



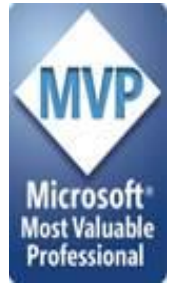
# Open Source Approach to Teams Provisioning

Tuesday, June 1, 2021  
12 - 1 PM Eastern Time

# Peter Carson



- President, Extranet User Manager
- Office Apps and Services Microsoft MVP
- [peter.carson@extranetusermanager.com](mailto:peter.carson@extranetusermanager.com)
- [blog.petercarson.ca](http://blog.petercarson.ca)
- [www.extranetusermanager.com](http://www.extranetusermanager.com)
- Twitter @carsonpeter
- President Toronto SharePoint User Group



2008

Envision IT built custom Extranet solution

2010



2012

Extranet User Manager (EUM) Installer created



Office 365 support

2014

2016



Azure B2B support

User-Centric EUM Login Teams, SPFx, and Flow

2017

Partner Program launched

2019

2009



2011

Productization of code base begins

2015

EUM Brand and Website launched



International Association of Microsoft Channel Partners  
Apps Development Partner Award 2015  
WINNER - CANADA Region

2018

EUM V4 Launched



2021

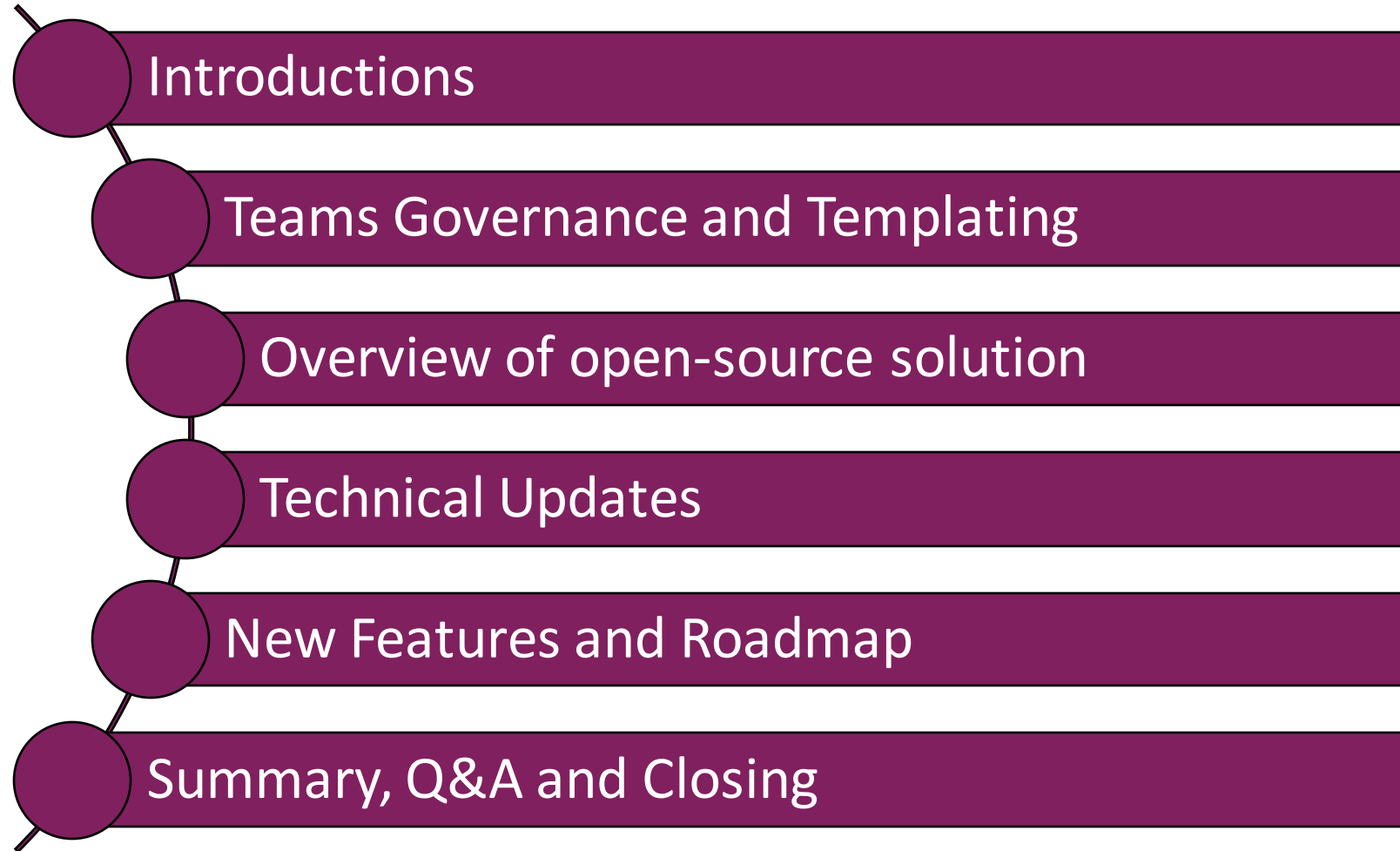
EUM Products Website Relaunched

# Customers around the Globe



100+ Customers Deployed Globally

# Agenda



# Microsoft Forms Poll



3. Which of the following do use today or are planning on using?

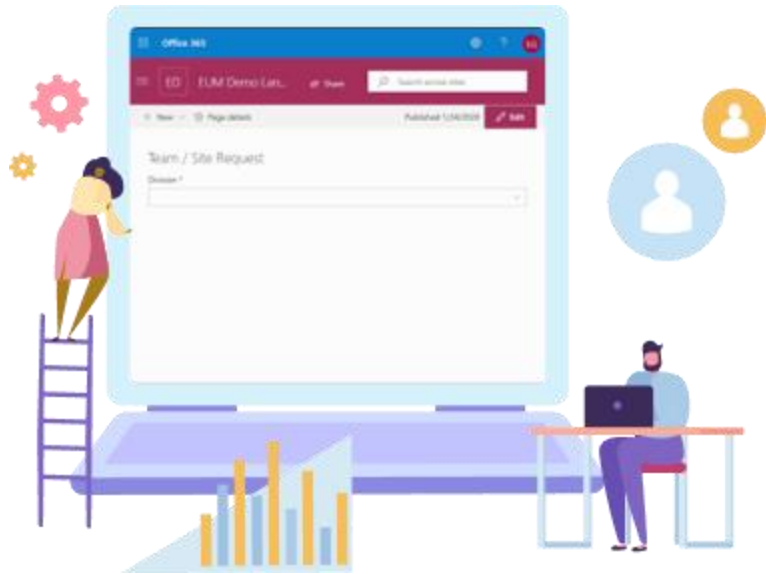
	Not sure what this is	Interested	Investigating	Actively using
Teams Provisioning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SharePoint Framework (SPFx)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Azure Logic Apps	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
PowerShell	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Azure Automation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Service Principals	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Azure DevOps	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Continuous Integration	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

