SYMPRAXIS CONSULTING

Pro Code Solutions for Scalable Workflow Management in Microsoft 365

Julie Turner

Julie Turner

Partner/CTO

SYMPRAXIS CONSULTING

Working with SharePoint since 2007

Microsoft MVP since 2017

Microsoft 365 & Power Platform Community Team since 2019

Open-source project co-maintainer: PnPjs & hTWOo

Co-host: Code. Deploy. Go Live show

https://julieturner.net/me

Agenda

What are webhooks and why use them

Architectural pattern for managing subscriptions and events

Cloud Services Overview

Boilerplate code walkthrough

Event handlers

What are Webhooks/Change Events?

…altering the behavior of a web page or web application with custom callbacks.

In Microsoft 365 – SharePoint “webhooks” are supported for list items.

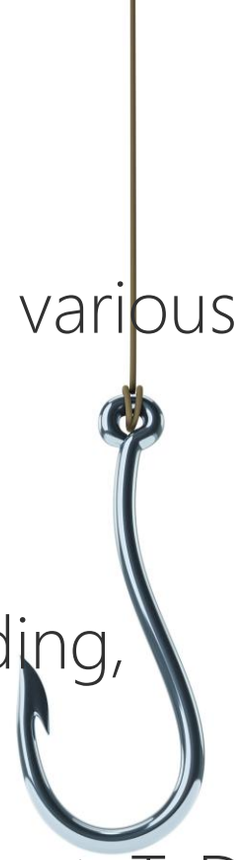
Lists/Libraries

- Expires in 180 days
- Only handles async events (-ed)
- ItemAdded, ItemUpdated, ItemDeleted, ItemCheckedOut, ItemCheckedIn, ItemUncheckedOut, ItemAttachmentAdded, ItemAttachmentDeleted, ItemFileMoved, ItemVersionDeleted, ItemFileConverted

What are Webhooks/Change Events?

In Microsoft 365 – Microsoft Graph Change Events are supported for various objects. Object type indicates limitations.

- Cloud printing, Copilot AI Interactions, OneDrive Items, Groups, SharePoint Lists, Group Conversations, Outlook Messages, Events, Contacts, Security alerts, Teams Approvals, Call Record, Call Recording, Call Transcript, Teams Chat, Chat Message, Teams Channel, Conversation Member, Online Meeting, Presence, Teams Team, Teams Shift, Offer Requests, Shift Change Requests, Time Off Request, ToDo Task, User, SharePoint Sites*
- Many resources have limits or quotas on how many subscriptions can be made against that resource.

