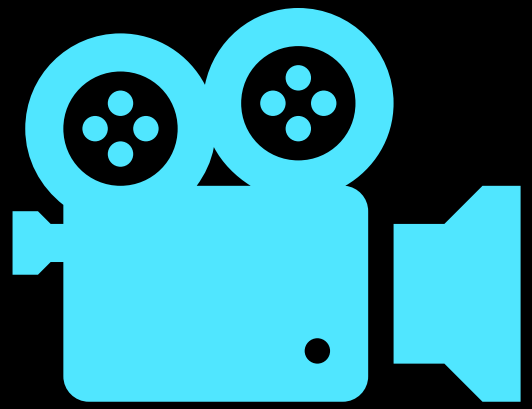
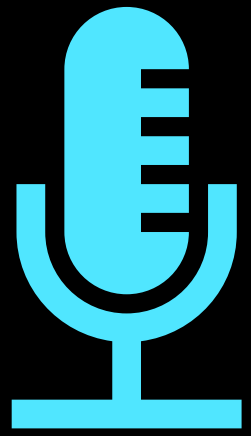
Microsoft

Enterprise Scale Landing Zones

August 2021 Community Call

Microsoft





This meeting is being recorded

Agenda

- Welcome
- What's New?
- Questions from the community - https://github.com/Azure/Enterprise-Scale/issues/668
- Contributing
- Q & A

Before we get started...

At any point, if you have a question please put it in the chat!

(we have the entire team here to help 😎)

Also we may stop and discuss your question/point at that time, we want this to be an open discussion with all of you 🙂

New “What’s New?” page

https://aka.ms/ES/WhatsNew

Updates

Here's what's changed in Enterprise Scale:

August 2021

Docs

- Lots of updates to the Terraform Module for Cloud Adoption Framework Enterprise-scale wiki

Tooling

- Terraform Module for Cloud Adoption Framework Enterprise-scale release v0.4.0
  - Brings support for Hub Connectivity & Identity landing zone peering - read more in the release notes linked above
- Do-It-Yourself deployment instructions for Enterprise-Scale using Azure PowerShell released

Policy

- Some minor changes to parameters and variables, tidying up some code.
  - See PR #727

Other

No updates, yet.

July 2021

Docs

- Added guidance for Resource Group usage for Azure Networking topologies in Hub & Spoke & Virtual WAN CAF docs - closing issue #632
- Updated Connectivity to Azure PaaS services CAF docs based on customer feedback around Private Link /Service Endpoints differences and guidance, including ExpressRoute peering options relating to this. Closing issue - #519 on CAF repository
- Updated Contoso, Adventure Works & Wingtip Toys reference implementations with new Deploy To Azure buttons for new portal experience
  - Also updated guidance and option availability for each of them respectively
- User Guide updated to reflect latest release and new portal experience
- New Article to Deploy Azure Red Hat OpenShift (ARO) in enterprise-scale landing zones

Tooling

- Portal Experience Updated
  - Merged Contoso, AdventureWorks, and Wingtip into one ESLZ deployment experience via first-party deployment in the portal ("Deploy To Azure" button) experience
    - Support "N" network topologies in same experience (Hub and Spoke, Virtual WAN, Hub and Spoke with NVA)

Azure Landing Zone Accelerator portal experience

Azure landing zone accelerator

For organizations where this conceptual architecture fits with the operating model and resource structure they plan to use, there is a ready-made deployment experience available which we call the **Azure landing zone accelerator**.

The accelerator is an Azure portal-based deployment that will provide a full implementation of the conceptual architecture, along with opinionated configurations for key components such as management groups and policies.

Deploy to Azure

There are other deployment options available, some that deliver the full architecture using third-party deployment technologies, and others that start from a smaller footprint. For more information, see Implementation options.

