Microsoft

ESLZ User Guide

Contents

What is Enterprise-Scale?

Enterprise-Scale architecture provides prescriptive guidance coupled with Azure best practices, and it follows 5 design principles across the 8 critical design areas for organizations to define their target state for their Azure architecture. Enterprise-Scale will continue to evolve alongside the Azure platform roadmap and is ultimately defined by the various design decisions that organizations must make to define their Azure journey.

The Enterprise-Scale architecture is modular by design and allow organizations of any size to start with the foundational landing zones that support their application portfolios, and the architecture enables organizations to start as small as needed and scale alongside their business requirements regardless of scale point.

What is Enterprise-Scale reference implementation?

The Enterprise-Scale reference implementations support Azure adoption at scale and provides guidance and architecture based on the authoritative design for the Azure platform as a whole.

Enterprise-Scale reference implementations are tying together all the Azure platform primitives and creates a proven, well-defined Azure architecture based on a multi-subscription design, leveraging native platform capabilities to ensure organizations can create and operationalize their landing zones in Azure at scale.

The following table outlines key customer requirements in terms of landing zones, and how it is being addressed with Enterprise-Scale:

Key customer landing zone requirement	Enterprise-Scale reference implementations
Timelines to reach security and compliance requirements for a workload	Enabling all recommendations during setup, will ensure resources are compliant from a monitoring and security perspective
Provides a baseline architecture using multi-subscription design	Yes, for the entire Azure tenant regardless of customer’s scale-point
Best-practices from cloud provider	Yes, proven and validated with customers
Be aligned with cloud provider’s platform roadmap	Yes
UI Experience and simplified setup	Yes, Azure portal

Key customer landing zone requirement	Enterprise-Scale reference implementations
All critical services are present and properly configured according to recommend best practices for identity & access management, governance, security, network and logging	Yes, using a multi-subscription design, aligned with Azure platform roadmap
Automation capabilities (IaC/DevOps)	Yes: ARM, Policy, GitHub/Azure DevOps CICD pipeline option included
Provides long-term self-sufficiency	Yes, enterprise-scale architecture -> 1:N landing zones. Approach & architecture prepare the customer for long-term self-sufficiency, the RIs are there to get you started
Enables migration velocity across the organization	Yes, enterprise-scale architecture -> 1:N landing zones, Architecture includes designs for segmentation and separation of duty to empower teams to act within appropriate landing zones
Achieves operational excellence	Yes. Enables autonomy for platform and application teams with a policy driven governance and management

Pricing

There’s no cost associated with Enterprise-Scale, and you only pay for the Azure services that are being enabled, and the services your organization will deploy into the landing zones. For example, you don’t pay for the management groups or the policies that are being assigned, but policy to enable Azure Security Center on the landing zone subscriptions will generate cost on those subscriptions.

What if I already have an existing Azure footprint?

Enterprise-Scale reference implementation will meet you where you are, and the design has catered for existing subscriptions and workloads in Azure.

See the following article to learn more how you can transition into Enterprise-Scale.

How Enterprise-Scale works

This section describes at a high level how Enterprise-Scale reference implementation works. Your landing zones are the output of a multi-subscription environment for all your Azure services, where compliance, guardrails, security, networking, and identity is provided at scale by the platform.

Enterprise-Scale design principles

The enterprise-scale architecture prescribed in this guidance is based on the design principles described here. These principles serve as a compass for subsequent design decisions across critical technical domains. Familiarize yourself with these principles to better understand their impact and the trade-offs associated with nonadherence.

Subscription Democratization

Subscriptions should be used as a unit of management and scale aligned with business needs and priorities to support business areas and portfolio owners to accelerate application migrations and new application development. Subscriptions should be provided to business units to support the design, development, and testing of new workloads and migration of workloads.

Policy Driven Governance

Azure Policy should be used to provide guardrails and ensure continued compliance with your organization's platform, along with the applications deployed onto it. Azure Policy also provides application owners with sufficient freedom and a secure unhindered path to the cloud.

Single Control and Management Plane

Enterprise-scale architecture shouldn't consider any abstraction layers, such as customer-developed portals or tooling. It should provide a consistent experience for both AppOps (centrally managed operation teams) and DevOps (dedicated application operation teams). Azure provides a unified and consistent control plane across all Azure resources and provisioning channels subject to role-based access and policy-driven controls. Azure can be used to establish a standardized set of policies and controls for governing the entire enterprise estate.

Application Centric and Archetype-neutral

Enterprise-scale architecture should focus on application-centric migrations and development rather than pure infrastructure lift-and-shift migrations, such as moving virtual machines. It shouldn't differentiate between old and new applications, infrastructure as a service, or platform as a service applications. Ultimately, it should provide a safe and secure foundation for all application types to be deployed onto your Azure platform.

Azure native design and aligned with platform roadmap

The enterprise-scale architecture approach advocates using Azure-native platform services and capabilities whenever possible. This approach should align with Azure platform roadmaps to ensure that new capabilities are available within your environments. Azure platform roadmaps should help to inform the migration strategy and enterprise-scale trajectory.

Separating platform and landing zones

One of the key tenets of Enterprise-Scale is to have a clear separation of the Azure *platform* and the *landing zones*. This allows organizations to scale their Azure architecture alongside with their business requirements, while providing autonomy to their application teams for deploying, migrating and doing net-new development of their workloads into their landing zones. This model fully supports workload autonomy and distinguish between central and federated functions.

Platform responsibilities and functions

Platform resource are managed by a cross-functional platform team. The team consist mainly out of the following functions. These functions working in close collaboration with the SME functions across the organization:

- PlatformOps: Responsible for management and deployment of control plane resource types such as subscriptions, management groups via IaC and the respective CI/CD pipelines. Management of the platform related identify resources on Azure AD and cost management for the platform.
  Operationalization of the Platform for an organization is under the responsibility of the platform function.
- SecOps: Responsible for definition and management of Azure Policy and RBAC permissions on the platform for landing zones and platform management groups and subscriptions. Security operations including monitoring and the definition and the operation of reporting and auditing dashboard.
- NetOps: Definition and management of the common networking components in Azure including the hybrid connectivity and firewall resource to control internet facing networking traffic. NetOps team is responsible to handout virtual networks to landing zone owners or team.

Landing zone owners responsibilities

Enterprise-scale landing zones supporting a both centralized and federated application DevOps models. Most common model are dedicated **DevOps** team aligned with a single workload. In case of smaller workloads or COTS or 3rd party application a single **AppDevOps** team is responsible for workload operation. Independent of the model every DevOps team manages several workload staging environments (DEV, UAT, PROD) deployed to individual landing zones/subscriptions. Each landing zone has a set of RBAC permissions managed with Azure AD PIM provided by the Platform SecOps team.

When the landing zones/subscriptions are handed over to the DevOps team the team is end-to-end responsible for the workload. They can independently operate within the security guardrails provided by the platform team. If dependency on central teams or functions are discovered, it is highly recommended to review the process and eliminated as soon as possible to unblock DevOps teams.

Structure of Enterprise-Scale

The Management Group structure implemented with Enterprise-Scale is as follows:

- **Top-level Management Group** (directly under the tenant root group) is created with a prefix provided by the organization, which purposely will avoid the usage of the root group to allow organizations to move existing Azure subscriptions into the hierarchy, and also enables future scenarios. This Management Group is parent to all the other Management Groups created by Enterprise-Scale
- **Platform:** This Management Group contains all the *platform* child Management Groups, such as Management, Connectivity, and Identity. Common Azure Policies for the entire platform is assigned at this level
- **Management:** This Management Group contains the dedicated subscription for management, monitoring, and security, which will host Azure Log Analytics, Azure

Automation, and Azure Sentinel. Specific Azure policies are assigned to harden and manage the resources in the management subscription.

- **Connectivity:** This Management Group contains the dedicated subscription for connectivity, which will host the Virtual WAN/Virtual Network for the hub, Azure Firewall, DNS, Express Route, VPN Gateway etc. Specific Azure policies are assigned to harden and manage the resources in the connectivity subscription.
- **Identity:** This Management Group contains the dedicated subscription for identity, which is a placeholder for Windows Server Active Directory VMs, or Azure Active Directory Domain Services to enable AuthN/AuthZ for workloads within the landing zones. Specific Azure policies are assigned to harden and manage the resources in the identity subscription.
- **Landing Zones:** This is the parent Management Group for all the landing zone subscriptions and will have workload agnostic Azure Policies assigned to ensure workloads are secure and compliant.
- **Online:** This is the dedicated Management Group for Online landing zones, meaning workloads that may require direct inbound/outbound connectivity.
- **Corp:** This is the dedicated Management Group for Corp landing zones, meaning workloads that requires connectivity/hybrid connectivity with the corporate network thru the hub in the connectivity subscription.
- **Sandboxes:** This is the dedicated Management Group for subscriptions that will solely be used for testing and exploration by an organization's application teams. These subscriptions will be securely disconnected from the Corp and Online landing zones.
- **Decommissioned:** This is the dedicated Management Group for landing zones that are being cancelled, which then will be moved to this Management Group before deleted by Azure after 30-60 days.

What happens when you deploy Enterprise-Scale?

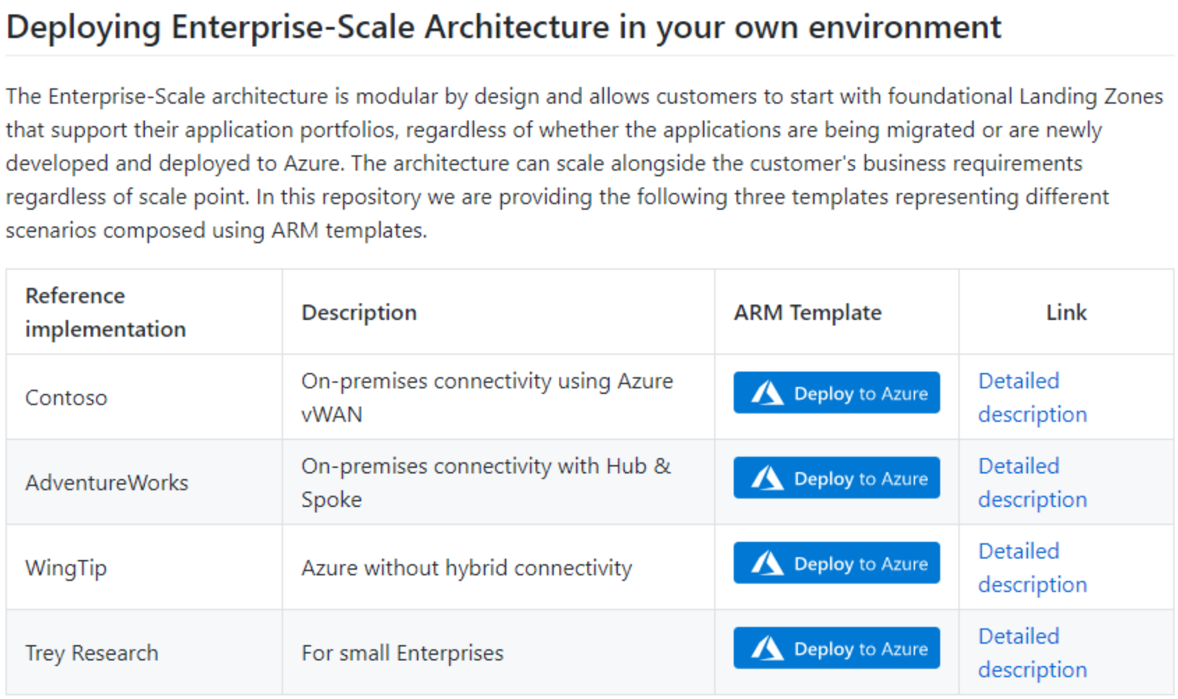
By default, all recommendations are enabled, and you must explicitly disable them if you don't want it to be deployed and configured.

- A scalable Management Group hierarchy aligned to core platform capabilities, allowing you to operationalize at scale using centrally managed Azure RBAC and Azure Policy where platform and workloads have clear separation.
- Azure Policies that will enable autonomy for the platform and the landing zones.
- An Azure subscription dedicated for **Management**, which enables core platform capabilities at scale using Azure Policy such as:
  - A Log Analytics workspace and an Automation account
  - Azure Security Center monitoring
  - Azure Security Center (Standard or Free tier)
  - Azure Sentinel
  - Diagnostics settings for Activity Logs, VMs, and PaaS resources sent to Log Analytics

- When deploying **Adventure Works** and **Contoso**: An Azure subscription dedicated for **Connectivity**, which deploys core Azure networking resources such as:
  - A hub virtual network
  - Azure Firewall
  - ExpressRoute Gateway
  - VPN Gateway
  - Azure Private DNS Zones for Private Link
- (Optionally) An Azure subscription dedicated for **Identity** in case your organization requires to have Active Directory Domain Controllers in a dedicated subscription.
- (Optionally) Integrate your Azure environment with GitHub (Azure DevOps will come later), where you provide the PA Token to create a new repository and automatically discover and merge your deployment into Git.
- Landing Zone Management Group for **Corp** connected applications that require connectivity to on-premises, to other landing zones or to the internet via shared services provided in the hub virtual network.
  - This is where you will create your subscriptions that will host your corp-connected workloads.
- Landing Zone Management Group for **Online** applications that will be internet-facing, where a virtual network is optional and hybrid connectivity is not required.
  - This is where you will create your Subscriptions that will host your online workloads.
- Landing zone subscriptions for Azure native, internet-facing **Online** applications and resources.
- Landing zone subscriptions for **Corp** connected applications and resources, including a virtual network that will be connected to the hub via VNet peering.
- Azure Policies for online and corp-connected landing zones, which include:
  - Enforce VM monitoring (Windows & Linux)
  - Enforce VMSS monitoring (Windows & Linux)
  - Enforce Azure Arc VM monitoring (Windows & Linux)
  - Enforce VM backup (Windows & Linux)
  - Enforce secure access (HTTPS) to storage accounts
  - Enforce auditing for Azure SQL
  - Enforce encryption for Azure SQL
  - Prevent IP forwarding
  - Prevent inbound RDP from internet
  - Ensure subnets are associated with NSG

Deploying Enterprise-Scale

Enterprise-Scale can be deployed both from the Azure portal directly, or from GitHub: https://github.com/Azure/Enterprise-Scale#deploying-enterprise-scale-architecture-in-your-own-environment



Deploying Enterprise-Scale Architecture in your own environment

The Enterprise-Scale architecture is modular by design and allows customers to start with foundational Landing Zones that support their application portfolios, regardless of whether the applications are being migrated or are newly developed and deployed to Azure. The architecture can scale alongside the customer's business requirements regardless of scale point. In this repository we are providing the following three templates representing different scenarios composed using ARM templates.