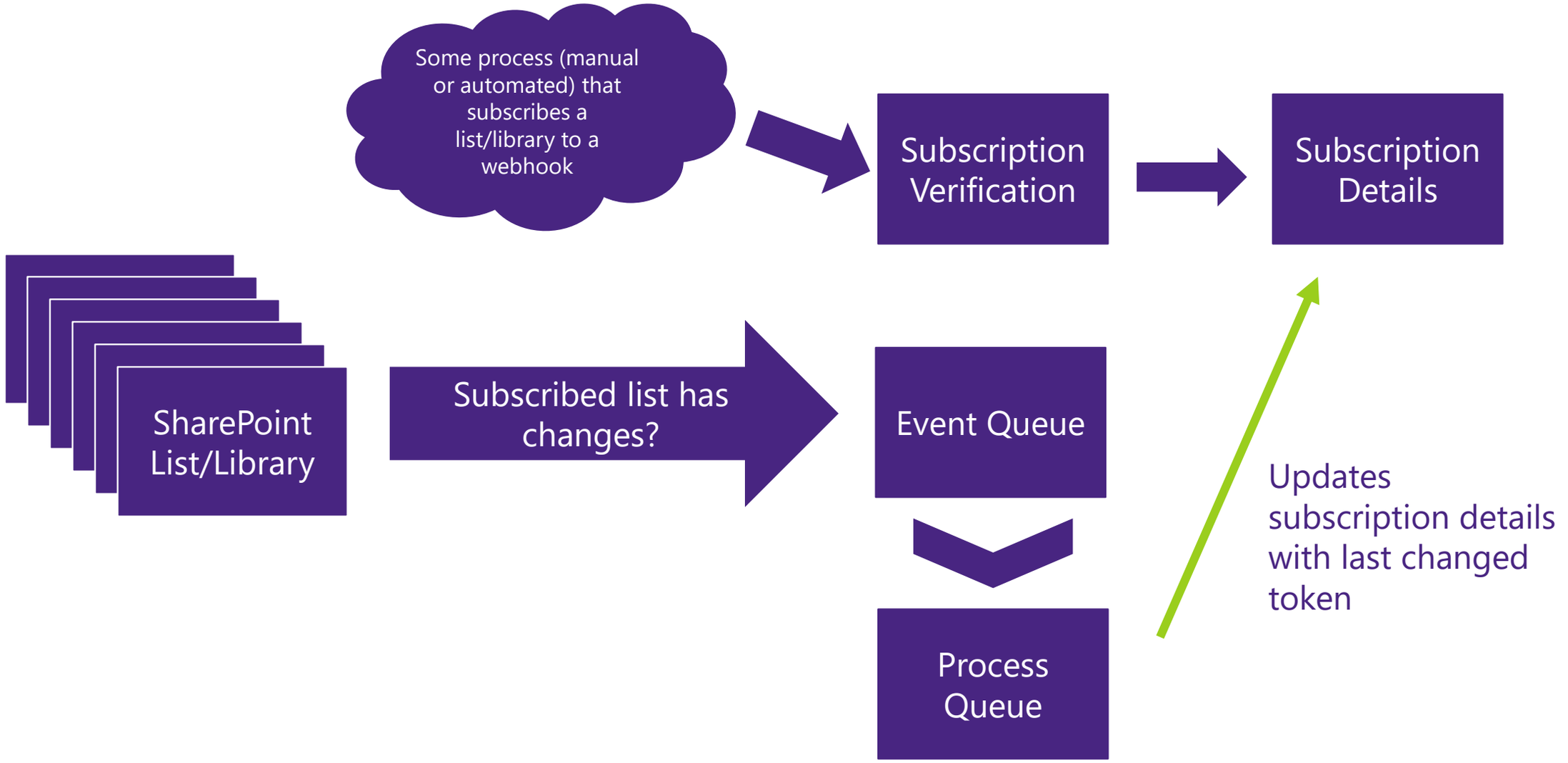


* Not documented but is supported.

