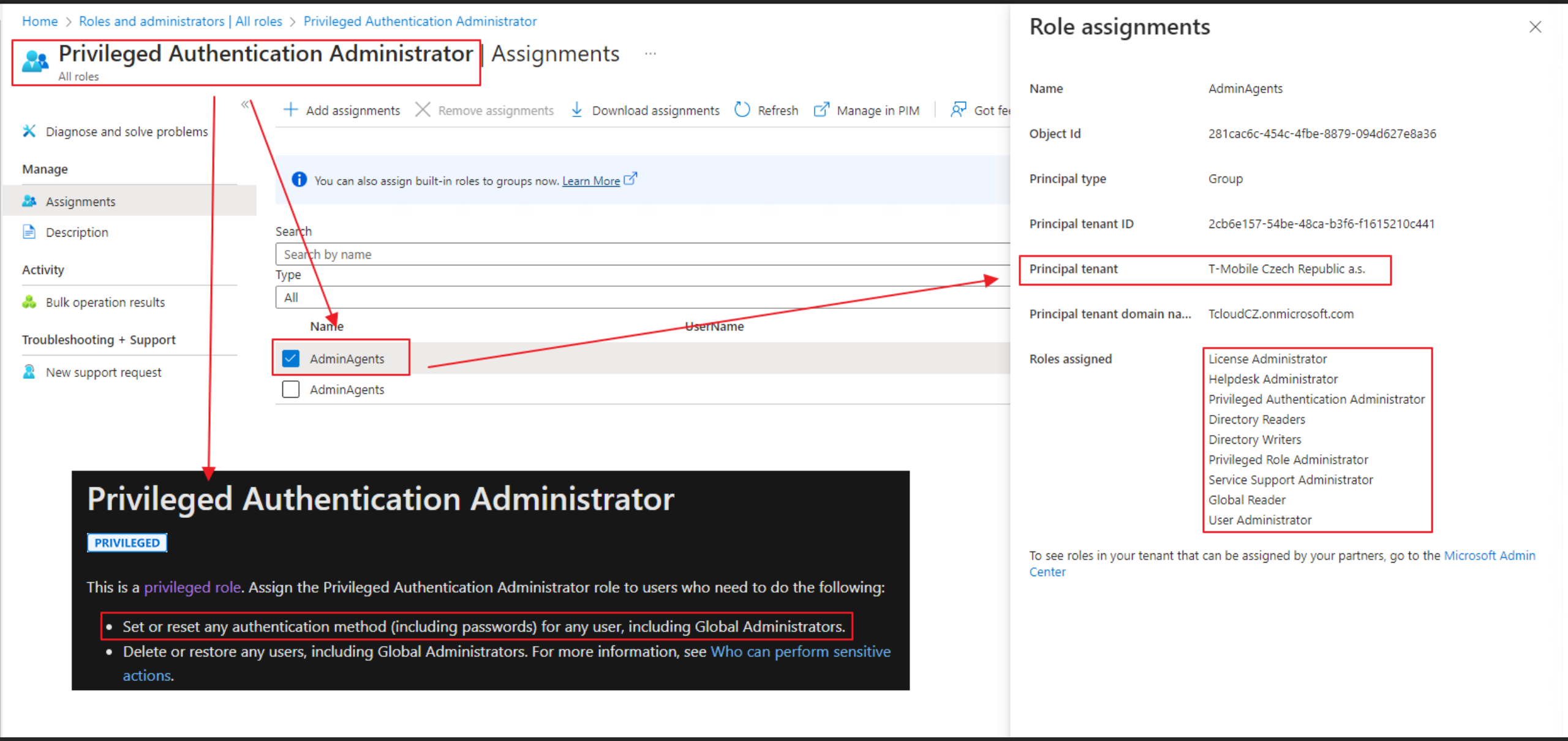
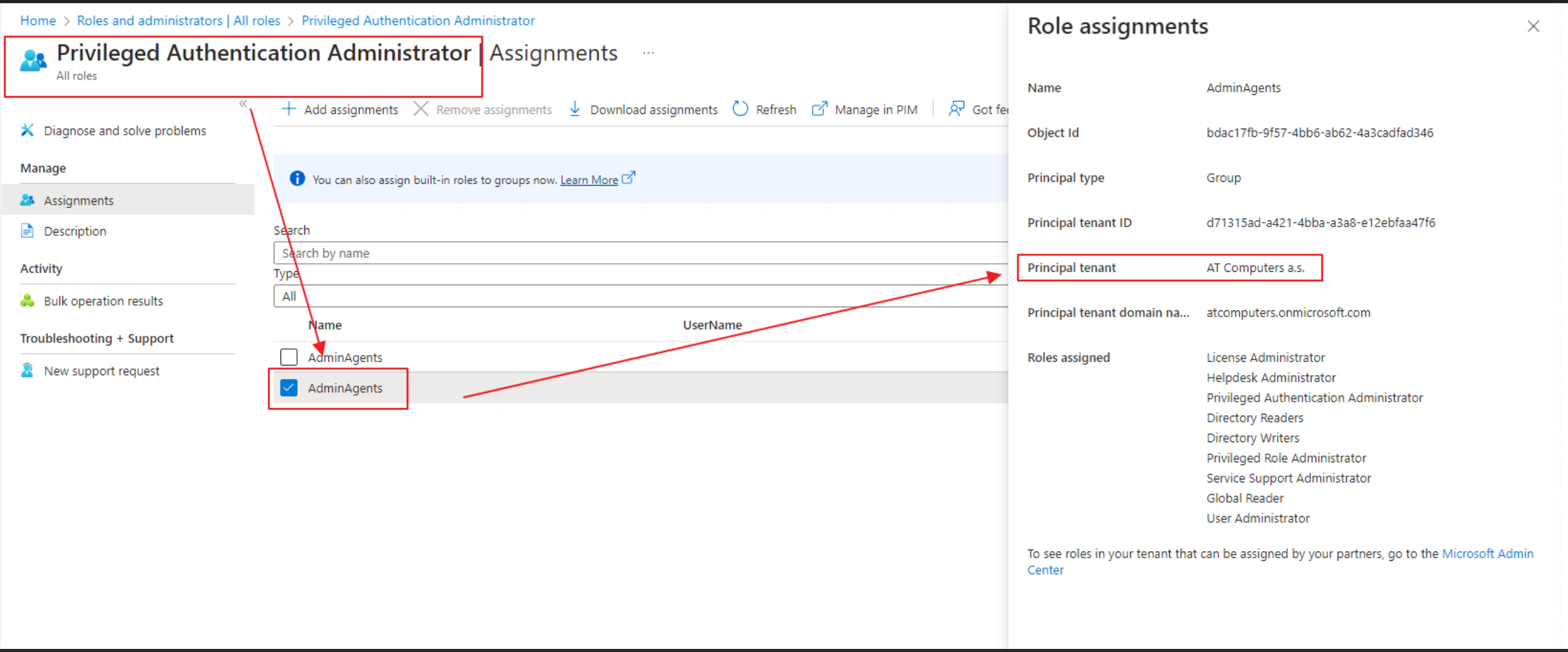
Martin Haller

