CLOUD IDENTITY SUMMIT ‘22

Identity Management Track

Azure Attack Paths

Fabian Bader (glueckkanja-gab AG)

Community Event by

Azure Meetup
BONN

About me

- Cloud Security Architect @ glueckkanja-gab AG
- cloudbrothers.info
- @fabian_bader on Twitter
- Organizer of @HHPSUG
- fabian@bader.cloud

MVP Microsoft Most Valuable Professional

Microsoft Certified AZURE SOLUTIONS ARCHITECT EXPERT

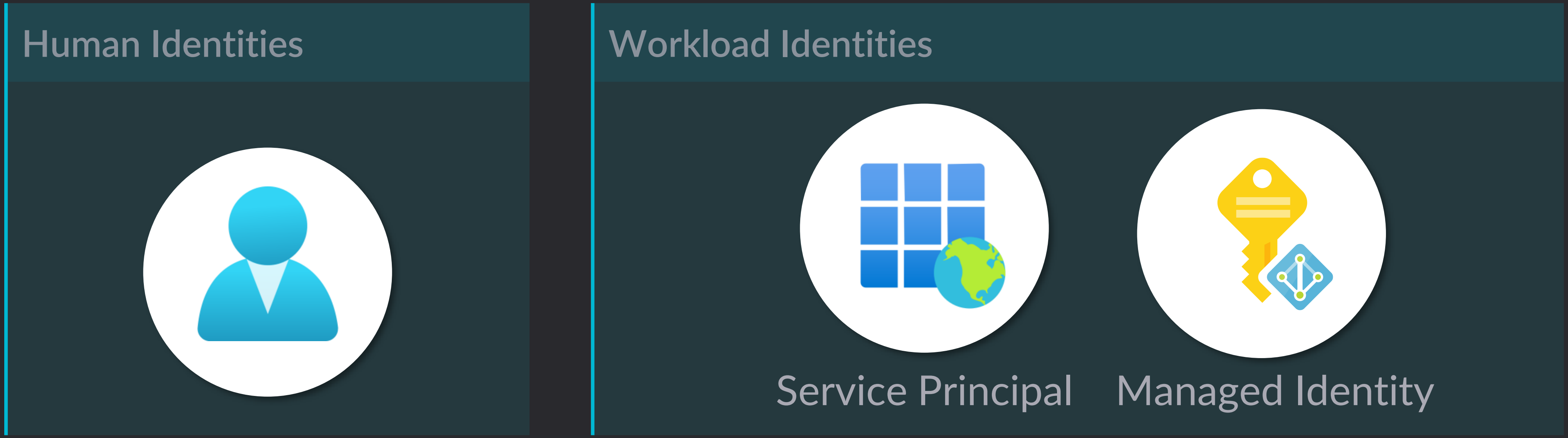
Microsoft Certified AZURE SECURITY ENGINEER ASSOCIATE

