SPECTEROPS

Abusing AUs, Confusing the SOC

Entra Administrative Unit Attack Paths

Katie Knowles

Cloud Security Researcher, Datadog

Agenda

intro Administrative Units + Scoped Roles

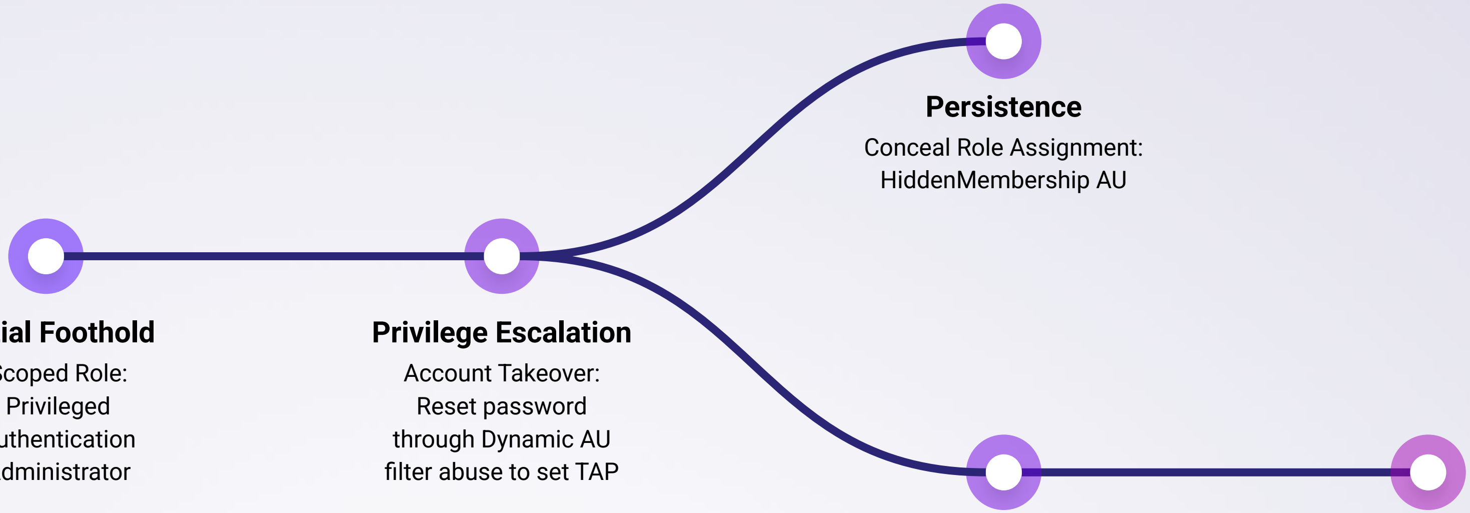
priv esc Dynamic AU Role Assignments

persist HiddenMembership AUs

persist Restricted Management AUs

bug Persistent Restricted Users

Attack Path Overview



Initial Foothold

Scoped Role:
Privileged
Authentication
Administrator

Privilege Escalation

Account Takeover:
Reset password
through Dynamic AU
filter abuse to set TAP

Persistence

Conceal Role Assignment:
HiddenMembership AU

Persistence

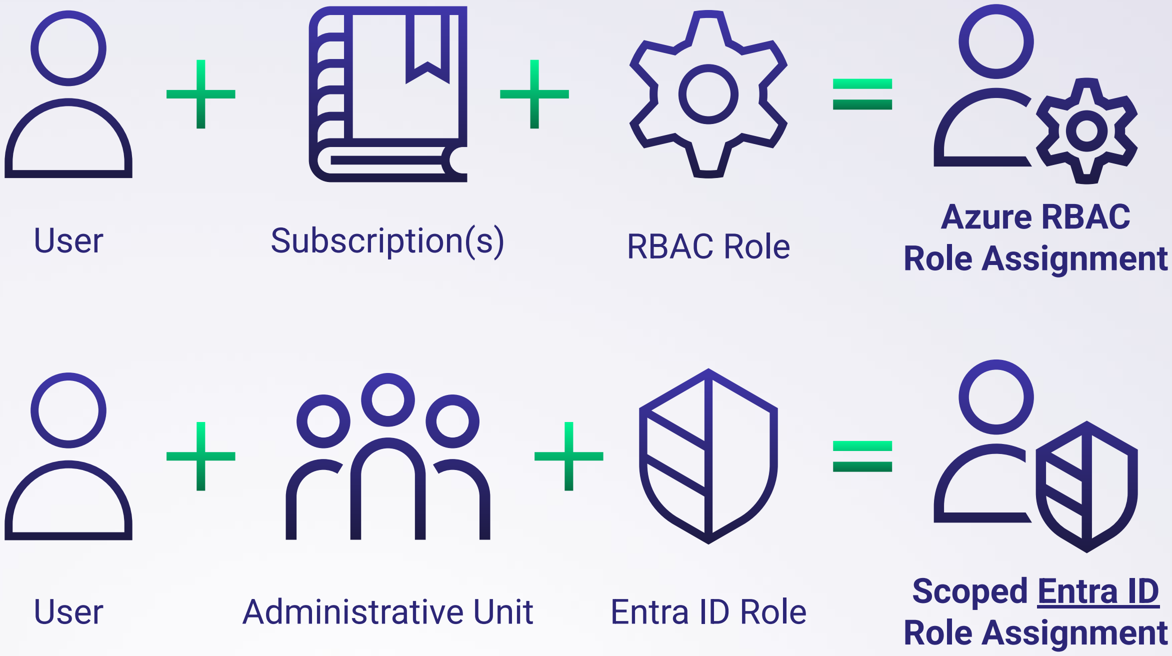
Protect Account:
Restricted
Management AU

Bug

Protect Account:
Eternally Restricted
User Account

Intro to Administrative Units

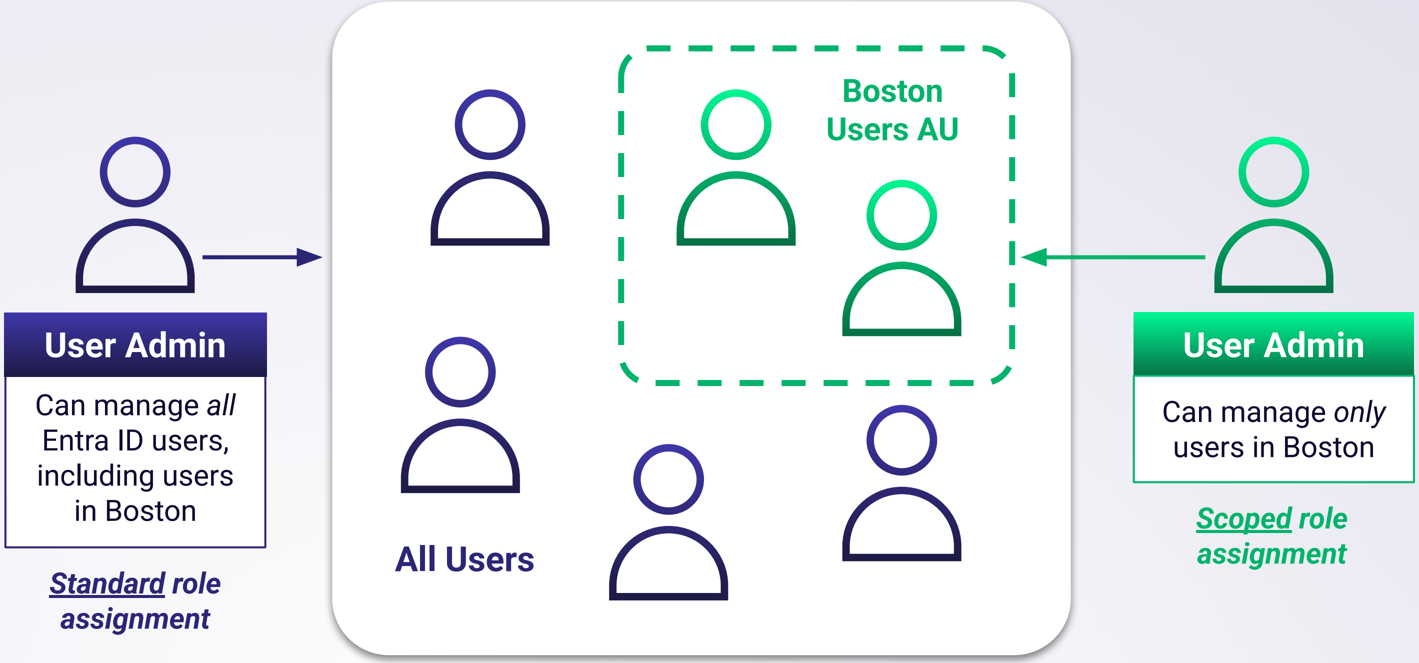
What Are Administrative Units?