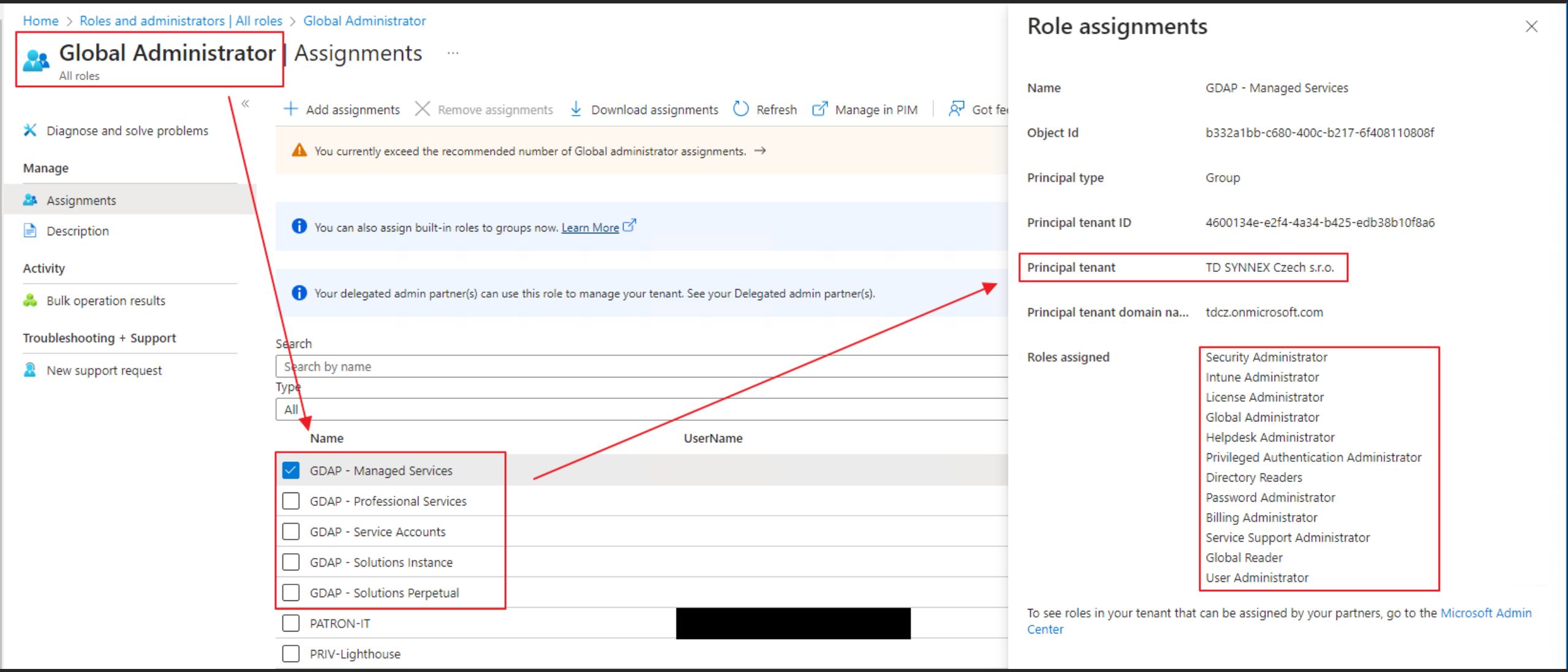
⟨Jak na delegovanou správu Office/Microsoft 365⟩