Microsoft Certified IDENTITY AND ACCESS ADMINISTRATOR ASSOCIATE

Microsoft Certified SECURITY OPERATIONS ANALYST ASSOCIATE

HAMBURG POWERSHELL

Identities in Azure

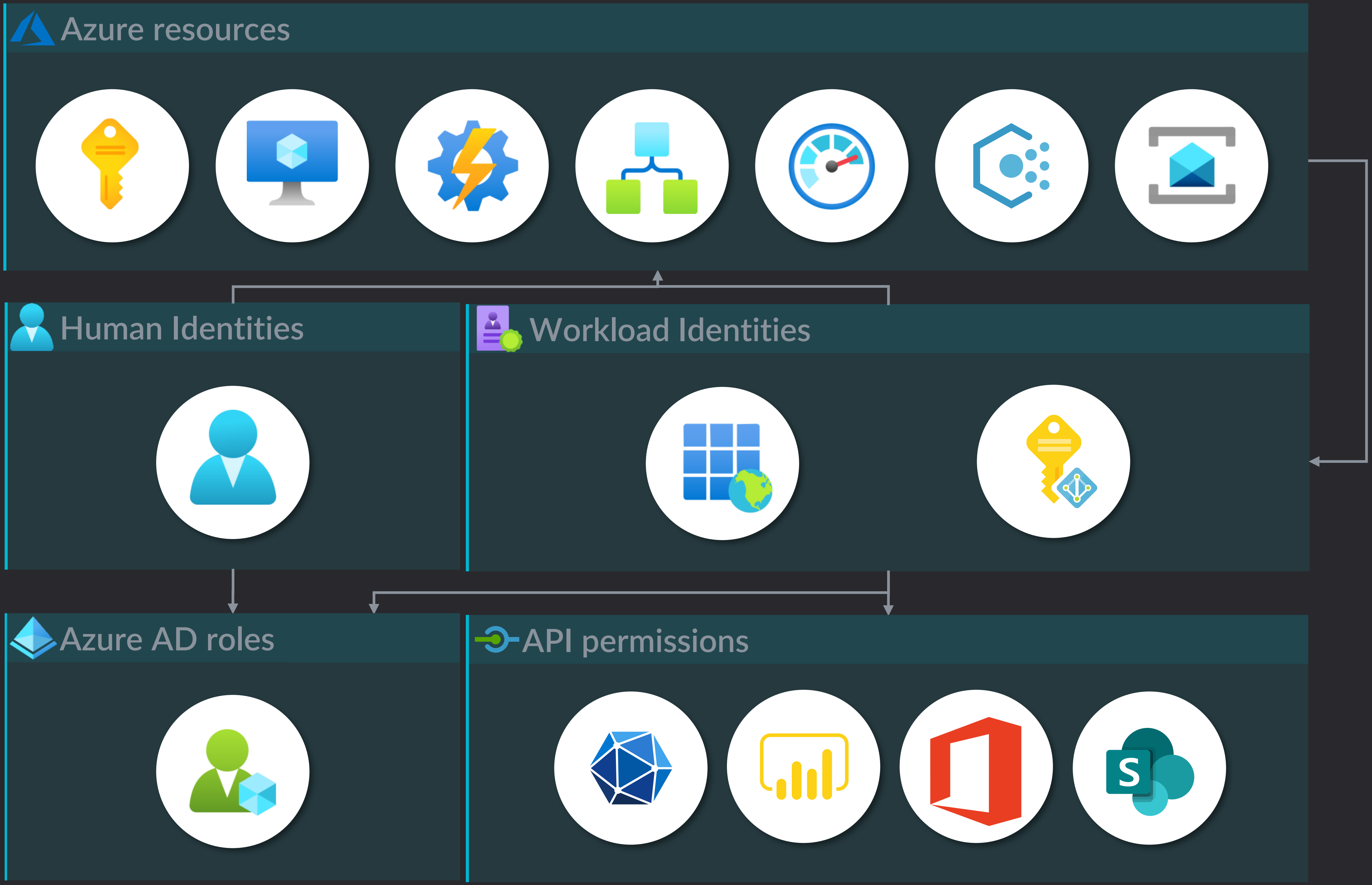


Human Identities

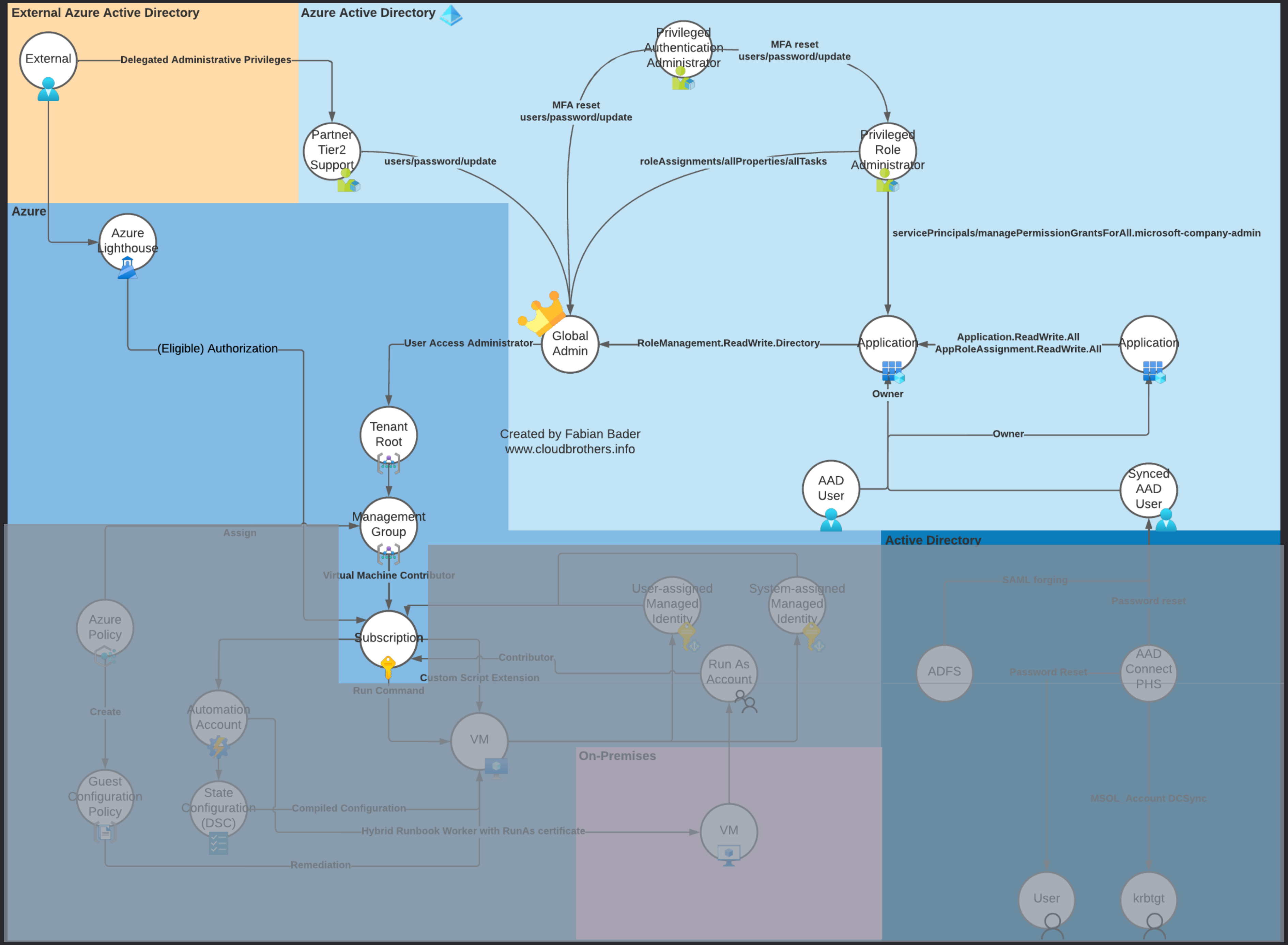
Workload Identities

Service Principal

Managed Identity


Azure resources
Human Identities
Workload Identities
Azure AD roles
API permissions