User + Subscription(s) + RBAC Role = **Azure RBAC Role Assignment**

User + Administrative Unit + Entra ID Role = **Scoped Entra ID Role Assignment**

Scoped Role Assignments



User Admin

Can manage *all* Entra ID users, including users in Boston

***Standard** role assignment*

Boston Users AU

All Users

User Admin

Can manage *only* users in Boston

***Scoped** role assignment*

Interesting Scoped Role Assignments

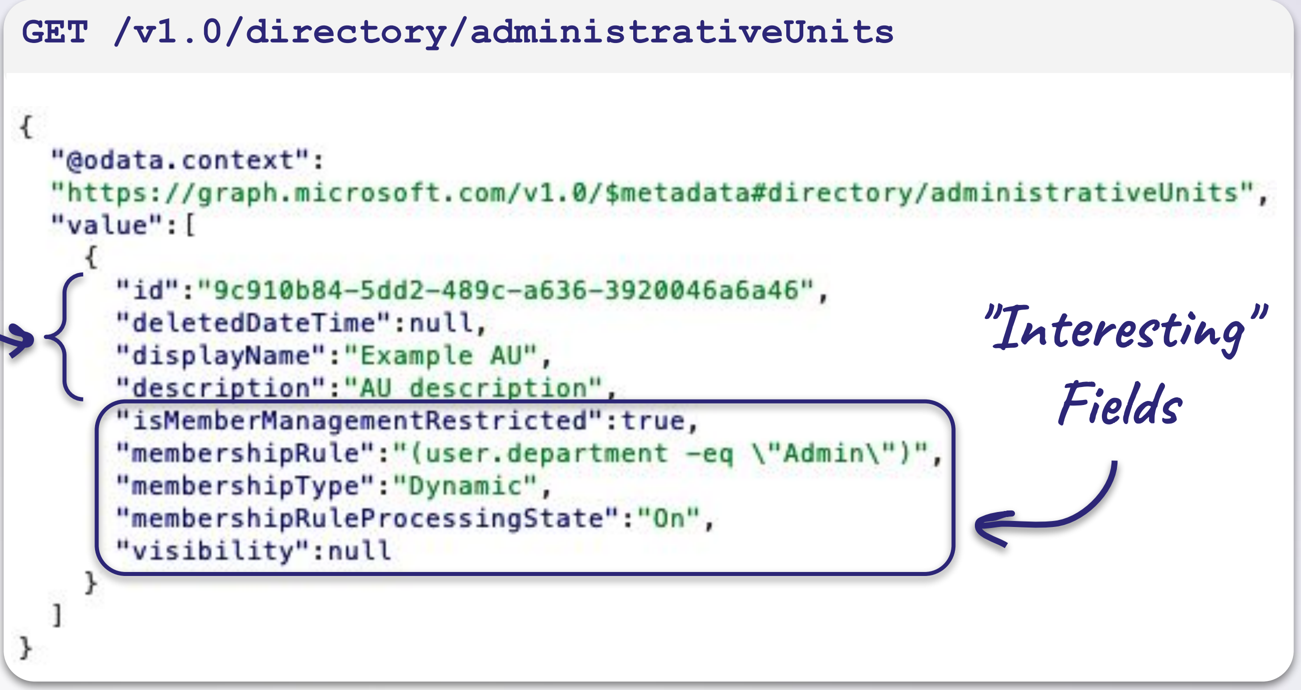
Scoped Role Assignment	Password Reset *	MFA Management *	Manage Groups **	Update Basic User Properties
Privileged Auth. Admin	**Y**	**Y**	N	**Y**
Authentication Admin	Partial	Partial	N	**Y**
Helpdesk Admin	Partial	N	N	N
Password Admin	Partial	N	N	N
User Admin	Partial	N	**M365 + Azure**	**Y**
Groups Admin	N	N	**M365 + Azure**	N
Teams Admin	N	N	M365 Only	N
SharePoint Admin	N	N	M365 Only	N

* Password Reset Details: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/privileged-roles-permissions
https://posts.specterops.io/azure-privilege-escalation-via-service-principal-abuse-210ae2be2a5

** Group Management Details: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-group-permissions
Entra ID role-assignable group modification requires Privileged Role Administrator

Administrative Unit Properties

AU Basics



```
GET /v1.0/directory/administrativeUnits
```

```
{
  "@odata.context":
  "https://graph.microsoft.com/v1.0/$metadata#directory/administrativeUnits",
  "value":[
    {
      "id":"9c910b84-5dd2-489c-a636-3920046a6a46",
      "deletedDateTime":null,
      "displayName":"Example AU",
      "description":"AU description",
      "isMemberManagementRestricted":true,
      "membershipRule":"(user.department -eq \"Admin\")",
      "membershipType":"Dynamic",
      "membershipRuleProcessingState":"On",
      "visibility":null
    }
  ]
}
```

"Interesting" Fields

Attributes of Interest

Dynamic Membership

`membershipRule`,
`membershipType`

Microsoft:

"With dynamic administrative units, you no longer have to manually manage membership of your administrative units. Instead, Azure AD **allows you to specify a query based on user or device attributes**, and then maintains the membership for you."

HiddenMembership

`visibility`

Microsoft:

"Controls whether the administrative unit and its members are hidden or public. When set to HiddenMembership, **only members of the administrative unit can list other members** of the administrative unit."

Restricted Management

`isMemberManagement`
`Restricted`

Microsoft:

"Restricted management administrative units allow you to **protect specific objects in your tenant from modification** by anyone other than a specific set of administrators that you designate."