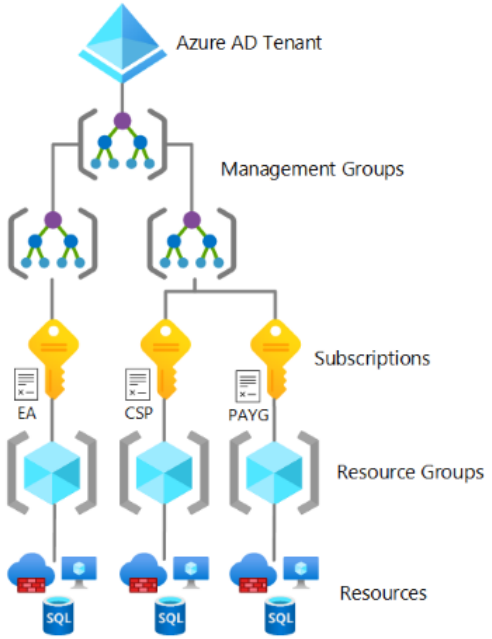
Updated article

[Enterprise Agreement enrollment and Azure Active Directory tenants - Cloud Adoption Framework | Microsoft Docs]

Enterprise Agreement enrollment and Azure Active Directory tenants

08/18/2021 • 10 minutes to read • +7

The Azure service presents a range of active subscription offers, and customers can use these offers at the same time to gain flexible billing options. Example subscriptions include Enterprise Agreement (Enterprise Agreement) Support, Microsoft Customer Agreement, Cloud Service Provider, and others.

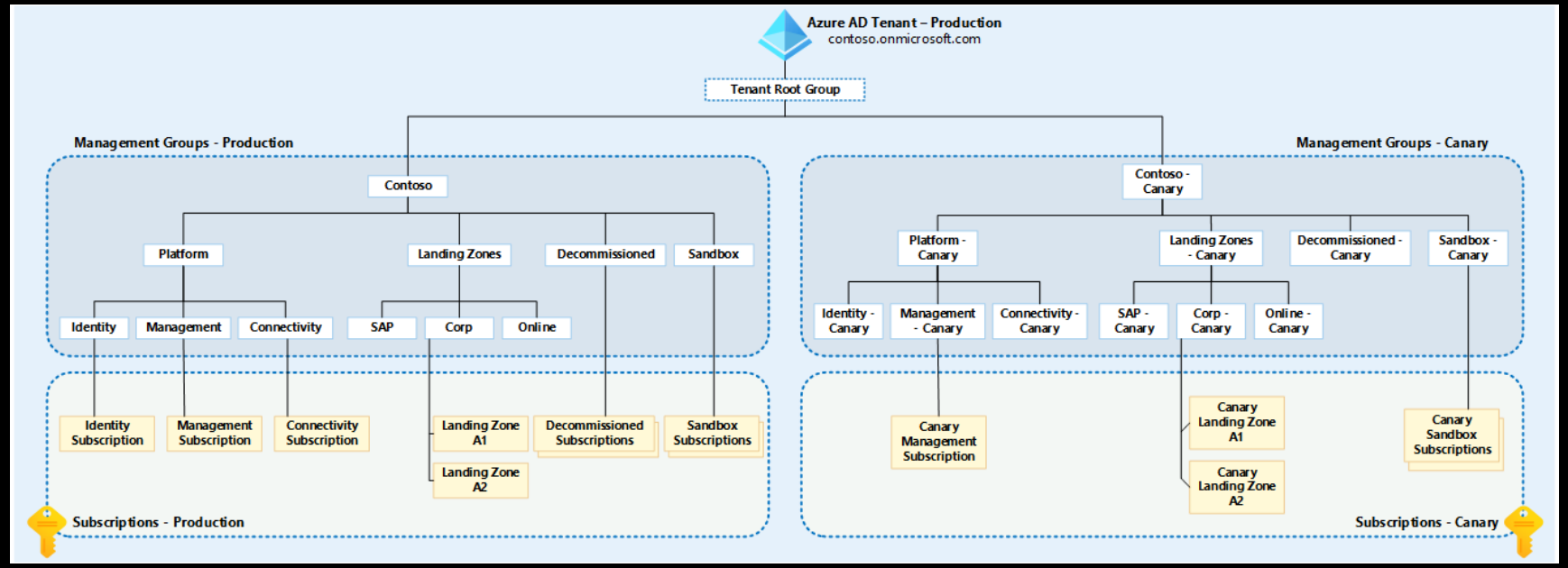


Enterprise-scale architecture supports subscriptions from any Azure offer. Subscriptions should exist within one Azure Active Directory (Azure AD) tenant to then relocate into the management group hierarchy within that tenant. They can then be managed by the various controls with enterprise-scale platforms like Azure Policy and role-based access control (RBAC).