TD SYNNEX

PATRON ⟨IT⟩ OCHRANA A SPRÁVA SÍTÍ


Home > Roles and administrators | All roles > Privileged Authentication Administrator
Privileged Authentication Administrator | Assignments
All roles
Add assignments
Remove assignments
Download assignments
Refresh
Manage in PIM
Got fe
Diagnose and solve problems
Manage
Assignments
Description
Activity
Bulk operation results
Troubleshooting + Support
New support request
You can also assign built-in roles to groups now. Learn More
Search
Search by name
Type
All
Name
UserName
AdminAgents
AdminAgents
Privileged Authentication Administrator
PRIVILEGED
This is a privileged role. Assign the Privileged Authentication Administrator role to users who need to do the following:
Set or reset any authentication method (including passwords) for any user, including Global Administrators.
Delete or restore any users, including Global Administrators. For more information, see Who can perform sensitive actions.
Role assignments
Name
AdminAgents
Object Id
281cac6c-454c-4fbe-8879-094d627e8a36
Principal type
Group
Principal tenant ID
2cb6e157-54be-48ca-b3f6-f1615210c441
Principal tenant
T-Mobile Czech Republic a.s.
Principal tenant domain na...
TcloudCZ.onmicrosoft.com
Roles assigned
License Administrator
Helpdesk Administrator
Privileged Authentication Administrator
Directory Readers
Directory Writers
Privileged Role Administrator
Service Support Administrator
Global Reader
User Administrator
To see roles in your tenant that can be assigned by your partners, go to the Microsoft Admin Center


Home > Roles and administrators | All roles > Privileged Authentication Administrator
Privileged Authentication Administrator | Assignments
All roles
Add assignments
Remove assignments
Download assignments
Refresh
Manage in PIM
Got fe
Diagnose and solve problems
Manage
Assignments
Description
Activity
Bulk operation results
Troubleshooting + Support
New support request
You can also assign built-in roles to groups now. Learn More
Search
Search by name
Type
All
Name
UserName
AdminAgents
AdminAgents
Role assignments
Name
AdminAgents
Object Id
bdac17fb-9f57-4bb6-ab62-4a3cadfad346
Principal type
Group
Principal tenant ID
d71315ad-a421-4bba-a3a8-e12ebfaa47f6
Principal tenant
AT Computers a.s.
Principal tenant domain na...
atcomputers.onmicrosoft.com
Roles assigned
License Administrator
Helpdesk Administrator
Privileged Authentication Administrator
Directory Readers
Directory Writers
Privileged Role Administrator
Service Support Administrator
Global Reader
User Administrator
To see roles in your tenant that can be assigned by your partners, go to the Microsoft Admin Center