Reference implementation	Description	ARM Template	Link
Contoso	On-premises connectivity using Azure vWAN	Deploy to Azure	Detailed description
AdventureWorks	On-premises connectivity with Hub & Spoke	Deploy to Azure	Detailed description
WingTip	Azure without hybrid connectivity	Deploy to Azure	Detailed description
Trey Research	For small Enterprises	Deploy to Azure	Detailed description

Pre-requisites

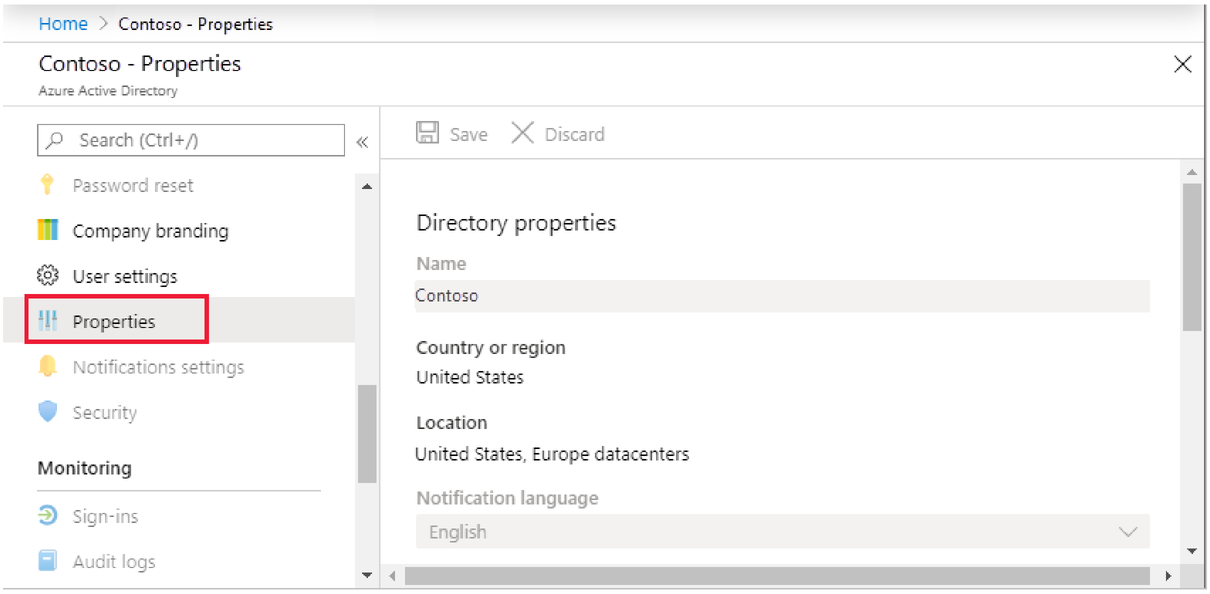
Since Enterprise-Scale can bootstrap an entire Azure tenant without any infrastructure dependencies, the user must first have Owner permission on the tenant *root* before deploying.

This requires the following:

- A user that is Global Admin in the Azure Active Directory
- Elevation of privileges of this user which grants him/her the “User Access Administrator” permission at the tenant root scope
- An explicit roleAssignment (RBAC) made at the tenant root scope via CLI or PowerShell (Note: There’s no portal UX to make this roleAssignment)

Elevate Access to manage Azure resources in the directory

1.1 Sign in to the Azure portal as a user being Global Administrator
1.2 Open Azure Active Directory
1.3 Under *Manage*, select *Properties*



Directory properties

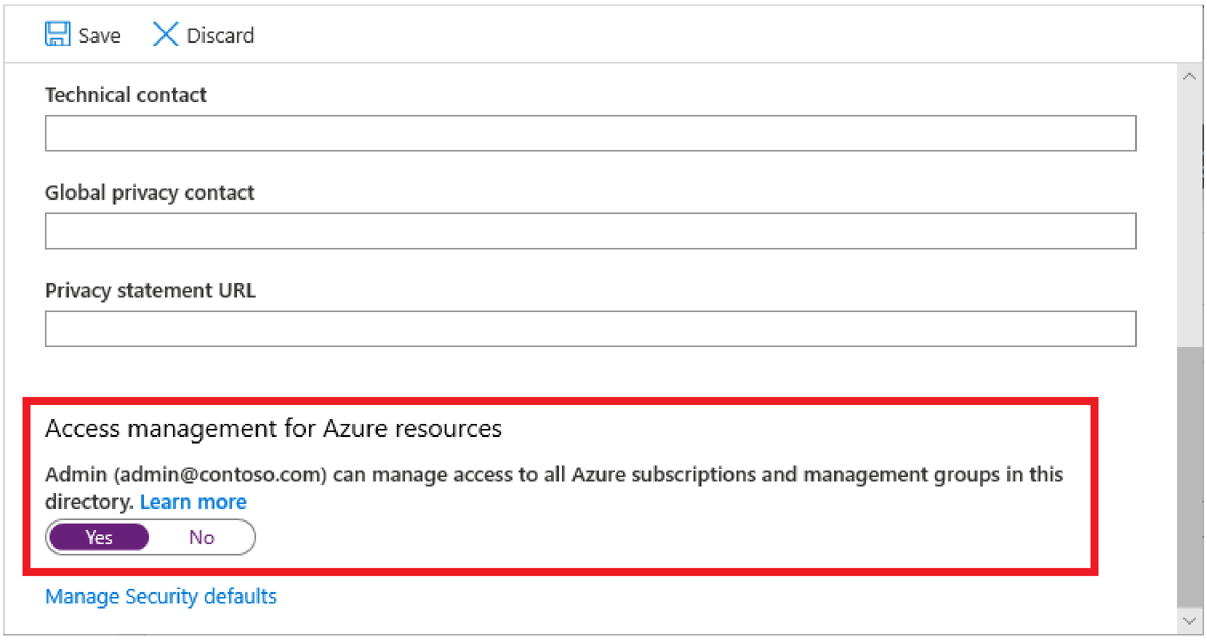
Name: Contoso

Country or region: United States

Location: United States, Europe datacenters

Notification language: English

1.4 Under *Access management for Azure resources,* set the toggle to *Yes*



Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

Admin (admin@contoso.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

● Yes ○ No

Grant Access to the User at *tenant root scope "/"* to deploy Enterprise-Scale

You can use either Bash (CLI) or PowerShell to create the roleAssignment for the current user – or a dedicated user – that will do the deployment

Bash:

```
az role assignment create  --scope '/' --role 'Owner' --assignee-object-id $(az
ad user show -o tsv --query objectId --id '<replace-me>@<my-aad-domain.com>')
```

Powershell:

```
#sign in to azure from Powershell (NOTE: no need to have AzureAD module to use
AzAD commands as they are part of Az.Resource module). In powershell 7.x you
will be redirected to webbrowser for authentication, if required
Connect-AzAccount

#check if you have proper subscription selected and select the right one if
required
Get-AzSubscription | Select-Object SubscriptionId, Name

#select right and replace SubscriptionId result of previous
Select-AzSubscription '<SubscriptionId>'

#get object Id of the user
$user = Get-AzADUser -UserPrincipalName '<replace-me>@<my-aad-domain.com>'

#Assign Owner role to Tenant root scope ("/") as a User Access Administrator
New-AzRoleAssignment -Scope '/' -RoleDefinitionName 'Owner' -ObjectId $user.Id
```

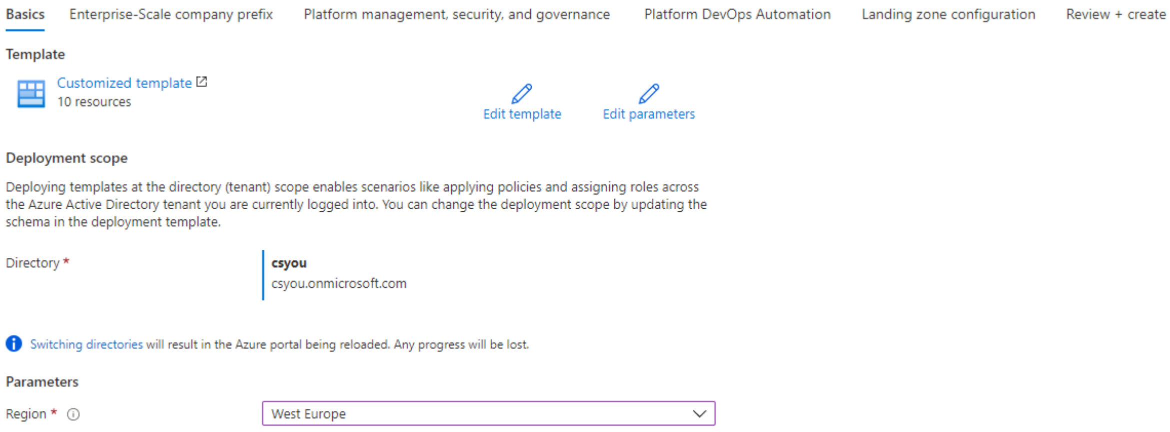
Please note: sometimes it can take up to 15 minutes for permission to propagate at tenant root scope. It is highly recommended that you log out and log back in to refresh the token before you proceed with the deployment

Deployment

When you click on *Deploy to Azure* for the selected Enterprise-Scale reference implementation, it will load the deployment experience into your default Azure tenant. In case you have access to multiple tenants, ensure you are selecting the right one.

Deployment region

On the first page, select the *Region*. This region will primarily be used to place the deployment resources in an Azure region, but also used as the initial region for some of the resources that are deployed, such as Azure Log Analytics and Azure automation.


Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps Automation
Landing zone configuration
Review + create
Edit template
Edit parameters

Template

Customized template
10 resources

Deployment scope

Deploying templates at the directory (tenant) scope enables scenarios like applying policies and assigning roles across the Azure Active Directory tenant you are currently logged into. You can change the deployment scope by updating the schema in the deployment template.

Directory * csyou
csyou.onmicrosoft.com

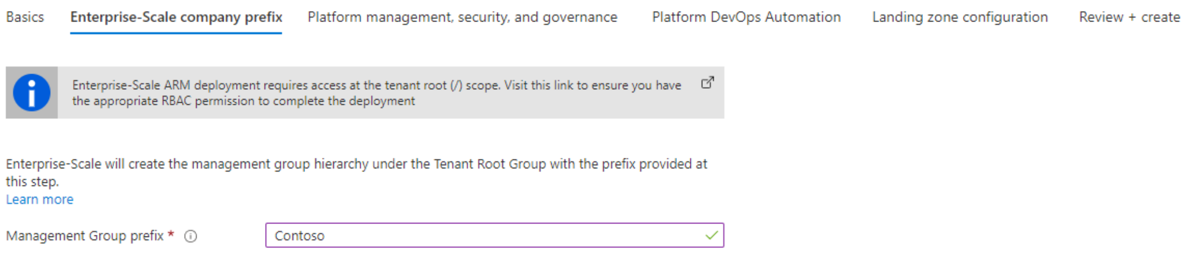
Switching directories will result in the Azure portal being reloaded. Any progress will be lost.

Parameters

Region * West Europe

Enterprise-Scale company prefix

Provide a prefix that will be used to create the management group hierarchy, and platform resources.



Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps Automation
Landing zone configuration
Review + create

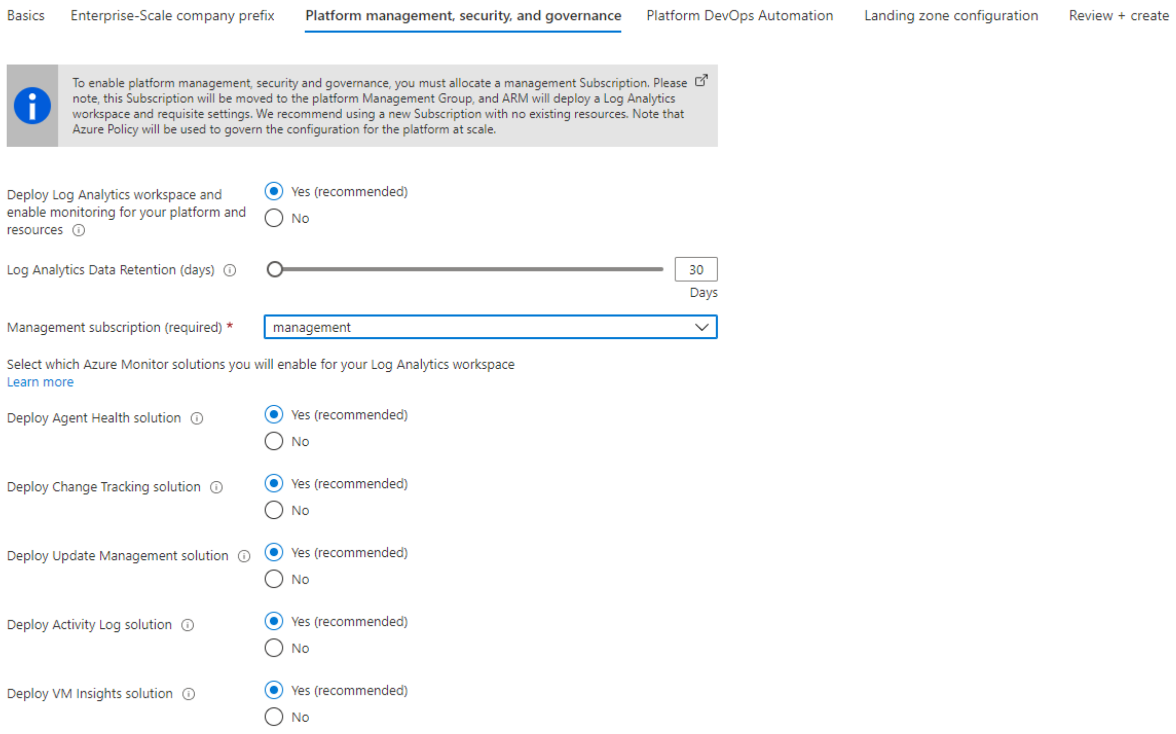
Enterprise-Scale ARM deployment requires access at the tenant root (/) scope. Visit this link to ensure you have the appropriate RBAC permission to complete the deployment

Enterprise-Scale will create the management group hierarchy under the Tenant Root Group with the prefix provided at this step.
Learn more

Management Group prefix * : Contoso ✓

Platform management, security, and governance

On *Platform management, security, and governance* blade, you will configure the core components to enable platform monitoring and security. The options you enable will also be enforced using Azure Policy to ensure resources, landing zones, and more are continuously compliant as your deployments scales and grows. To enable this, you must provide a dedicated (empty) subscription that will be used to host the requisite infrastructure.



Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps Automation
Landing zone configuration
Review + create

To enable platform management, security and governance, you must allocate a management Subscription. Please note, this Subscription will be moved to the platform Management Group, and ARM will deploy a Log Analytics workspace and requisite settings. We recommend using a new Subscription with no existing resources. Note that Azure Policy will be used to govern the configuration for the platform at scale.

Deploy Log Analytics workspace and enable monitoring for your platform and resources: ● Yes (recommended) ○ No

Log Analytics Data Retention (days): 30 Days

Management subscription (required) * : management

Select which Azure Monitor solutions you will enable for your Log Analytics workspace
Learn more

Deploy Agent Health solution: ● Yes (recommended) ○ No

Deploy Change Tracking solution: ● Yes (recommended) ○ No

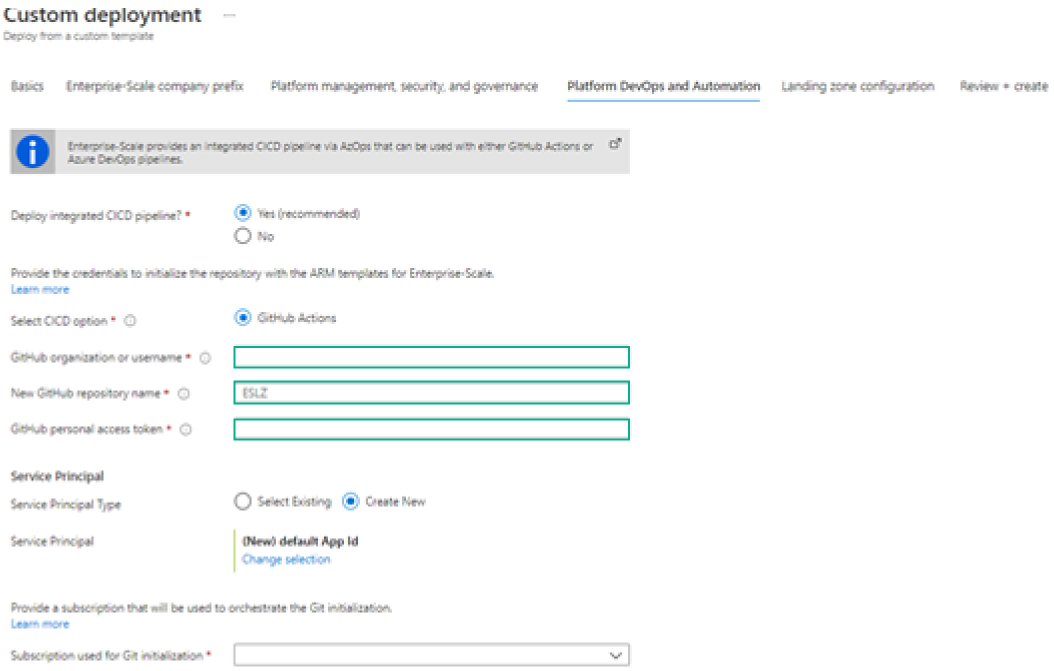
Deploy Update Management solution: ● Yes (recommended) ○ No

Deploy Activity Log solution: ● Yes (recommended) ○ No

Deploy VM Insights solution: ● Yes (recommended) ○ No

Platform DevOps and Automation

You can choose to bootstrap your CICD pipeline (GitHub with GitHub actions). Provide your GitHub user/org name, the preferred name of the GitHub repository that is to be created, as well as the PA token that the deployment will use to create a new repository and discover the Enterprise-Scale deployment ARM templates and merged into your main branch.



Custom deployment

Deploy from a custom template

Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps and Automation
Landing zone configuration
Review + create

Enterprise-Scale provides an integrated CICD pipeline via AzOps that can be used with either GitHub Actions or Azure DevOps pipelines.

Deploy integrated CICD pipeline? * ● Yes (recommended) ○ No

Provide the credentials to initialize the repository with the ARM templates for Enterprise-Scale.
Learn more

Select CICD option * ● GitHub Actions

GitHub organization or username *

New GitHub repository name * ESLZ

GitHub personal access token *

Service Principal

Service Principal Type ○ Select Existing ● Create New

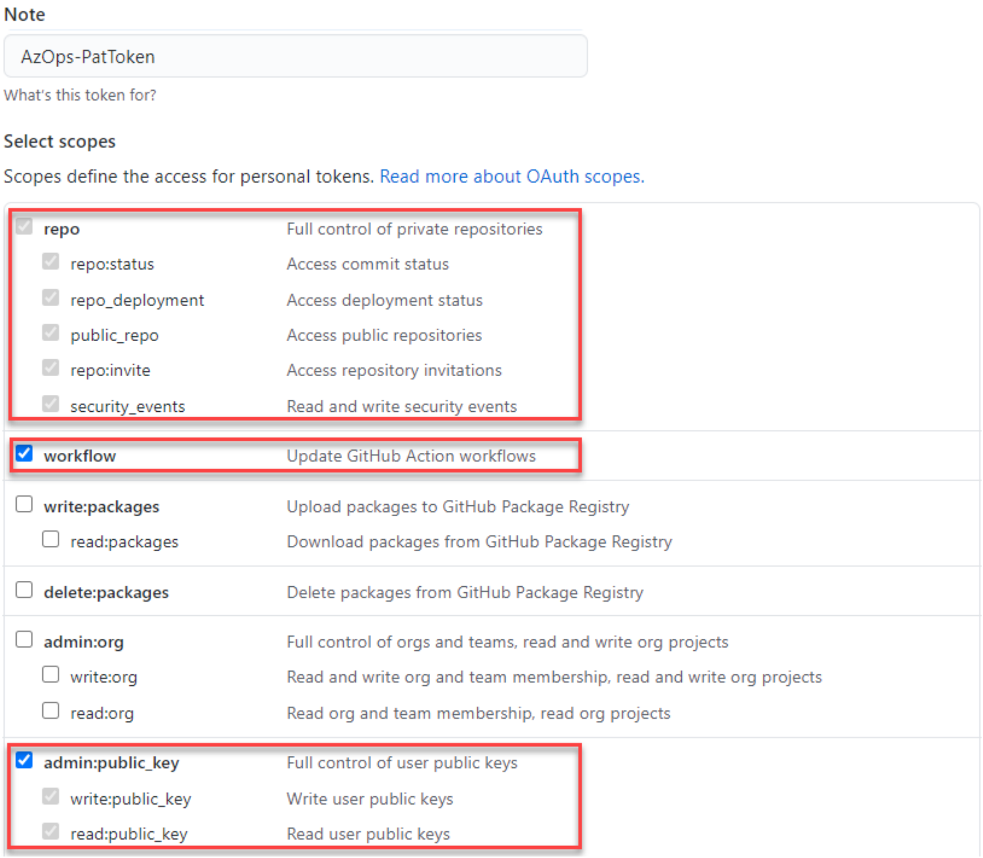
Service Principal **(New) default App Id**
Change selection

Provide a subscription that will be used to orchestrate the Git initialization.
Learn more

Subscription used for Git initialization *

1.1.1 To create a PA token, follow the instructions here: https://docs.github.com/en/github/authenticating-to-github/creating-a-personal-access-token

1.1.2 Ensure the PA token has the following permissions:



Note

AzOps-PatToken

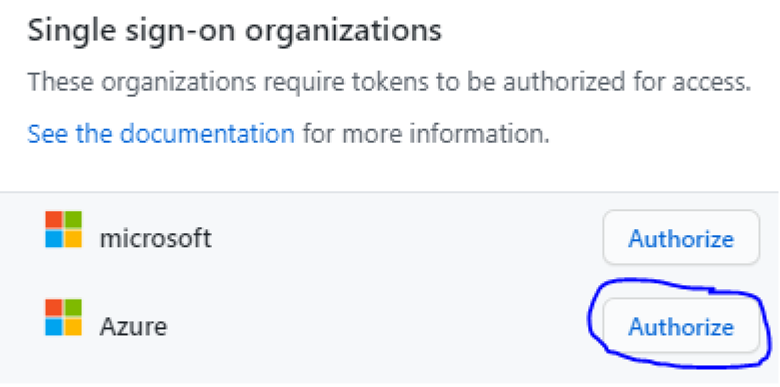
What's this token for?

Select scopes

Scopes define the access for personal tokens. Read more about OAuth scopes.

☑ **repo**	Full control of private repositories
☑ repo:status	Access commit status
☑ repo_deployment	Access deployment status
☑ public_repo	Access public repositories
☑ repo:invite	Access repository invitations
☑ security_events	Read and write security events
☑ **workflow**	Update GitHub Action workflows
□ **write:packages**	Upload packages to GitHub Package Registry
□ read:packages	Download packages from GitHub Package Registry
□ **delete:packages**	Delete packages from GitHub Package Registry
□ **admin:org**	Full control of orgs and teams, read and write org projects
□ write:org	Read and write org and team membership, read and write org projects
□ read:org	Read org and team membership, read org projects
☑ **admin:public_key**	Full control of user public keys
☑ write:public_key	Write user public keys
☑ read:public_key	Read user public keys

NOTE: For Microsoft employees who are enrolled into the Azure GitHub organization, you must also authorize the PA token to this Org!



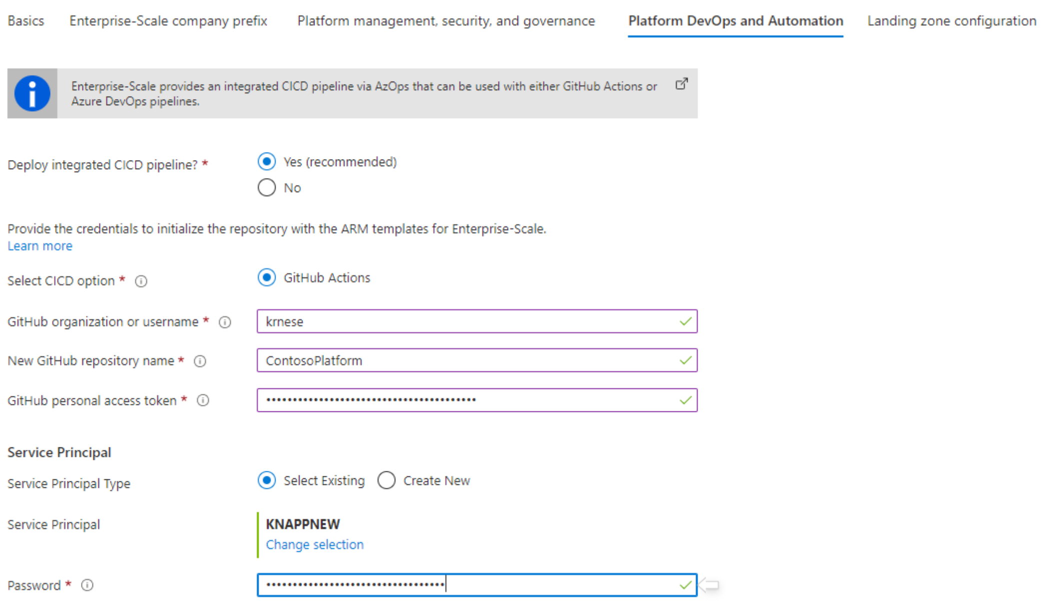
Single sign-on organizations

These organizations require tokens to be authorized for access.

See the documentation for more information.

1.2 Lastly, a Service Principal is required for Git to authenticate to – and be authorized to your Azure tenant. You can either use an existing Service Principal or create a new one. The Service Principal will be granted *Owner* permission on the top level Management Group that gets created.

1.2.1 If using an existing Service Principal, ensure you have the *client secret* as this must be provided as the *Password* for the service principal and confirm it has the right level of permission.



Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps and Automation
Landing zone configuration

Enterprise-Scale provides an integrated CICD pipeline via AzOps that can be used with either GitHub Actions or Azure DevOps pipelines.

