun 2024 13:43:23 GMT  
9 {  
10 "@odata.context": "https://graph.microsoft.com/beta/\$metadata#administrativeUnits/\$entity",  
"id": "93dad08e-9413-4f09-8a51-04a84ca24fcb",  
"deletedDateTime": null,  
"displayName": "Test AU",  
"description": "[]",  
"isMemberManagementRestricted": true,  
"visibility": null,  
"membershipRule": null,  
"membershipType": null,  
"membershipRuleProcessingState": null  
}



# Restricted Membership Behavior



*View as Global Admin!*

# Hidden Membership

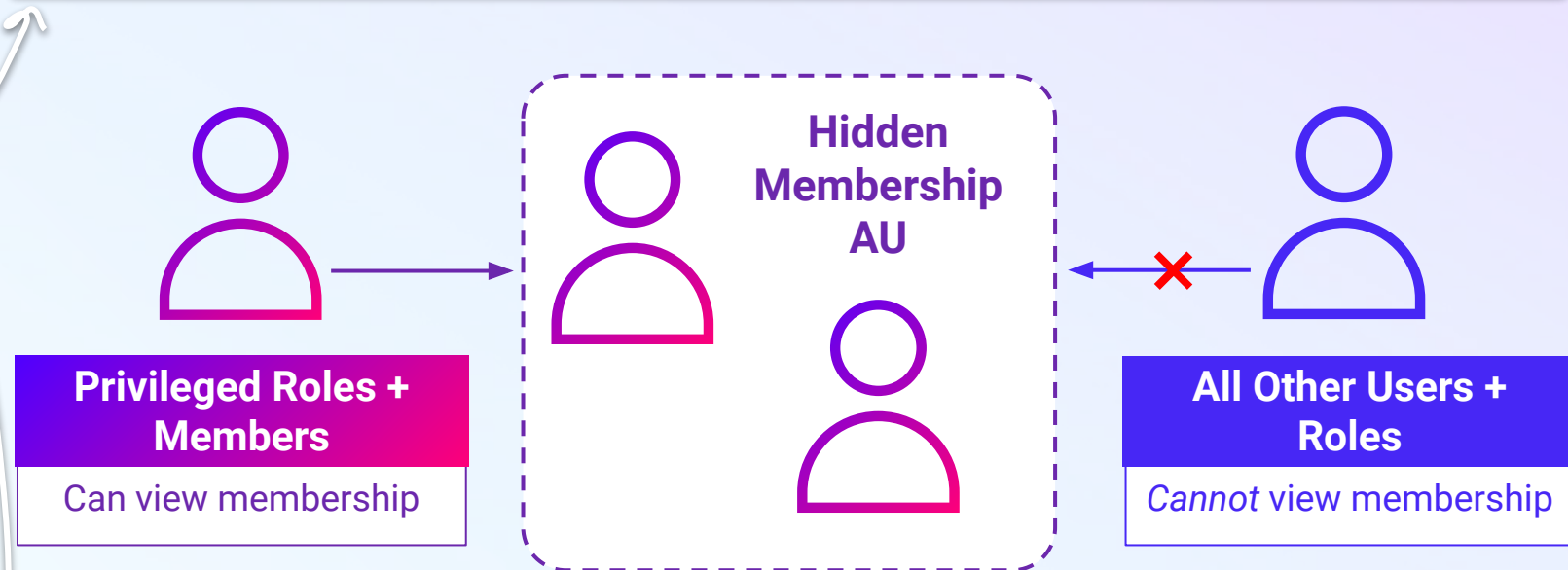
**HiddenMembership AU** membership can only be viewed by certain privileged\* roles + AU members

**AU and role assignments** are viewable by other users, but AU will appear empty

**HiddenMembership property** is not shown in Portal, or returned in API response for AU members

Can view:  
Authentication Administrator  
Global Administrator  
Groups Administrator  
Helpdesk Administrator

Privileged Authentication Administrator  
SharePoint Administrator  
Teams Administrator  
User Administrator  
Global Reader (Note: not Directory Reader)



Cannot view (notable examples):