Home > Roles and administrators | All roles > Global Administrator
Global Administrator | Assignments
All roles
Diagnose and solve problems
Manage
Assignments
Description
Activity
Bulk operation results
Troubleshooting + Support
New support request
Add assignments
Remove assignments
Download assignments
Refresh
Manage in PIM
You currently exceed the recommended number of Global administrator assignments.
You can also assign built-in roles to groups now. Learn More
Your delegated admin partner(s) can use this role to manage your tenant. See your Delegated admin partner(s).
Search
Search by name
Type
All
Name
UserName
GDAP - Managed Services
GDAP - Professional Services
GDAP - Service Accounts
GDAP - Solutions Instance
GDAP - Solutions Perpetual
PATRON-IT
PRIV-Lighthouse
Role assignments
Name
GDAP - Managed Services
Object Id
b332a1bb-c680-400c-b217-6f408110808f
Principal type
Group
Principal tenant ID
4600134e-e2f4-4a34-b425-edb38b10f8a6
Principal tenant
TD SYNNEX Czech s.r.o.
Principal tenant domain na...
tdcz.onmicrosoft.com
Roles assigned
Security Administrator
Intune Administrator
License Administrator
Global Administrator
Helpdesk Administrator
Privileged Authentication Administrator
Directory Readers
Password Administrator
Billing Administrator
Service Support Administrator
Global Reader
User Administrator
To see roles in your tenant that can be assigned by your partners, go to the Microsoft Admin Center

Riziko pro zákazníka i partnera

Zdroj: https://martinhaller.cz/bezpecnost/kacelo-se-v-nasem-lese/

K čemu potřebujeme „externí“ správu?

» Dodáváme/odebíráme nějakou službu – např. monitoring, technickou podporu, implementaci, konzultace …

Jak toho dosáhnout: Nativní uživatelé

Výhody:

- Přímočaré
- Veškerá funkcionalita

Nevýhody:

- (odběratel) Potřeba licencovat každého uživatele
- (dodavatel) Větší počet účtů pro každého zaměstnance
- (dodavatel) Pracnější on/offborading zaměstnanců
- (dodavatel) Horší user-experience při práci pro více odběratelů

Jak toho dosáhnout: Účty hosta

Výhody:

- Přímočaré
- (odběratel) Nejsou třeba další licence
- (dodavatel) Jeden účet na technika, podpora MFA a „Compliant device“

Nevýhody:

- (dodavatel) Pracnější on/offborading zaměstnanců
- (dodavatel) Horší user-experience při přepínání mezi odběrateli

Jak toho dosáhnout: GDAP

Výhody:

- (odběratel) Nejsou třeba další licence
- (dodavatel) Jeden účet na technika, podpora MFA a „Compliant device“
- (dodavatel) Jednoduchý on/offboarding zaměstnanců
- (dodavatel) Pohodlná práce nad více zákazníky současně
- (dodavatel) Možnost využít Lighthouse