Deploy integrated CICD pipeline? * ● Yes (recommended) ○ No

Provide the credentials to initialize the repository with the ARM templates for Enterprise-Scale.
Learn more

Select CICD option * ● GitHub Actions

GitHub organization or username * krnese

New GitHub repository name * ContosoPlatform

GitHub personal access token * ••

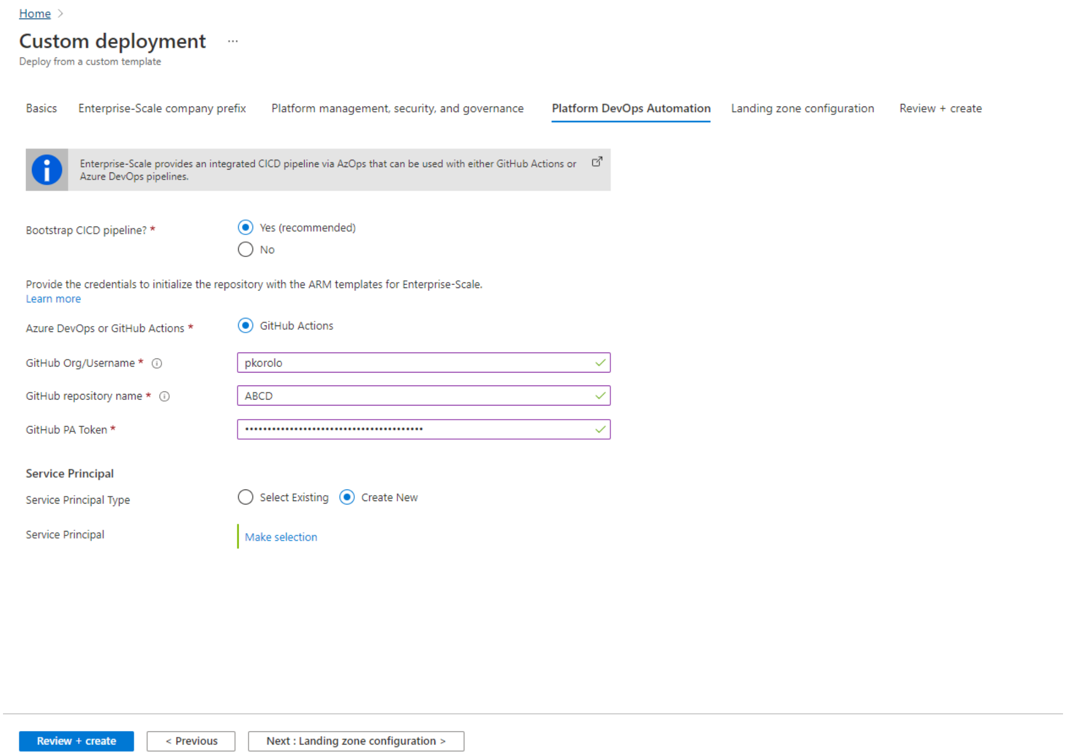
Service Principal

Service Principal Type ● Select Existing ○ Create New

Service Principal **KNAPPNEW**
Change selection

Password * ••••••••••••••••••••••••••••••••••••

1.2.2 If creating a new Service Principal, press “Change selection” and the portal will open a new blade for app registration



Home >

Custom deployment ···

Deploy from a custom template

Basics | Enterprise-Scale company prefix | Platform management, security, and governance | **Platform DevOps Automation** | Landing zone configuration | Review + create

Enterprise-Scale provides an integrated CICD pipeline via AzOps that can be used with either GitHub Actions or Azure DevOps pipelines.

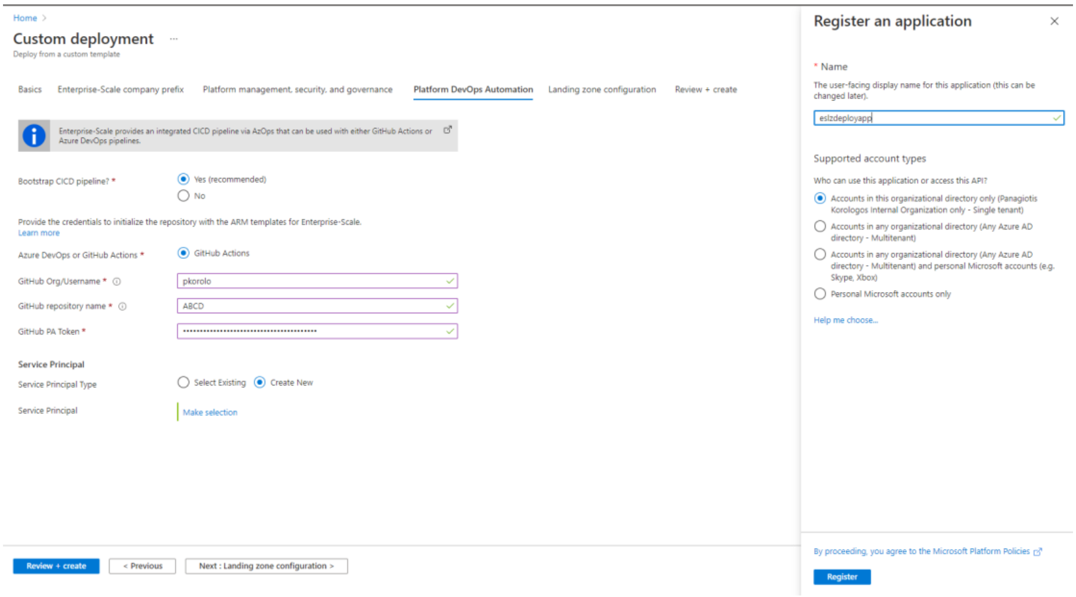
Bootstrap CICD pipeline? *	● Yes (recommended) ○ No

Provide the credentials to initialize the repository with the ARM templates for Enterprise-Scale.
Learn more

Azure DevOps or GitHub Actions *	● GitHub Actions
GitHub Org/Username * ⓘ	pkorolo ✓
GitHub repository name * ⓘ	ABCD ✓
GitHub PA Token *	•• ✓

Service Principal

Service Principal Type	○ Select Existing ● Create New
Service Principal	Make selection



Home >

Custom deployment ···

Deploy from a custom template

Basics | Enterprise-Scale company prefix | Platform management, security, and governance | **Platform DevOps Automation** | Landing zone configuration | Review + create

Enterprise-Scale provides an integrated CICD pipeline via AzOps that can be used with either GitHub Actions or Azure DevOps pipelines.

Bootstrap CICD pipeline? * ● Yes (recommended) ○ No

Provide the credentials to initialize the repository with the ARM templates for Enterprise-Scale.
Learn more

Azure DevOps or GitHub Actions * ● GitHub Actions
GitHub Org/Username * ⓘ pkorolo ✓
GitHub repository name * ⓘ ABCD ✓
GitHub PA Token * •• ✓

Service Principal
Service Principal Type ○ Select Existing ● Create New
Service Principal Make selection

Register an application ×

* Name

The user-facing display name for this application (this can be changed later).

eslzdeployapp ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Panagiotis Korologos Internal Organization only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

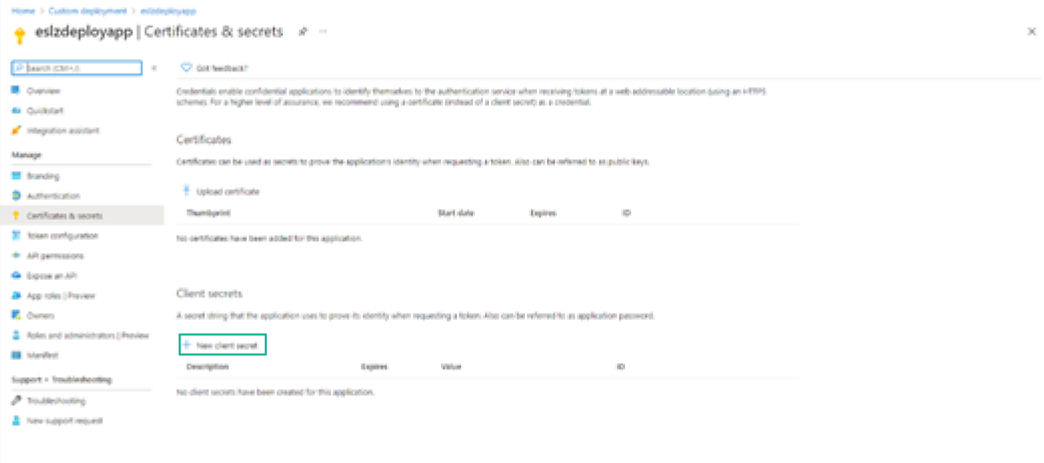
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

By proceeding, you agree to the Microsoft Platform Policies

Once the App has been registered, you must explicitly create a new secret.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

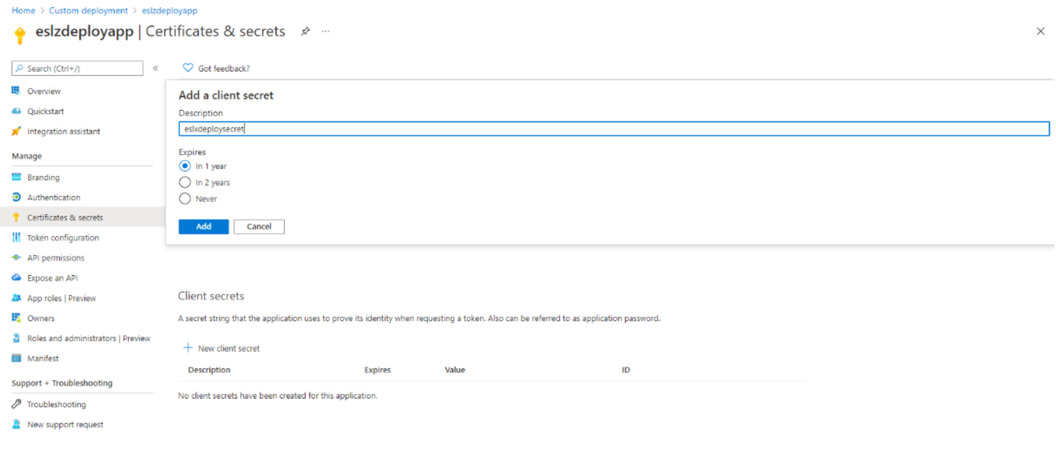
No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID

No client secrets have been created for this application.



Add a client secret

Description: eslxdeploysecret

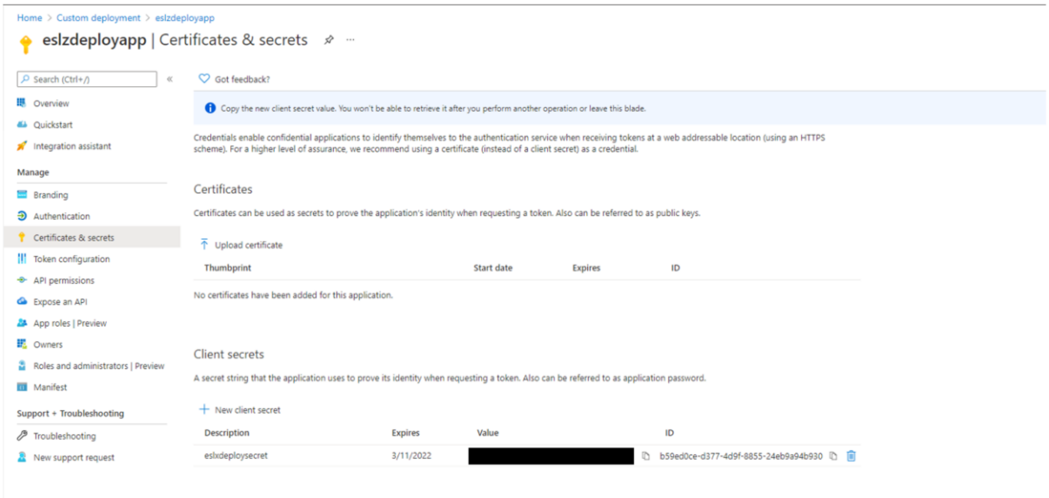
Expires
● In 1 year
○ In 2 years
○ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID

No client secrets have been created for this application.



Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

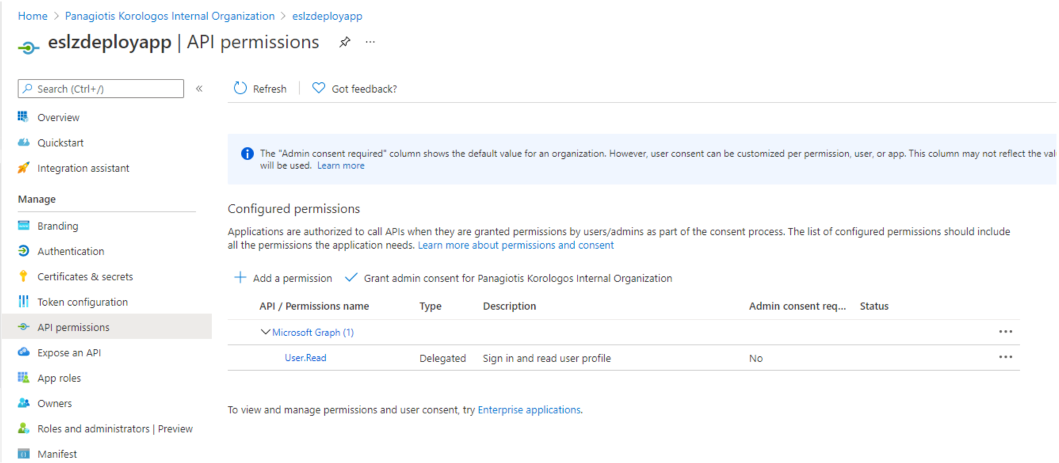
No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID
eslxdeploysecret	3/11/2022	[redacted]	b59ed0ce-d377-4d9f-8855-24eb9a94b930

The default API Permissions for this App are “User.Read”, as depicted below:



eslzdeployapp | API permissions

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 val will be used. Learn more

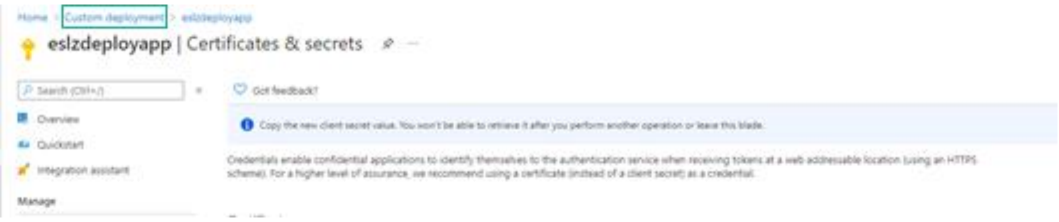
Configured permissions

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

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try Enterprise applications.

After copying the secret, go to “Custom Deployment” (in the upper left) to return to the deployment.