> **Note**
>
> Enterprise-scale architecture is only scoped and deployed to one Azure AD tenant; however, billing options can span across multiple Azure AD tenants. For example, an Enterprise Agreement enrollment supports Azure subscriptions across different Azure AD tenants.

New article

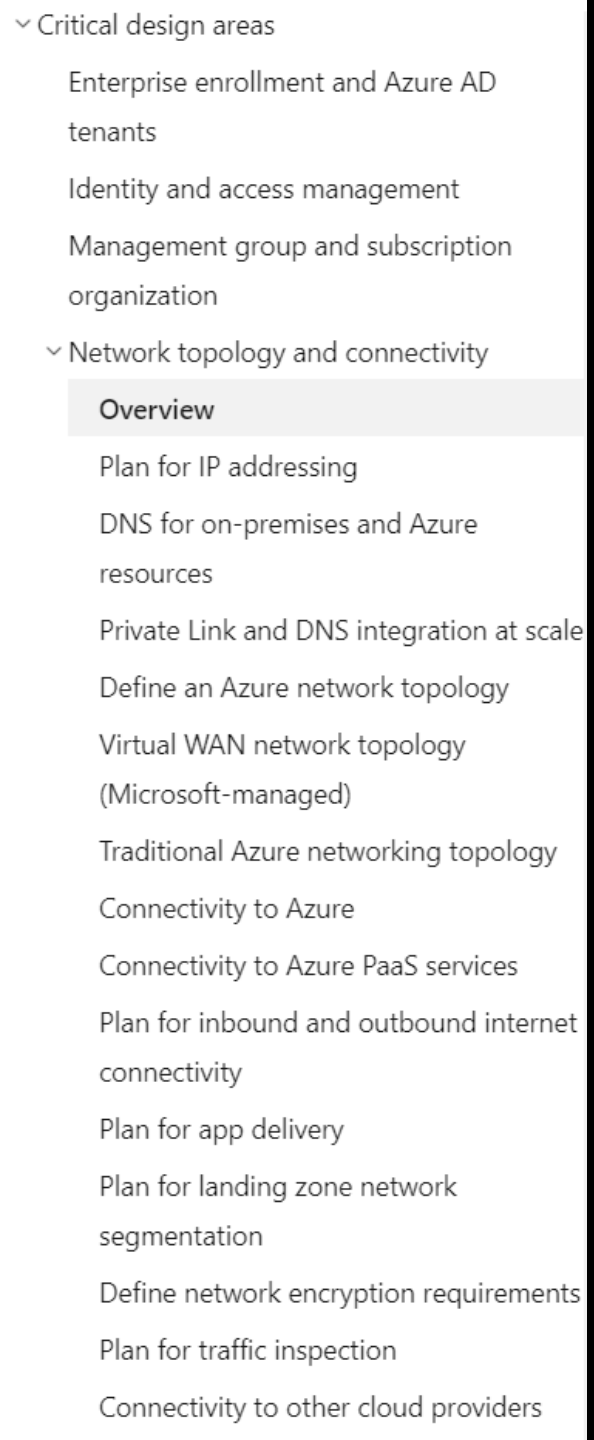
[Testing approach for enterprise-scale - Cloud Adoption Framework | Microsoft Docs]