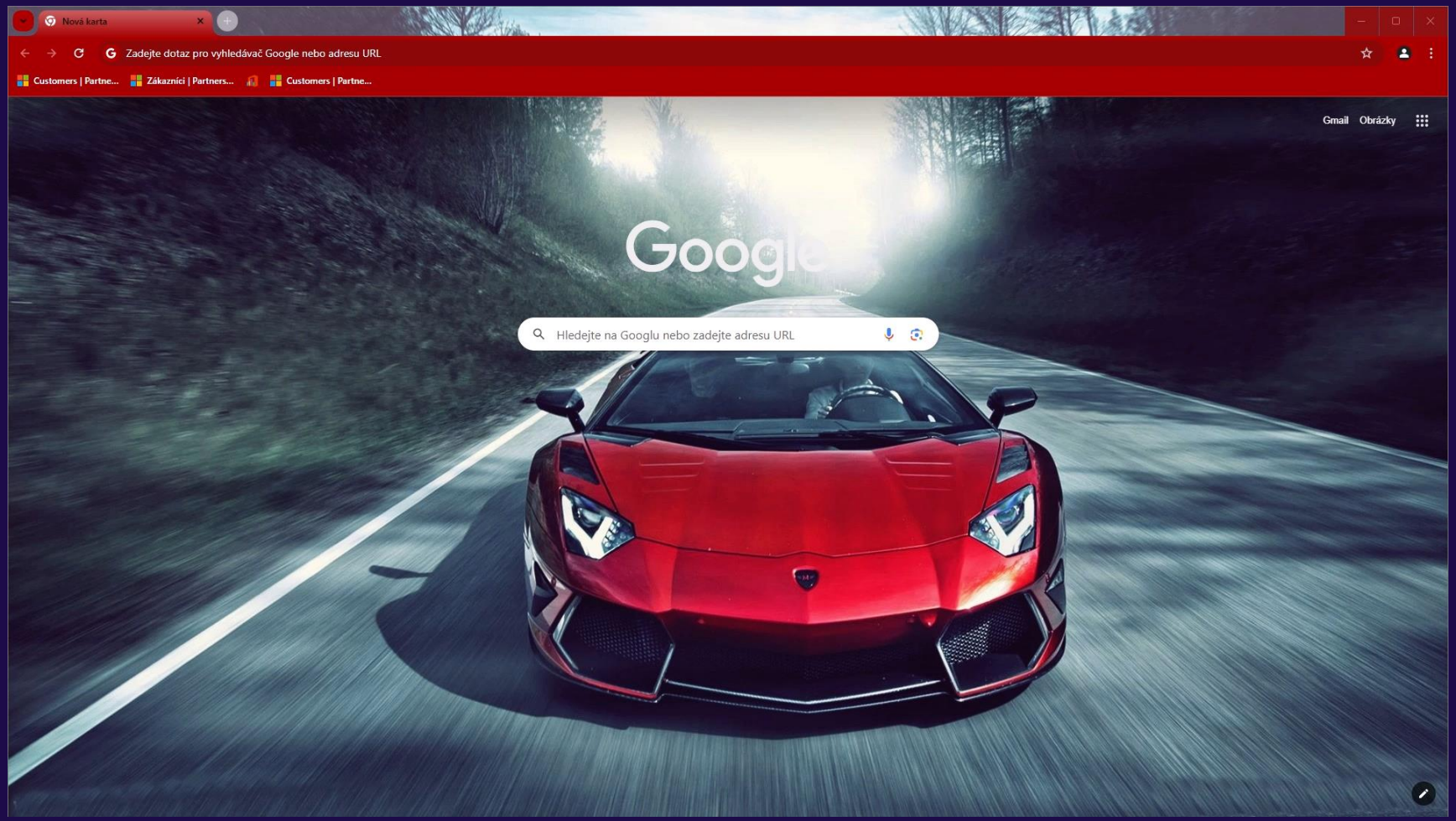
Nevýhody:

- (dodavatel) Není k dispozici plná funkcionalita (podporované akce)
- (odběratel) Menší kontrola nad tím kdo konkrétně ke mně přistupuje

Granular Delegated Admin Privileges (GDAP)

- https://learn.microsoft.com/en-us/partner-center/gdap-introduction
- Nástupce DAPu
- Dostupný Microsoft Partnerům

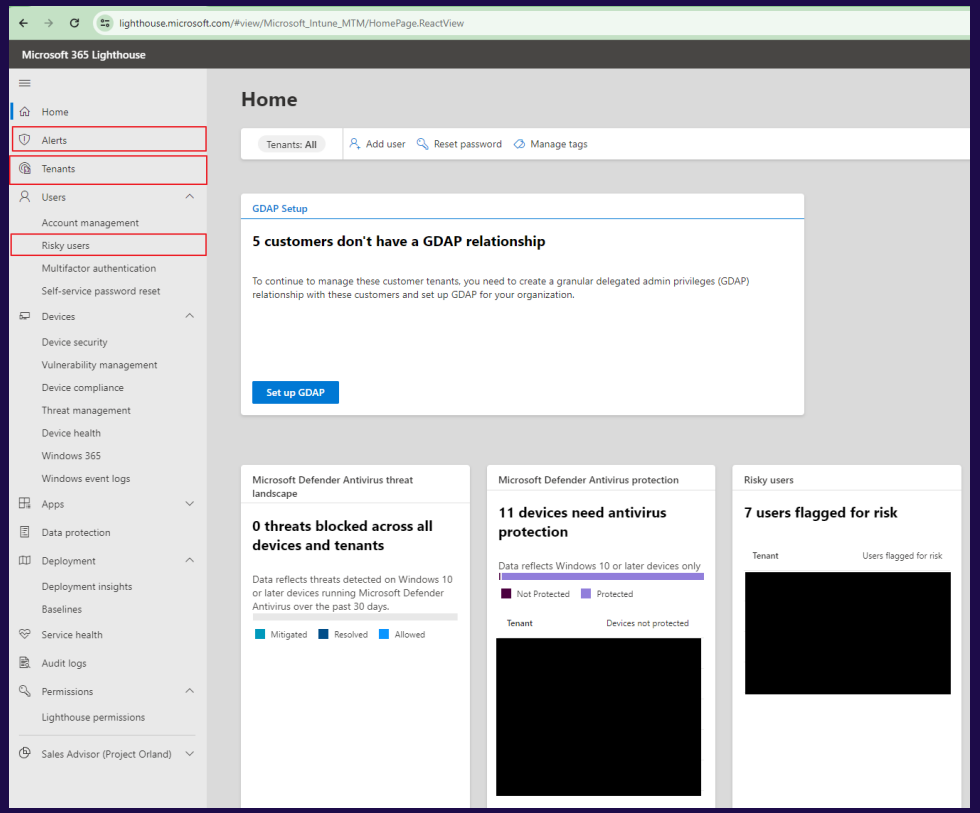
Granular Delegated Admin Privileges (GDAP)