Too much permissions, a common mistake

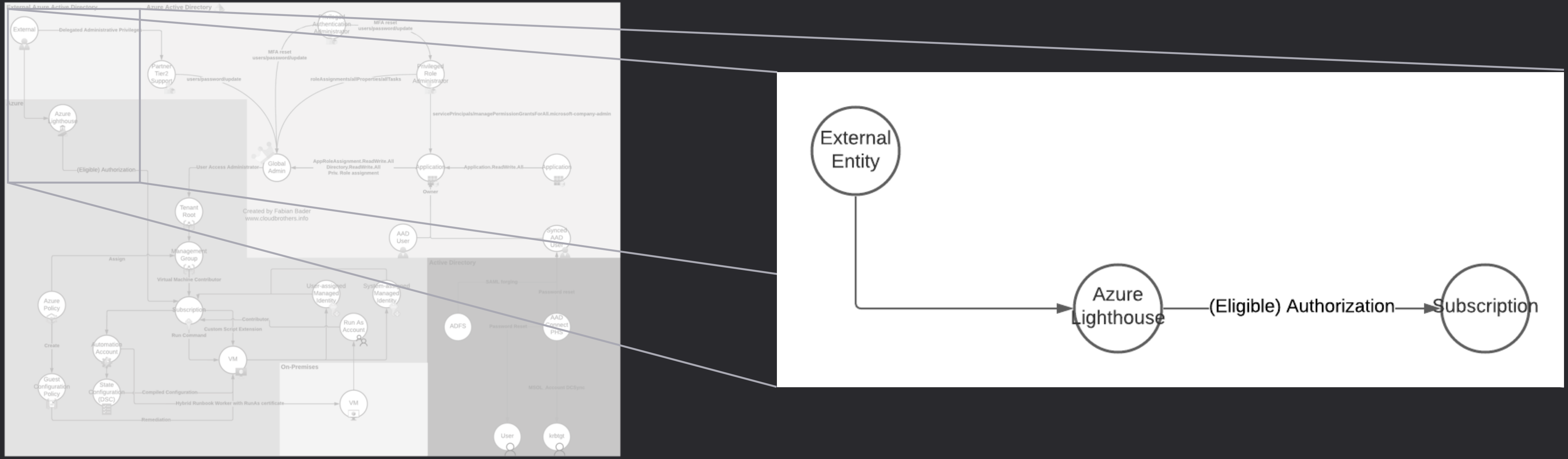

External Azure Active Directory
External
Delegated Administrative Privileges
Azure Active Directory
Privileged Authentication Administrator
MFA reset users/password/update
MFA reset users/password/update
Partner Tier2 Support
users/password/update
roleAssignments/allProperties/allTasks
Privileged Role Administrator
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
Azure
Azure Lighthouse
(Eligible) Authorization
User Access Administrator
Global Admin
RoleManagement.ReadWrite.Directory
Application
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Owner
Tenant Root
Created by Fabian Bader
www.cloudbrothers.info
AAD User
Synced AAD User
Management Group
Assign
Virtual Machine Contributor
Active Directory
SAML forging
Password reset
Azure Policy
User-assigned Managed Identity
System-assigned Managed Identity
Subscription
Contributor
Custom Script Extension
Run Command
Run As Account
ADFS
Password Reset
AAD Connect PHS
Create
Automation Account
VM
On-Premises
Guest Configuration Policy
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
VM
MSOL_Account DCSync
Remediation
User
krbtgt

Crown icon created by Freepik

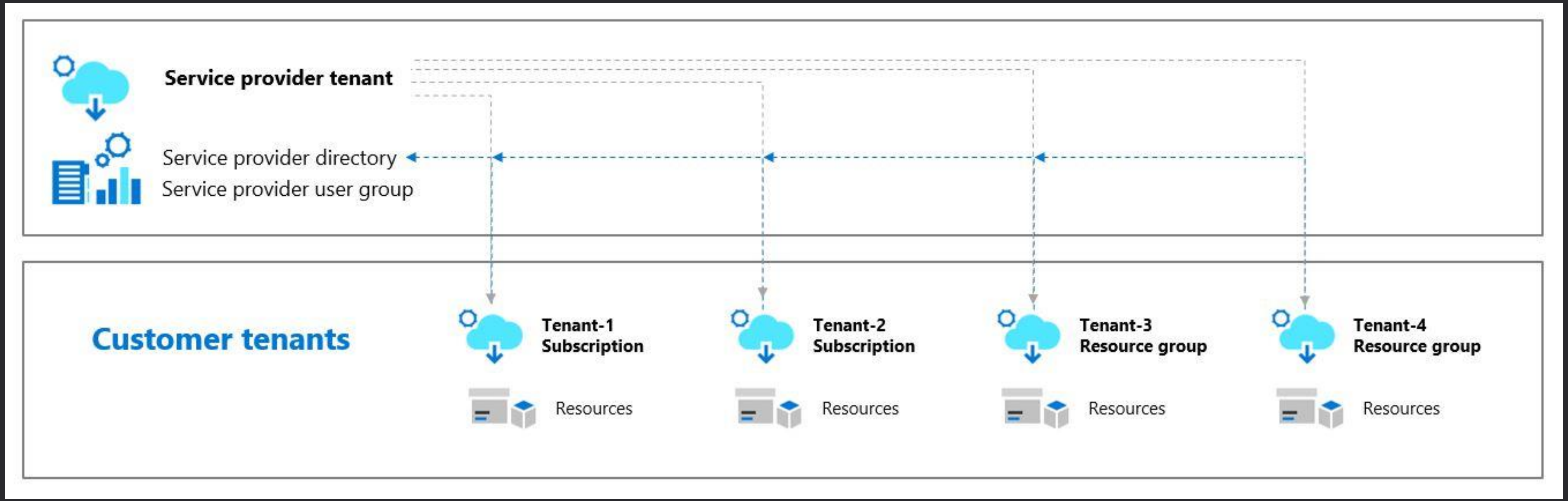
Attribution

- Sander Berkouwer - @SanderBerkouwer
- Huy Kha - @DebugPrivilege
- Sami Lamppu - @samilamppu
- Dirk-jan Mollema - @_dirkjan
- Thomas Naunheim - @Thomas_Live
- Andy Robbins - @_wald0
- Dr. Nestori Syynimaa - @DrAzureAD
- And many more…