<https://bit.ly/2RODCys>

# Business Case for Teams Governance and Templating

- **COVID and remote working has caused an explosion of Teams adoption**
- **Most of this has been unplanned**
  - No consistency between Teams or SharePoint sites
- **Self-service is important**
- **No one likes rules – don't force me to work in a certain way**

# Teams Governance, Templating, and Provisioning



EUM Open Source Solution  
<http://eum.co/teams>



Orchestry  
[www.orchestry.com](http://www.orchestry.com)



# Other Products

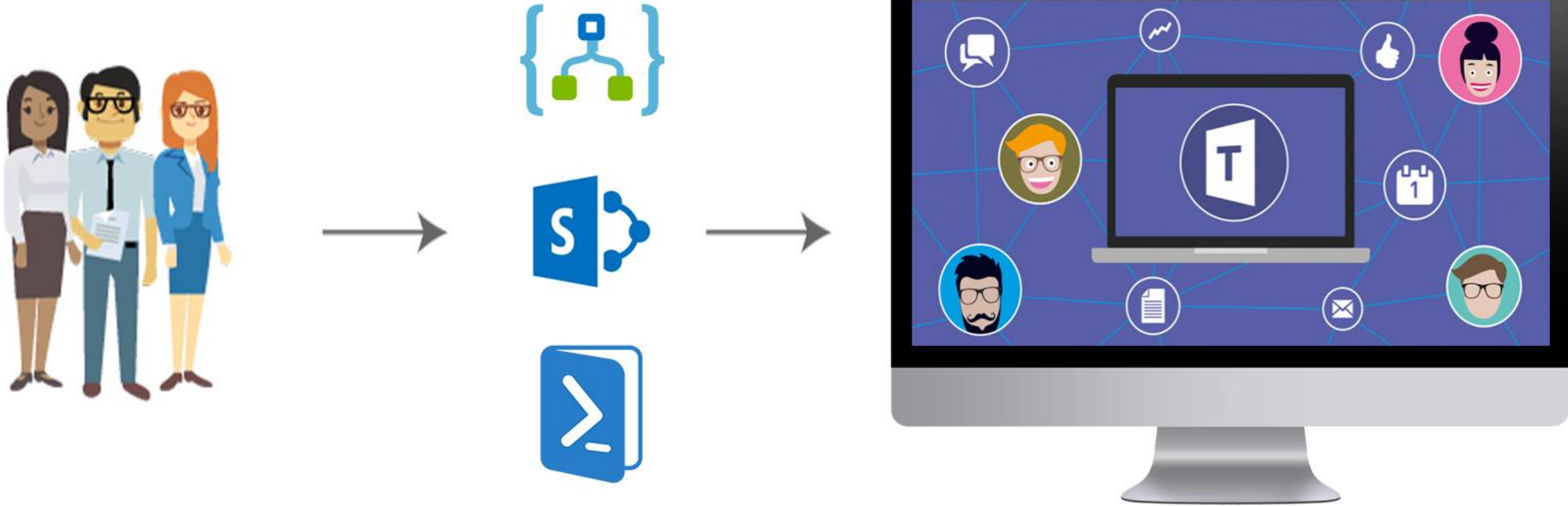
- [ShareGate Apricot](#)
- [AvePoint](#)
- [Valo Teamwork](#)
- [ProvisionPoint 365](#)

# Open-Source Overview

# Solution Requirements

- **Self service form for end users**
- **Approvals if required**
- **Easily extensible and customizable for each organization's requirements**
- **Leverage out of the box and customized site templates**
- **Support for Modern sites, Microsoft 365 Groups, and Microsoft Teams**
- **No Visual Studio or compiled code needed. PowerShell and configuration that IT Pros can get their heads around**

# Supporting Technologies



# When Creating a Team You Get



- **Microsoft 365 Group**
- **SharePoint Modern Team Site**
- **OneNote notebook**
- **Planner Plan**
- **Outlook Group**

# Requesting a Team, Microsoft 365 Group, or SharePoint Site

Team / Site Request

Division \*  
Demo

Site Template \*  
Modern Team Site

Title \*

Purpose

Alias

Public Group  
 Yes





Create Team  
 Yes

**Submit** Cancel

- **SPFx web part to make the self-service request**
- **Can be used from Teams or SharePoint**
- **Supports different Templates grouped under different Divisions**
- **Options for creating Teams, Groups, Sites, OneNotes, and Plans**
  - PnP template for SharePoint Site
  - Planner template for Buckets and Tasks
  - Templating of Tabs in Teams for above
- **Form fields are dynamically generated based on template content types**
  - Easy to add or change fields on the form – no programming required

# Sites List Web Part

Sites

 <b>Private Group - No Approvals</b>  This group is private and is not shown on the list page of all public groups. To join the group you need the invitation URL. Joining a group is done immediately with no approvals required.	 <b>Private Group with Approval</b>  This group is private and is not shown on the list page of all public groups. To join the group you need the invitation URL. Joining a group submits a request for approval before you are added to the group.	 <b>Public Group - No Approval</b>  This is a Public Group that anyone can join. It does not require approval.	 <b>Public Group with Approval</b>  This is a Public Group that anyone can request to join. The user will be notified via email once the request has been approved.
--	---	--	---

- **Displays Sites from the Sites list**
- **Filters down to sites under a Parent URL**
- **Different views**
  - Tile
  - List
  - A – Z List

