Stephan van Rooij

Microsoft MVP
Security
M365 Development

Secrets safe in KeyVault?

- Azure Functions App with managed identity
- Azure KeyVault
- Multi-tenant application

Azure Functions

1. Pick a name
2. Choose a runtime
   `.NET`, `8 (LTS), isolated`
3. Next, next, next....
4. Enable managed identity

ape-demo-2024-fa

Function App

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Microsoft Defender for Cloud
- Events (preview)
- Recommended services (preview)
- Functions
  - App keys
  - App files
  - Proxies
- Deployment
  - Deployment slots
  - Deployment Center
- Settings
  - Environment variables
  - Configuration
  - Authentication

Browse | Refresh | Stop | Restart | Swap | Get publish profile | Reset publish profile

Essentials

Resource group (move)	: ape-demo-2024-rg
Status	: Running
Location (move)	: North Europe
Subscription (move)	:
Subscription ID	:
Tags (edit)	: Add tags

Functions | Metrics | Properties | Notifications (0)

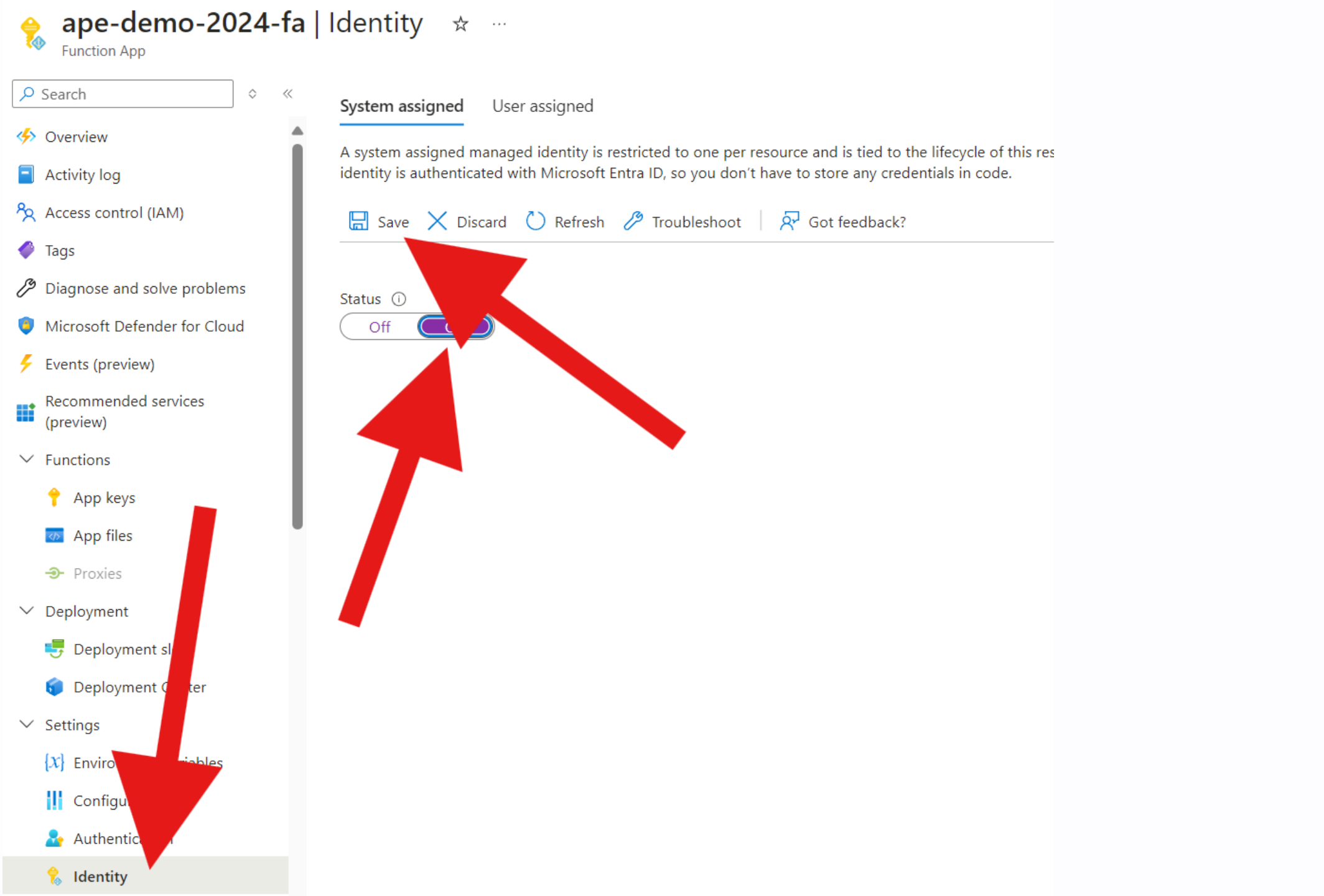
Create functions in you

VS Code Desktop

Best optimized for:

- Local development within VS Code
- Custom development tool requirements

Create with VS Code Desktop


ape-demo-2024-fa | Identity
Function App
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Microsoft Defender for Cloud
Events (preview)
Recommended services (preview)
Functions
App keys
App files
Proxies
Deployment
Settings
Identity
System assigned
User assigned
A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this res
identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.
Save
Discard
Refresh
Troubleshoot
Got feedback?
Status
Off