Security Administrator  
Security Operator  
Password Administrator

Security Reader  
Directory Reader

# HiddenMembership AU Creation

Edited request ▾		Response	
Pretty	Raw	Hex	Render
1	POST /beta/administrativeUnits	1	HTTP/2 201 Created
2	HTTP/2	2	Cache-Control: no-cache
3	Host: graph.microsoft.com	3	Content-Type:
7	User-Agent: []		application/json;odata.metadata=minimal;odata.streaming
8	Referer: https://portal.azure.com/	4	=true;IEEE754Compatible=false;charset=utf-8
9	Content-Type: application/json		Location:
10	X-Ms-Command-Name:		https://graph.microsoft.com/v2/
11	AdminUnit%20-%20CreateAdminUnit		/directoryObjects/19f612f0-691c-4b2d-a331-8
12	Authorization: Bearer []		6bf8ef60aa4/Microsoft.DirectoryServices.AdministrativeU
13	X-Ms-Effective-Locale: en.en-us	5	nit
14	X-Ms-Client-Request-Id:	6	[]
15	d632bec2-135c-4866-bd98-8dc7241b201d	7	Date: Fri, 21 Jun 2024 19:54:08 GMT
16	X-Ms-Client-Session-Id:	8	{
17	ded27a87d8ab4e17ab189be57c0cb0c1		"@odata.context":
18	Content-Length: 118		"https://graph.microsoft.com/beta/\$metadata#administr
19	Origin: https://portal.azure.com		ativeUnits/\$entity",
20	Te: trailers		"id":"19f612f0-691c-4b2d-a331-86bf8ef60aa4",
21	{		"deletedDateTime":null,
22	"displayName":"Test Hidden [] AU",		"displayName":"Test Hidden [] AU",
	"isMemberManagementRestricted":		"description":null,
	false,		"isMemberManagementRestricted":false,
	"visibility":"HiddenMembership"		"visibility":"HiddenMembership",
	}		"membershipRule":null,
			"membershipType":null,
			"membershipRuleProcessingState":null
			}

# HiddenMembership Behavior

The image displays two side-by-side screenshots of the Microsoft Azure portal, illustrating the 'HiddenMembership Behavior' for a 'Hidden AU' (Administrative Unit).

**Left Screenshot (GlobalAdmin@):** This screenshot shows the user management interface for the 'Hidden AU'. The user 'GlobalAdmin@' is highlighted in a red box. Below the user list, a table shows two users: 'CEO' and 'Katie Knowles', both with the role 'Member'. The table is also highlighted with a red box.

	User type	User principa
<input type="checkbox"/> CEO	Member	
<input type="checkbox"/> Katie Knowles	Member	

**Right Screenshot (SecurityAdmin@):** This screenshot shows the user management interface for the 'Hidden AU' when the user 'SecurityAdmin@' is selected. The user list is empty, and a red box highlights the text 'No results.'.

*"Can View" Role*

*"Cannot View" Role*



**How did we get that list...?**

## EXPECTATIONS



# Permissions Check

**488 Microsoft Graph** permissions  
**109 Entra ID** built-in role templates

---

Surely these permissions....  
align with API actions?  
In documents?

## REALITY



*"Your best bet at the moment is to rely on the directory role permission descriptions and find the Microsoft Graph APIs you would use to perform that action."*

- Microsoft Employee(?) on r/AZURE

---

*"Tiering Entra roles and application permissions based on known attack paths", Emilien Socchi*