## Demo Sites

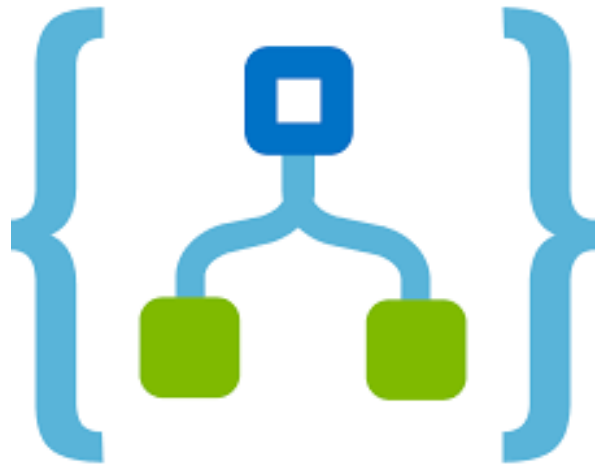
[Private Group - No Approvals](#)  
[Private Group with Approval](#)  
[Public Group - No Approval](#)  
[Public Group with Approval](#)

## All Sites

A B C E F H I K L M N O P R S T V W

[About Us](#)  
[Annual reports](#)

# Azure Logic Apps



- Platform underneath Power Automate
- Same designer
- Slightly different set of actions
  - No pre-built approval
- Visual Studio and Azure DevOps integration

<https://azure.microsoft.com/en-ca/services/logic-apps/>

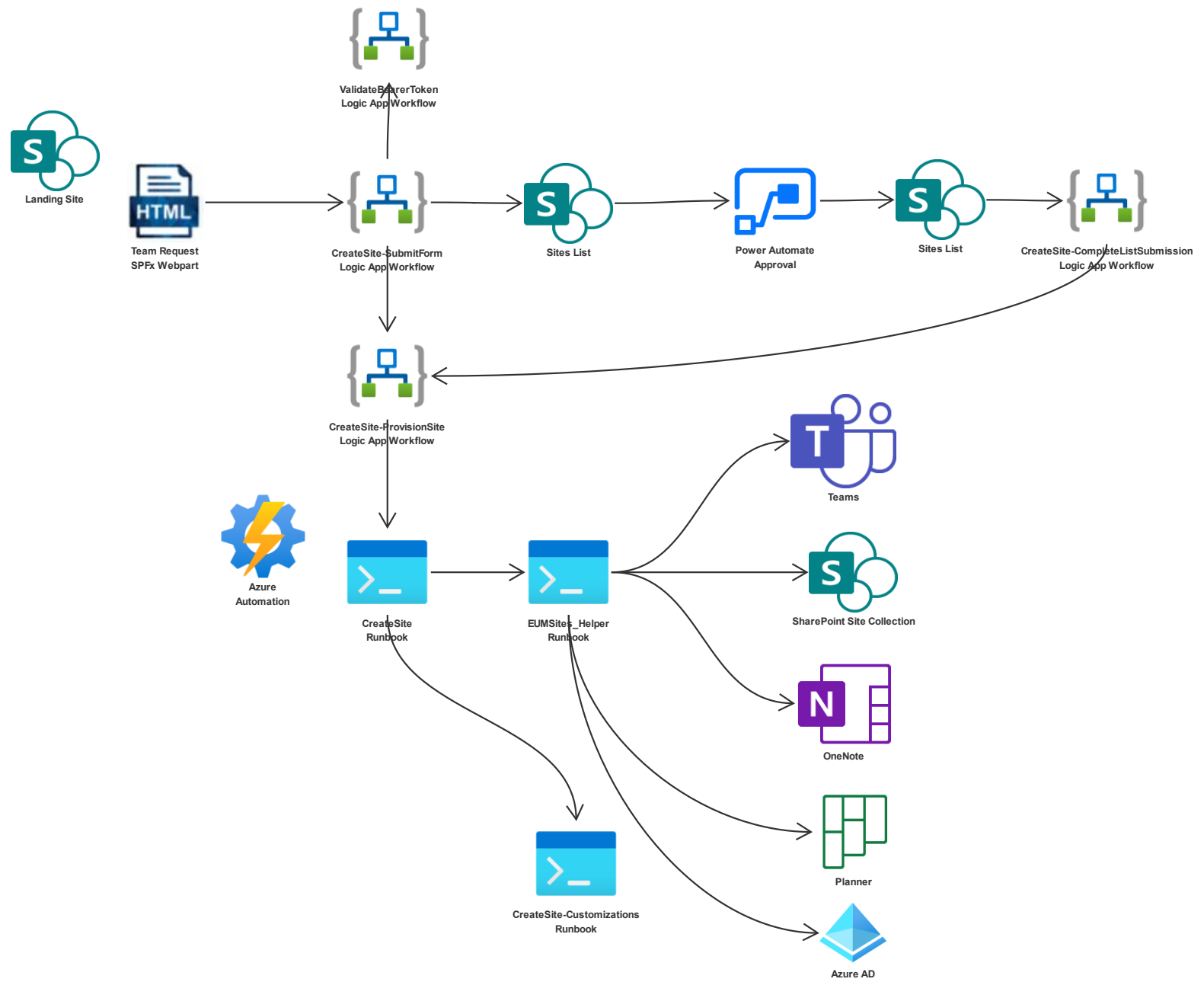


# Azure Automation



- **Run PowerShell scripts in the cloud**
- **No management of the VM needed, Azure takes care of that**
- **Very cost effective**
  - 500 minutes of runtime included free per month
  - \$.002/minute USD after that

<https://azure.microsoft.com/en-ca/services/automation>



Search (Ctrl+V)

Add 
 Edit columns 
 Delete resource group 
 Refresh 
 Export to CSV 
 Open query 
 Assign tags 
 Move 
 Delete 
 Export template 
 Feedback 
 Open in mobile

- Overview
- Activity log
- Access control (IAM)
- Tags
- Events
- Settings**
- Deployments
- Security
- Policies
- Properties
- Locks
- Cost Management**
- Cost analysis
- Cost alerts (preview)
- Budgets
- Advisor recommendations
- Monitoring**
- Insights (preview)
- Alerts
- Metrics
- Diagnostic settings
- Logs
- Advisor recommendations
- Workbooks

Essentials

Subscription (change) : [Envision IT Dev Pay-As-You-Go](#) Deployments : **11 Succeeded**