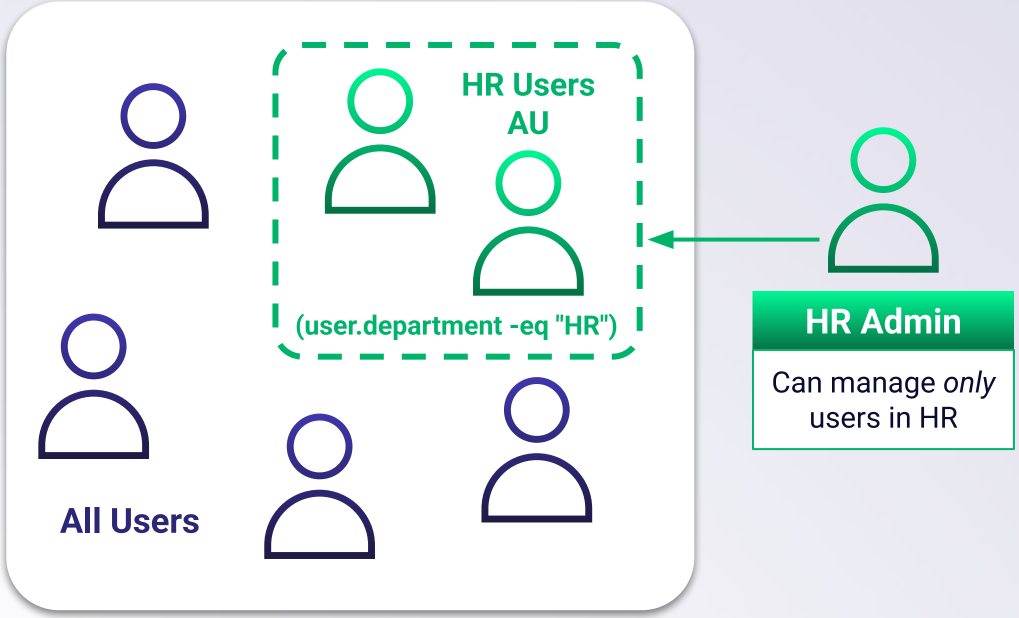
Dynamic Filters

Dynamic Membership

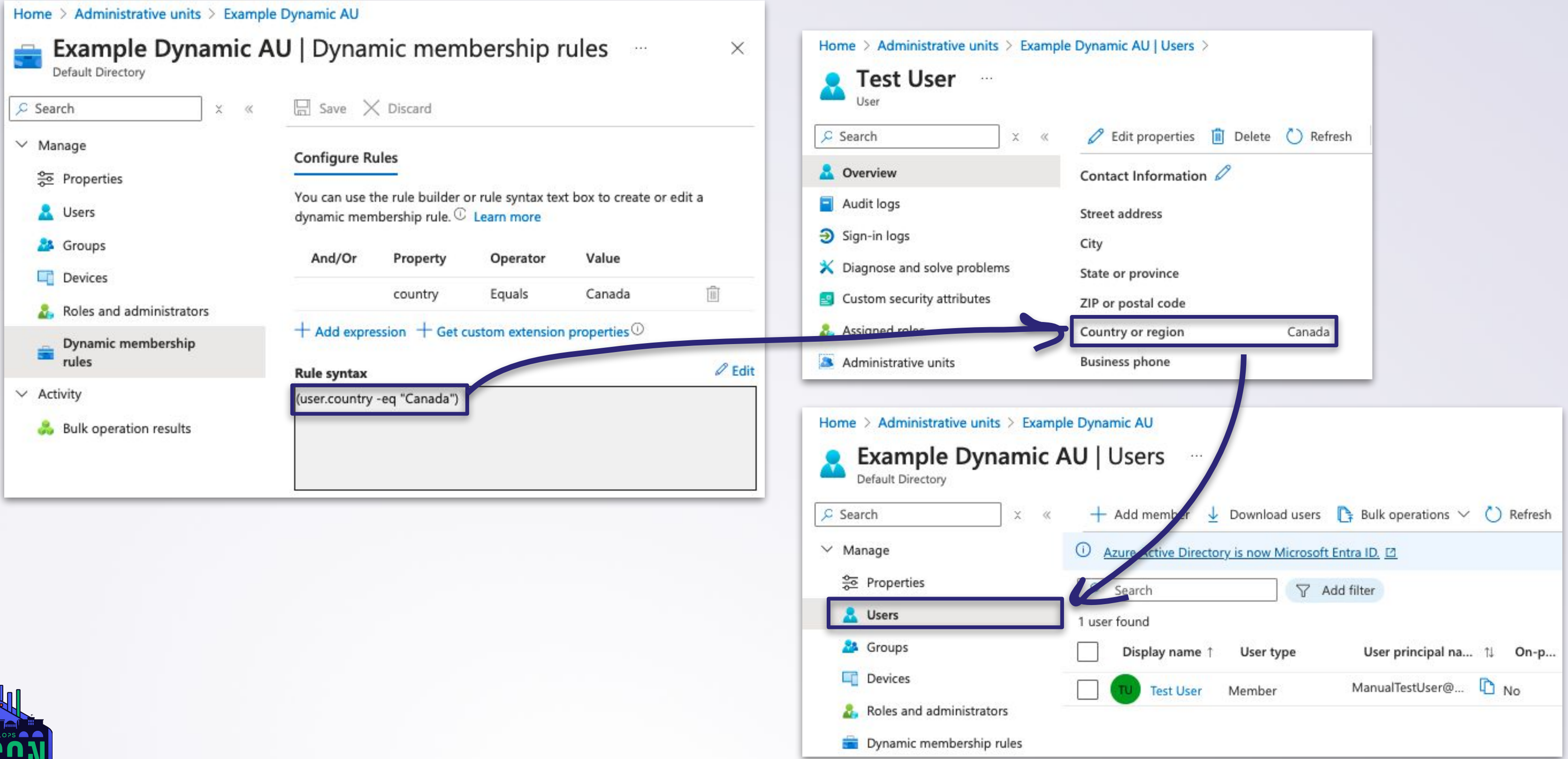
Dynamic Membership AUs use a filter to determine which users are included in an AU

AU filters update regularly to include all users matching their specified filter

Filters on inaccurate properties may lead to administrative scope over unintended users, such as those who have changed departments



Dynamic Membership Behavior



Example Dynamic AU | Dynamic membership rules

Default Directory

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
	country	Equals	Canada

Rule syntax

```
(user.country -eq "Canada")
```

Home > Administrative units > Example Dynamic AU | Users >
Search
Edit properties
Delete
Refresh
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units

Test User

User

Contact Information

Street address

City

State or province

ZIP or postal code

Country or region Canada

Business phone

Example Dynamic AU | Users

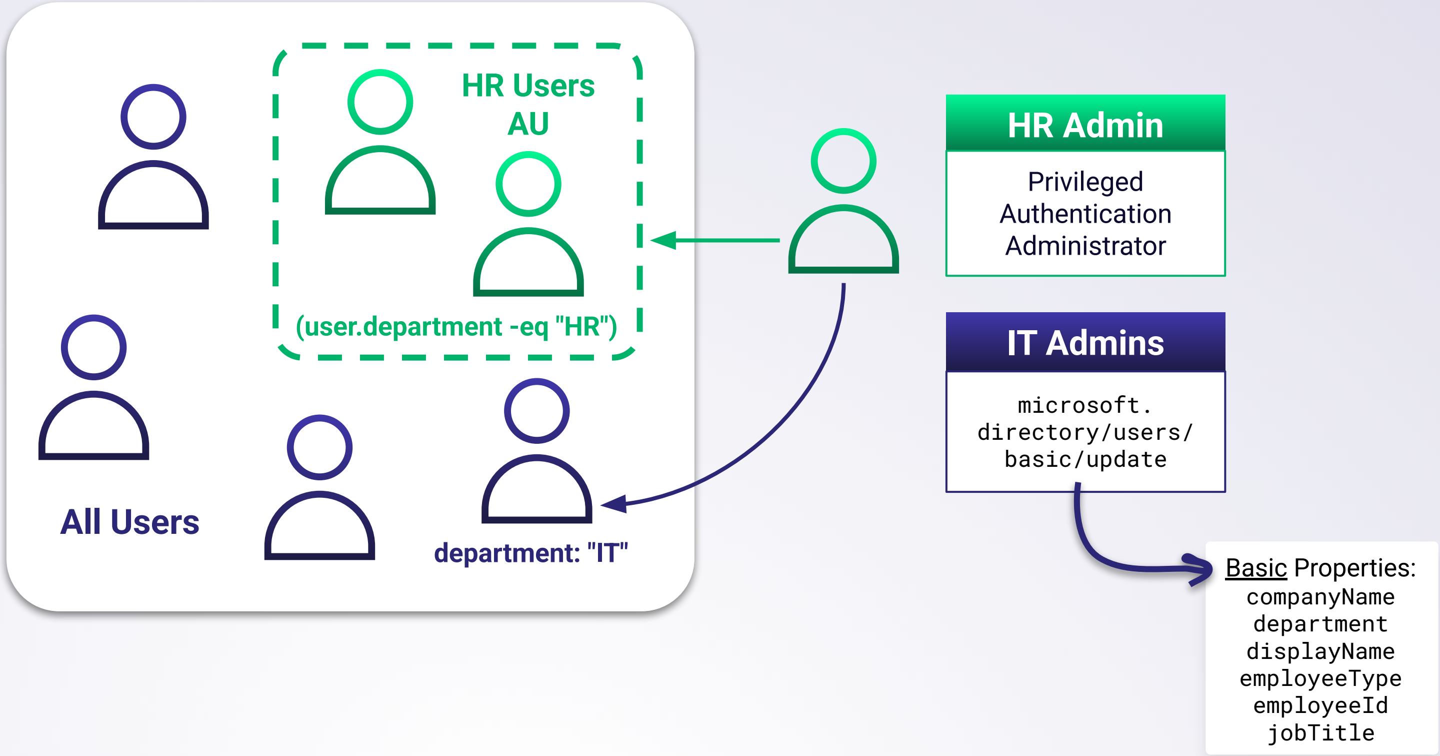
Default Directory

Azure Active Directory is now Microsoft Entra ID.

1 user found

	Display name ↑	User type	User principal na...	On-p...
□	TU Test User	Member	ManualTestUser@...	No

Reframing Filter Impact



HR Users AU

(user.department -eq "HR")

All Users

department: "IT"

HR Admin

Privileged Authentication Administrator

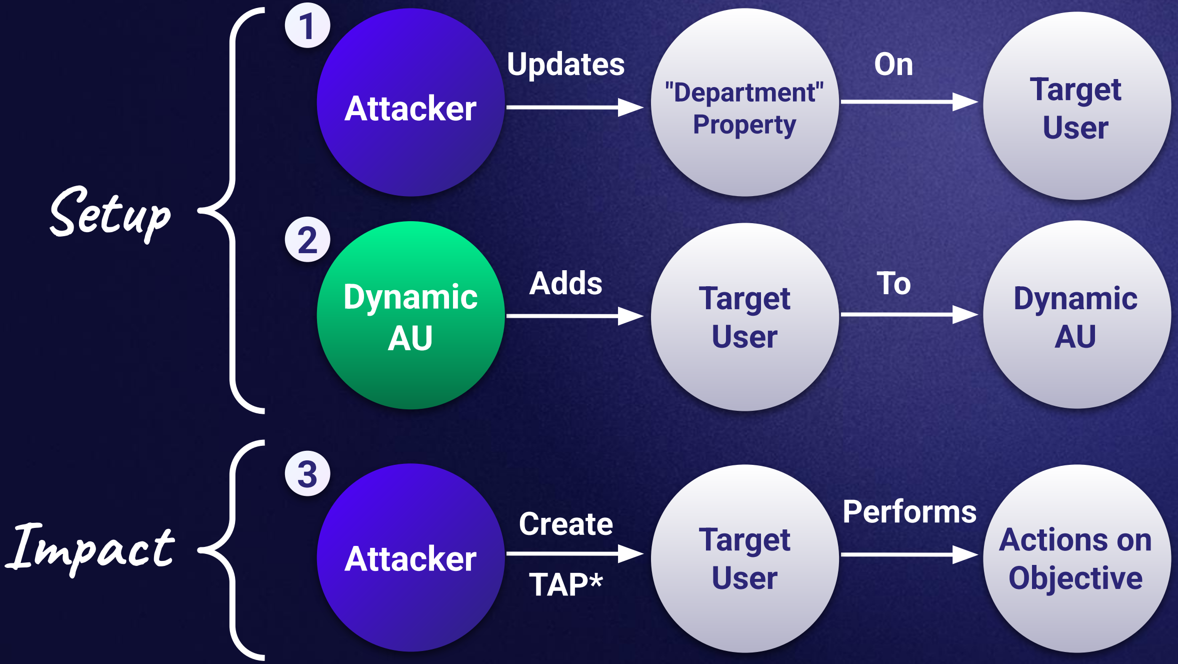
IT Admins

```
microsoft.
directory/users/
basic/update
```