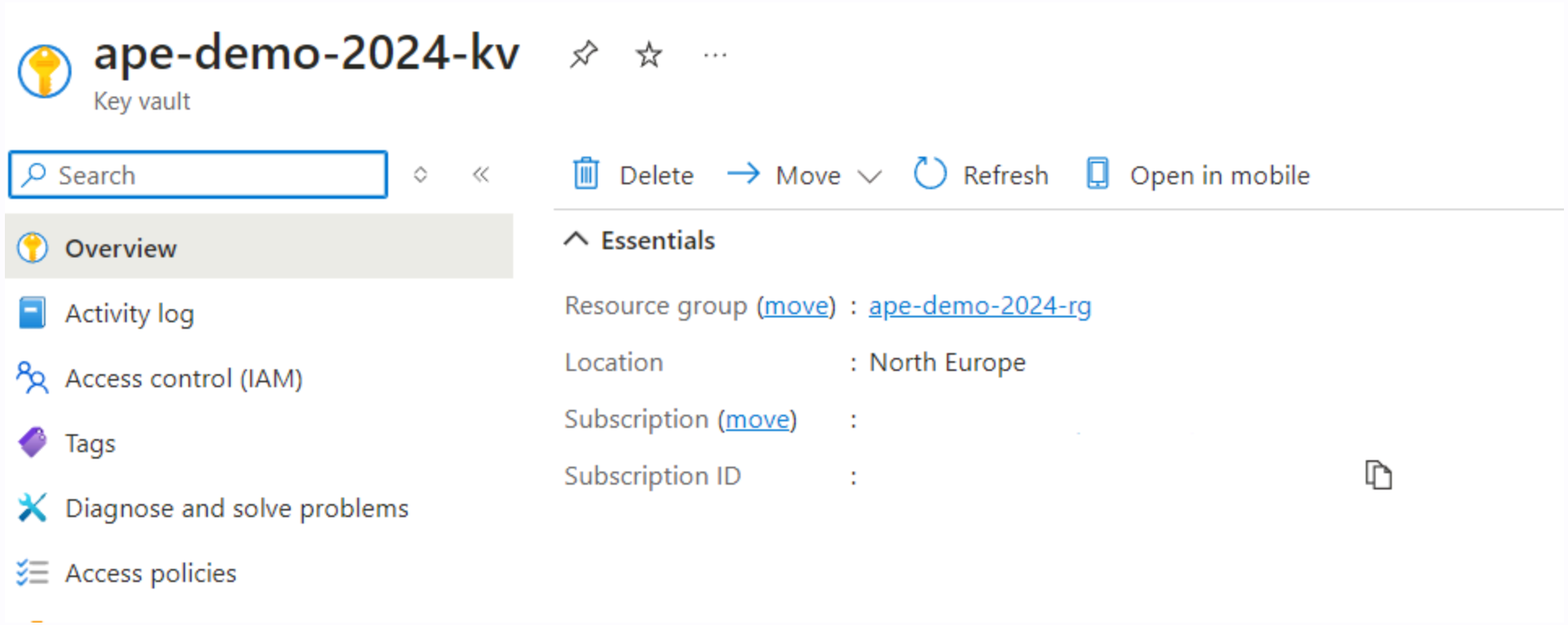
Enable system assigned managed identity

'ape-demo-2024-fa' will be registered with Microsoft Entra ID. Once it is registered, 'ape-demo-2024-fa' can be granted permissions to access resources protected by Microsoft Entra ID. Do you want to enable the system assigned managed identity for 'ape-demo-2024-fa'?

Yes | No

Azure KeyVault

1. Create KeyVault
2. Pick name, region, pricing
3. `Azure role-based access control`
4. `All Networks` and `Enable public endpoint`
5. Finish


ape-demo-2024-kv
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Delete
Move
Refresh
Open in mobile
Essentials
Resource group (move) : ape-demo-2024-rg
Location : North Europe
Subscription (move) :
Subscription ID :

Method of Certificate Creation	Generate
Certificate Name *	APE-Application-Certificate
Type of Certificate Authority (CA)	Self-signed certificate
Subject *	CN=ape-demo.invalid
DNS Names	0 DNS names
Validity Period (in months) *	12
Content Type	PKCS #12 / PEM
Lifetime Action Type	E-mail all contacts at a given percentage lifetime
Percentage Lifetime *	80
Advanced Policy Configuration	Not configured
Tags	0 tags

Multi-tenant application

1. Register app in Azure AD
2. `Accounts in any organizational dir`
3. Add API permissions `User.Read.All` (Application permission for MS Graph)
4. Generate a certificate in the KeyVault
5. Download and add to the app registration

Ape Demo application | API permissions

Search

Refresh | Got feedback?

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

- New support request

You are editing permission(s) to your application, users will have to consent even if they've already done so previously.

Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that users have already granted on their own behalf aren't affected. Learn more

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

Add a permission | Grant admin consent for Coding Stephan

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				
User.Read	Delegated	Sign in and read user profile	No	
User.ReadBasic.All	Application	Read all users' basic profiles	Yes	Not granted for Coding ...