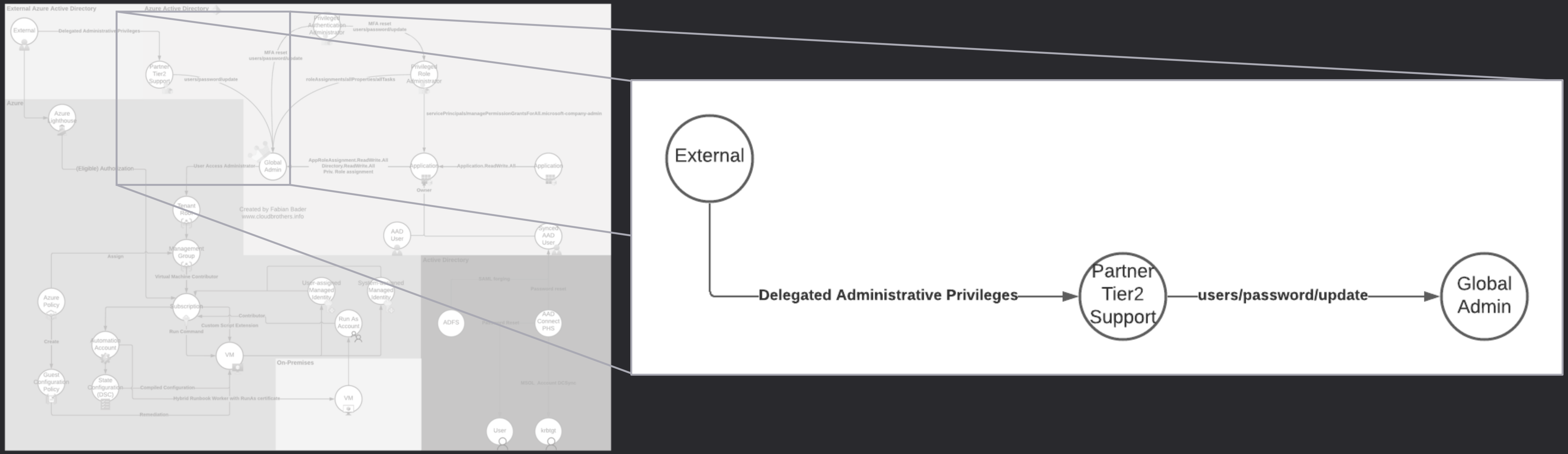
Azure Lighthouse



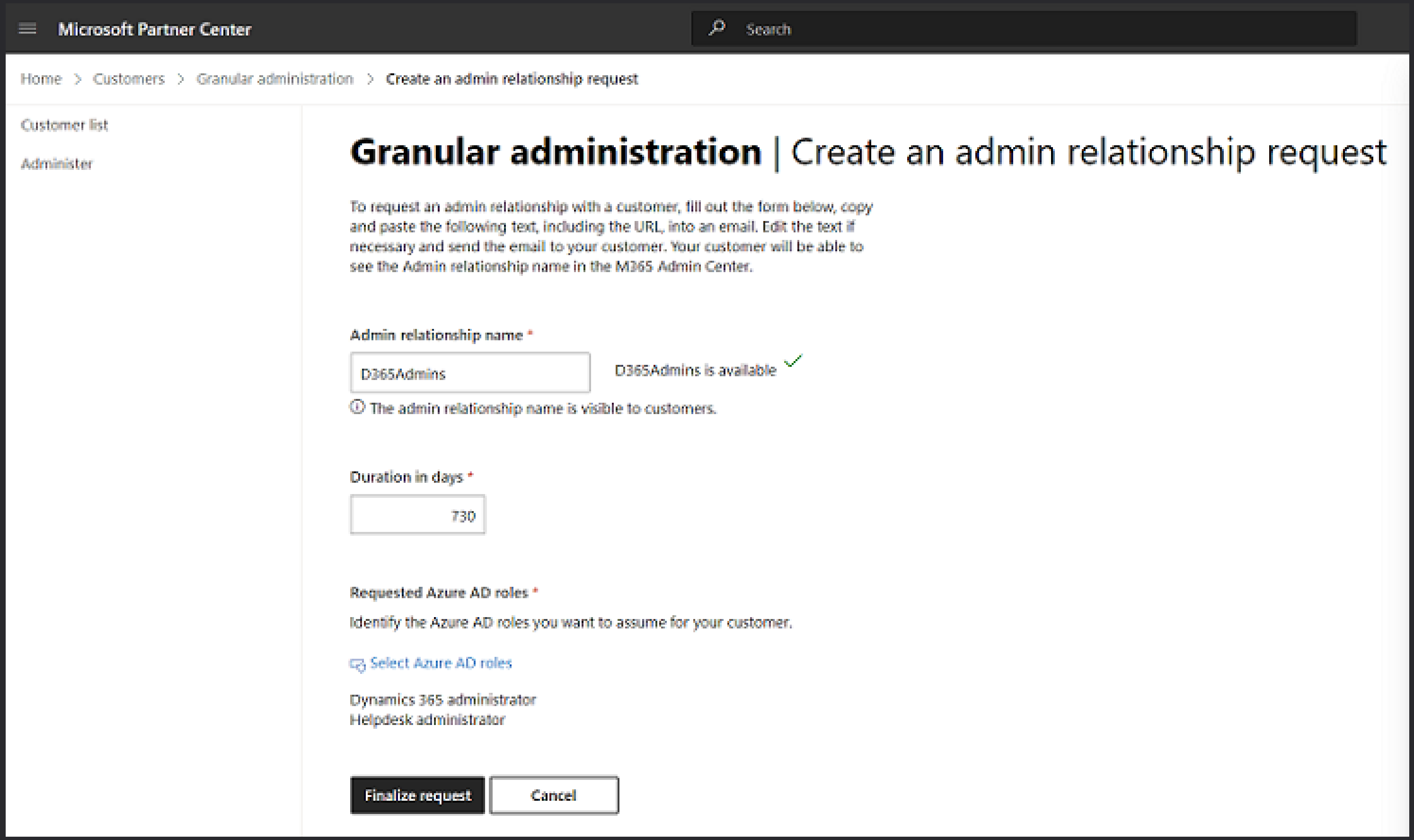
Azure Lighthouse



Delegated Administrative Privileges



Granular DAP



Microsoft Partner Center
Search
Home > Customers > Granular administration > Create an admin relationship request
Customer list
Administer

Granular administration | Create an admin relationship request

To request an admin relationship with a customer, fill out the form below, copy and paste the following text, including the URL, into an email. Edit the text if necessary and send the email to your customer. Your customer will be able to see the Admin relationship name in the M365 Admin Center.