---

*"Directory.ReadWrite.All Is Not As Powerful As You Might Think", Andy Robbins*

# 597 Service Principals later...

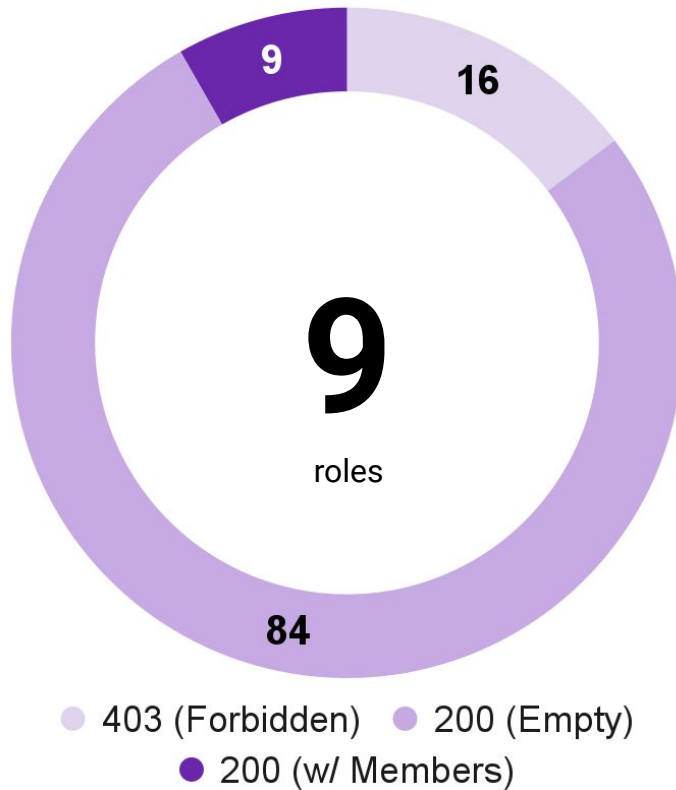


```
data.http.graph_tokens["Community.ReadWrite.All"]: Reading...
data.http.graph_tokens["TeamsTab.ReadWriteForTeam.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["EduAdministration.Read.All"]: Reading...
data.http.graph_tokens["Device.ReadWrite.All"]: Reading...
data.http.graph_tokens["DeviceManagementConfiguration.ReadWrite.All"]: Reading...
data.http.graph_tokens["ApprovalSolution.Read.All"]: Read complete after 1s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["UserTeamwork.Read.All"]: Reading...
data.http.graph_tokens["ProfilePhoto.Read.All"]: Read complete after 1s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["SharePointTenantSettings.Read.All"]: Reading...
data.http.graph_tokens["Community.ReadWrite.All"]: Read complete after 1s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["EduCurricula.ReadWrite.All"]: Reading...
data.http.graph_tokens["AgreementAcceptance.Read.All"]: Reading...
data.http.graph_tokens["EntitlementManagement.ReadWrite.All"]: Reading...
data.http.graph_tokens["UserTeamwork.Read.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["DeviceManagementConfiguration.ReadWrite.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft
data.http.graph_tokens["User.Export.All"]: Reading...
data.http.graph_tokens["EduAdministration.Read.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["Device.ReadWrite.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["Calendars.ReadBasic.All"]: Reading...
data.http.graph_tokens["SharePointTenantSettings.Read.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["EduCurricula.ReadWrite.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["AgreementAcceptance.Read.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["EntitlementManagement.ReadWrite.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["Calendars.ReadBasic.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["Mail.Read"]: Reading...
data.http.graph_tokens["ChannelSettings.Read.All"]: Reading...
data.http.graph_tokens["SecurityIdentitiesSensors.Read.All"]: Reading...
data.http.graph_tokens["CustomTags.ReadWrite.All"]: Reading...
data.http.graph_tokens["User.Export.All"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens
data.http.graph_tokens["Bookings.Read.All"]: Reading...
data.http.graph_tokens["PrivilegedAssignmentSchedule.Read.AzureADGroup"]: Reading...
data.http.graph_tokens["Mail.Read"]: Read complete after 0s [id=https://login.microsoftonline.com/40thcoffee.onmicrosoft.com/oauth2/v2.0/tokens]
```