Subscription ID : b906693c-5167-4a56-bbf3-b56142ee7219 Location : Canada Central

Tags (change) : [Click here to add tags](#)

Filter for any field... Type == all Location == all + Add filter

Showing 1 to 14 of 14 records.  Show hidden types

No grouping

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/> azureautomation	API Connection	Canada Central
<input type="checkbox"/> office365	API Connection	Canada Central
<input type="checkbox"/> sharepointonline	API Connection	Canada Central
<input type="checkbox"/> teams	API Connection	Canada Central
<input type="checkbox"/> eitdev-siteprovisioning	Automation Account	Canada Central
<input type="checkbox"/> kvEUMSites	Key vault	Canada Central
<input type="checkbox"/> CreateSite-CompleteListSubmission	Logic app	Canada Central
<input type="checkbox"/> CreateSite-ProvisionSite	Logic app	Canada Central
<input type="checkbox"/> CreateSite-SubmitForm	Logic app	Canada Central
<input type="checkbox"/> ValidateBearerToken	Logic app	Canada Central
<input type="checkbox"/> CreateSite (eitdev-siteprovisioning/CreateSite)	Runbook	Canada Central
<input type="checkbox"/> CreateSite-Customizations (eitdev-siteprovisioning/CreateSite-Customizations)	Runbook	Canada Central
<input type="checkbox"/> EUMSites_Helper (eitdev-siteprovisioning/EUMSites_Helper)	Runbook	Canada Central
<input type="checkbox"/> UpdateSitesList (eitdev-siteprovisioning/UpdateSitesList)	Runbook	Canada Central

# Project Documentation

- **Source code is available on GitHub at [GitHub - petercarson/eum-sites at V5](https://github.com/petercarson/eum-sites)**
- **Full consolidated whitepaper with step by step instructions**  
<https://www.extranetusermanager.com/resources/articles/teams-and-channels-governance-and-automation-whitepaper>
  - Requires updating to latest deployment process

# Technical Updates

# Moving to Microsoft's PnP Core Libraries

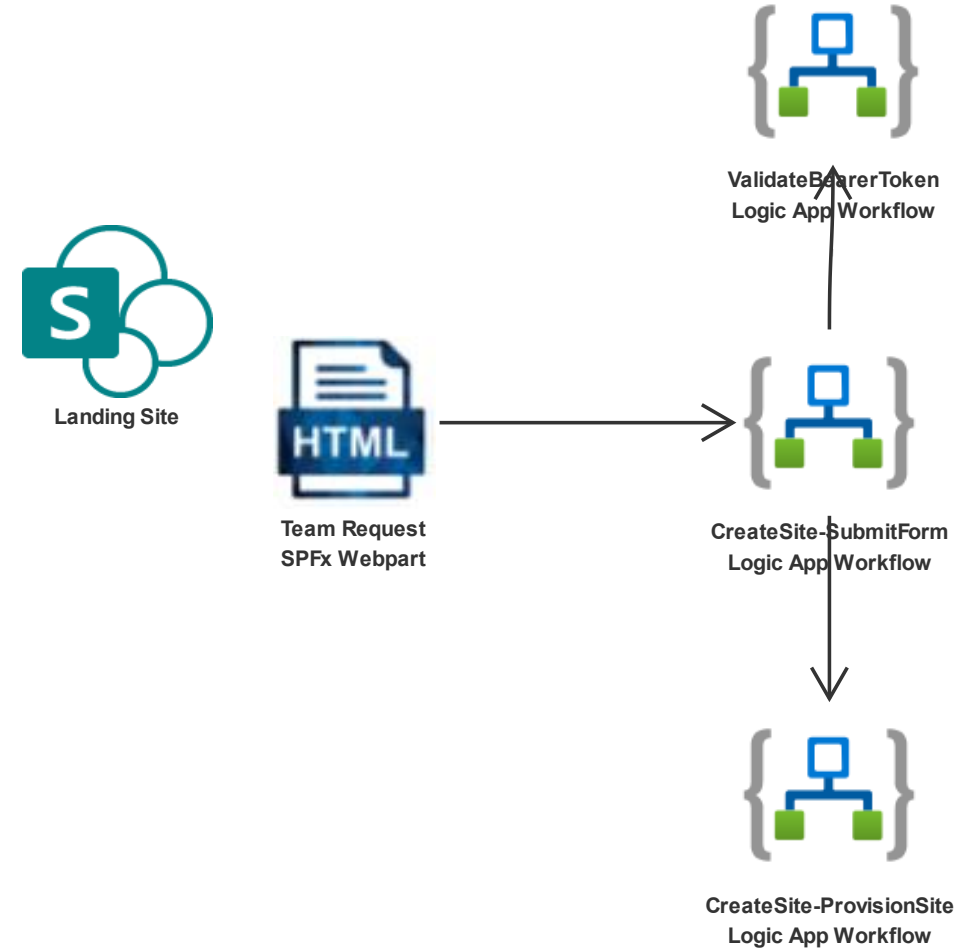
- **PnP Core SDK is a modern .NET SDK designed to work for Microsoft 365**
- **.NET 5 and .NET Standard 2.0 cross-platform support**
- **Unified object model**
  - SDK handles determining the best API
  - Graph, SharePoint, REST or CSOM
- **Batching support at the API level**
  - Reduce calls to the service with retry logic to handle cases such as service throttling
- **Includes a templating engine to capture and apply templates to SharePoint sites**
- **Better support for service principals to improve security of solutions**

[Getting started with PnP Core SDK - Microsoft Tech Community](#)

[PnP provisioning engine and the Core library | Microsoft Docs](#)