Basic Properties:

```
companyName
department
displayName
employeeType
employeeId
jobTitle
```

Escalating Privileges with Dynamic Membership AUs



** Temporary Access Pass*

Dynamic Membership AU Demo

Hidden Membership

NOTE

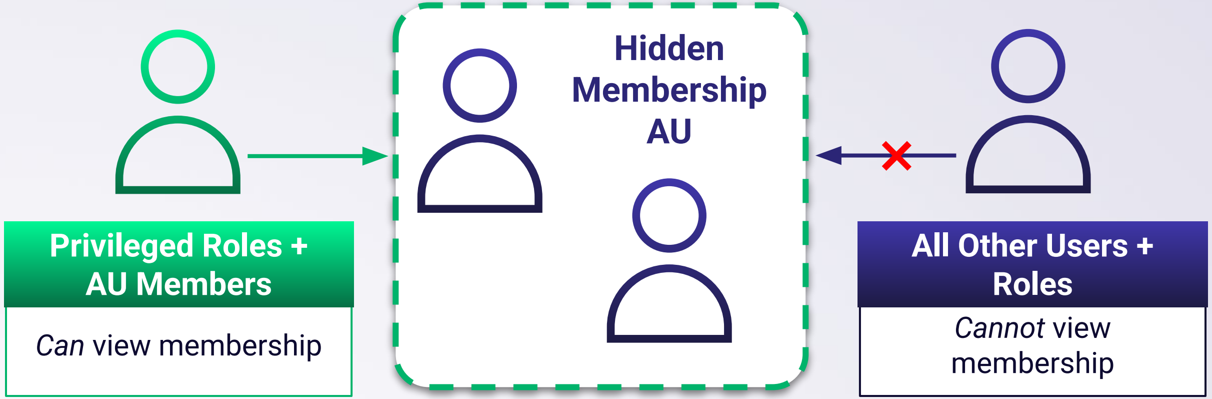
Hidden & Restricted AU scenarios require Global Administrator or Privileged Role Administrator

Hidden Membership

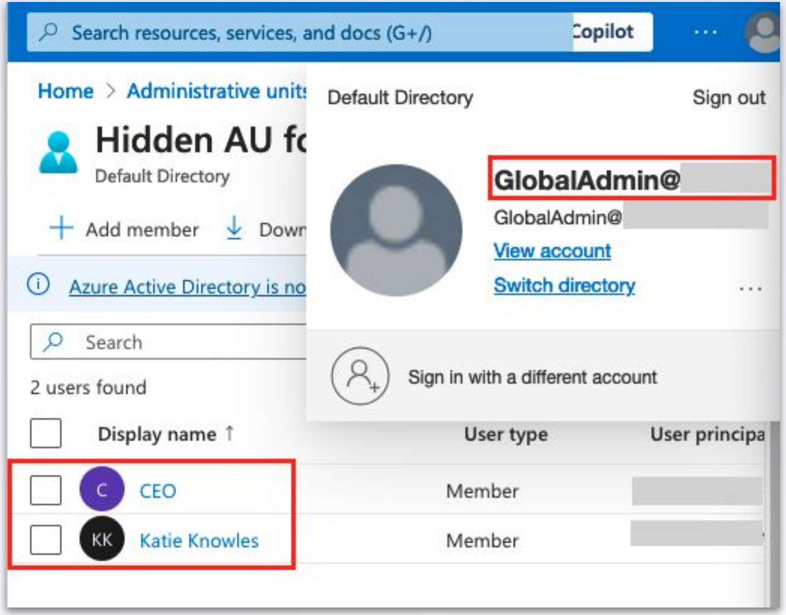
Hidden Membership AU membership can only be viewed by certain privileged roles + AU members

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 calls for AU membership



Hidden Membership Behavior



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

Copilot

Home > Administrative units

Hidden AU fo

Default Directory

+ Add member ↓ Down

Azure Active Directory is no

Search

2 users found

	Display name ↑	User type	User principa
□	C CEO	Member	[redacted]
□	KK Katie Knowles	Member	[redacted]

Default Directory Sign out

GlobalAdmin@[redacted]

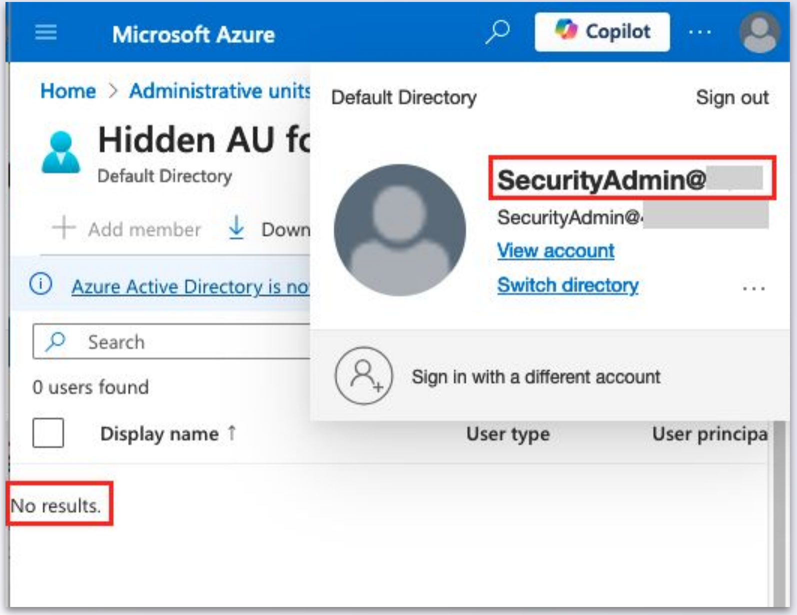
GlobalAdmin@[redacted]

View account

Switch directory

Sign in with a different account

"Can View" Role



Microsoft Azure

Copilot

Home > Administrative units

Hidden AU fo

Default Directory

+ Add member ↓ Down

Azure Active Directory is no

Search

0 users found

	Display name ↑	User type	User principa

No results.

Default Directory Sign out

SecurityAdmin@[redacted]

SecurityAdmin@[redacted]

View account

Switch directory

Sign in with a different account

"Cannot View" Role

Hidden Member "Viewer" Roles

Entra ID Permissions	Associated Built-In Roles
`microsoft.directory/administrativeUnits/allProperties/read`	Global Reader
`microsoft.directory/administrativeUnits/allProperties/allTasks`	Global Administrator Privileged Role Administrator

`microsoft.directory/groups/hiddenMembers/read`
+
`microsoft.directory/administrativeUnits/members/read`
	Groups Administrator
	Teams Administrator
	User Administrator
	SharePoint Administrator
	Helpdesk Administrator
	Authentication Administrator

Microsoft Graph Permissions
`Member.Read.Hidden`
+

Any of:
`AdministrativeUnit.Read.All`
`AdministrativeUnit.ReadWrite.All`
`Directory.Read.All`
`Directory.ReadWrite.All`