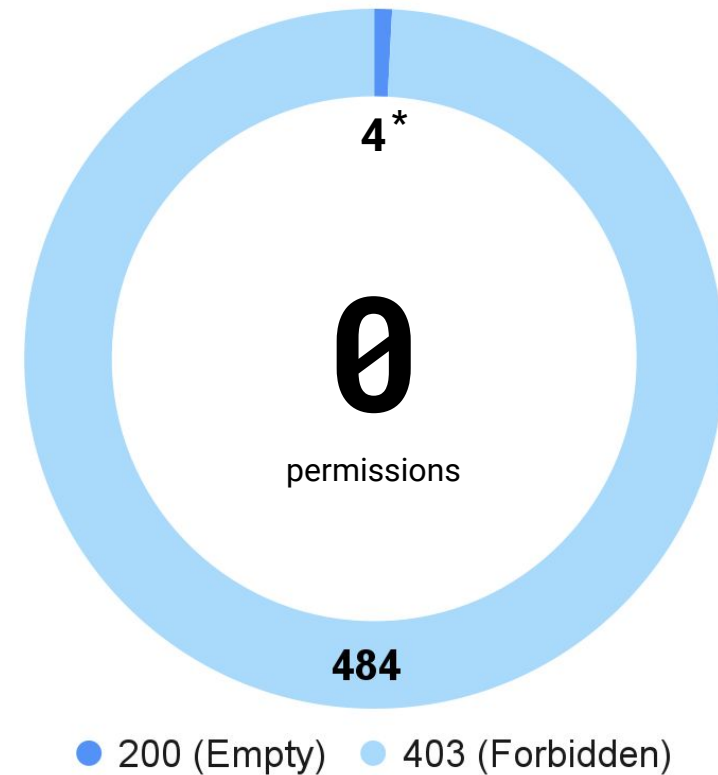


# Results: HiddenMembership view

## Entra ID Built-in Roles



## Microsoft Graph Permissions



\* *AdministrativeUnit.Read.All, Directory.Read.All*



# Results: 9 Entra ID roles w/ HiddenMembership view

<b>microsoft.directory/ administrativeUnits/ allProperties/allTasks</b>	Global Administrator	Privileged Role Administrator
<b>microsoft.directory/ administrativeUnits/ allProperties/read</b>	Global Reader	
<b>Unknown Source Permission</b>	Groups Administrator Teams Administrator User Administrator	SharePoint Administrator Helpdesk Administrator Authentication Administrator



*Can't assign all permissions to custom  
role templates :(*

**Okay... figured that out.**

# Recap: AU Benefits & Features



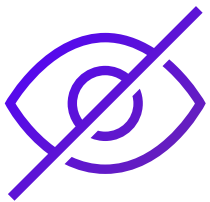
## Administrative Unit (AU)

Allows scoped assignment of specific Entra ID roles to admins over users, devices, or group objects. Limit blast radius of role assignment. Can use dynamic filters.



## Restricted Management AU

Changes members' role assignments from `if("tenant role" OR "scoped role")` to `if("scoped role")`. Ensures sensitive users are only modified by specific users.



## HiddenMembership AU

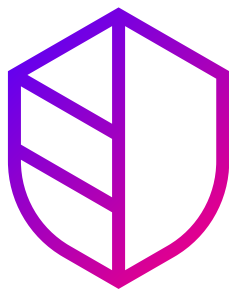
Conceals membership from all users except 9 administrative roles and the AUs' own members. Others can see only the AU object and its scoped role assignments.