Admin relationship name *

D365Admins

D365Admins is available ✓

ⓘ The admin relationship name is visible to customers.

Duration in days *

730

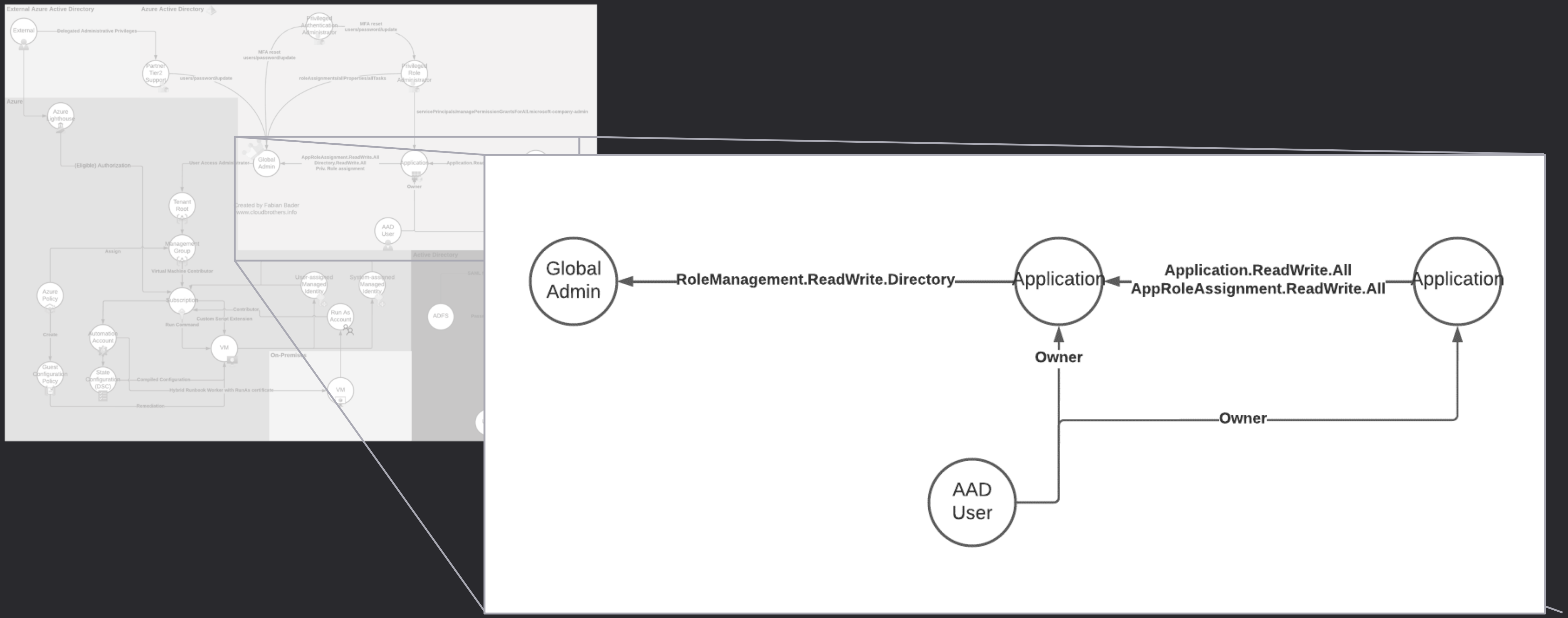
Requested Azure AD roles *

Identify the Azure AD roles you want to assume for your customer.