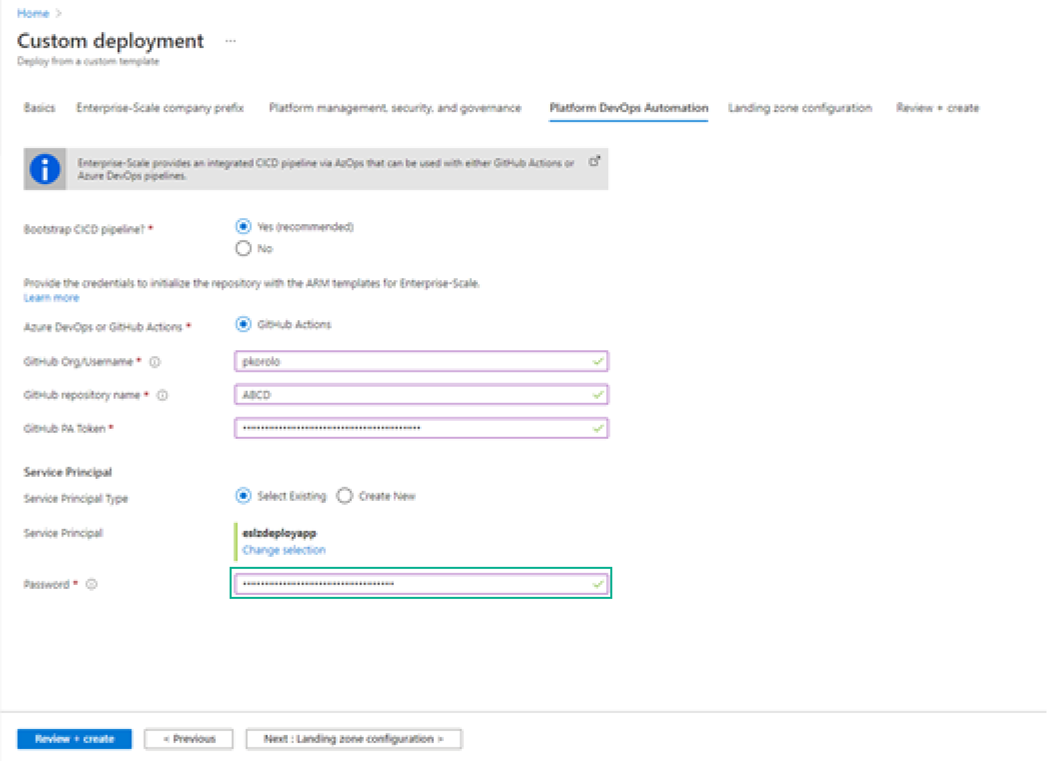


eslzdeployapp | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

At this point, paste the password into the appropriate field.


Home >
Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps Automation
Landing zone configuration
Review + create
Review + create
< Previous
Next : Landing zone configuration >

Custom deployment

Deploy from a custom template

Enterprise-Scale provides an integrated CICD pipeline via AzOps that can be used with either GitHub Actions or Azure DevOps pipelines.

Bootstrap CICD pipeline? * ● Yes (recommended) ○ No

Provide the credentials to initialize the repository with the ARM templates for Enterprise-Scale.
Learn more

Azure DevOps or GitHub Actions * ● GitHub Actions

GitHub Org/Username * : pkorolo

GitHub repository name * : ABCD

GitHub PA Token * : ••

Service Principal

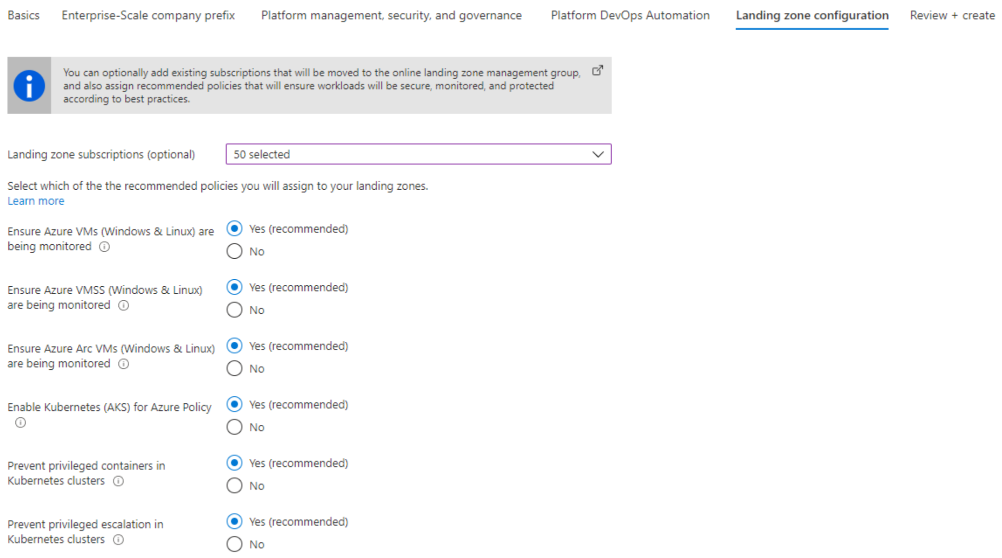
Service Principal Type ● Select Existing ○ Create New

Service Principal: eslzdeployapp
Change selection

Password * : ••••••••••••••••••••••••••••••••••

Landing zone configuration

You can optionally bring in N number of subscriptions that will be bootstrapped as landing zones, governed by Azure Policy. Select which policy you want to assign broadly to all of your landing zones.



Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps Automation
Landing zone configuration
Review + create

You can optionally add existing subscriptions that will be moved to the online landing zone management group, and also assign recommended policies that will ensure workloads will be secure, monitored, and protected according to best practices.

Landing zone subscriptions (optional): 50 selected

Select which of the the recommended policies you will assign to your landing zones.
Learn more

Ensure Azure VMs (Windows & Linux) are being monitored: ● Yes (recommended) ○ No

Ensure Azure VMSS (Windows & Linux) are being monitored: ● Yes (recommended) ○ No

Ensure Azure Arc VMs (Windows & Linux) are being monitored: ● Yes (recommended) ○ No

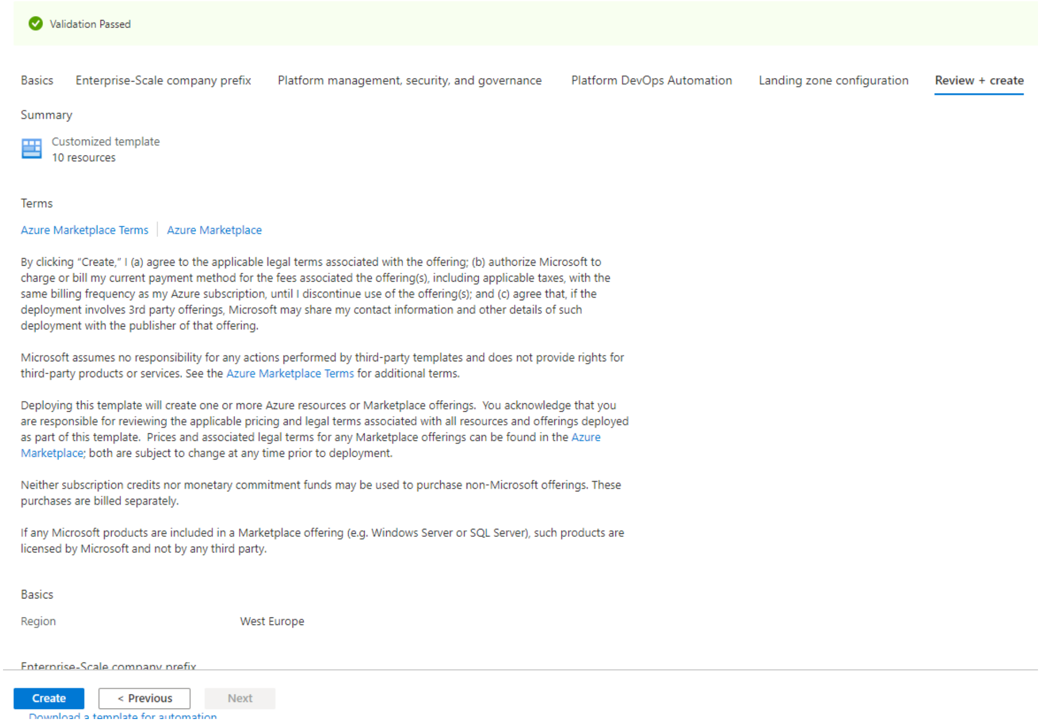
Enable Kubernetes (AKS) for Azure Policy: ● Yes (recommended) ○ No

Prevent privileged containers in Kubernetes clusters: ● Yes (recommended) ○ No

Prevent privileged escalation in Kubernetes clusters: ● Yes (recommended) ○ No

Review + create.

Review + Create page will validate your permission and configuration before you can click deploy. Once it has been validated successfully, you can click *Create.*



✓ Validation Passed

Basics
Enterprise-Scale company prefix
Platform management, security, and governance
Platform DevOps Automation
Landing zone configuration
Review + create

Summary

Customized template
10 resources

Terms

Azure Marketplace Terms | Azure Marketplace

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

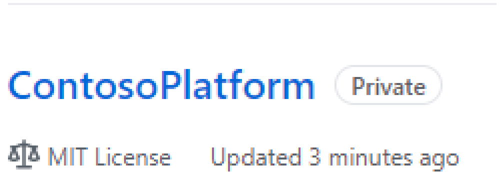
Region: West Europe

Enterprise-Scale company prefix

Validation post deployment (GitHub)

Once Enterprise-Scale has deployed and you enabled the CICD bootstrap, you should validate that:

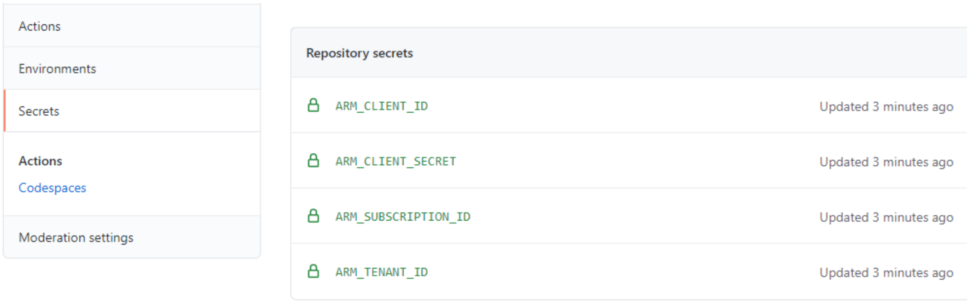
- A new repository has been created, with the name provided during setup.



ContosoPlatform Private

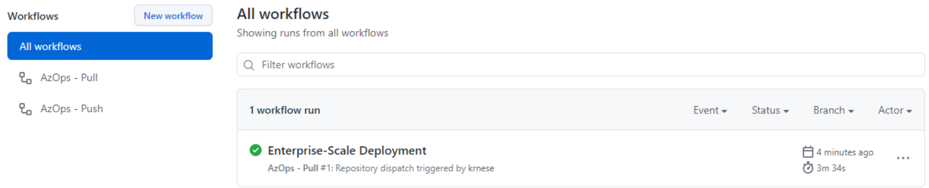
MIT License Updated 3 minutes ago

- 4 Secrets are created into this GitHub repository.



Repository secrets	
ARM_CLIENT_ID	Updated 3 minutes ago
ARM_CLIENT_SECRET	Updated 3 minutes ago
ARM_SUBSCRIPTION_ID	Updated 3 minutes ago
ARM_TENANT_ID	Updated 3 minutes ago

- A Pull Request is in progress/has completed and automatically merged into the main branch.



All workflows

Showing runs from all workflows

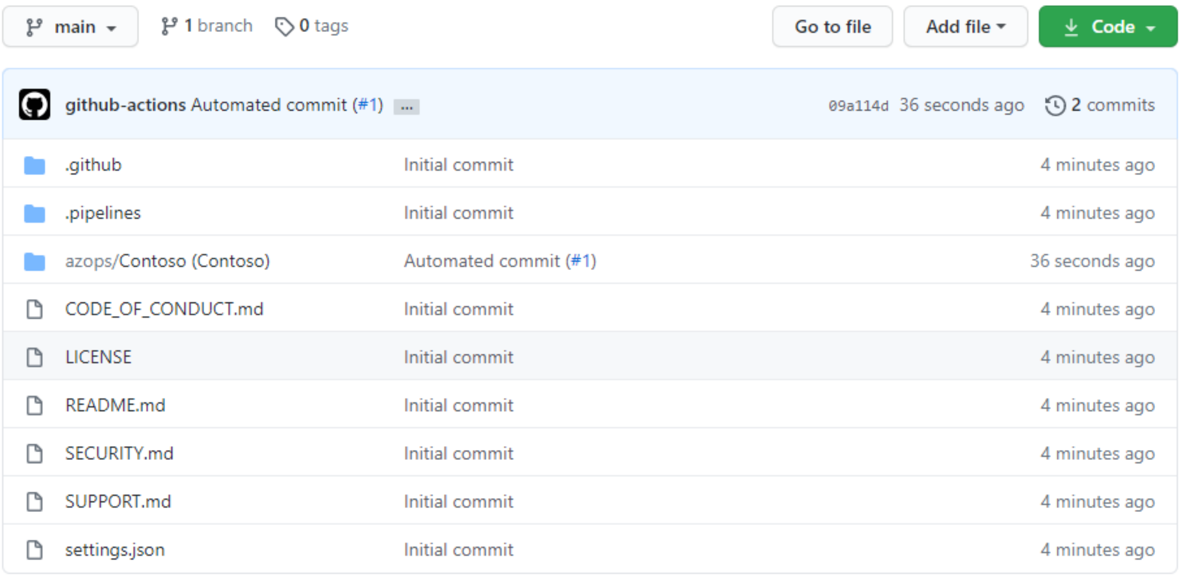
Enterprise-Scale Deployment

AzOps - Pull #1: Repository dispatch triggered by krnese

4 minutes ago

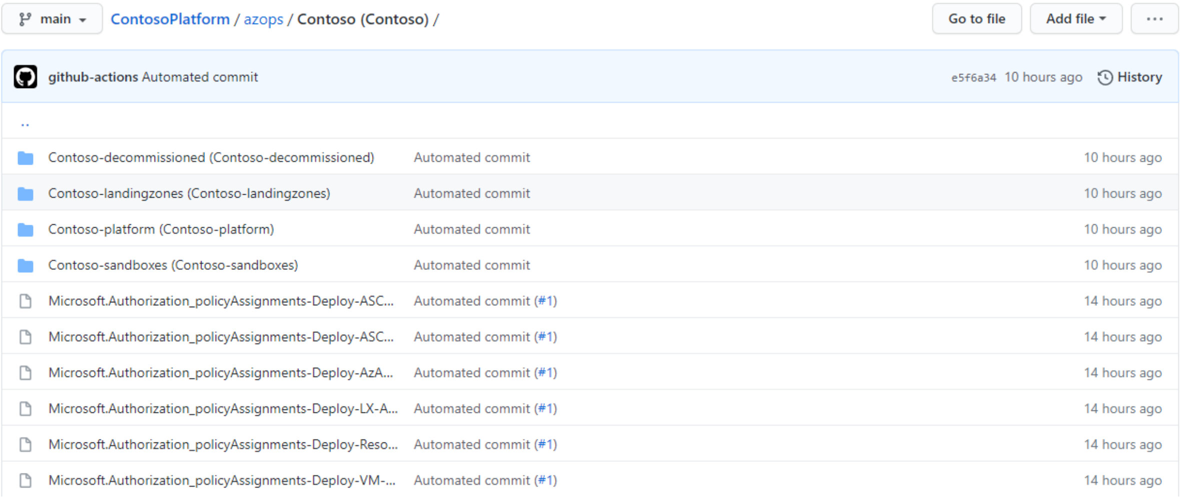
3m 34s

- The Azure hierarchy that got created using ARM templates as part of the Enterprise-Scale setup, such as management groups, subscription organization as well as policy definitions, policy assignments and role assignments are hydrated and organized into Git



github-actions Automated commit (#1) ... 09a114d 36 seconds ago 2 commits

.github	Initial commit	4 minutes ago
.pipelines	Initial commit	4 minutes ago
azops/Contoso (Contoso)	Automated commit (#1)	36 seconds ago
CODE_OF_CONDUCT.md	Initial commit	4 minutes ago
LICENSE	Initial commit	4 minutes ago
README.md	Initial commit	4 minutes ago
SECURITY.md	Initial commit	4 minutes ago
SUPPORT.md	Initial commit	4 minutes ago
settings.json	Initial commit	4 minutes ago