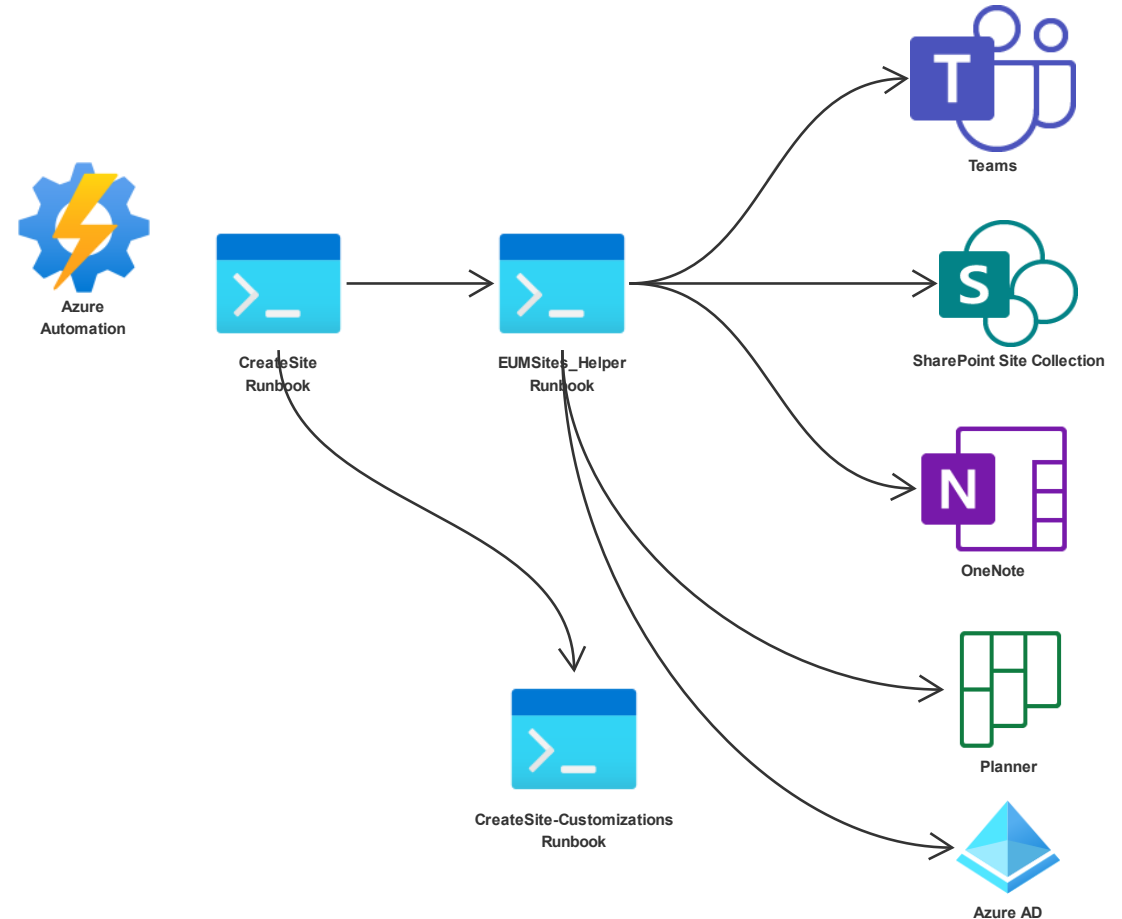
# Logic Apps Workflow

- **Modularized workflows**
- **CreateSite Logic App triggered by a POST from the webpart**
- **Validates the bearer token submitted to secure the endpoint**
- **Determines if there is an Approver defined on the SharePoint List**
  - If Rejected, email is sent letting requestor know reason for rejection
- **Calls Azure Automation Runbook which provisions the Team / Site**
- **Notification email / Teams chat is sent**



# Azure Automation

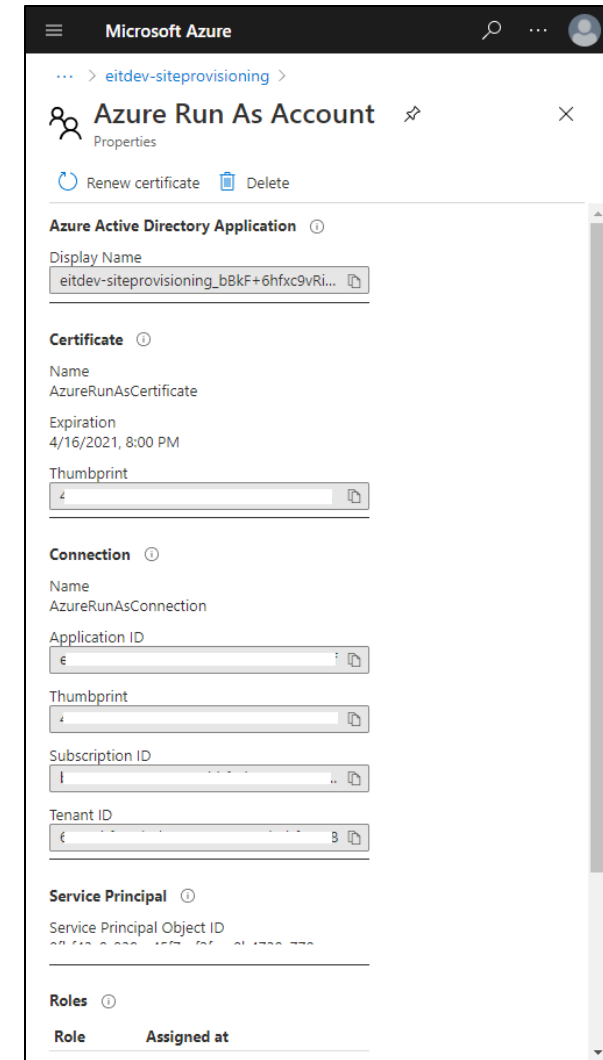
- PowerShell scripts updated to latest PnP Core
- Built using Service Principal app access
- RunAs account in Azure Automation manages the certificate and app registration in Azure AD
- API roles assigned to RunAs service principal
- Still some challenges with Planner
  - Graph API doesn't support App Only access
  - Need a user token for delegated access
  - User needs access to all the Plans
  - We store a delegated refresh token in Key Vault that is valid for 90 days
  - Need to re-authenticate every 90 days