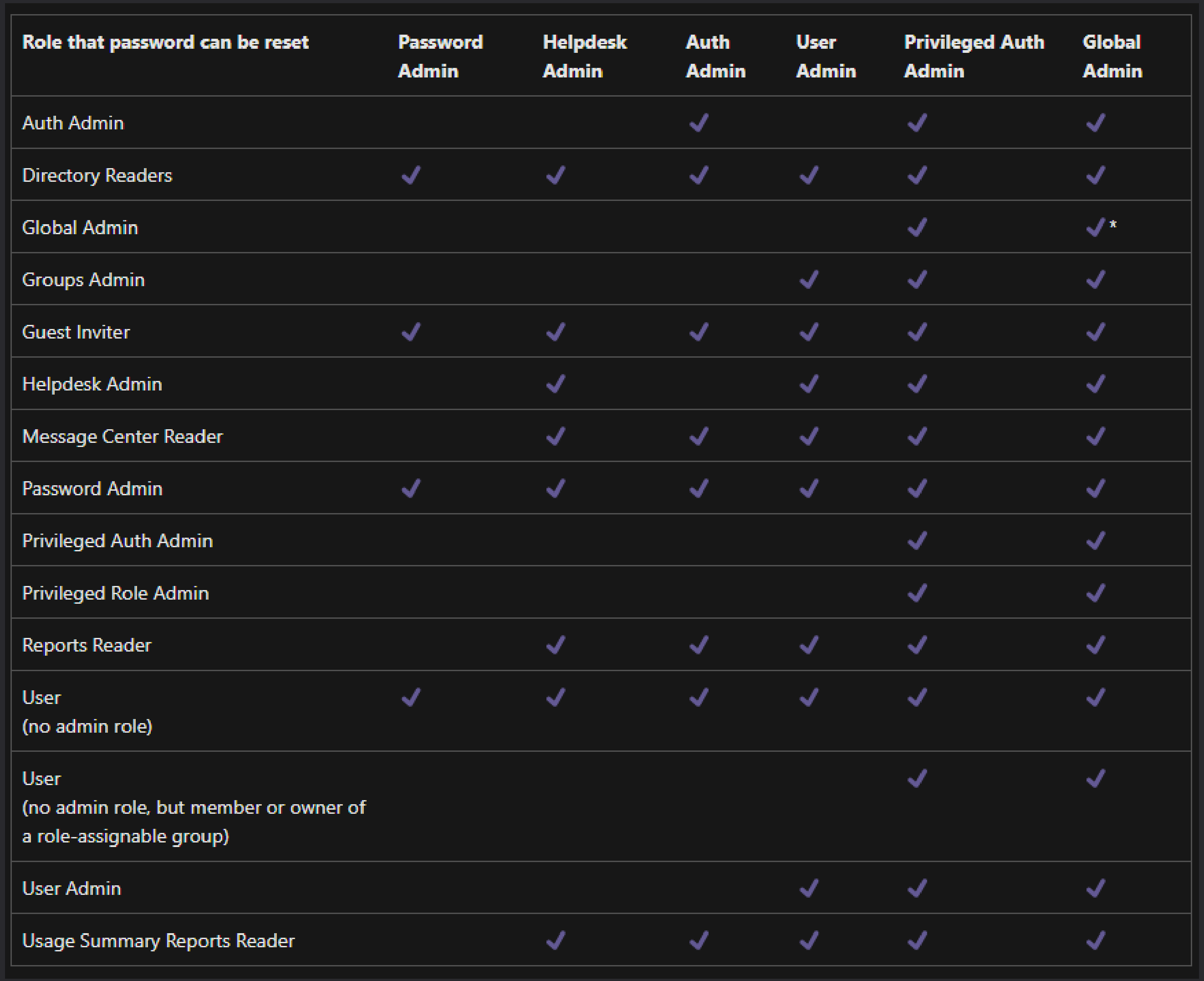
Select Azure AD roles

Dynamics 365 administrator
Helpdesk administrator

Abuse extensive API Permissions


External Azure Active Directory
Azure Active Directory
External
Delegated Administrative Privileges
Partner Tier2 Support
users/password/update
Privileged Authentication Administrator
MFA reset users/password/update
MFA reset users/password/update
Privileged Role Administrator
roleAssignments/allProperties/allTasks
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
Azure
Azure Lighthouse
(Eligible) Authorization
User Access Administrator
Global Admin
AppRoleAssignment.ReadWrite.All
Directory.ReadWrite.All
Priv. Role assignment
Application
Owner
Created by Fabian Bader
www.cloudbrothers.info
AAD User
Tenant Root
Management Group
Assign
Virtual Machine Contributor
Azure Policy
Subscription
Contributor
Custom Script Extension
Run Command
Create
Automation Account
VM
Guest Configuration Policy
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
Remediation
User-assigned Managed Identity
System-assigned Managed Identity
Run As Account
On-Premises
VM
Active Directory
ADFS
Global Admin
RoleManagement.ReadWrite.Directory
Application
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Owner
AAD User