# Administrative Unit **persistence scenarios**



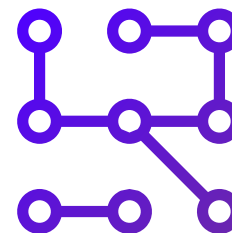
# Privileged Persistence Techniques



**Scenario 1:**  
Restricted  
Backdoor Account



**Scenario 2:**  
Hidden Permissions  
on Users



**Combined Scenario:**  
Recap Impact

*\* Scenarios require Global Administrator  
or Privileged Role Administrator*

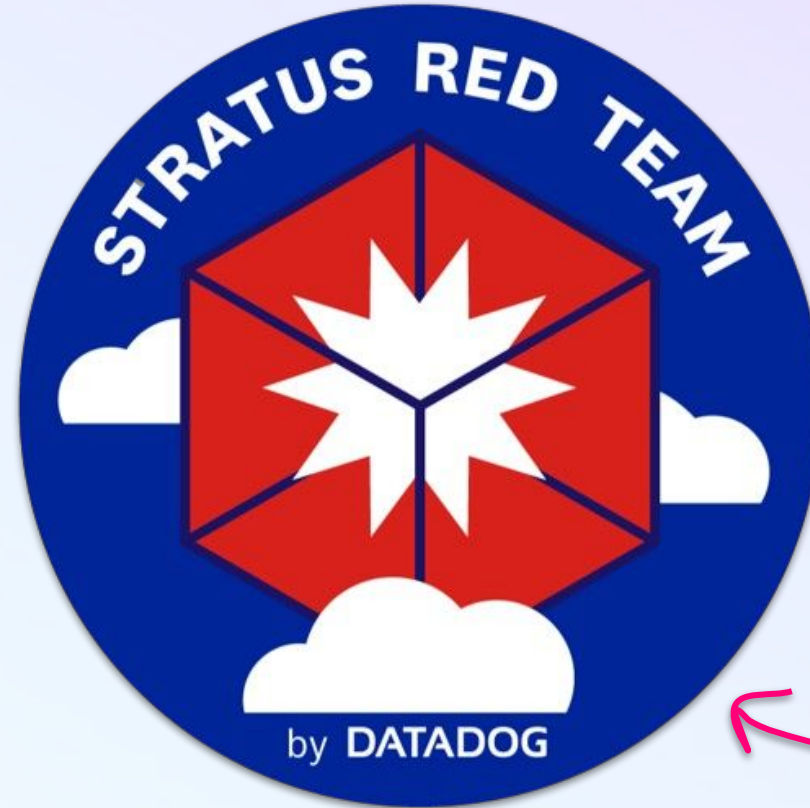
# Stratus Red Team

**Easily execute** offensive techniques against live environments and validate detection logic

**60 techniques** across AWS, GCP, Azure, & Kubernetes

**New!** Entra ID support + techniques for fwd:cloudsec EU, including Restricted + HiddenMembership AUs

<https://github.com/DataDog/stratus-red-team>



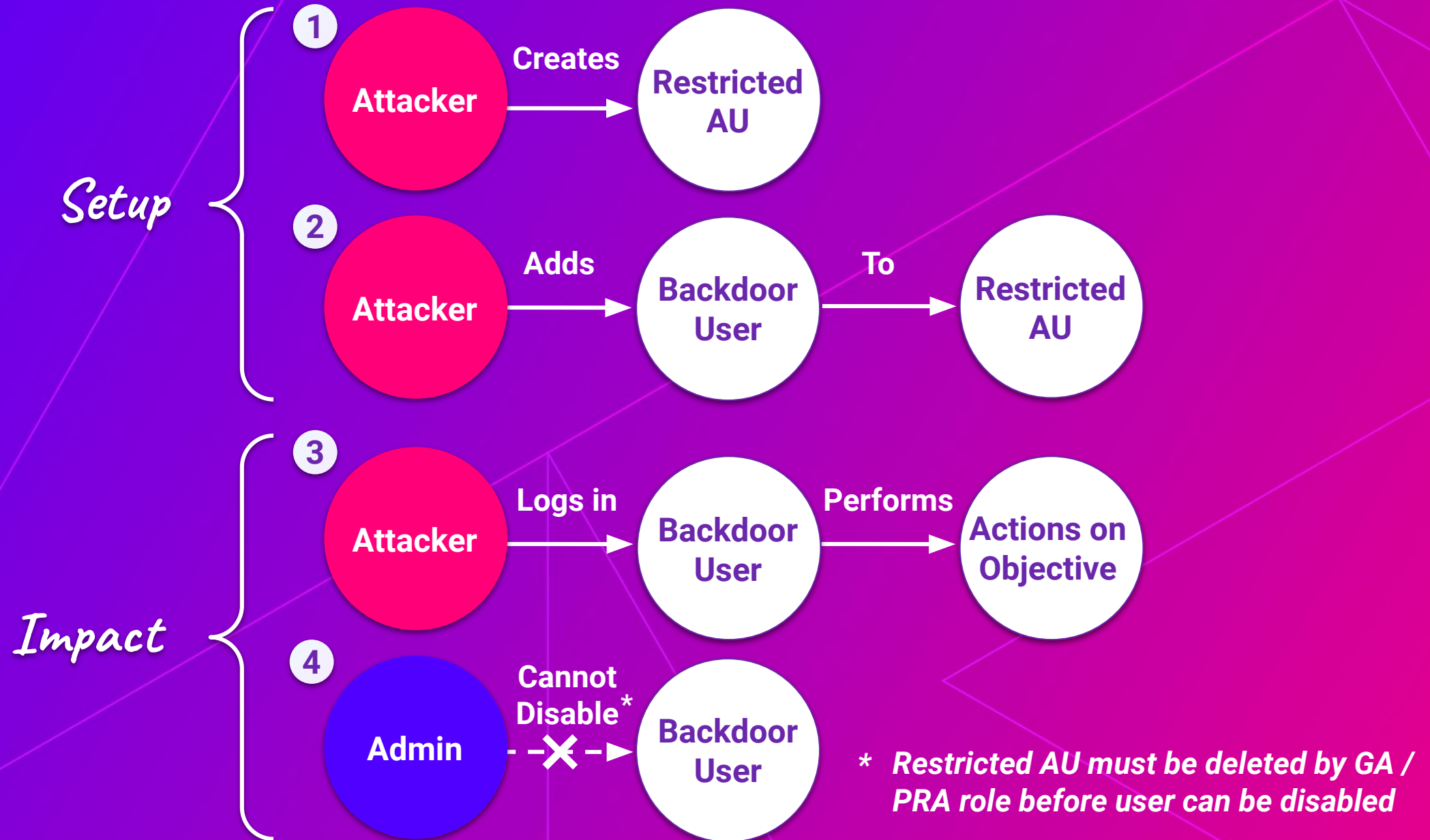
*Free +  
Open Source*

```
15:28:59 $ stratus list
```