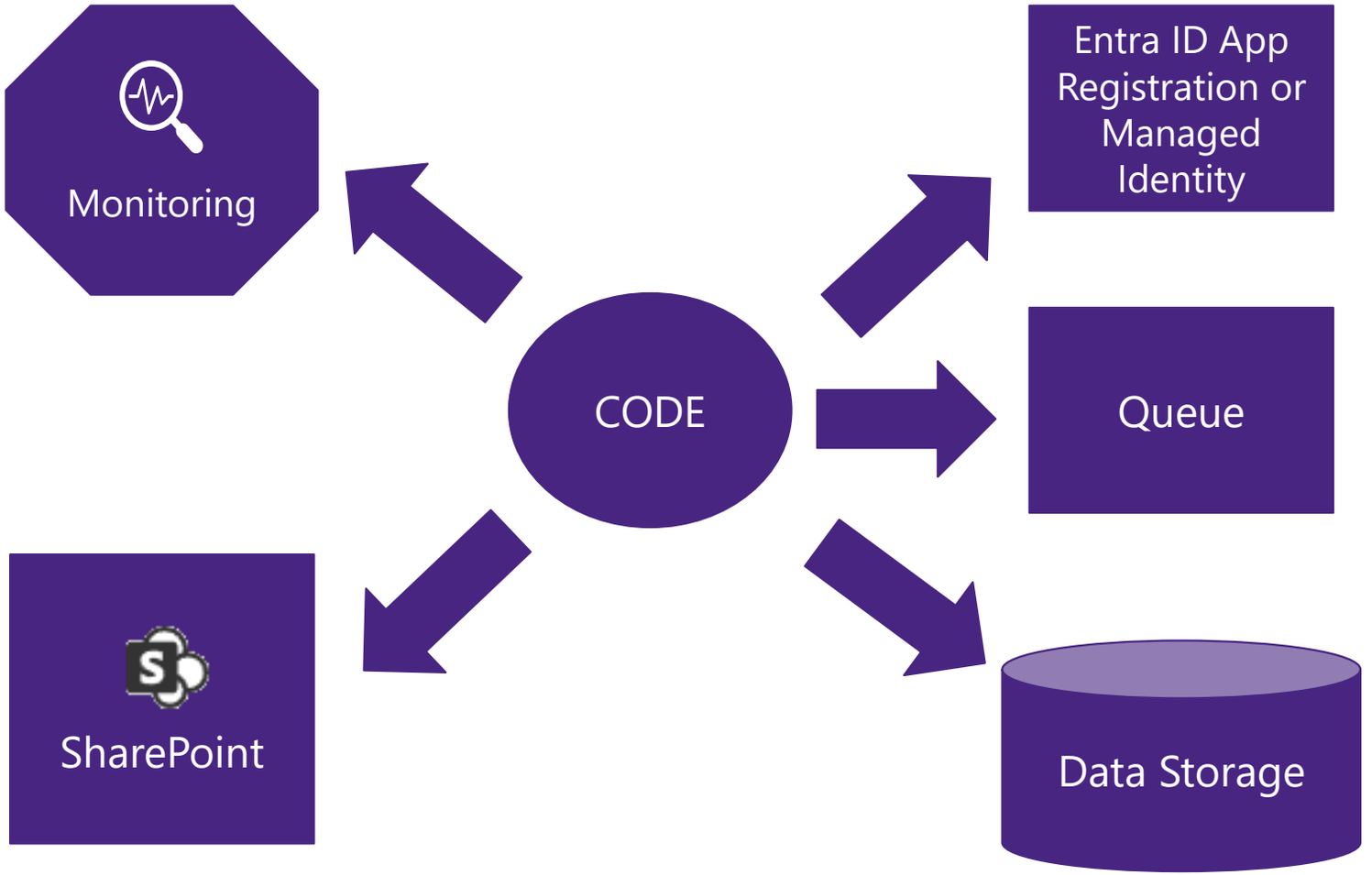
Why use Webhooks/Change Events?

- Other Options: PowerAutomate flows, Azure LogicApps
  - PowerAutomate and LogicApps SharePoint connector is in user context
  - You must manage multiple instances for each object that you want to monitor
  - Actual monitoring of success/failure built into the product
- Webhooks/Change Events are a good option:
  - Complex business process
  - Requires application vs user context
  - Need to act on multiple objects with the same/similar logic

Process


Some process (manual or automated) that subscribes a list/library to a webhook
Subscription Verification
Subscription Details
SharePoint List/Library
Subscribed list has changes?
Event Queue
Process Queue
Updates subscription details with last changed token

Architectural Overview



Provides Application access to SharePoint

Library change notifications are written to the queue to be processed

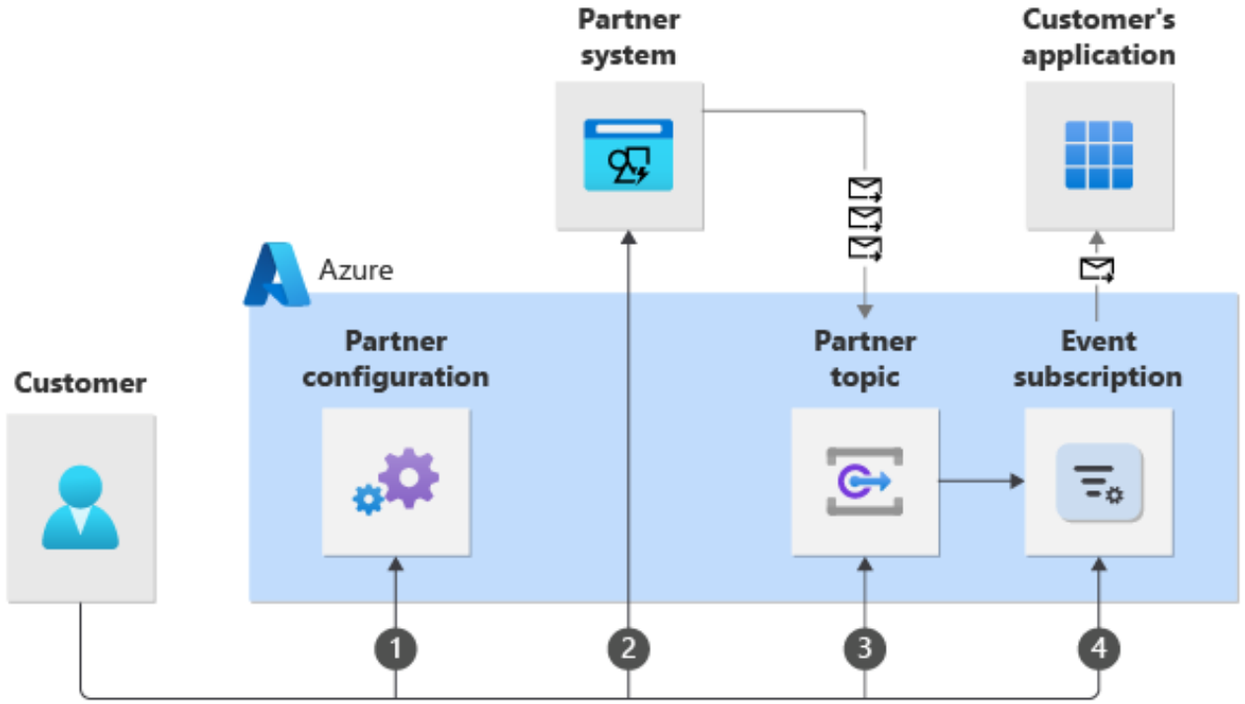
Site Collection Subscriptions
List Webhook Subscriptions
Last Change Token for Webhook