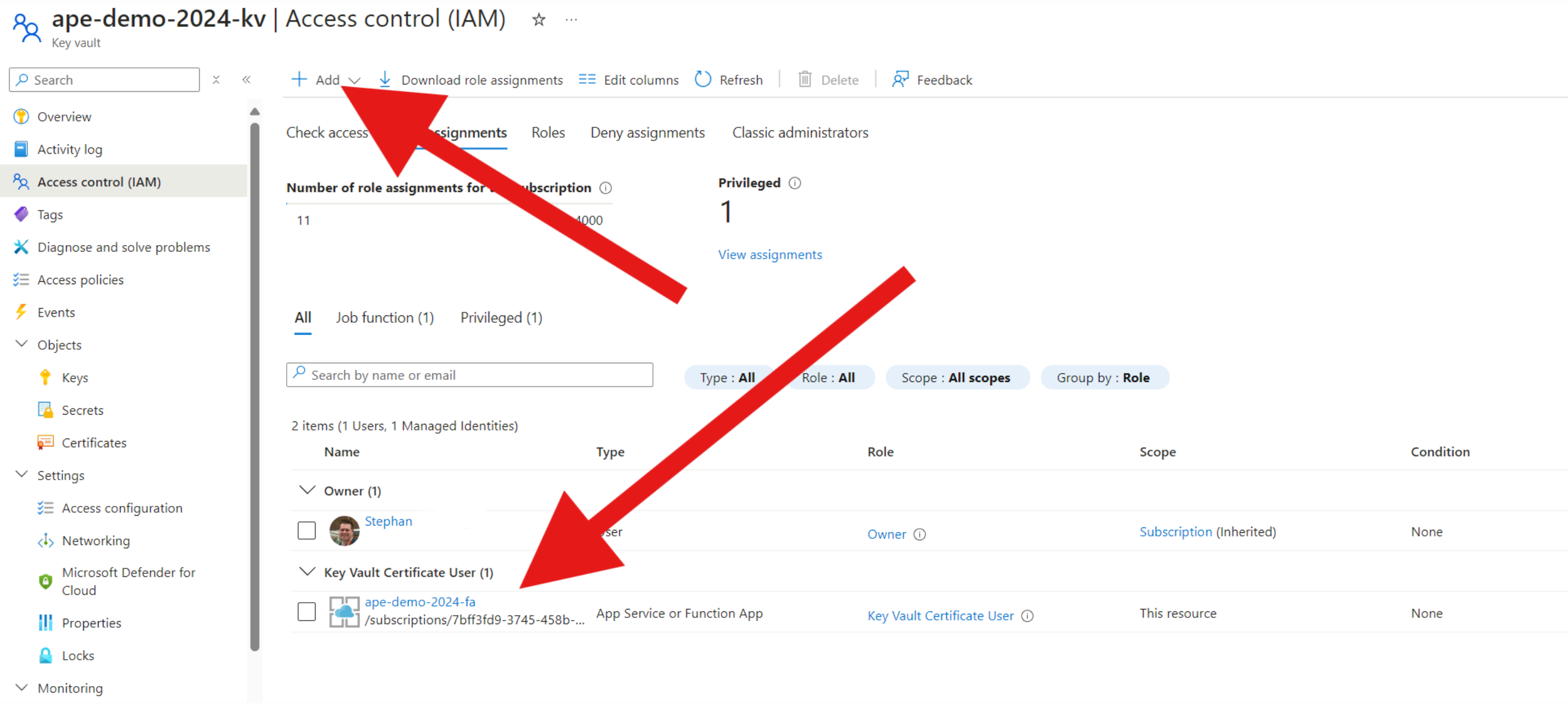
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Grant admin consent

“Thanks for noticing, I forgot to grant admin consent...”

Allow Functions app to access the KeyVault

1. Go to the KeyVault
2. Access Control (IAM)
3. Add role assignment
4. `Key Vault Certificate User`
5. Select the Functions app


ape-demo-2024-kv | Access control (IAM)
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Events
Objects
Keys
Secrets
Certificates
Settings
Access configuration
Networking
Microsoft Defender for Cloud
Properties
Locks
Monitoring
Add
Download role assignments
Edit columns
Refresh
Delete
Feedback
Check access
ssignments
Roles
Deny assignments
Classic administrators
Number of role assignments for
ubscription
11
4000
Privileged
1
View assignments
All
Job function (1)
Privileged (1)
Search by name or email
Type : All
Role : All
Scope : All scopes
Group by : Role
2 items (1 Users, 1 Managed Identities)
Name
Type
Role
Scope
Condition
Owner (1)
Stephan
ser
Owner
Subscription (Inherited)
None
Key Vault Certificate User (1)
ape-demo-2024-fa
/subscriptions/7bff3fd9-3745-458b-...
App Service or Function App
Key Vault Certificate User
This resource
None

Deploy the app

Right-click, publish to Azure...

Deploy the app 2

with CI / CD off course..

rightclickpublish.com

Demo 1 - Use the certificate

1. Use *managed identity* to *get* the certificate
2. Use the certificate to get a token
3. Use to token to show 3 users from MS Graph

Steal certificate

1. Use *managed identity* to **get** the certificate
2. Use the certificate **with private key** to do whatever you want

Demo 3 - Cloud signing

1. Prepare token request
2. Sign the token request with the certificate
3. Send the token request to Entra
4. Use the token to show 3 users from MS Graph