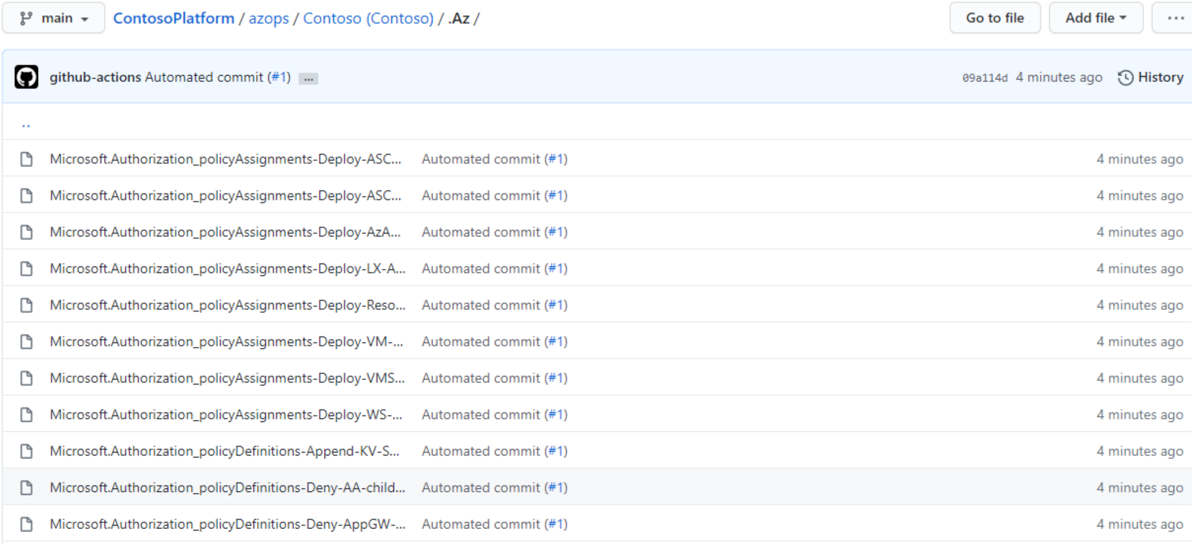


main ▾ ContosoPlatform / azops / Contoso (Contoso) /

github-actions Automated commit e5f6a34 10 hours ago History

..		
Contoso-decommissioned (Contoso-decommissioned)	Automated commit	10 hours ago
Contoso-landingzones (Contoso-landingzones)	Automated commit	10 hours ago
Contoso-platform (Contoso-platform)	Automated commit	10 hours ago
Contoso-sandboxes (Contoso-sandboxes)	Automated commit	10 hours ago
Microsoft.Authorization_policyAssignments-Deploy-ASC...	Automated commit (#1)	14 hours ago
Microsoft.Authorization_policyAssignments-Deploy-ASC...	Automated commit (#1)	14 hours ago
Microsoft.Authorization_policyAssignments-Deploy-AzA...	Automated commit (#1)	14 hours ago
Microsoft.Authorization_policyAssignments-Deploy-LX-A...	Automated commit (#1)	14 hours ago
Microsoft.Authorization_policyAssignments-Deploy-Reso...	Automated commit (#1)	14 hours ago
Microsoft.Authorization_policyAssignments-Deploy-VM-...	Automated commit (#1)	14 hours ago

- In each folder, you will find the ARM templates that were deployed at the scopes during the Enterprise-Scale setup. E.g., on the intermediate root group, you will find all policy definitions, and depending on the selection you made during the deployment, you will find resource templates in the platform subscriptions. Users can – whenever they are ready, start using these templates and bring their own templates to manage the platform using ARM templates and infrastructure as code.



main ▾ ContosoPlatform / azops / Contoso (Contoso) / .Az /

github-actions Automated commit (#1) ... 09a114d 4 minutes ago History

..		
Microsoft.Authorization_policyAssignments-Deploy-ASC...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-ASC...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-AzA...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-LX-A...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-Reso...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-VM-...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-VMS...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyAssignments-Deploy-WS-...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyDefinitions-Append-KV-S...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyDefinitions-Deny-AA-child...	Automated commit (#1)	4 minutes ago
Microsoft.Authorization_policyDefinitions-Deny-AppGW-...	Automated commit (#1)	4 minutes ago

Post deployment activities

Once Enterprise-Scale has deployed, you can grant your application teams/business units access to their respective landing zones. Whenever there's a need for a new landing zone, you can place them into their respective management groups (Online or Corp) given the characteristics of assumed workloads and their requirements.

Create new landing zones

Application team's responsibility

Operating the Azure platform using AzOps (Infrastructure as Code with GitHub Actions)

When you have deployed Enterprise-Scale with GitHub integration, you will have a ready-to-go repository with integrated GitHub Actions containing all the ARM templates that were used during deployment, organized in the following way:

- Management group tree structure represented as folders in Git
- Subscriptions represented as folders in their respective management group folder in Git
- Resource Groups represented as folders in their respective subscription folder in Git
- Policy Definitions, Policy Set Definitions, Role Definitions, and Role Assignments as composite ARM resource templates partitioned at the folder representing the respective scope in Azure (management group, subscription)
- Resources (e.g., virtual networks, Log Analytics workspace, Automation account etc.) represented as composite ARM resource templates into their respective resource group (folder)

You can edit/update the existing ARM templates in your repository and GitHub actions will push (deploy) to the respective Azure scope, and you can author and bring your own ARM template and deploy them to the respective Azure scope.

The following section will demonstrate how one can operationalize the Enterprise-Scale platform using ARM templates, via the GitHub repository that got created using AzOps (GitHub Actions).

What is AzOps?

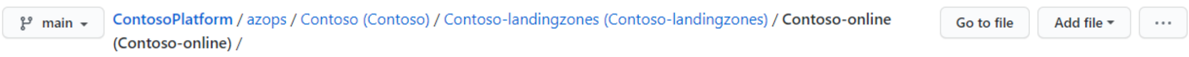
AzOps is an opinionated CICD pipeline to operationalize the Azure *platform* and *landing zones* that enables organizations to focus on the ARM template development, and not having to deal with multiple deployment scripts targeting different Azure scopes. The organization and folder structure in Git is dynamically representing the Azure graph (management groups (parent, child relationships), and subscription organization), so the platform operators can easily determine at which *scope* they want to invoke the ARM template deployment by simply making a PR with the ARM template(s) and parameter files (optionally), and AzOps will invoke the deployment accordingly.

Also, when there's a new *scope* (management groups, subscriptions, and resource groups) being created, either explicitly via the pipeline – and also out of band (via Portal, CLI, PS etc.), AzOps will discover these and represent them correctly back into Git.

Create new Policy Assignment for validation

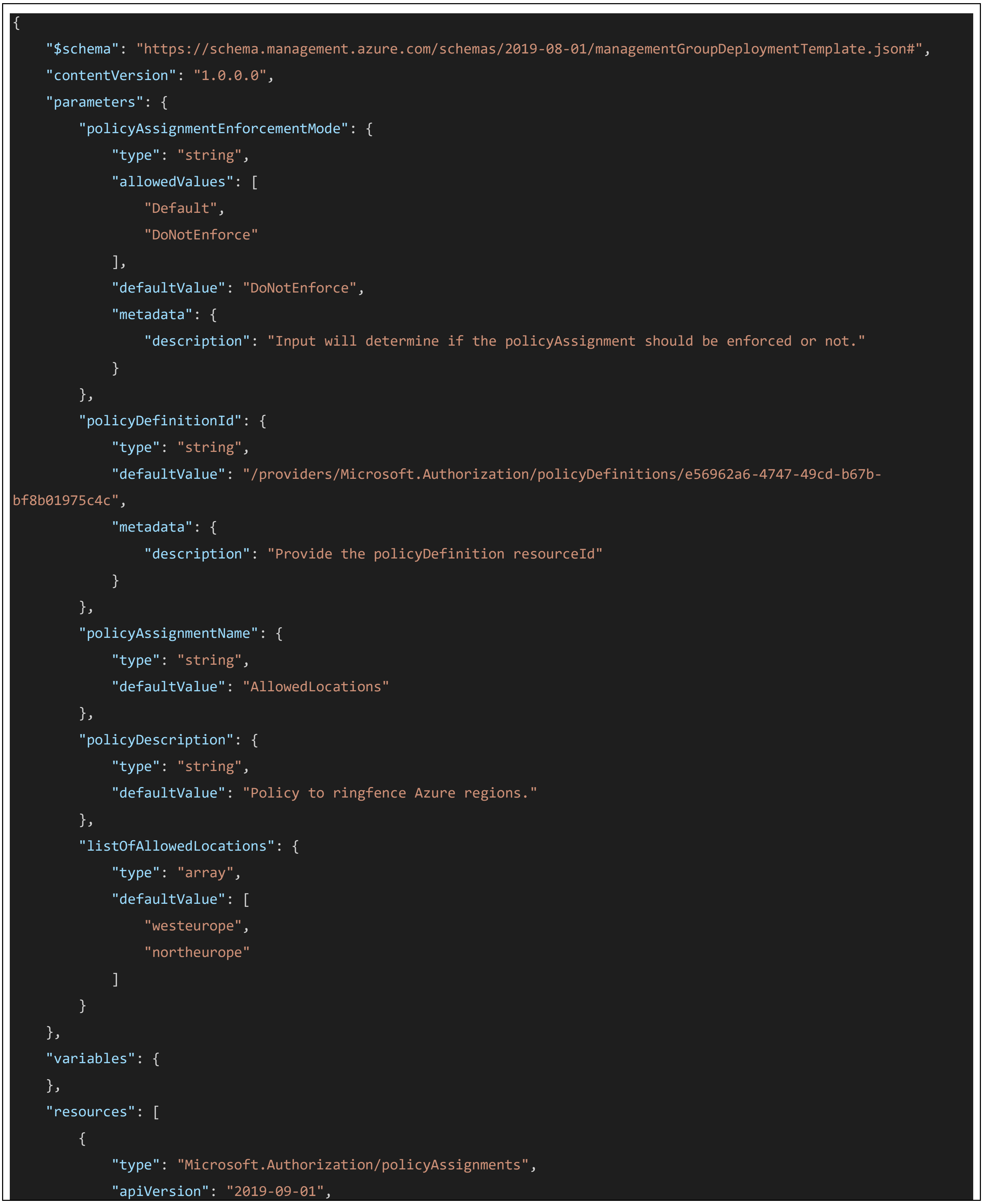
Enterprise-Scale with its Policy Driven Governance principle relies heavily on Azure Policy to determine the goal state of the overall platform. As an example, this exercise will demonstrate how a developer can make a new policy assignment at the "Online" landing zone management group scope.

1. In GitHub, navigate to your repository and click on the 'azops' folder. From here, navigate to your <prefix>-online folder which represents the management group for all your online landing zones.