View the list of all available attack techniques at: <https://stratus-red-team.cloud/attack-techniques/list/>

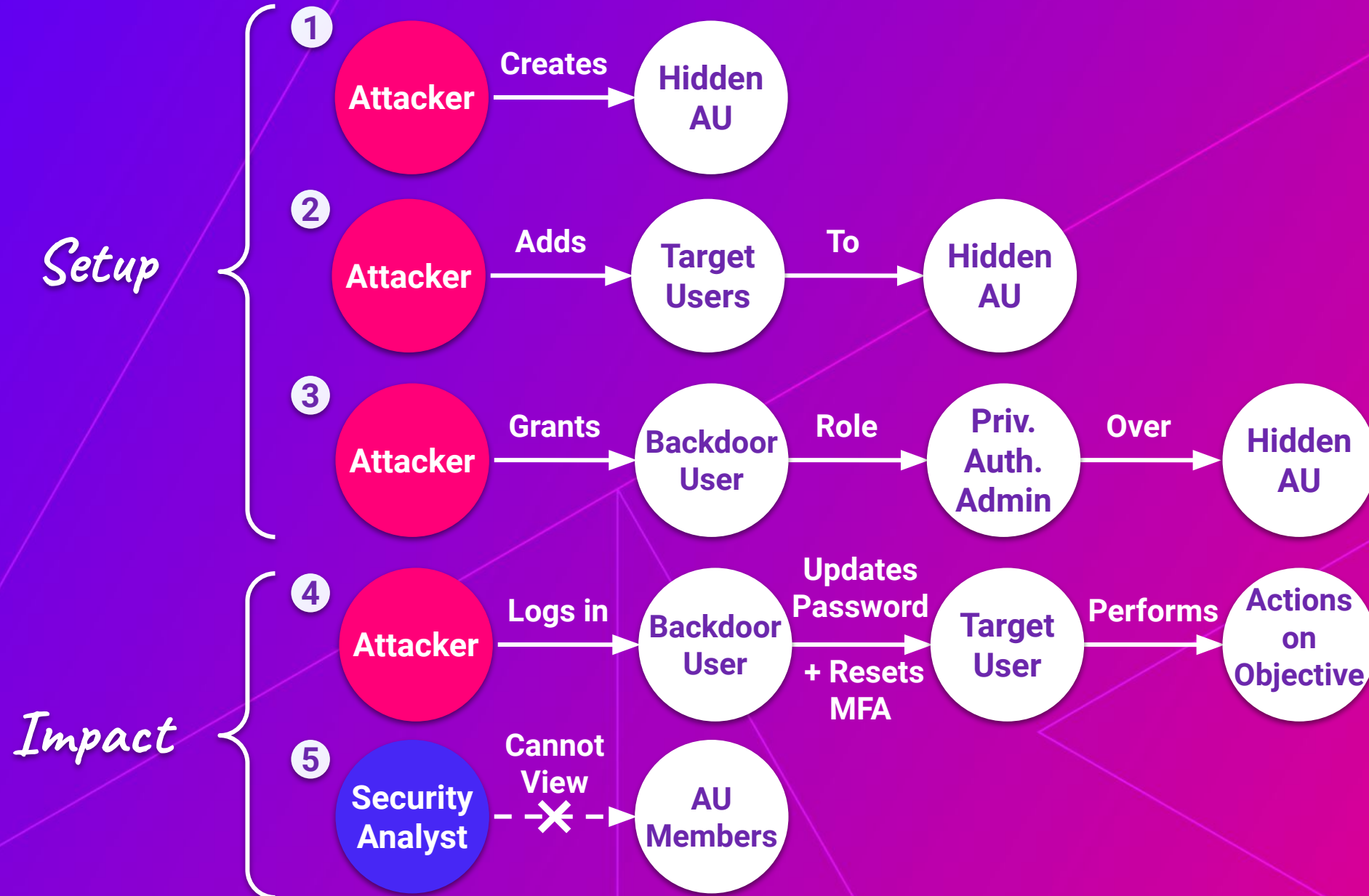
TECHNIQUE ID	TECHNIQUE NAME
aws.credential-access.ec2-get-password-data	Retrieve EC2 Password Data
aws.credential-access.ec2-steal-instance-credentials	Steal EC2 Instance Credentials
aws.credential-access.secretsmanager-batch-retrieve-secrets	Retrieve a High Number of Secrets Manager secrets (Batch)
aws.credential-access.secretsmanager-retrieve-secrets	Retrieve a High Number of Secrets Manager secrets
aws.credential-access.ssm-retrieve-securestring-parameters	Retrieve And Decrypt SSM Parameters
aws.defense-evasion.cloudtrail-delete	Delete CloudTrail Trail
aws.defense-evasion.cloudtrail-event-selectors	Disable CloudTrail Logging Through Event Selectors
aws.defense-evasion.cloudtrail-lifecycle-rule	CloudTrail Logs Impairment Through S3 Lifecycle Rule