Microsoft 365 Lighthouse

» https://learn.microsoft.com/en-us/microsoft-365/lighthouse/m365-lighthouse-overview

» Dostupný Microsoft CSP Partnerům



GDAP bezpečně

Jaká jsou rizika

Kaseya: Roughly 1,500 businesses hit by REvil ransomware attack

Kaseya says the REvil supply-chain ransomware attack breached the systems of roughly 60 of its direct customers using the company's VSA on-premises product.

SERGIU GATLAN JULY 06, 2021 07:59 AM 0

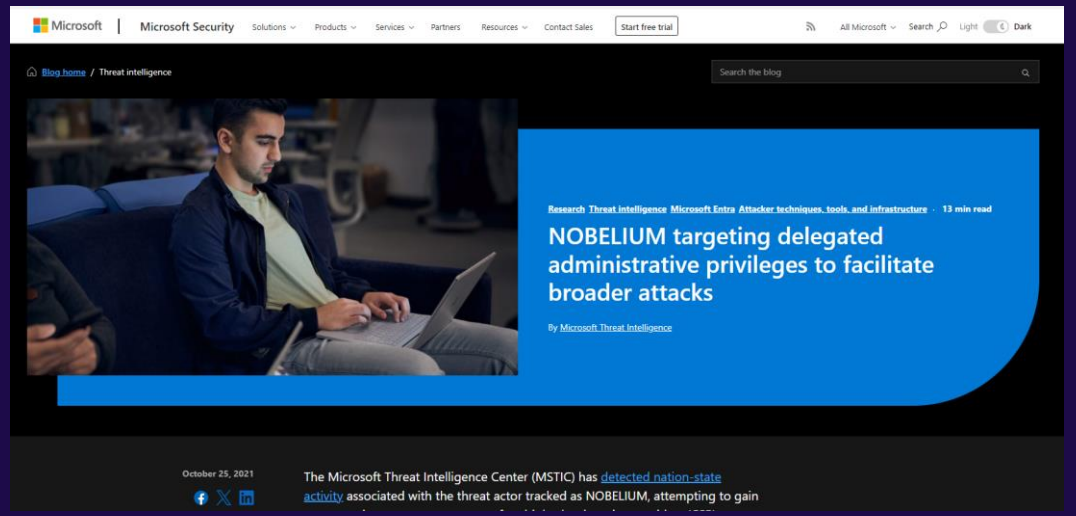
Zdroj: https://www.bleepingcomputer.com/news/security/kaseya-roughly-1-500-businesses-hit-by-revil-ransomware-attack/

Cyberattack on IT provider CTS impacts dozens of UK law firms

A cyberattack on CTS, a leading managed service provider (MSP) for law firms and other organizations in the UK legal sector, is behind a major outage impacting numerous law firms and home buyers in the country since Wednesday.

SERGIU GATLAN NOVEMBER 24, 2023 12:13 PM 0

Zdroj: https://www.bleepingcomputer.com/news/security/cyberattack-on-it-provider-cts-impacts-dozens-of-uk-law-firms/



Zdroj: https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

GDAP Bezpečně

1. Potřebuji vůbec získat/delegovat oprávnění?

GDAP Bezpečně

1. Potřebuji vůbec získat/delegovat oprávnění?
2. Jaká jsou nejmenší možná oprávnění (Principle of Least Privilege)

Learn / Microsoft Entra / Microsoft Entra ID / Role-based access control /

Least privileged roles by task in Microsoft Entra ID

Article • 03/28/2024 • 28 contributors

Feedback

In this article

Application proxy
External Identities/B2C
Company branding
Connect

Show 28 more

In this article, you can find the information needed to restrict a user's administrator permissions by assigning least privileged roles in Microsoft Entra ID. You will find tasks organized by feature area and the least privileged role required to perform each task, along with additional non-Global Administrator roles that can perform the task.

You can further restrict permissions by assigning roles at smaller scopes or by creating your own custom roles. For more information, see Assign Microsoft Entra roles at different scopes or Create and assign a custom role in Microsoft Entra ID.