Cloud Services - Azure

Service	Used for
Resource Group	A container for all your Azure resources related to this solution
Azure Storage	Queue store to manage event notifications and subscription info
Key Vault	Stores secrets and certificates
Function App	Code to manage subscription and execute custom event handlers
AAD App Registrations	Provides app credentials for the function apps.
Application Insights (Opt)	Provides diagnostic logging support
Azure Event Grid	Provides relay for change events

Event Grid

1. Authorize partner to create a partner topic in a resource group you designate.
2. Partner provisions a partner topic in the specified resource group of your Azure subscription.
3. Activate the partner topic.
4. Subscribe to events by creating one or more event subscriptions for the partner topic.



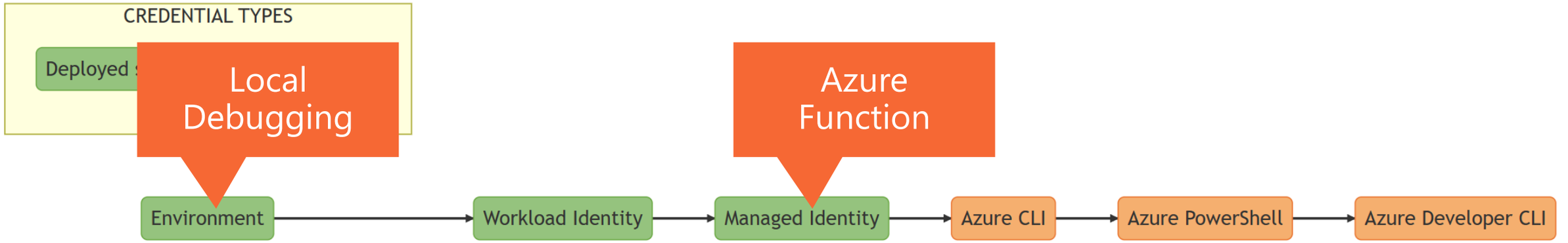
Security

- EntraId App Registrations/ MSAL
- Managed Identity/ Azure Identity

@Azure/Identity

DefaultAzureCredential

- Environment - account information specified via environment variables and use it to authenticate.
- Workload Identity - deployed to Azure Kubernetes Service with Managed Identity enabled
- Managed Identity - deployed to an Azure host with Managed Identity enabled
- Azure CLI - developer has authenticated an account via the Azure CLI az login command
- Azure PowerShell - developer has authenticated using the Azure PowerShell module Connect-AzAccount command
- Azure Developer CLI - developer has authenticated an account via the Azure Developer CLI azd auth login comman