# Scenario 1: Restricted AU Backdoor Account



# Restricted AU Demo

# Scenario 2: HiddenMembership AU Role Assignment



# HiddenMembership AU Demo

# Recap: Combining Techniques for Impact





# Administrative Unit **monitoring + remediation**





# Events to Monitor: Entra ID Audit Logs



**Service:** Core Directory

**Category:** AdministrativeUnit

## Event Names:

- Add administrative unit
- Add member to administrative unit
- Add member to restricted management administrative unit
- Bulk add members to administrative unit
- Update administrative unit



**Service:** Core Directory

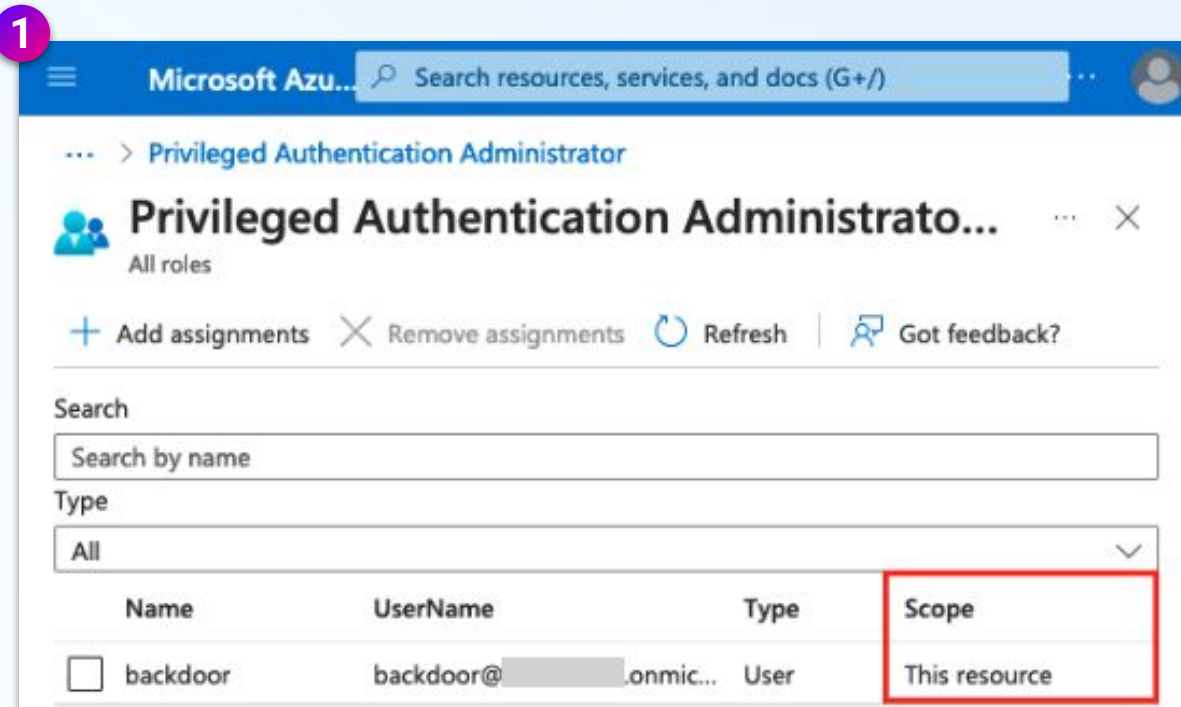
**Category:** RoleManagement

## Event Names:

- Add **scoped** member to role
- Add member to role **scoped** over restricted management administrative unit