Zdroj: https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task

GDAP Bezpečně

1. Potřebuji vůbec získat/delegovat oprávnění?
2. Jaká jsou nejmenší možná oprávnění (Principle of Least Privilege)
3. Udělit nejmenšímu množství uživatelů (zákazník doufá, partner ví)

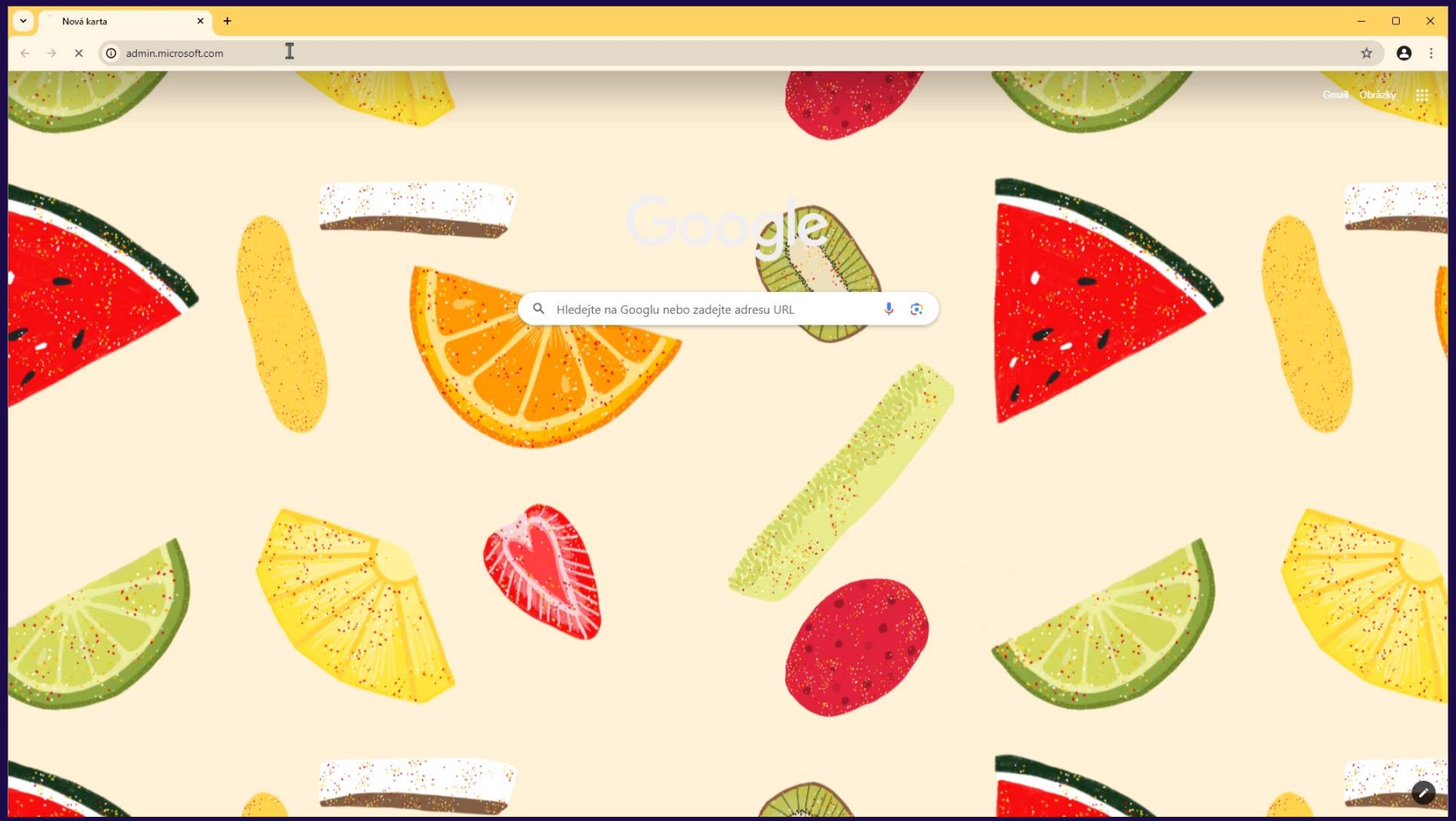
GDAP Bezpečně

1. Potřebuji vůbec získat/delegovat oprávnění?
2. Jaká jsou nejmenší možná oprávnění (Principle of Least Privilege)
3. Udělit nejmenšímu množství uživatelů (zákazník doufá, partner ví)
4. Nepřidělovat privilegia běžnému uživatelskému účtu