New Networking Navigation

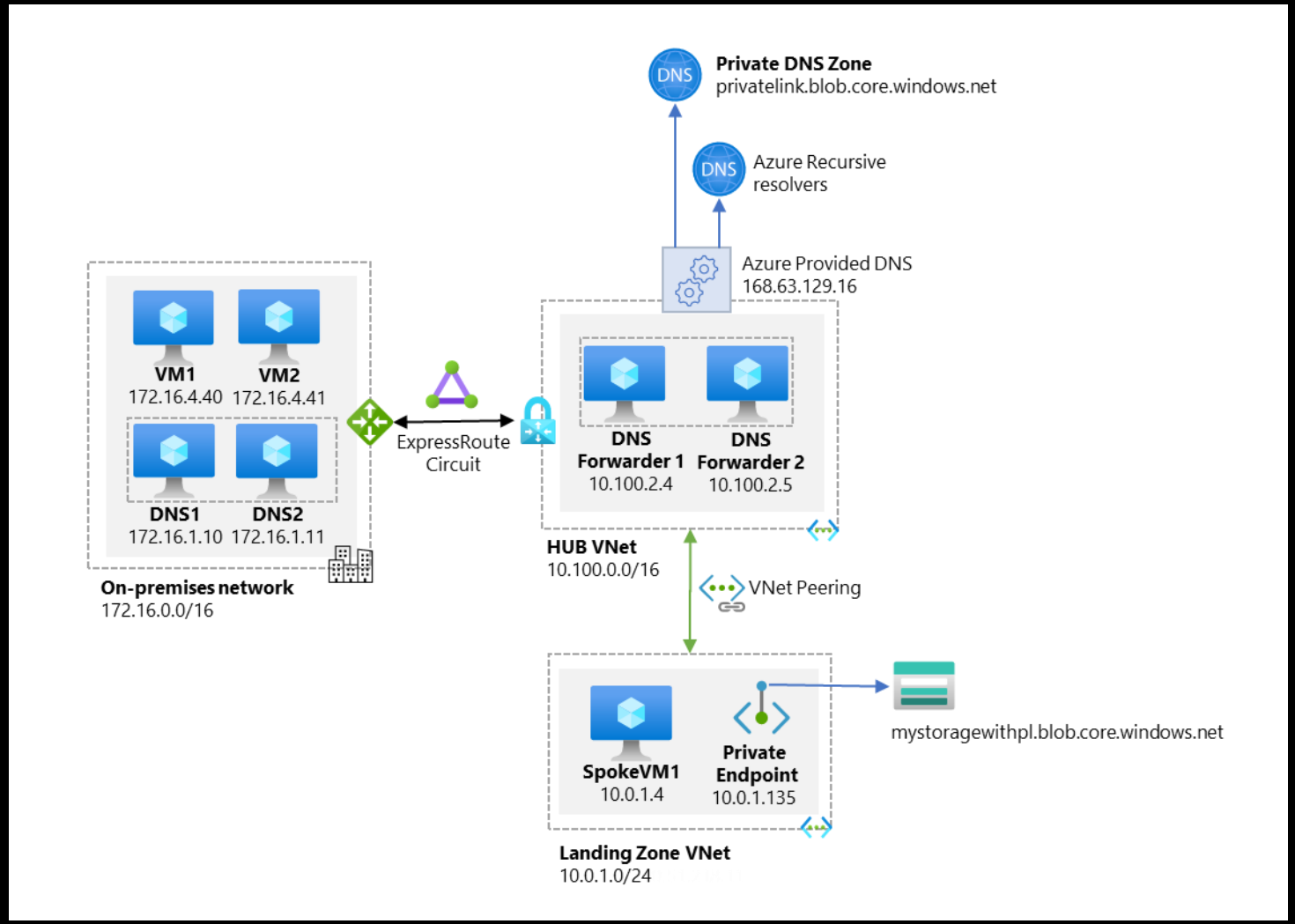
https://aka.ms/EnterpriseScale/Networking

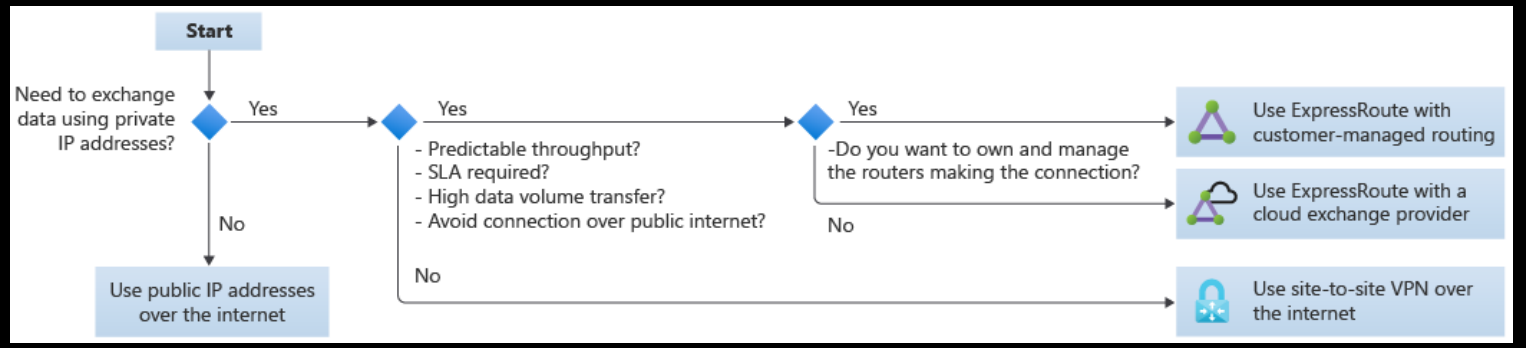
- Multiple smaller articles instead of a single large one