RESEARCH SEPTEMBER 16, 2024

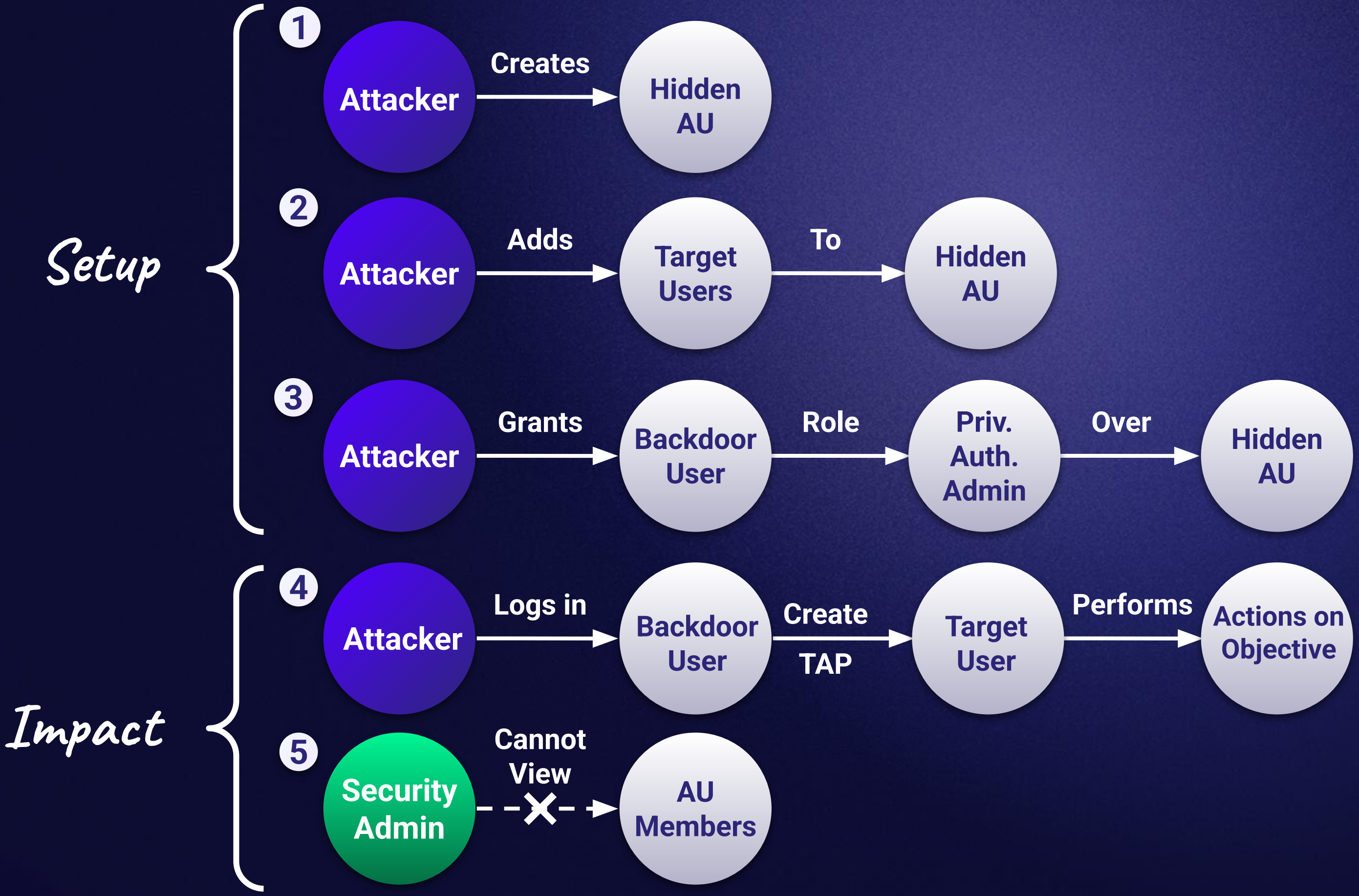
Hidden in Plain Sight: Abusing Entra ID Administrative Units for Sticky Persistence

AZURE

More Details!

Hidden in Plain Sight: https://securitylabs.datadoghq.com/articles/abusing-entra-id-administrative-units/

Concealing Role Scope with Hidden Membership AUs



Setup

1. Attacker → Creates → Hidden AU
2. Attacker → Adds → Target Users → To → Hidden AU
3. Attacker → Grants → Backdoor User → Role → Priv. Auth. Admin → Over → Hidden AU

Impact

4. Attacker → Logs in → Backdoor User → Create TAP → Target User → Performs → Actions on Objective
5. Security Admin → Cannot View → AU Members

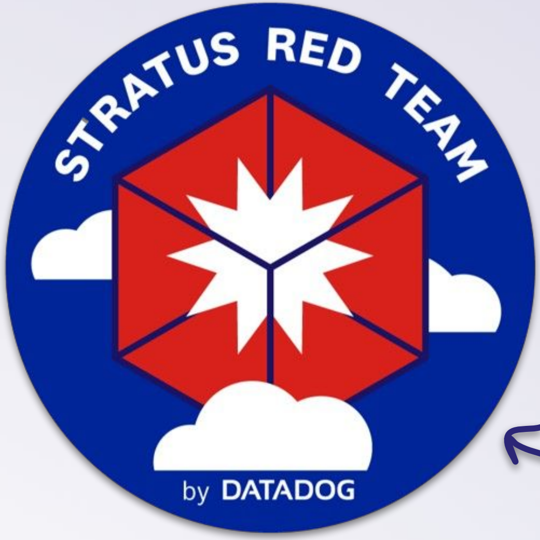
Stratus Red Team

Easily demonstrate offensive cloud techniques and validate detection logic

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

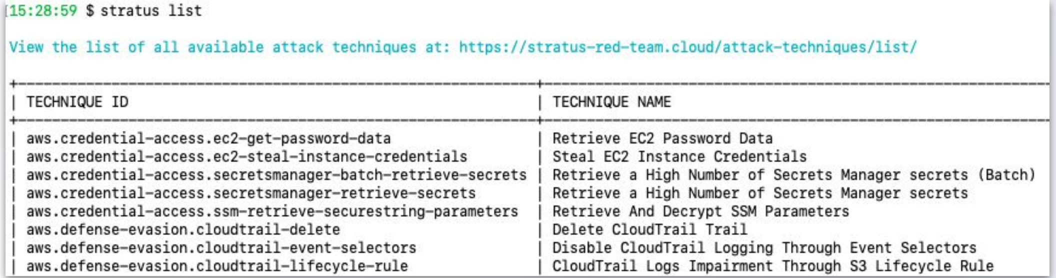
Modular Go + Terraform codebase for easy deployment, cleanup, and new techniques

Contribute new techniques: https://kknowl.es/posts/stratus-contributor/



Free + Open Source

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



```
[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
```

Hidden Membership AU Demo

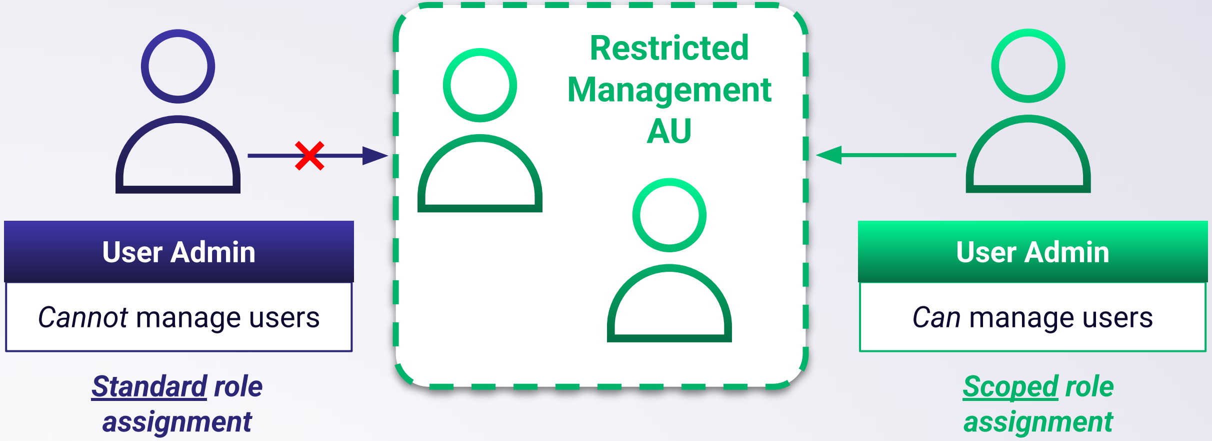
Restricted Management

Restricted Management

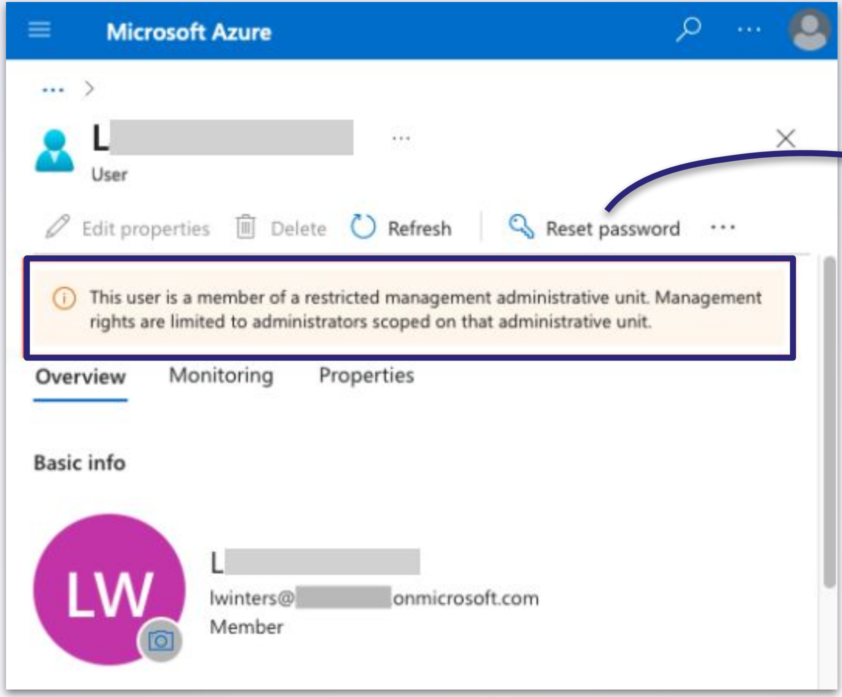
Restricted AU members cannot be modified by tenant scoped roles
(e.g. Global Admin)

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 Behavior



L[redacted]

User

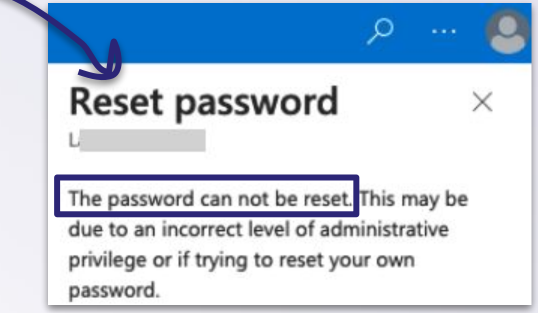
This user is a member of a restricted management administrative unit. Management rights are limited to administrators scoped on that administrative unit.