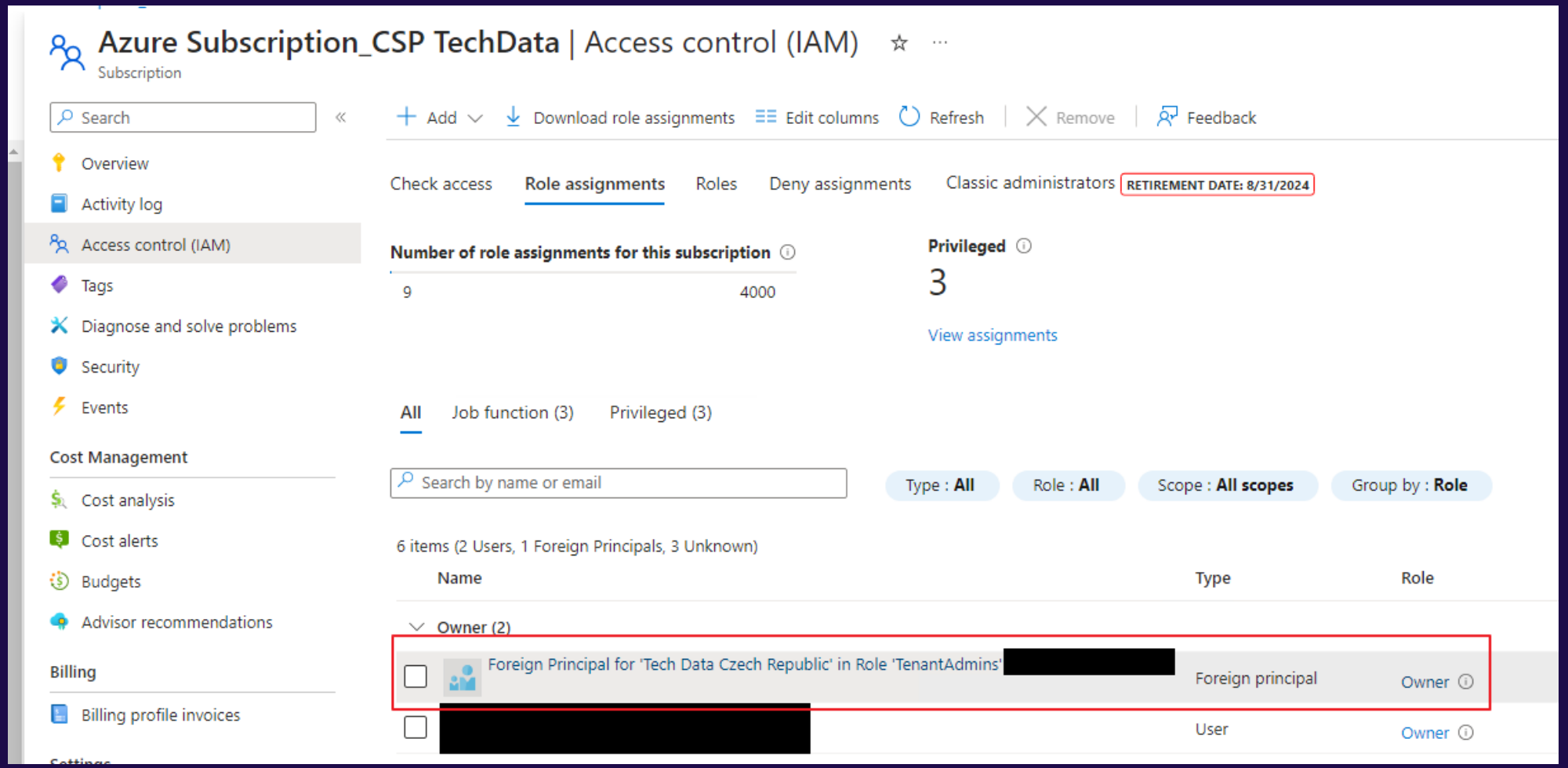
GDAP Bezpečně

1. Potřebuji vůbec získat/delegovat oprávnění?
2. Jaká jsou nejmenší možná oprávnění (Principle of Least Privilege)
3. Udělit nejmenšímu množství uživatelů (zákazník doufá, partner ví)
4. Nepřidělovat privilegia běžnému uživatelskému účtu
5. Limitovat privilegované účty skrze CA (MFA, auth strength, compliant device, company device, IP address, working hours)

Auditování oprávnění



To be continued ... ?



Děkuji za ⟨pozornost⟩