Make sure to check out…

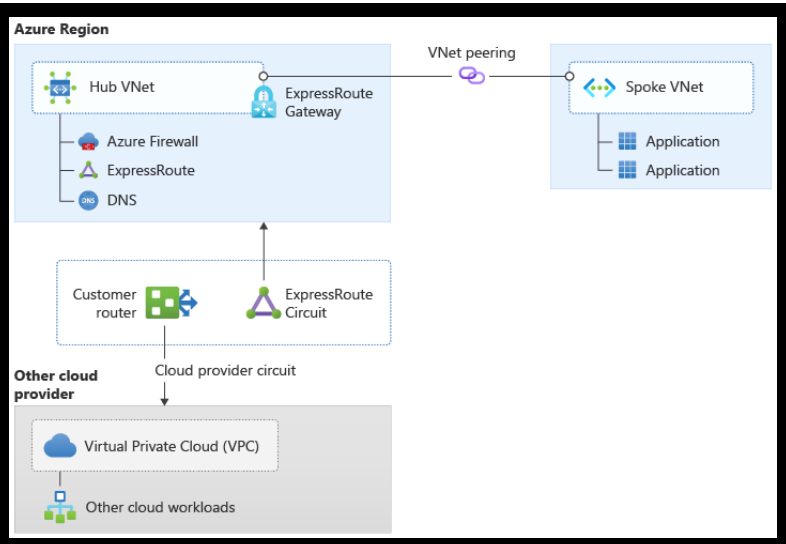
[Private Link and DNS integration at scale - Cloud Adoption Framework | Microsoft Docs]