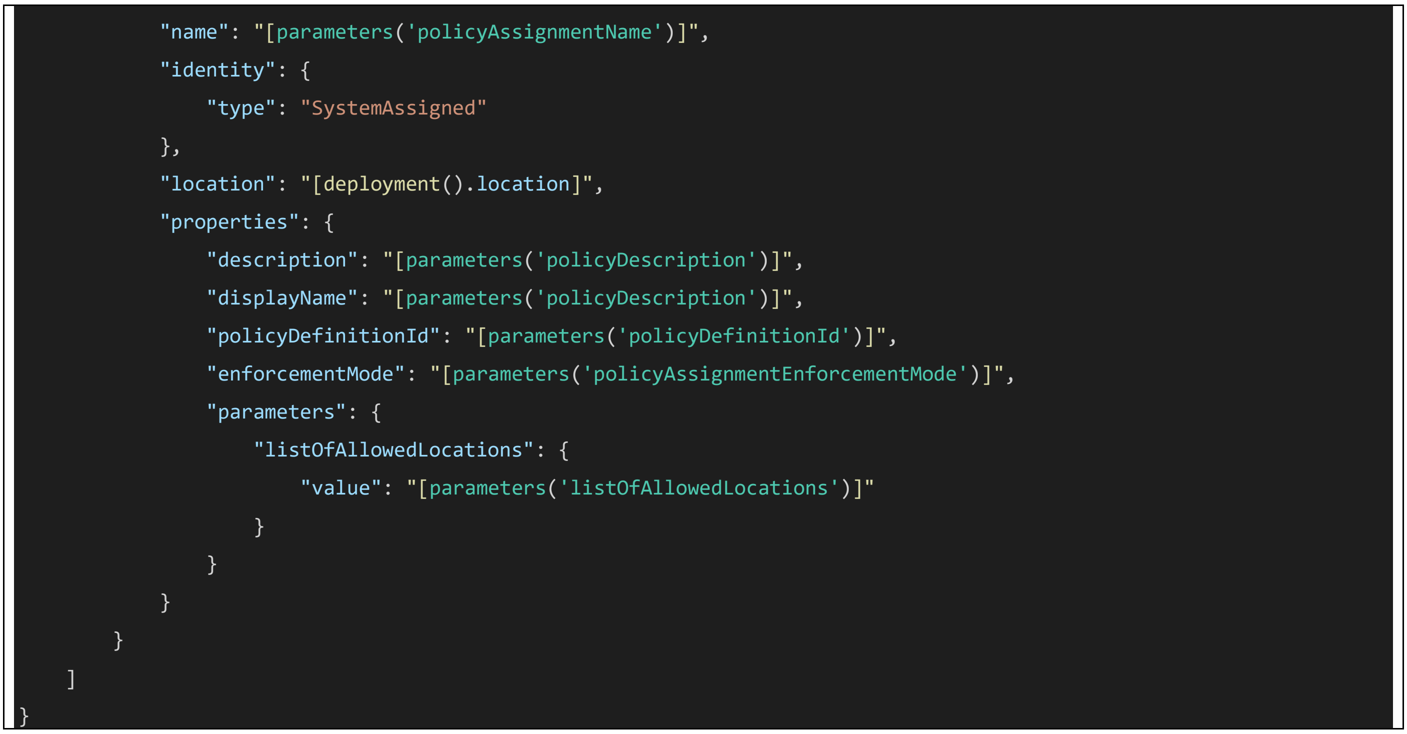

ContosoPlatform / azops / Contoso (Contoso) / Contoso-landingzones (Contoso-landingzones) / Contoso-online (Contoso-online) /

2. Click on 'Add file', and 'Create new file'.
3. Name the file '`locationAssignment.json`'

4. Copy and paste the following ARM template json

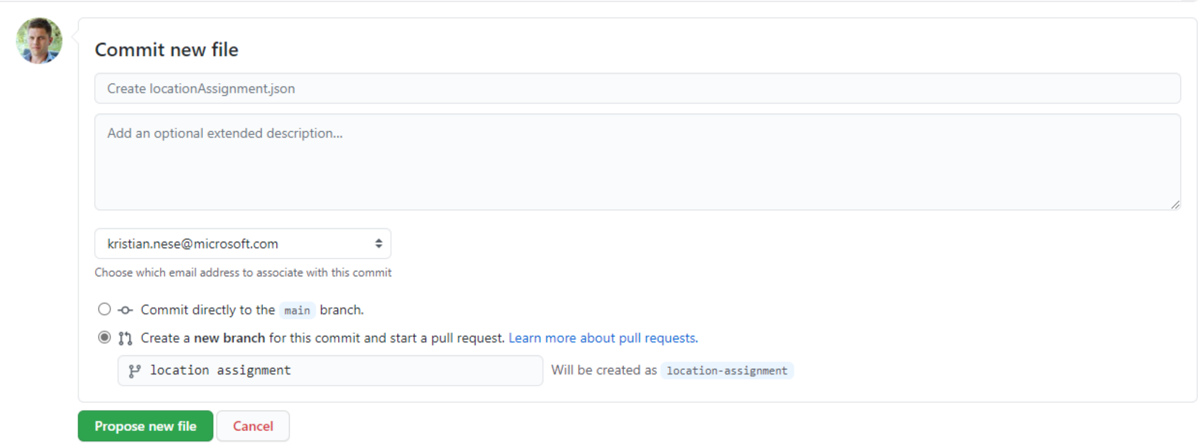


```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-08-01/managementGroupDeploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "policyAssignmentEnforcementMode": {
            "type": "string",
            "allowedValues": [
                "Default",
                "DoNotEnforce"
            ],
            "defaultValue": "DoNotEnforce",
            "metadata": {
                "description": "Input will determine if the policyAssignment should be enforced or not."
            }
        },
        "policyDefinitionId": {
            "type": "string",
            "defaultValue": "/providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4c",
            "metadata": {
                "description": "Provide the policyDefinition resourceId"
            }
        },
        "policyAssignmentName": {
            "type": "string",
            "defaultValue": "AllowedLocations"
        },
        "policyDescription": {
            "type": "string",
            "defaultValue": "Policy to ringfence Azure regions."
        },
        "listOfAllowedLocations": {
            "type": "array",
            "defaultValue": [
                "westeurope",
                "northeurope"
            ]
        }
    },
    "variables": {
    },
    "resources": [
        {
            "type": "Microsoft.Authorization/policyAssignments",
            "apiVersion": "2019-09-01",
```



```
            "name": "[parameters('policyAssignmentName')]",
            "identity": {
                "type": "SystemAssigned"
            },
            "location": "[deployment().location]",
            "properties": {
                "description": "[parameters('policyDescription')]",
                "displayName": "[parameters('policyDescription')]",
                "policyDefinitionId": "[parameters('policyDefinitionId')]",
                "enforcementMode": "[parameters('policyAssignmentEnforcementMode')]",
                "parameters": {
                    "listOfAllowedLocations": {
                        "value": "[parameters('listOfAllowedLocations')]"
                    }
                }
            }
        }
    ]
}
```

5. Examine the file and note that we are using default values for the parameters. You could modify these, or you could also provide a `locationAssignment.parameters.json` file to provide the parameters.
6. On the 'Commit new file' option, select 'Create a new branch for this commit and start a pull request', and give it a name.



Commit new file

Create locationAssignment.json

Add an optional extended description...

kristian.nese@microsoft.com

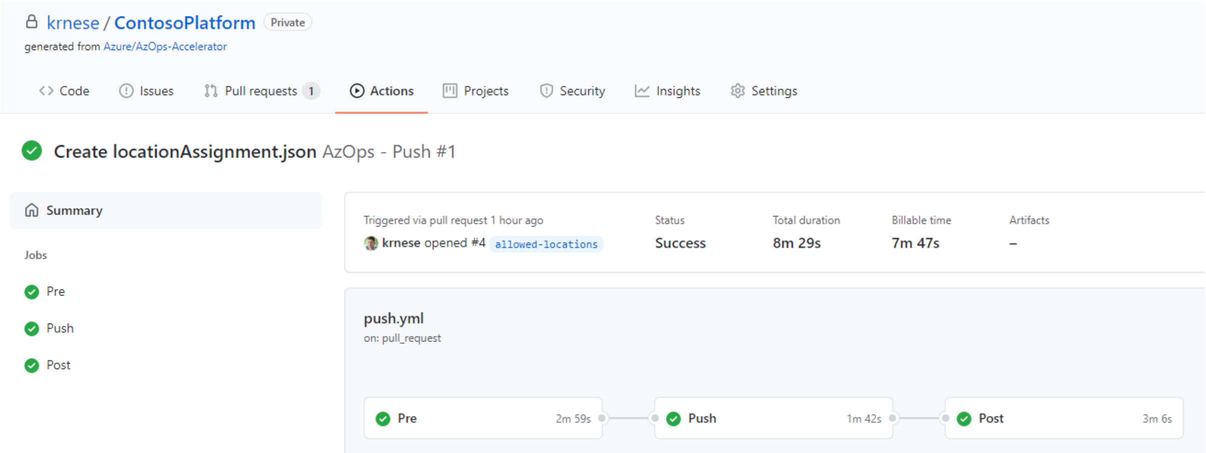
Choose which email address to associate with this commit

○ Commit directly to the `main` branch.

● Create a **new branch** for this commit and start a pull request. Learn more about pull requests.

`location assignment` Will be created as `location-assignment`

7. Click 'Propose new file' and a new PR is being created which will trigger the Push workflow. Go to Actions to monitor the process.



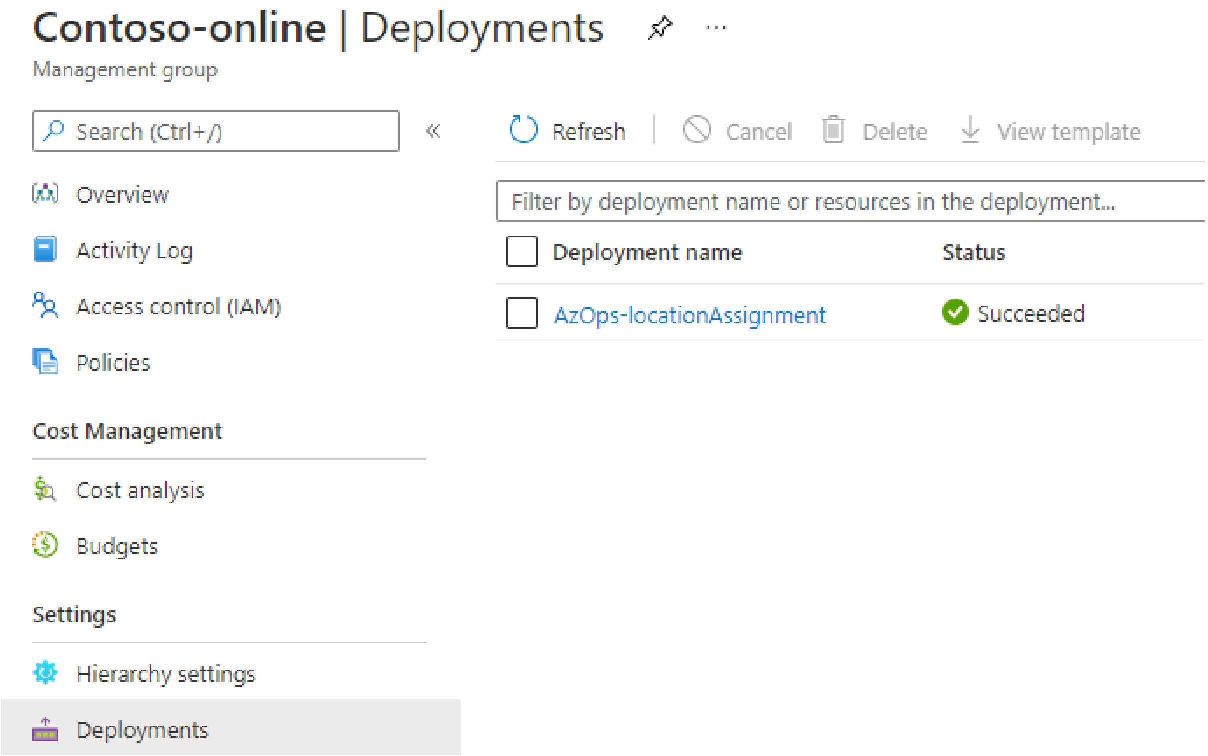
Create locationAssignment.json AzOps - Push #1

Triggered via pull request 1 hour ago	Status	Total duration	Billable time	Artifacts
krnese opened #4 `allowed-locations`	Success	8m 29s	7m 47s	–

push.yml
on: pull_request

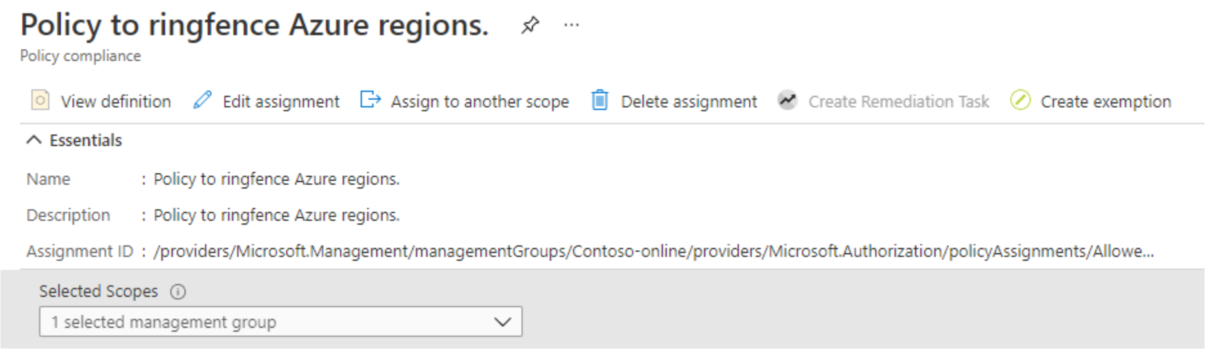
Pre	Push	Post
2m 59s	1m 42s	3m 6s

8. Once completed, you can merge the pull request.
9. In Azure portal, you can navigate to the <prefix>-online management group and verify that the deployment resource got created and deployed successfully. Each deployment invoked via AzOps will have an ‘AzOps’ prefix.



Deployment name	Status
AzOps-locationAssignment	Succeeded

10. Navigate to ‘Policies’ on the <prefix>-online management group and verify that there’s a new assignment called ‘Policy to ringfence Azure regions’.



Policy to ringfence Azure regions.

Policy compliance

Essentials

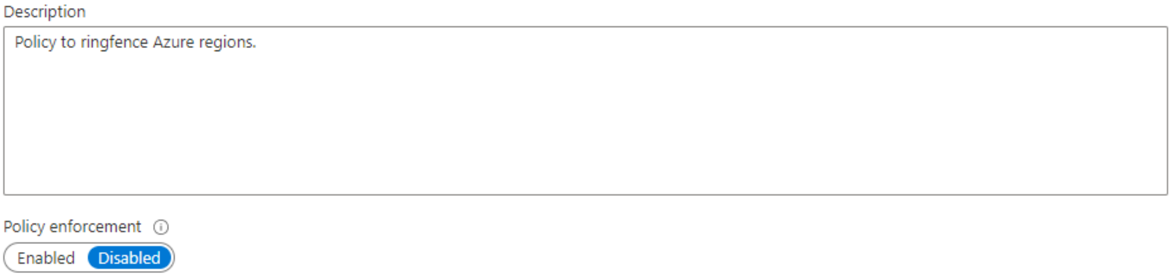
Name : Policy to ringfence Azure regions.