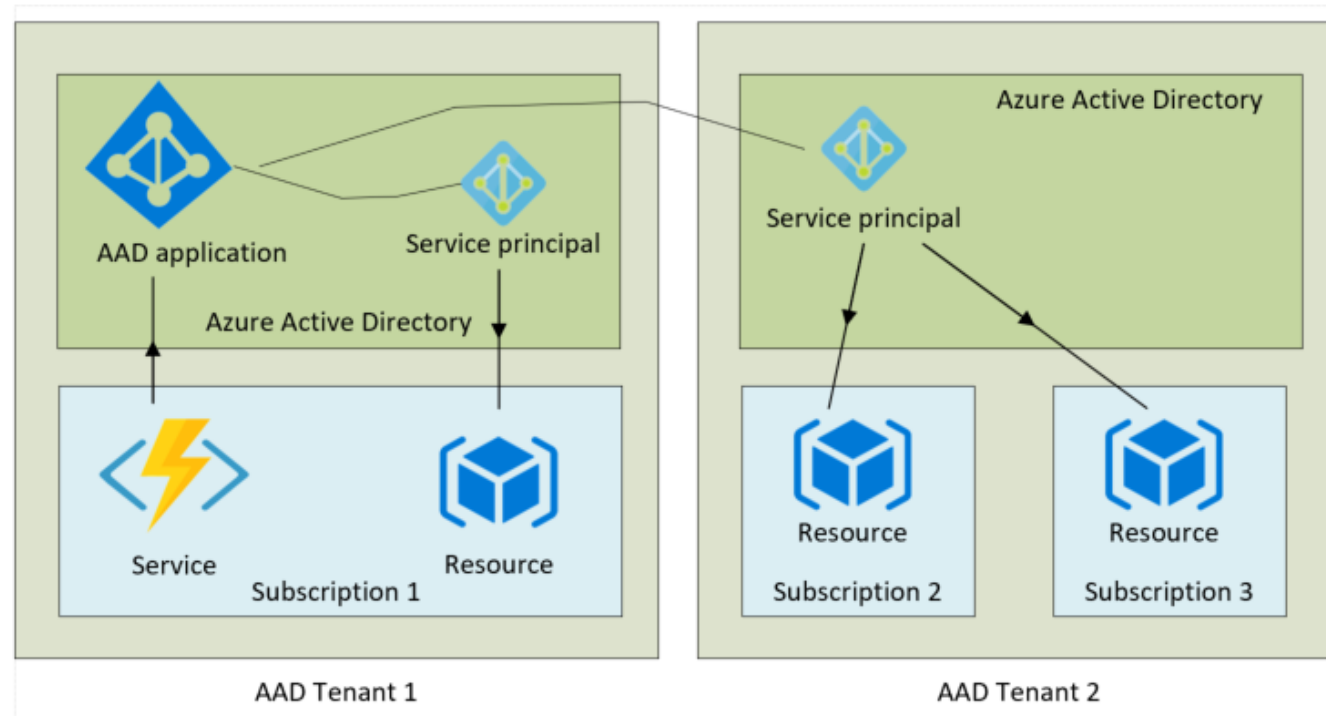
# Security Best Practices

- **Setup Web Part to authenticate to Logic App securely through bearer token**
  - Validated by Azure AD
  - Token can be parsed to determine who made the request
- **No rights needed to SharePoint sites list by requestor**
- **A-Z webpart uses search to search sites the user has access to**
- **Azure Run As Account in Azure Automation**
  - Creates an identity in Azure AD for the Automation Account
  - Uses certificates to authenticate
  - Azure Automation takes care of certificate management
  - Assign limited permissions against Graph API



# Azure AD Apps and Service Principals

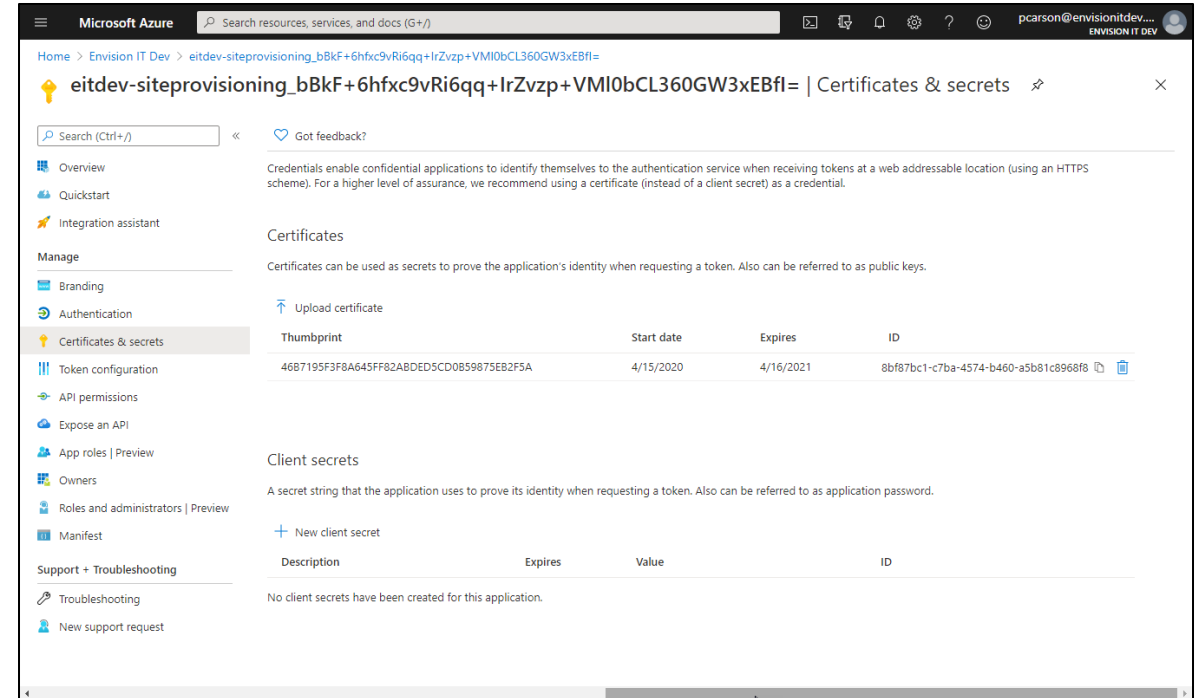
[Apps & service principals in Azure AD - Microsoft identity platform | Microsoft Docs](#)



[Managing applications using Azure AD, service principals and managed identities: A permissions story | endjin](#)

# Automation Account RunAs App

- **Public key cert registered in Azure AD**
- **Private key cert stored in hidden key vault for the Automation Account**
- **API Permissions and Roles are assigned to the service principal**
- **Service Principal connection details retrieved by PowerShell running in Azure Automation**
- **Used to authenticate to new PnP, Azure AD, and Teams**