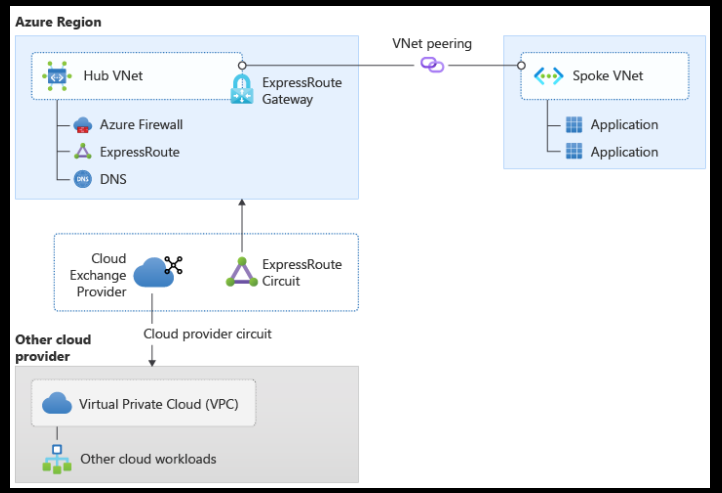


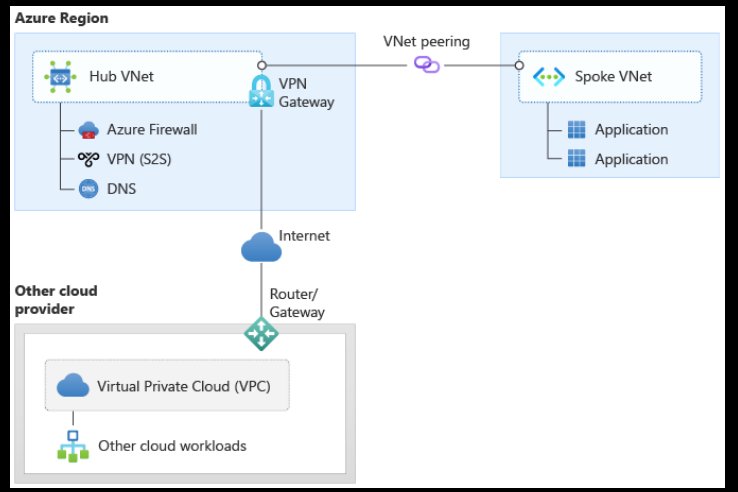


Make sure to check out…

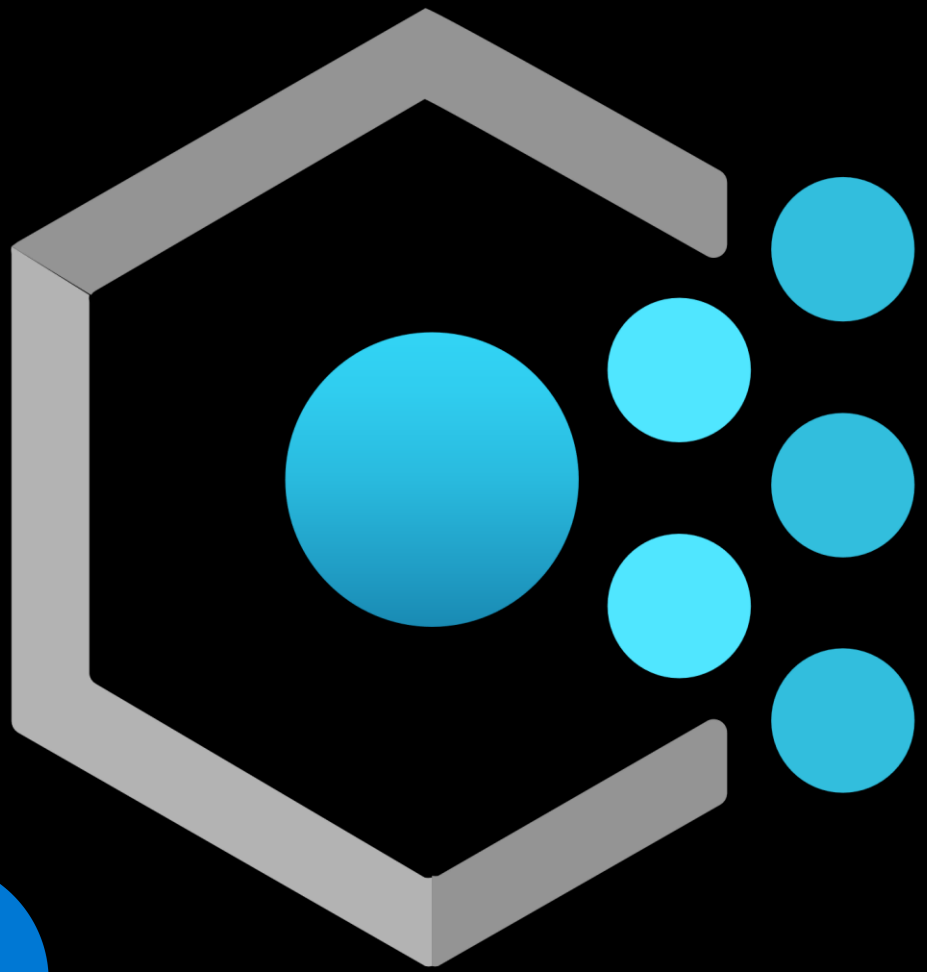
[Connectivity to other cloud providers - Cloud Adoption Framework | Microsoft Docs]







Azure Policy updates



AINE and DINE enhancements – *Available Now!*

- EvaluationDelay - **Understand how effects work - Azure Policy | Microsoft Docs**
  - Control when the child resource gets evaluated
    - AfterProvisioning / AfterProvisioningSuccess / AfterProvisioningFailure or an ISO 8601 duration between 0 and 360 minutes
  - Default time is 10 minutes – unchanged from today

- DINE now triggers on 'Microsoft.Resources/subscriptions'
  - Brings it inline with all other resource behaviour for DINE