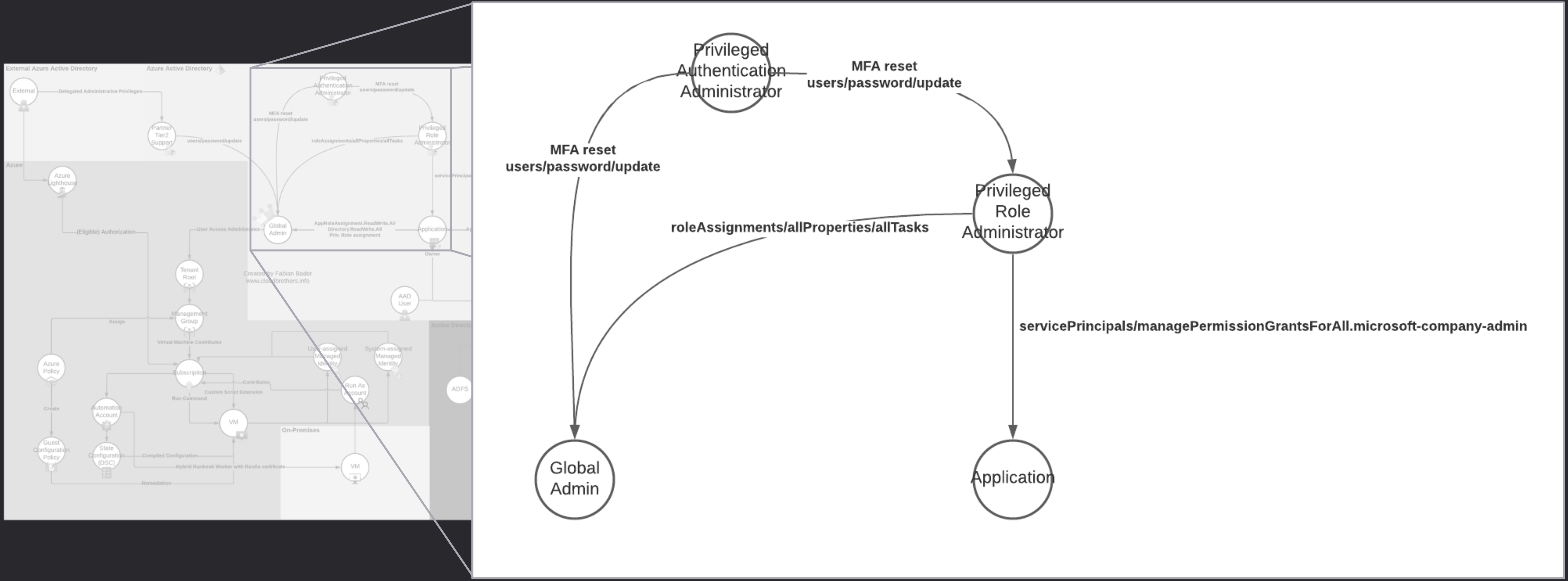
Azure AD Roles



Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
Auth Admin			✓		✓	✓
Directory Readers	✓	✓	✓	✓	✓	✓
Global Admin					✓	✓*
Groups Admin				✓	✓	✓
Guest Inviter	✓	✓	✓	✓	✓	✓
Helpdesk Admin		✓		✓	✓	✓
Message Center Reader		✓	✓	✓	✓	✓
Password Admin	✓	✓	✓	✓	✓	✓
Privileged Auth Admin					✓	✓
Privileged Role Admin					✓	✓
Reports Reader		✓	✓	✓	✓	✓
User (no admin role)	✓	✓	✓	✓	✓	✓
User (no admin role, but member or owner of a role-assignable group)					✓	✓
User Admin				✓	✓	✓
Usage Summary Reports Reader		✓	✓	✓	✓	✓