# ARM Template Deployment and Packaging

- **ARM Templates provide an easy way to deploy resources through the Azure Portal**
- **PowerShell scripts to automate the generation of the ARM template, and the deployment of it**
- **Parameterization of the ARM template and the related Logic Apps and Azure Automation accounts**

# Parameters

**Custom deployment** ...  
Deploy from a custom template

Select a template **Basics** Review + create

Template  
Customized template 16 resources  
Edit template Edit parameters

Project details  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*   
Resource group \*   
[Create new](#)

Instance details  
Region \*

Connections\_officed365\_name \*   
Connections\_office365\_name \*   
Connections\_labautomation\_name \*   
Connections\_sharepointonline\_name \*   
Workflows\_validateBearerToken\_name \*   
Workflows\_createSite\_SubmitForm\_name \*   
Workflows\_createSite\_ProvisionSite\_name \*   
Workflows\_createSite\_CompleteListSubmission\_name \*

Automation  
Accounts\_eitdevsiteprovisioning\_name \*

Divisions List GUID   
Operator Email   
Site Address   
Sites List GUID

Automation Account Name   
Primary Domain   
Resource Group Name   
Root URL   
Site Collection Administrator   
Site Collection Relative URL   
Teams SPFx App Id

[Review + create](#) [< Previous](#) [Next: Review + create >](#)



ARM Template  
(JSON)



Name \*   
Type \*   
Default Value   
Actual Value

Name \*   
Type \*   
Default Value   
Actual Value

Name \*   
Type \*   
Default Value   
Actual Value

Name \*   
Type \*   
Default Value   
Actual Value

Name \*   
Type \*   
Default Value   
Actual Value

[Add Parameter](#)



Logic App  
Parameters

**fx eitdev-siteprovisioning | Variables** ...

Automation Account

Search (Ctrl+v) [+ Add a variable](#) [Refresh](#)

Shared Resources

- Schedules
- Modules
- Modules gallery
- Python packages
- Credentials
- Connections
- Certificates
- Variables**

Name	Type	Value	Last modified
AutomationAccountNa...	String	eitdev-siteprovisioning	4/17/2020, 7:32 PM
PrimaryDomain	String	envisionitdev.onmicrosoft.com	4/11/2021, 2:56 PM
ResourceGroupName	String	EUMSites	4/17/2020, 7:33 PM
RootURL	String	https://envisionitdev.sharepoint.com	4/11/2021, 2:51 PM
SiteCollectionAdminist...	String	pcarson@envisionitdev.onmicrosoft.com	4/17/2020, 7:35 PM
SiteCollectionRelativeU...	String	/sites/landing	4/11/2021, 2:51 PM
TeamsSPFxAppId	String	c62c7bd0-0313-4438-895e-a26ac6a97024	4/17/2020, 7:36 PM



Automation Account  
Variables

# Generating the ARM Template

## Export from the Azure Portal

- **Export at Resource Group level**
- **Exports all resources into one template**
- **No parameters defined for Logic Apps or Automation Accounts**
- **Manual editing of JSON file to add parameters**
  - Time consuming and error prone
  - Needs to be repeated for each deployment packaging

## ARMTemplateGenerator.ps1 PowerShell

- **Targets a Resource Group and exports all resources into one template**
- **Also exports individual templates for source control**
  - Let's you manage and track changes at the resource level
- **Parameter definition file**
  - Defines ARM template parameters to be added
  - Defines mappings to Logic App parameters and Automation variables
- **Repeatable process**

# Deploying the ARM Template

## Azure Portal

- Load the template and parameter JSON files into the portal
- Adjust the parameters as required
- Fix up the Logic Apps and Automation Accounts if not wired into the template parameters
- Create the RunAs account for Automation
- Set the API permissions and grant consent
- Deploy the Runbook scripts

## ARMTemplateDeployer.ps1 PowerShell

- Deploys the template and parameters into the target Resource Group
- Parameters are already properly connected
- Create the RunAs account
  - Certificate
  - Azure AD registration of service principal
  - Provisioning of account
  - Set the API permissions
- Deploys the Runbook scripts
- Admin needs to grant consent for API permissions

# Related Webinars



## [Secure Development with Microsoft 365 and Azure AD \(Part 1 of 2\)](#)

**Apr 20, 2021**

Ensuring your development practices are secure is extremely important. At Extranet User Manager and Envision IT, we set out high standards to follow with Microsoft 365 and Azure AD at the core of our practice.