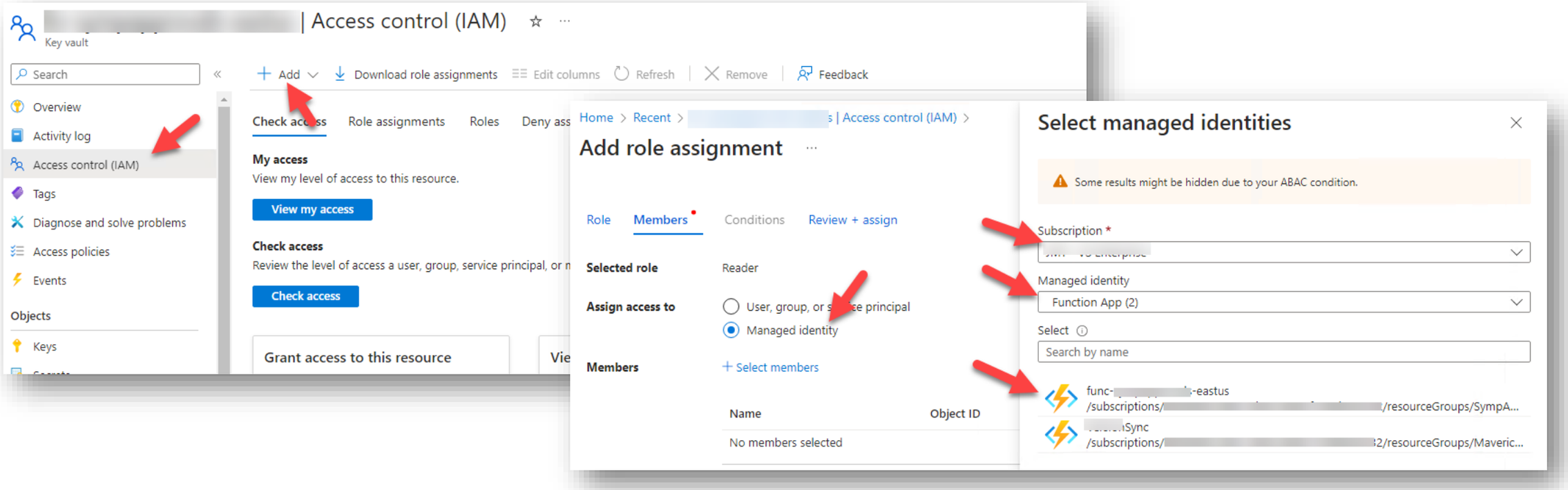


Managed Identity

Managed identities in Azure are a service that allows Azure resources to authenticate cloud services without the need for storing credentials in code or configuration files.

- You don't need to manage credentials.
  - Credentials aren’t even accessible to you.
- You can use managed identities to authenticate to any resource that supports Microsoft Entra authentication, including your own applications.
- Managed identities can be used at no extra cost.
- System-assigned
  - 1:1 relationship with the azure resource and its lifecycle is tied to the resource
- User-assigned
  - 1:many relationship to azure resources
- You authorize a managed identity to have access to one or more services

Authorizing a managed identity




```
m365 login --authType browser

m365 aad approleassignment add --appObjectId "1022615c-4433-4731-a933-53a9d2770e76" --resource "Microsoft Graph" --scopes "Files.ReadWrite.All,Group.
Read.All,Mail.Send,User.Read.All"

m365 aad approleassignment add --appObjectId "1022615c-4433-4731-a933-53a9d2770e76" --resource "SharePoint" --scopes "Sites.FullControl.All"

m365 aad approleassignment add --appObjectId "1022615c-4433-4731-a933-53a9d2770e76" --resource "SharePoint" --scopes "TermStore.ReadWrite.All"
```

DEMO

Summary

- Set up the Azure Infrastructure
- Created a NodeJS project and configured it
- Added helper functions for logging and authentication
- Created TypeScript Interfaces for SharePoint list changes and EventGrid subscriptions
- Created triggers to handle subscription renewal and events, putting the events on a queue to be processed
- Processed the change events and stored the last change token so that we only pick up changes that we haven't successfully processed when a new event fires.

Resources

- Overview of SharePoint webhooks
- Microsoft Graph Subscription Resource
- Microsoft Graph API change notifications
- Subscribe to events published by a partner with Azure Event Grid
- Receive Microsoft Graph API change events through Azure Event Grid
- How to find SharePoint site collections and OneDrive for Business drives