Basic info

L[redacted]

lwinters@[redacted]onmicrosoft.com

Member



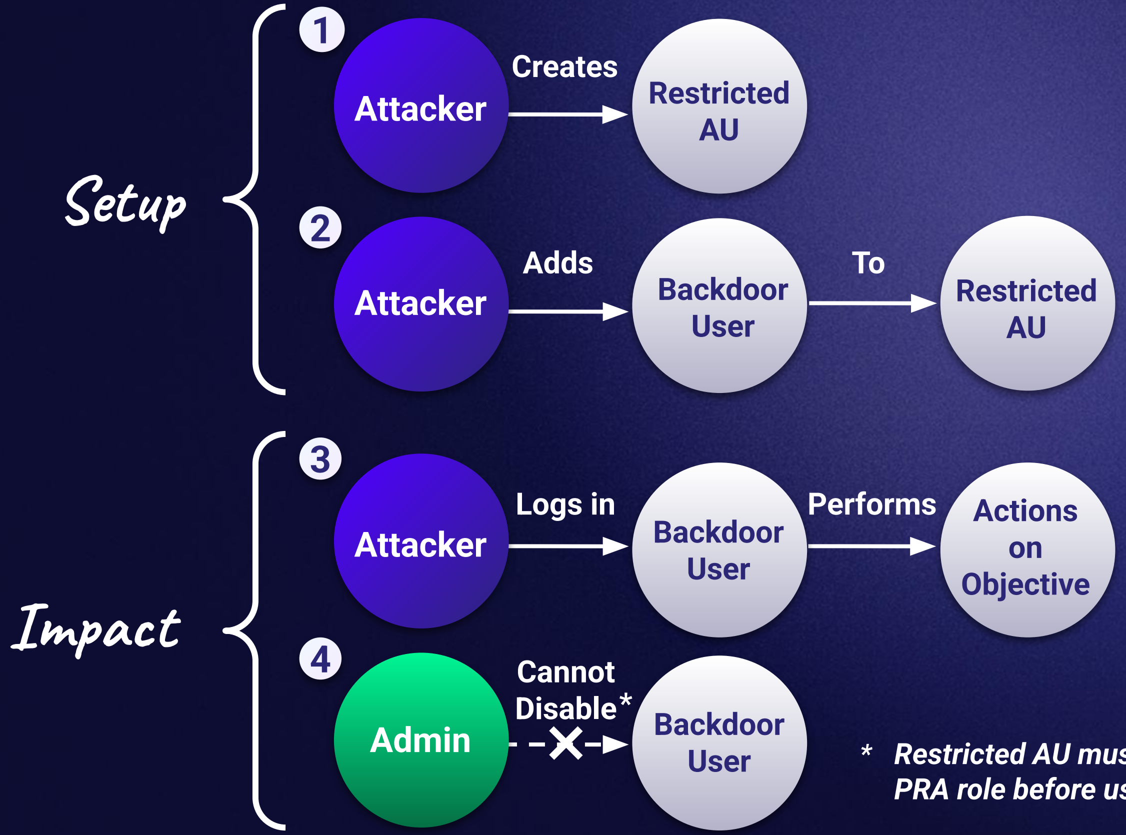
Reset password

L[redacted]

The password can not be reset. This may be due to an incorrect level of administrative privilege or if trying to reset your own password.

View as Global Admin!