Description : Policy to ringfence Azure regions.

Assignment ID : /providers/Microsoft.Management/managementGroups/Contoso-online/providers/Microsoft.Authorization/policyAssignments/Allowe...

Selected Scopes : 1 selected management group

11. Click on ‘Edit assignment’ to verify that the Policy is not being enforced but will only scan for compliance and validate resources per the policy rule defined in the policy definition.



Description: Policy to ringfence Azure regions.

Policy enforcement: Enabled [✓ Disabled]

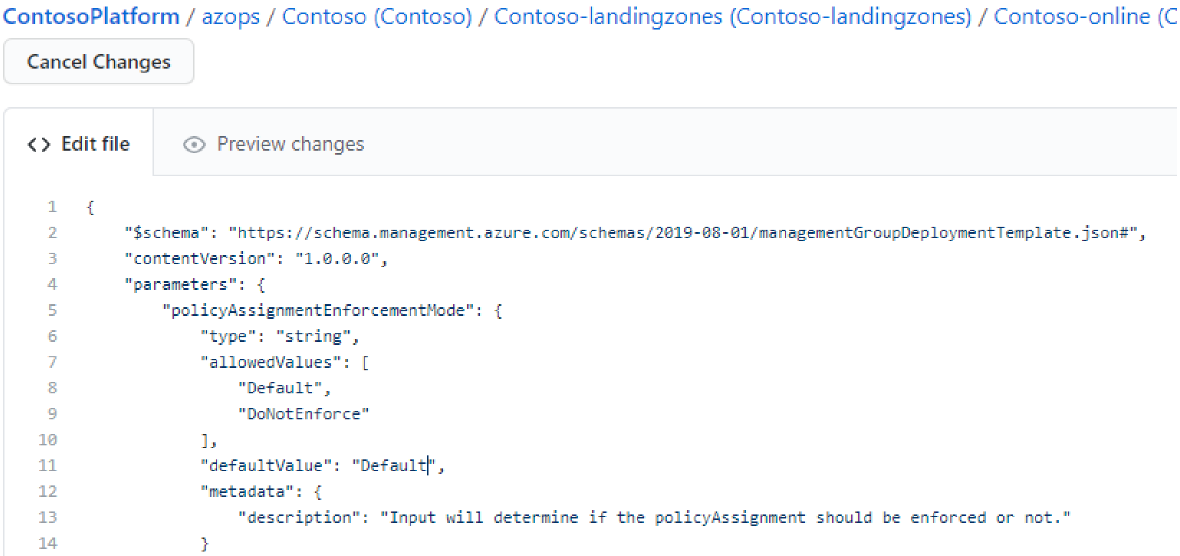
Once the policy compliance scan has completed, you will get a compliance result for the policy you assigned to validate the effect is working as intended, before going to the next step to update the enforcement mode. I.e., this policy will prevent resources being created outside of the allowed locations specified.

You can now merge the pull request and delete the branch.

Update a Policy Assignment to enforce

In this exercise, we will modify the existing policy assignment to ensure the policy effect will be enforced.

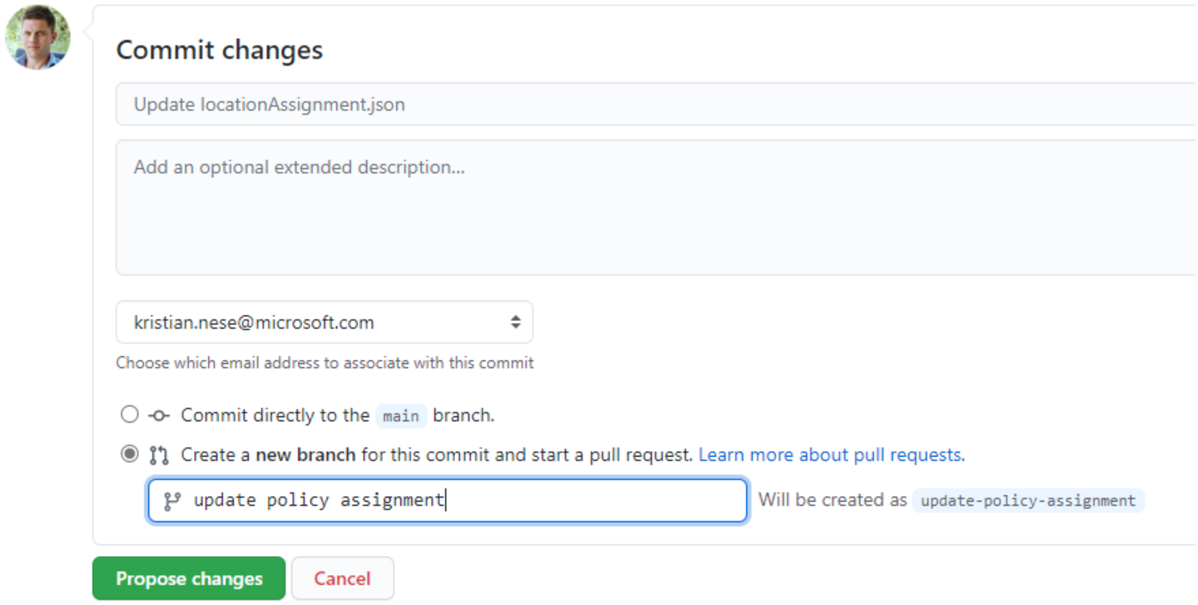
1. Navigate the locationAssignment.json file you placed into the <prefix>-online folder, representing the online landing zone.
2. Click on ‘Edit this file’ ✎
3. Change the parameter “policyAssignmentEnforcementMode” default value to be ‘Default’.



ContosoPlatform / azops / Contoso (Contoso) / Contoso-landingzones (Contoso-landingzones) / Contoso-online (C

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-08-01/managementGroupDeploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "policyAssignmentEnforcementMode": {
            "type": "string",
            "allowedValues": [
                "Default",
                "DoNotEnforce"
            ],
            "defaultValue": "Default",
            "metadata": {
                "description": "Input will determine if the policyAssignment should be enforced or not."
            }
```

4. On the ‘Commit changes’ dialogue box, select ‘Create a new branch for this commit and start a pull request’, and provide a branch name. Click ‘Propose changes’ and create the pull request



Commit changes

Update locationAssignment.json

Add an optional extended description...

kristian.nese@microsoft.com

Choose which email address to associate with this commit

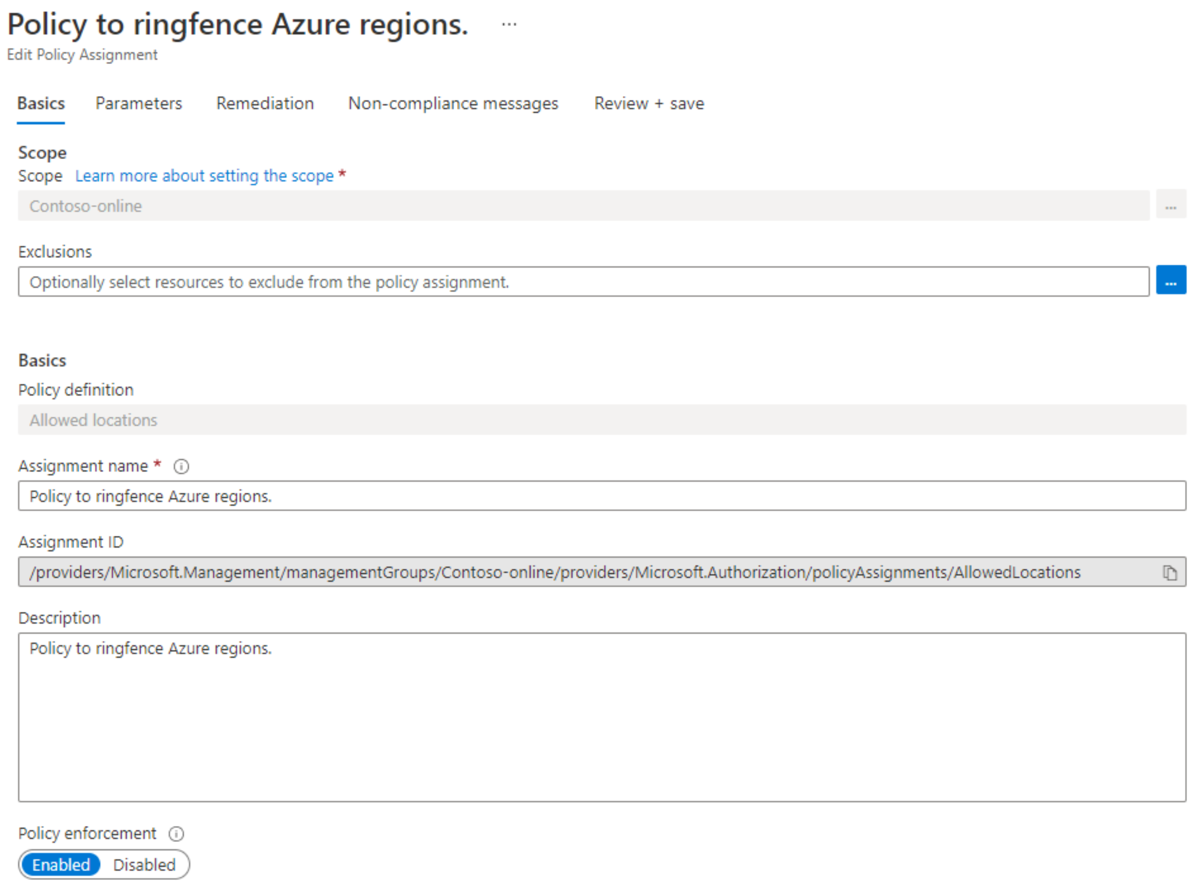
○ Commit directly to the `main` branch.

● Create a **new branch** for this commit and start a pull request. Learn more about pull requests.

update policy assignment — Will be created as `update-policy-assignment`

This will now start the AzOps push workflow and deploy the template with the updated property so that the policy effect will be enforced (in this case, deny resource creation outside of the ringfenced Azure regions).

Once the job has completed, you can revisit the policy in Azure portal and see that the policy enforcement is set to ‘Enabled’.



Policy to ringfence Azure regions.

Edit Policy Assignment

Scope

Scope Learn more about setting the scope *

Contoso-online

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

Allowed locations

Assignment name *

Policy to ringfence Azure regions.

Assignment ID

/providers/Microsoft.Management/managementGroups/Contoso-online/providers/Microsoft.Authorization/policyAssignments/AllowedLocations

Description

Policy to ringfence Azure regions.

Policy enforcement

[✓ Enabled] Disabled

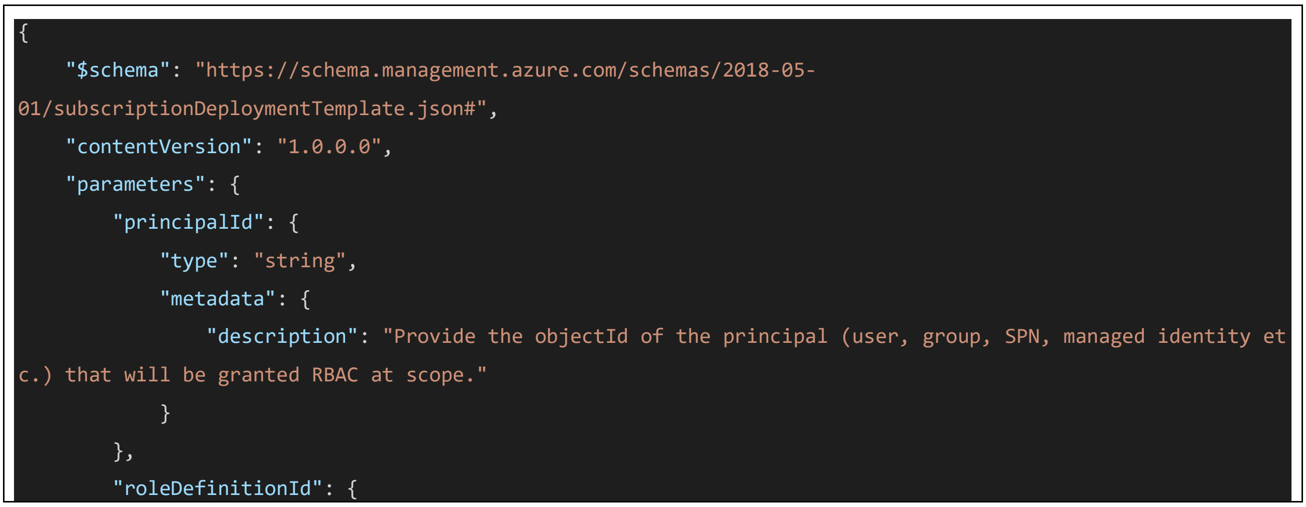
You can now merge the pull request and delete the branch.

Create new landing zones

Create new Role Assignment on a landing zone

To grant a user, a group, or a service principal access to a landing zone (subscription), you can use the following ARM template where you provide the principalId (object id of the user, group, or service principal) as input to the parameter, and place the template into the subscription folder into your landing zone management group(s).

<add detailed step-by-step instructions>



```
{
    "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "principalId": {
            "type": "string",
            "metadata": {
                "description": "Provide the objectId of the principal (user, group, SPN, managed identity etc.) that will be granted RBAC at scope."
            }
        },
        "roleDefinitionId": {
            "type": "string",
            "defaultValue": "b24988ac-6180-42a0-ab88-20f7382dd24c",
            "metadata": {
                "description": "Provide the id of the built-in roleDefinition. Default is 'Contributor'."
            }
        }
    },
    "resources": [
        {
            "type": "Microsoft.Authorization/roleAssignments",
            "apiVersion": "2017-09-01",
            "name": "[guid(parameters('principalId'))]",
            "properties": {
                "principalId": "[parameters('principalId')]",
                "roleDefinitionId": "[concat('/providers/Microsoft.Authorization/roleDefinitions/', paramete
rs('roleDefinitionId'))]"
            }
        }
    ]
}
```