## [Microsoft 365 SDLC Best Practices \(Part 2 of 2\)](#)

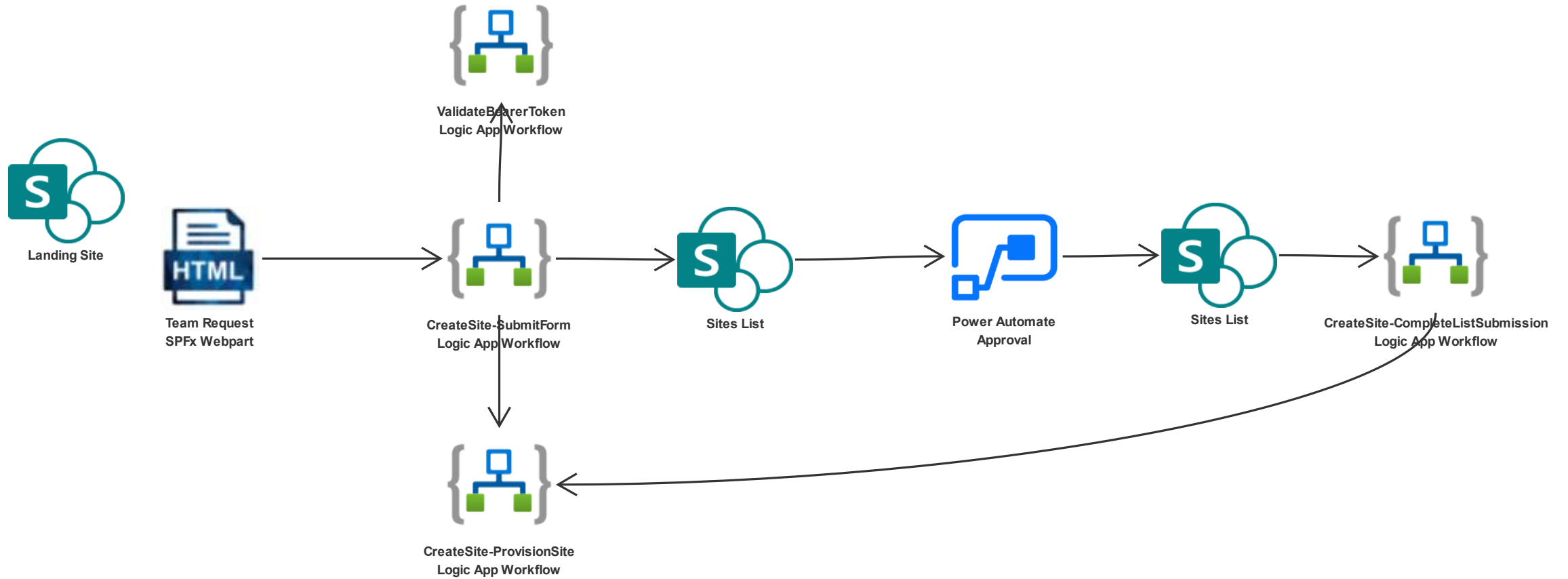
**May 4, 2021**

This webinar is Part 2 of 2 in our Secure Development in the Microsoft Cloud webinar series. Previously we reviewed how to make Azure AD core to your application security strategy.



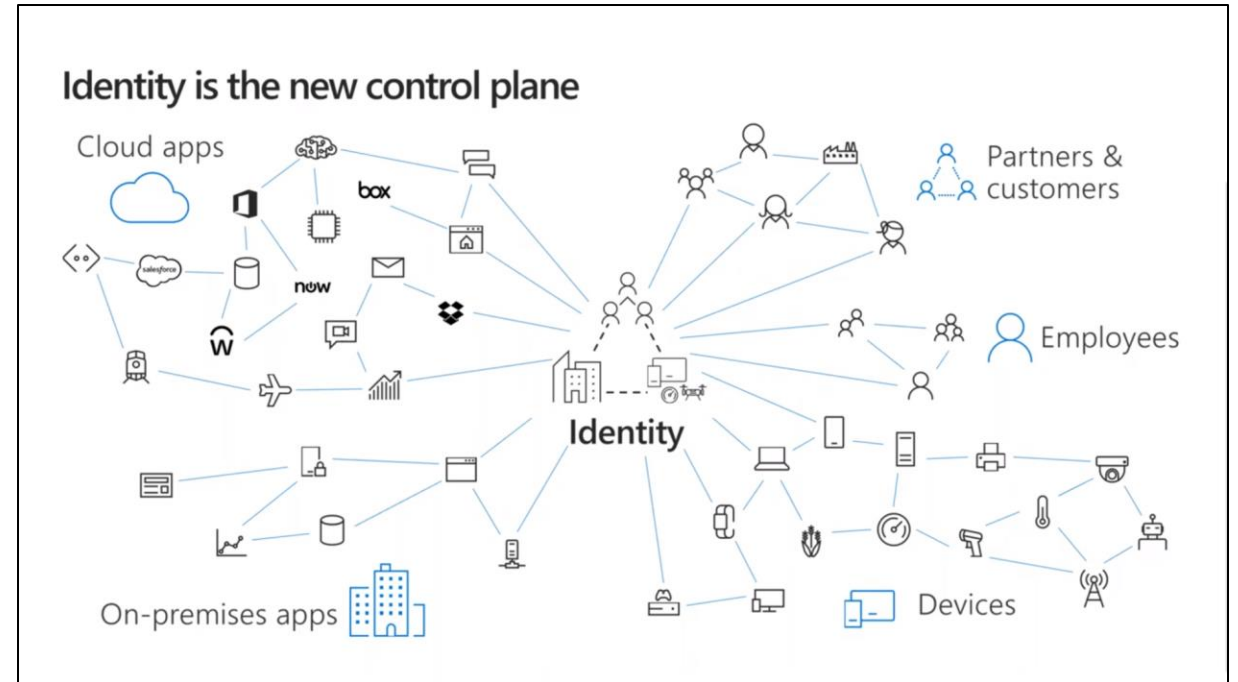
# Roadmap

# Power Automate Approval Workflows



# Integrating with Azure AD Access Reviews

- Azure AD Premium P2 License Requirement



[What are access reviews? - Azure Active Directory | Microsoft Docs](#)

# Additional Features

- **Request additional Team owners**
- **Team prefix defined by site template**
  - Currently supported by division
- **Whitelisted Domain Support for External Template**
- **Add expected collaboration end date**
- **Add owners for external shared Teams to AAD Guest Inviter role**
- **Support applying sensitivity labels based on template chosen**

# Wrap-Up Points

- **Updated to use latest version of PnP PowerShell**
  - <https://github.com/pnp/powershell>
- **Uses Azure RunAs service principal for authentication**
  - Improved security
  - No need for user accounts with MFA disabled
- **Packaged in an ARM Template for easy deployment**
- **Simplified architecture**
  - No API to deploy
  - Request webpart POSTs directly to Logic App securely

# Additional Open-Source Teams Provisioning Resources

- [Teams and Channel Governance and Automation Whitepaper](#)
- [Join Your ERP and Microsoft Teams At The Hip \(Part 1 of 2\)](#)
- [Join Your ERP and Microsoft Teams At The Hip – Technical Deep Dive \(Part 2 of 2\)](#)
- [TSPUG: Building a Teams and SharePoint Provisioning Solution with SPFx, Logic Apps, Azure Automation, and PnP](#)
- [Provisioning in Microsoft Teams with Extranet User Manager Open Source Article](#)

# Upcoming Webinars



## Managing Complex Projects with Microsoft 365

June 8, 2021  
12 pm – 1 pm EST



## Microsoft 365 Unstructured and Structured External Sharing

July 13, 2021  
12 pm – 1 pm EST



## New Azure AD External Identities Features

July 27, 2021  
12 pm – 1 pm EST

Register for all upcoming events at <http://eum.co/resources/events>

# Thank you!

## Questions?