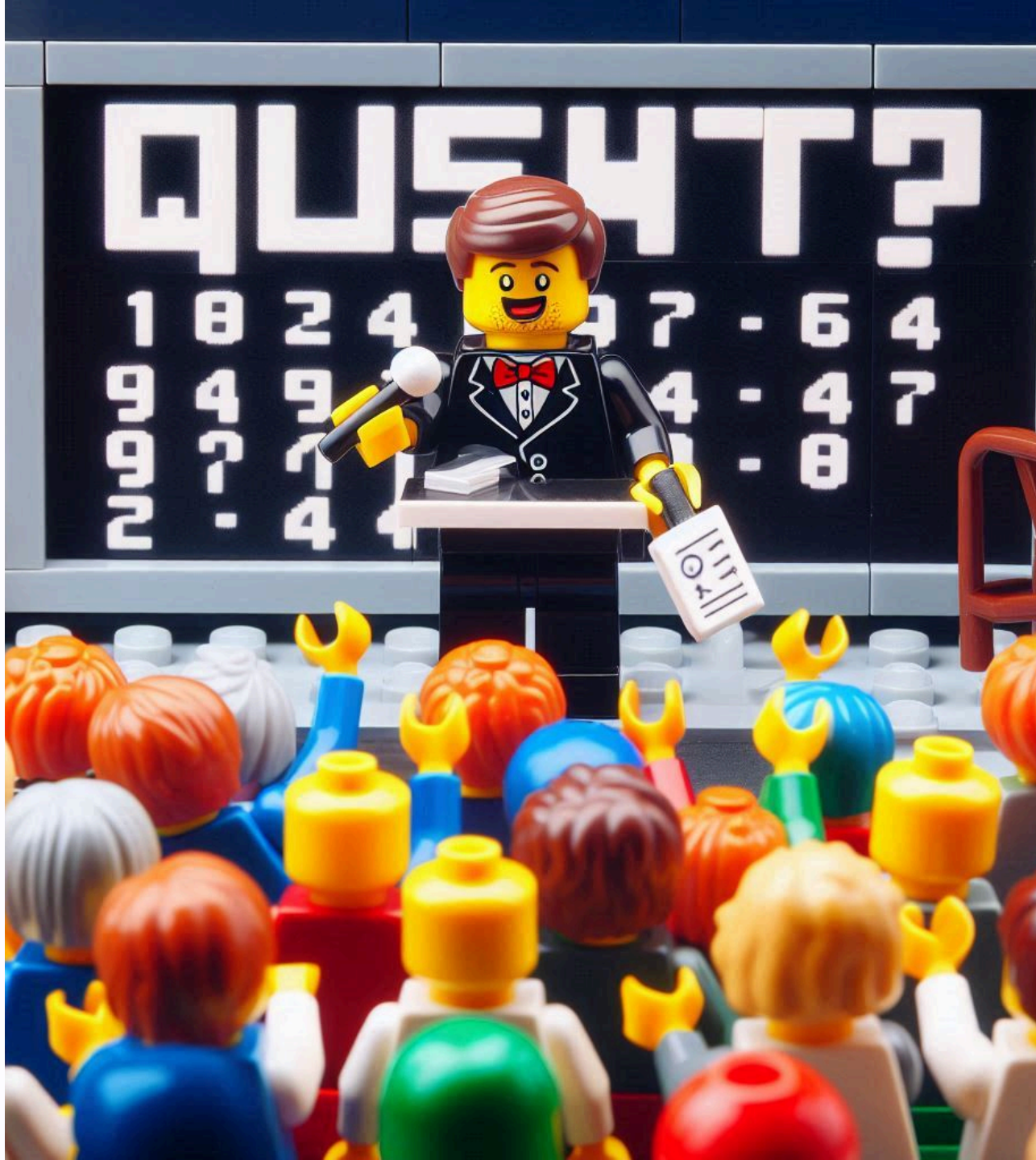
Managed identity?

- Wait, is your functions app running locally?
- How do you get the certificate?
- Show us the Access Control (IAM) in the KeyVault

Takeaways

- Managed identities **need monitoring**
- Mark certificates as `non-exportable`
- Use **sign api** instead of getting the private key
- No public network, private endpoint only

Questions?



Resources

- Source of demo app
- ISV key vault access

I'm Stephan van Rooij

@svrooij Bluesky

Blog: svrooij.io

Slides: slides.svrooij.io