# Remediation

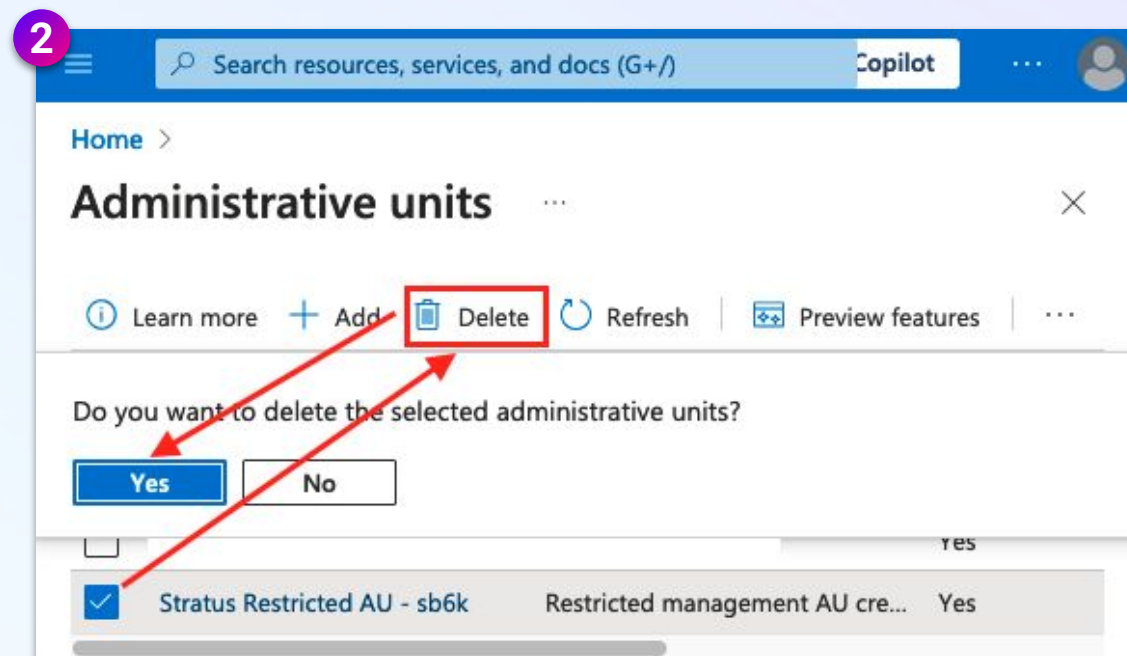
1



Microsoft Azure portal interface showing the **Privileged Authentication Administrator** page. The page displays a table of administrative units. A red box highlights the **Scope** column, which shows **This resource** for the **backdoor** user.

Name	UserName	Type	Scope
<input type="checkbox"/> backdoor	backdoor@...onmic...	User	This resource

2



Microsoft Azure portal interface showing the **Administrative units** page. A red box highlights the **Delete** button. Red arrows indicate the flow from the **Delete** button to the **Yes** button in the confirmation dialog and to the checkbox of the selected administrative unit, **Stratus Restricted AU - sb6k**.

Do you want to delete the selected administrative units?

☒ **Stratus Restricted AU - sb6k** Restricted management AU cre... Yes

# Recap



**Administrative Units (AUs)** allow scoped role assignment of Entra ID roles to a subset of Entra objects.

---



**Restricted management AUs** allow only admins with scoped assignment to manage objects. This feature can protect sensitive accounts. Attackers may abuse this to protect their own accounts.

---



**HiddenMembership AUs** allow only AU members and certain admins to view membership. Attackers may abuse this to conceal which users are impacted by a malicious scoped role assignment.

---



**Monitor AU activities & prepare playbooks:** Review Entra ID Audit logs for "AdministrativeUnit" and "RoleManagement" categories. Prepare administrators to remove or modify malicious AUs.

# Additional Resources



## Administrative Unit Abuse

- Article on Datadog Security Labs: <https://securitylabs.datadoghq.com/articles/abusing-entra-id-administrative-units/>
- Try these techniques in Stratus! <https://github.com/DataDog/stratus-red-team>



## Administrative Units

- <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units>
- <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-restricted-management>
- <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-restricted-management>



## Entra ID + Microsoft Graph Permissions

- ["Directory.ReadWrite.All Is Not As Powerful As You Might Think"](#), Andy Robbins
- ["Tiering Entra roles and application permissions based on known attack paths"](#), Emilien Socchi

# Thank you



**DATADOG**