Immutable Users with Restricted Management AUs

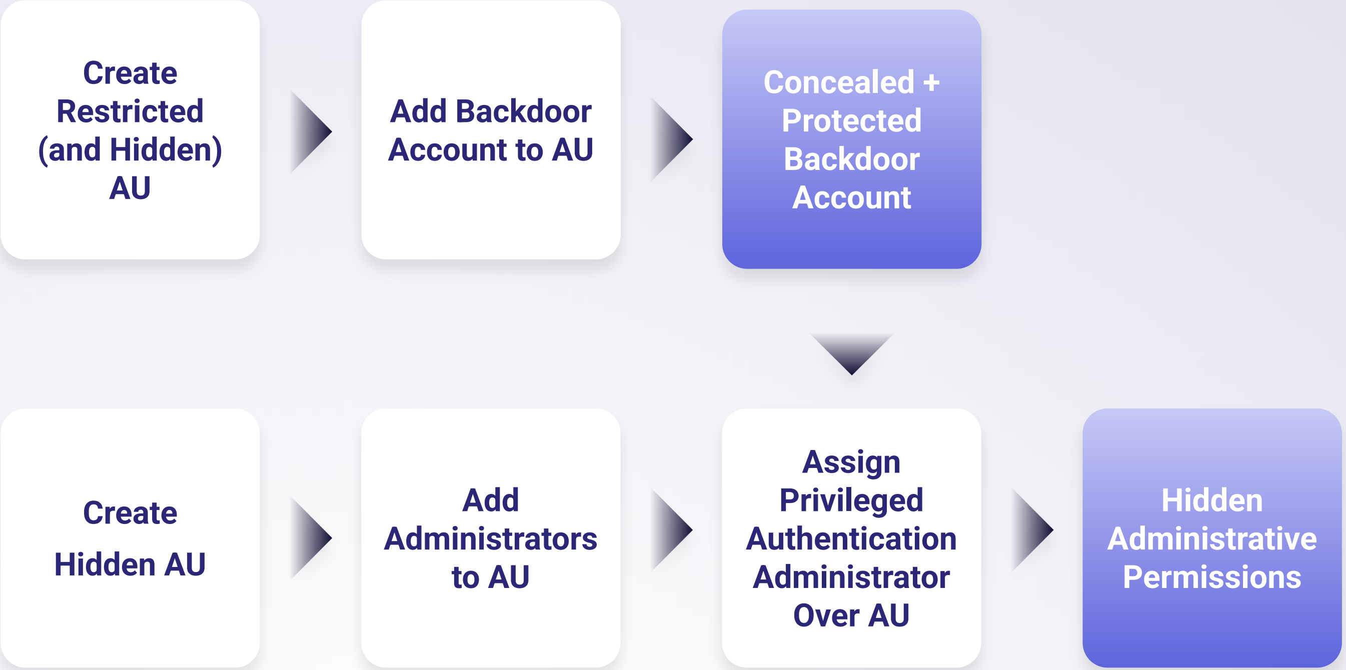


* *Restricted AU must be deleted by GA / PRA role before user can be disabled*

Restricted Management AU Demo

Impact: Confusing the SOC

Combining Techniques for Impact



Create Restricted (and Hidden) AU

Add Backdoor Account to AU

Concealed + Protected Backdoor Account

Create Hidden AU

Add Administrators to AU

Assign Privileged Authentication Administrator Over AU

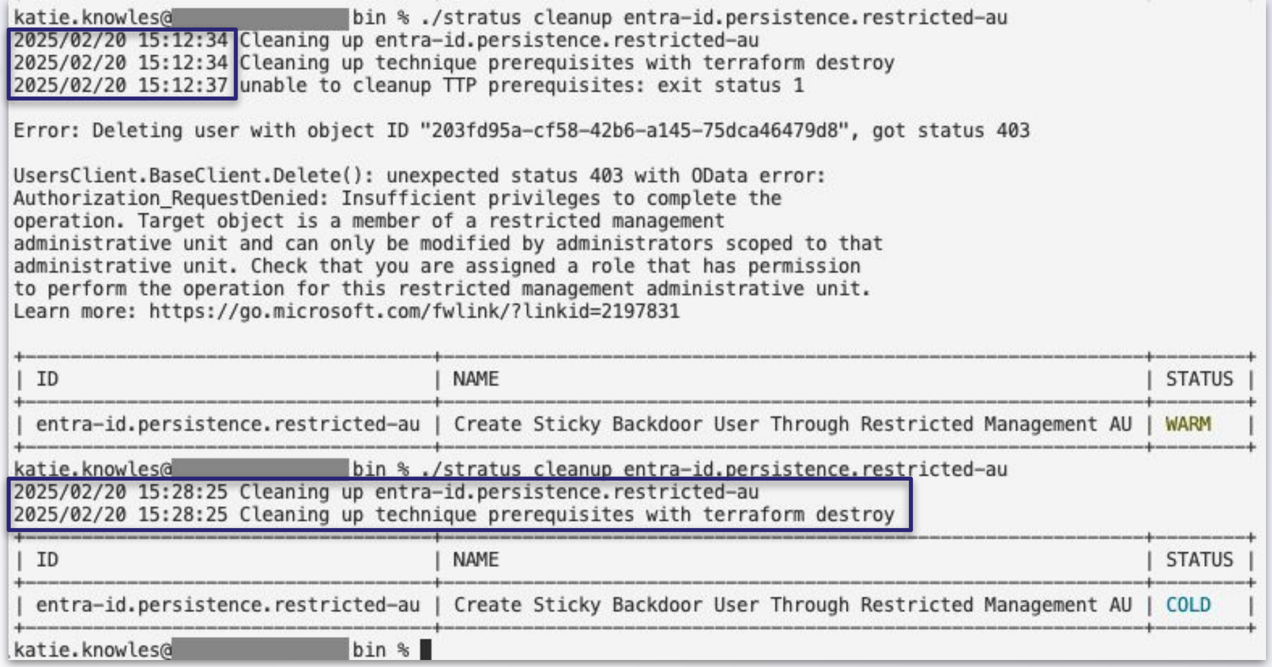
Hidden Administrative Permissions

Investigating Combined Scenario

Eternally Restricted Users

An Unexpected Behavior

Delay in cleanup



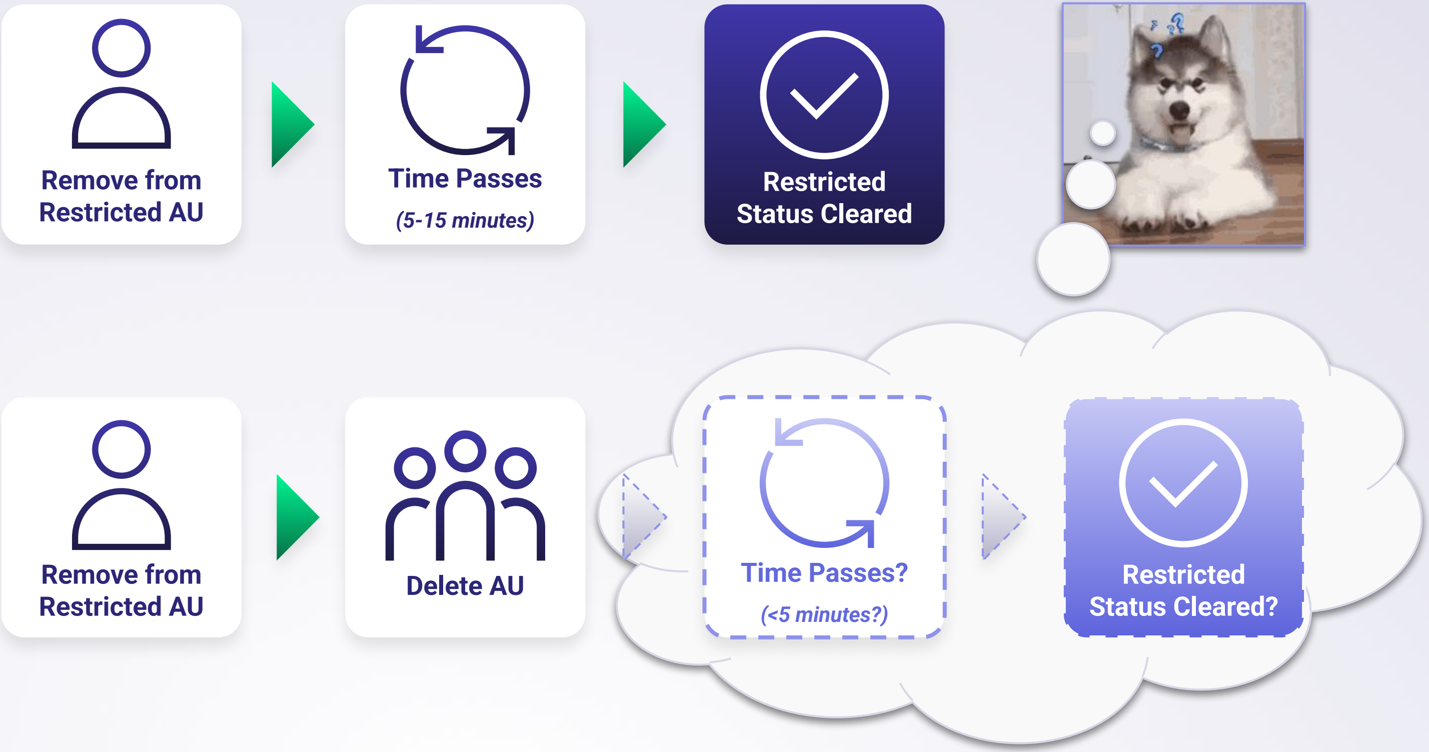
```
katie.knowles@[redacted] bin % ./stratus cleanup entra-id.persistence.restricted-au
2025/02/20 15:12:34 Cleaning up entra-id.persistence.restricted-au
2025/02/20 15:12:34 Cleaning up technique prerequisites with terraform destroy
2025/02/20 15:12:37 unable to cleanup TTP prerequisites: exit status 1

Error: Deleting user with object ID "203fd95a-cf58-42b6-a145-75dca46479d8", got status 403

UsersClient.BaseClient.Delete(): unexpected status 403 with OData error:
Authorization_RequestDenied: Insufficient privileges to complete the
operation. Target object is a member of a restricted management
administrative unit and can only be modified by administrators scoped to that
administrative unit. Check that you are assigned a role that has permission
to perform the operation for this restricted management administrative unit.
Learn more: https://go.microsoft.com/fwlink/?linkid=2197831

+-----------------------------------+--------------------------------------------------------------+--------+
| ID                                | NAME                                                         | STATUS |
+-----------------------------------+--------------------------------------------------------------+--------+
| entra-id.persistence.restricted-au | Create Sticky Backdoor User Through Restricted Management AU | WARM   |
+-----------------------------------+--------------------------------------------------------------+--------+
katie.knowles@[redacted] bin % ./stratus cleanup entra-id.persistence.restricted-au
2025/02/20 15:28:25 Cleaning up entra-id.persistence.restricted-au
2025/02/20 15:28:25 Cleaning up technique prerequisites with terraform destroy
+-----------------------------------+--------------------------------------------------------------+--------+
| ID                                | NAME                                                         | STATUS |
+-----------------------------------+--------------------------------------------------------------+--------+
| entra-id.persistence.restricted-au | Create Sticky Backdoor User Through Restricted Management AU | COLD   |
+-----------------------------------+--------------------------------------------------------------+--------+
katie.knowles@[redacted] bin %
```

Trying A Different Approach



Remove from Restricted AU

Time Passes

(5-15 minutes)

Restricted Status Cleared

Remove from Restricted AU

Delete AU

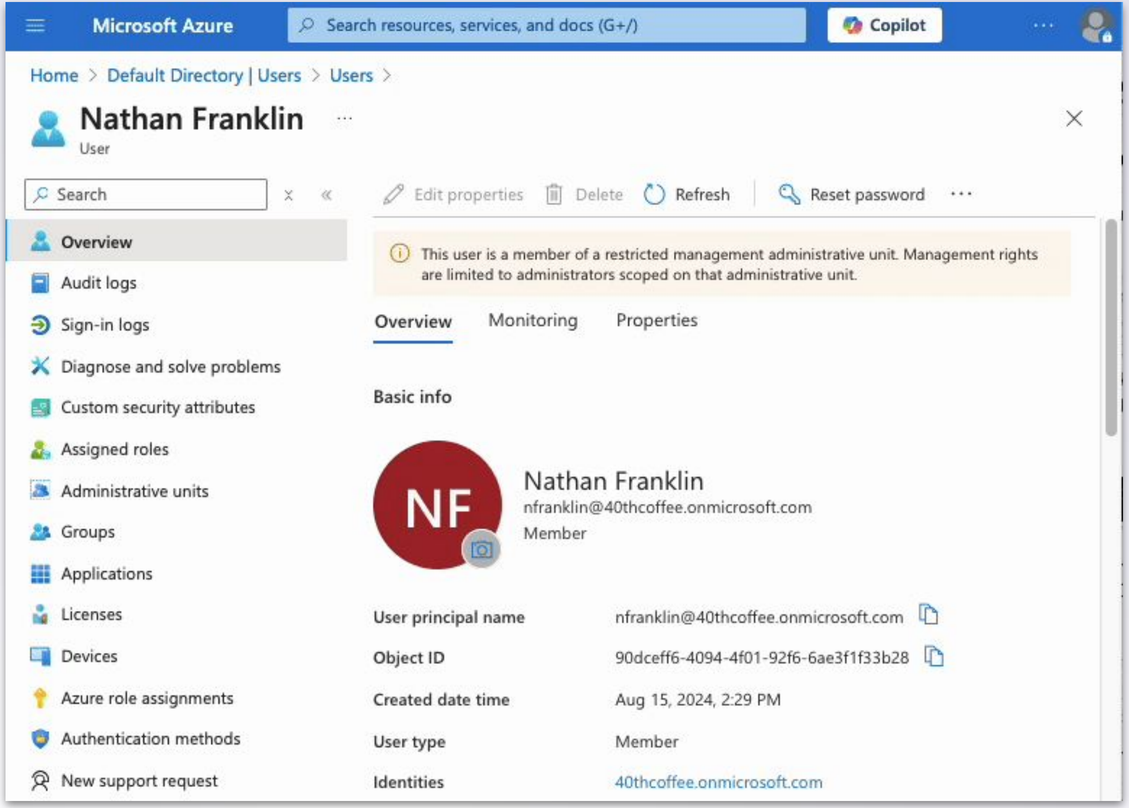
Time Passes?