https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords

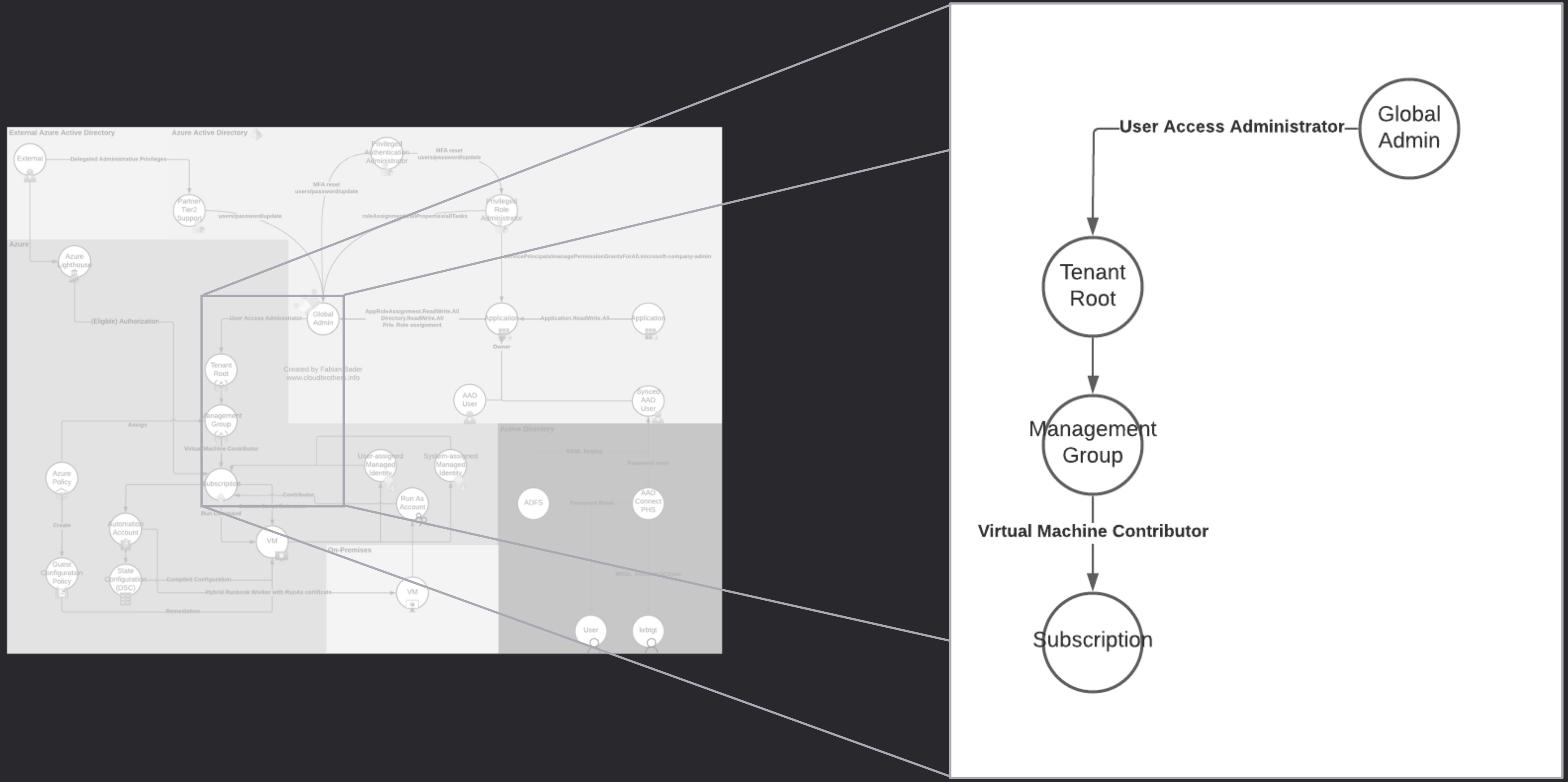
Azure AD Roles

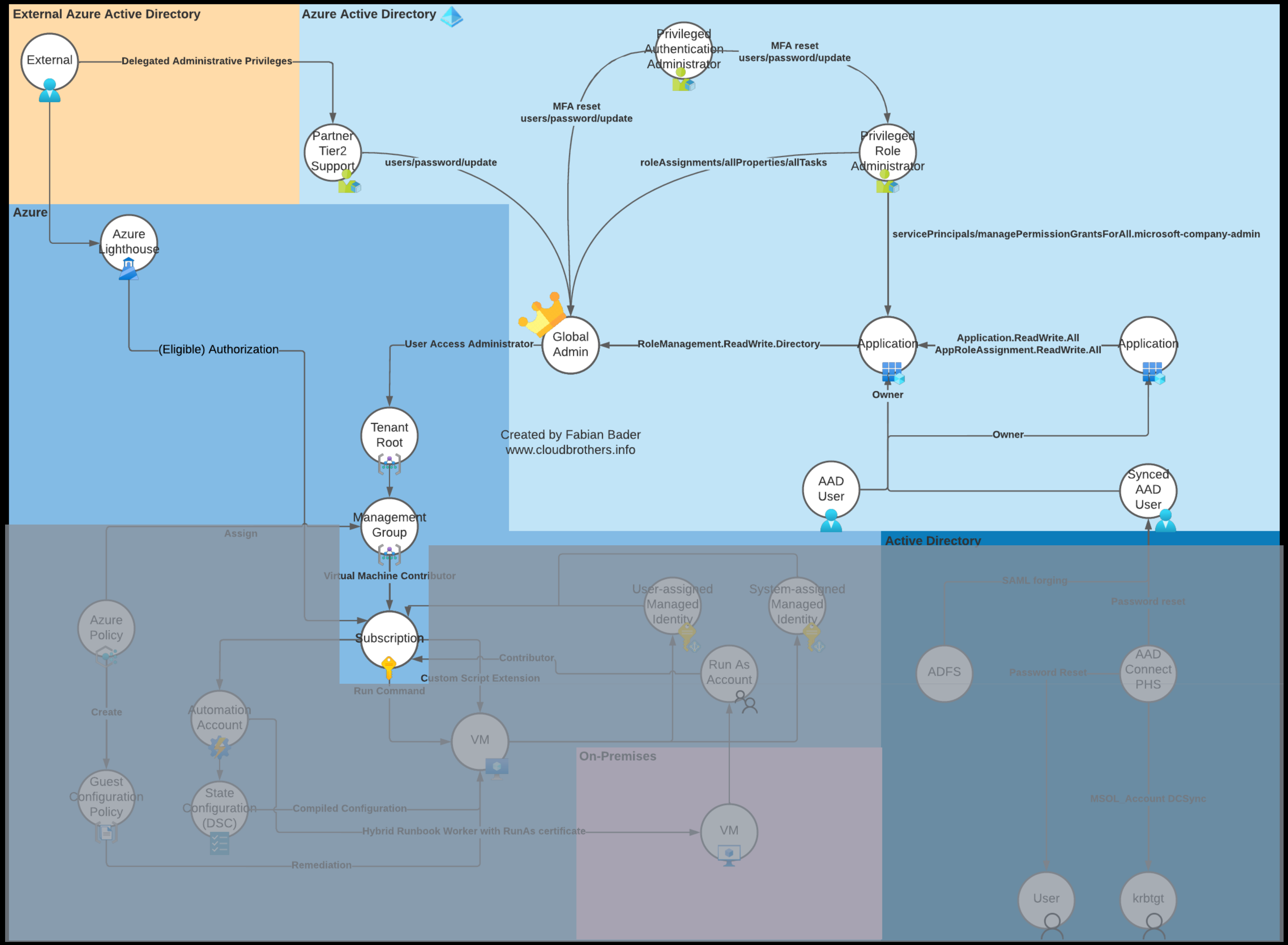


Created by Fabian Bader
www.cloudbrothers.info

External Azure Active Directory
Azure Active Directory
External
Delegated Administrative Privileges
Partner Tier2 Support
users/password/update
Azure
Azure Lighthouse
(Eligible) Authorization
User Access Administrator
Tenant Root
Management Group
Assign
Virtual Machine Contributor
Azure Policy
Create
Guest Configuration Policy
Subscription
Contributor
Custom Script Extension
Run Command
Automation Account
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
Remediation
VM
User-assigned Managed Identity
System-assigned Managed Identity
Run As Account
On-Premises
VM
Active Directo
ADFS
AAD User
Owner
AppRoleAssignment.ReadWrite.All
Directory.ReadWrite.All
Priv. Role assignment
Privileged Authentication Administrator
MFA reset
users/password/update
MFA reset
users/password/update
Privileged Role Administrator
roleAssignments/allProperties/allTasks
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
Global Admin
Application

Elevate Azure Subscription Access




External Azure Active Directory
Azure Active Directory
External
Delegated Administrative Privileges
Partner Tier2 Support
users/password/update
Privileged Authentication Administrator
MFA reset users/password/update
MFA reset users/password/update
Privileged Role Administrator
roleAssignments/allProperties/allTasks
servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin
Azure
Azure Lighthouse
(Eligible) Authorization
Global Admin
User Access Administrator
RoleManagement.ReadWrite.Directory
Application
Application.ReadWrite.All
AppRoleAssignment.ReadWrite.All
Application
Owner
Owner
Tenant Root
AAD User
Synced AAD User
Management Group
Assign
Virtual Machine Contributor
Active Directory
Azure Policy
Subscription
User-assigned Managed Identity
System-assigned Managed Identity
Contributor
Custom Script Extension
Run Command
Run As Account
SAML forging
Password reset
ADFS
Password Reset
AAD Connect PHS
Create
Automation Account
VM
On-Premises
Guest Configuration Policy
State Configuration (DSC)
Compiled Configuration
Hybrid Runbook Worker with RunAs certificate
VM
MSOL_Account DCSync
Remediation
User
krbtgt

Created by Fabian Bader
www.cloudbrothers.info

Crown icon created by Freepik

Questions?

SCAN ME

https://cloudbrothers.info/en/azure-attack-paths

CLOUD IDENTITY SUMMIT '22

Thanks to our sponsors!

adesso business. people. technology.

glueckkanja gab

yubico

CLOUD IDENTITY SUMMIT ‘22

Thu, September 22nd, 2022

Ask Me Anything (AMA)

Roundtable discussion and Q&A
on experiences from the field and current trends!

Meet the speakers and exchange with members of the community!

Community Event by

Azure Meetup
BONN

Follow us on Twitter

@identitysummit

CLOUD IDENTITY SUMMIT ‘22

Your Feedback is Important!

https://www.identitysummit.cloud/feedback/

Community Event by

Azure Meetup
BONN

Follow us on Twitter

@identitysummit