(<5 minutes?)

Restricted Status Cleared?

Restricted User Demo

A Really Unexpected Behavior



Nathan Franklin
User

This user is a member of a restricted management administrative unit. Management rights are limited to administrators scoped on that administrative unit.

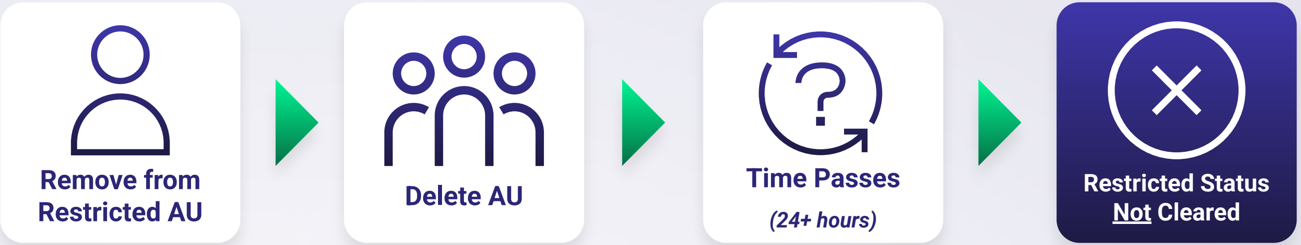
Basic info

Nathan Franklin
nfranklin@40thcoffee.onmicrosoft.com
Member

User principal name	nfranklin@40thcoffee.onmicrosoft.com
Object ID	90dceff6-4094-4f01-92f6-6ae3f1f33b28
Created date time	Aug 15, 2024, 2:29 PM
User type	Member
Identities	40thcoffee.onmicrosoft.com

Recap: AU Timing Bug

Create Restricted User:



Remove from Restricted AU

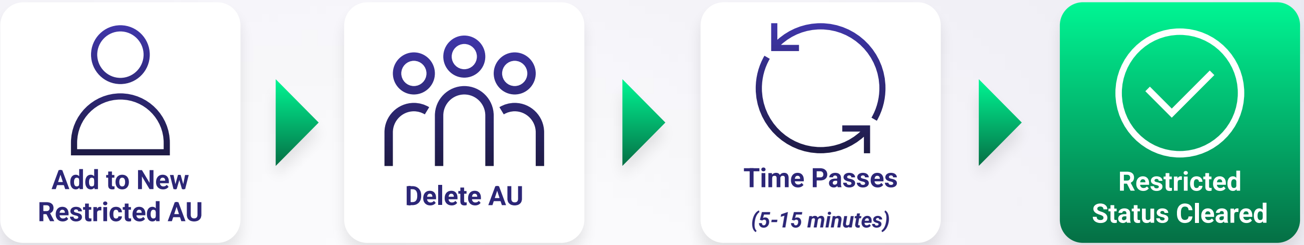
Delete AU

Time Passes

(24+ hours)

Restricted Status Not Cleared

Remediate Restricted User:



Add to New Restricted AU

Delete AU

Time Passes

(5-15 minutes)

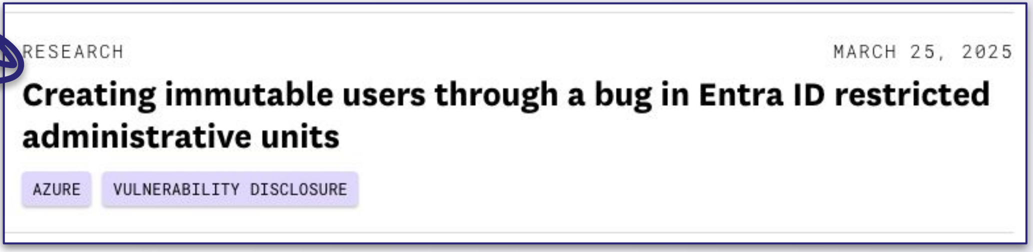
Restricted Status Cleared

Disclosure

Assessed as moderate severity security feature bypass by MSRC, bug based on how AU state is handled

Remediated by Microsoft on February 22, 2025

Full details & timeline available in our post "Creating immutable users with Entra ID's administrative units"



RESEARCH

MARCH 25, 2025

Creating immutable users through a bug in Entra ID restricted administrative units

AZURE

VULNERABILITY DISCLOSURE

https://securitylabs.datadoghq.com/articles/creating-immutable-users-entra-id-administrative-units/

Detection + Remediation

AU Monitoring

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

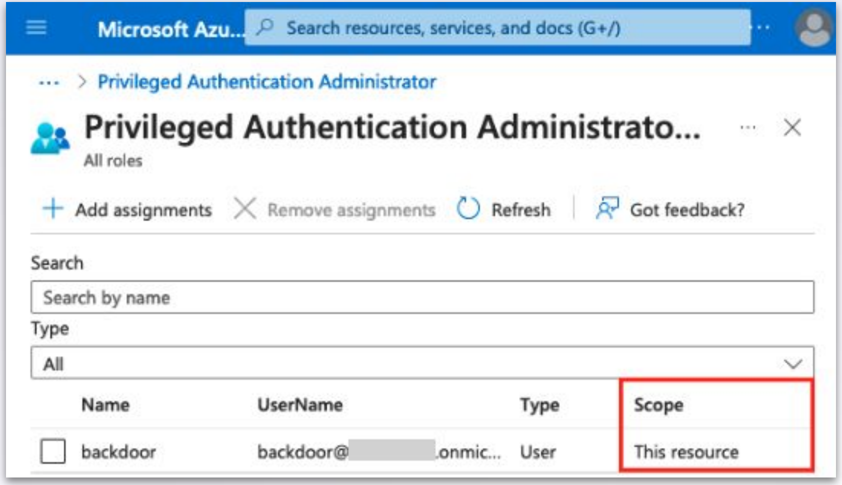
Event Names:

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

https://securitylabs.datadoghq.com/articles/abusing-entra-id-administrative-units
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-audit-activities

AU Remediation

1 Review scoped role assignment(s)


Microsoft Azu...
Search resources, services, and docs (G+/)
... > Privileged Authentication Administrator
Add assignments
Remove assignments
Refresh
Got feedback?

Privileged Authentication Administrato...

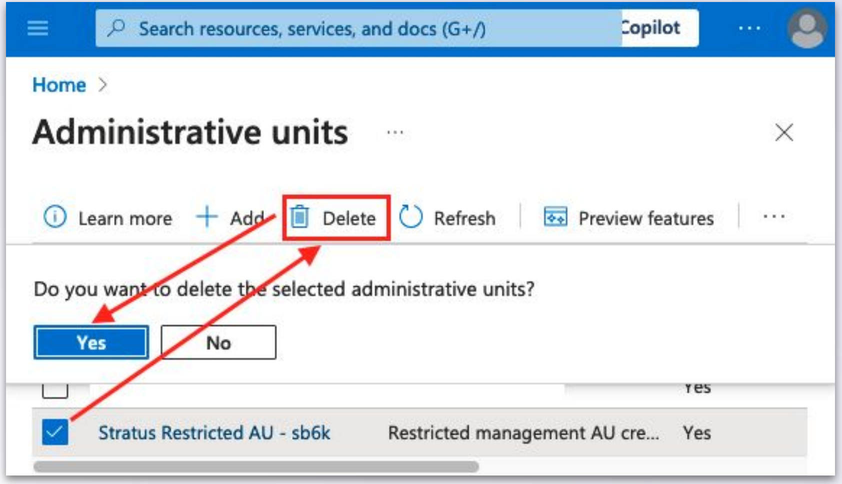
All roles

Search: Search by name

Type: All

	Name	UserName	Type	Scope
□	backdoor	backdoor@[redacted].onmic...	User	This resource

2 Delete AU *



Administrative units

Do you want to delete the selected administrative units?

□			Yes
☑	Stratus Restricted AU - sb6k	Restricted management AU cre...	Yes

* *With Global Administrator or Privileged Role Administrator role*

Recap: Using & Abusing AUs

Dynamic Membership AUs

Add members dynamically to an AU based on a specified filter. Attackers may target non-privileged user properties to expand the scope of users included in an AU.

Hidden Membership AUs

Allows only AU members and certain admins to view membership. Attackers may abuse this to conceal which users are included in a scoped role assignment.

Restricted Management AUs

Allows only admins with scoped assignment to manage objects. This feature can protect sensitive accounts, or by attackers to protect their own accounts.

Monitor AU activities

Review Entra ID Audit logs for Administrative Unit activities and role assignments. Consider Global Reader. Discuss how to undo malicious AU activities with administrators.

SPECTEROPS

Thank you

Katie Knowles | Security Researcher, Datadog

@_sigil | **/in/kaknowles** | **kknowl.es**