ESLZ Custom Policies Moving To Built-In – *Overtime!*

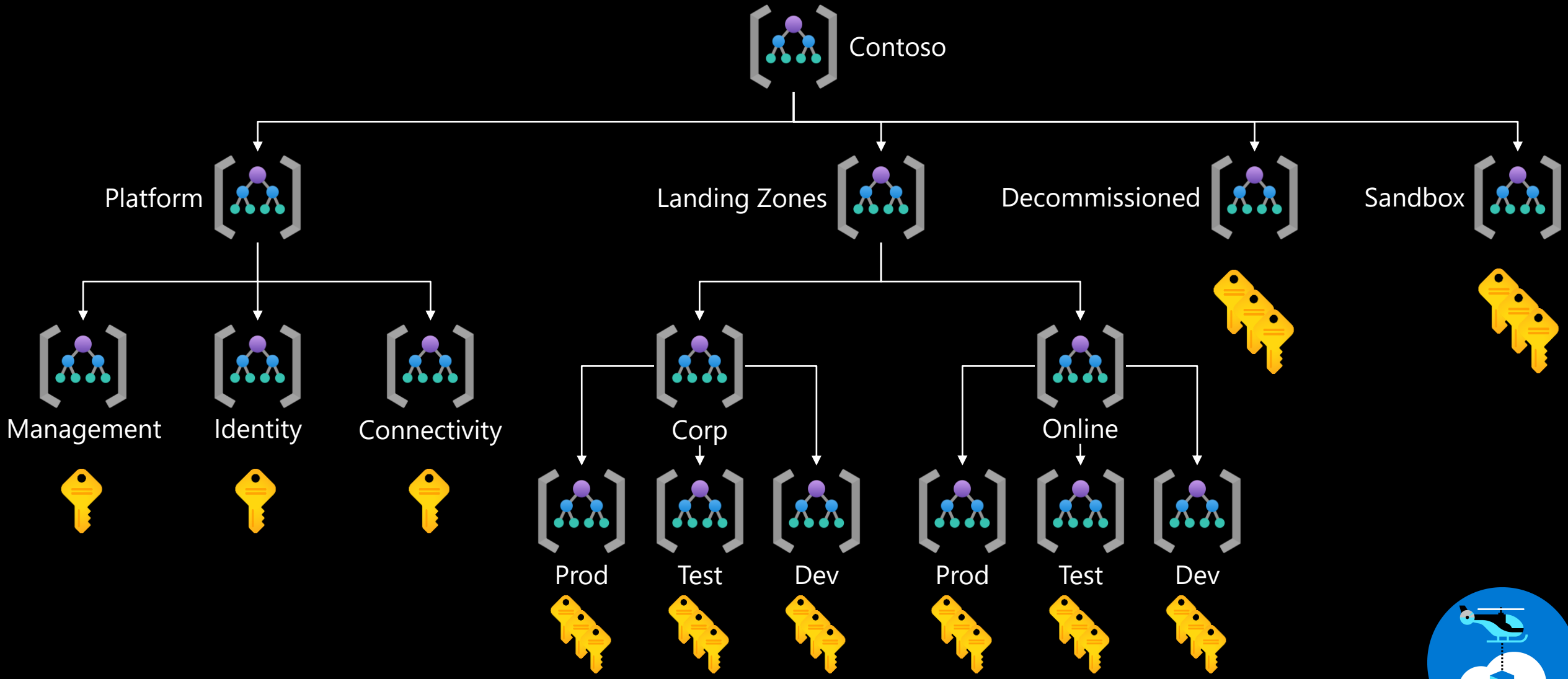
Azure Governance and Deployments Quarterly Customer Panel:
https://www.youtube.com/watch?v=tHyPDESIThk

ESLZ Roadmap

- Terraform Module (caf-enterprise-scale) – v0.4.0 out now
  - Please read release notes and upgrade notes
  - Hub Connectivity resource deployment – Hub & Spoke only, first!
  - Policy assignment upstream proivder changes in 'azurerm' provider v2.66.0 – see PR #12349
  - Wiki updates and YouTube series (coming soon) – subscribe to the IT Ops Talk YouTube Channel
- Bicep Templates for ESLZ – tracking for around October 2021
- Brownfield Gudiance Enhancements – EO CY2021

Handling Workload Environments in ESLZ

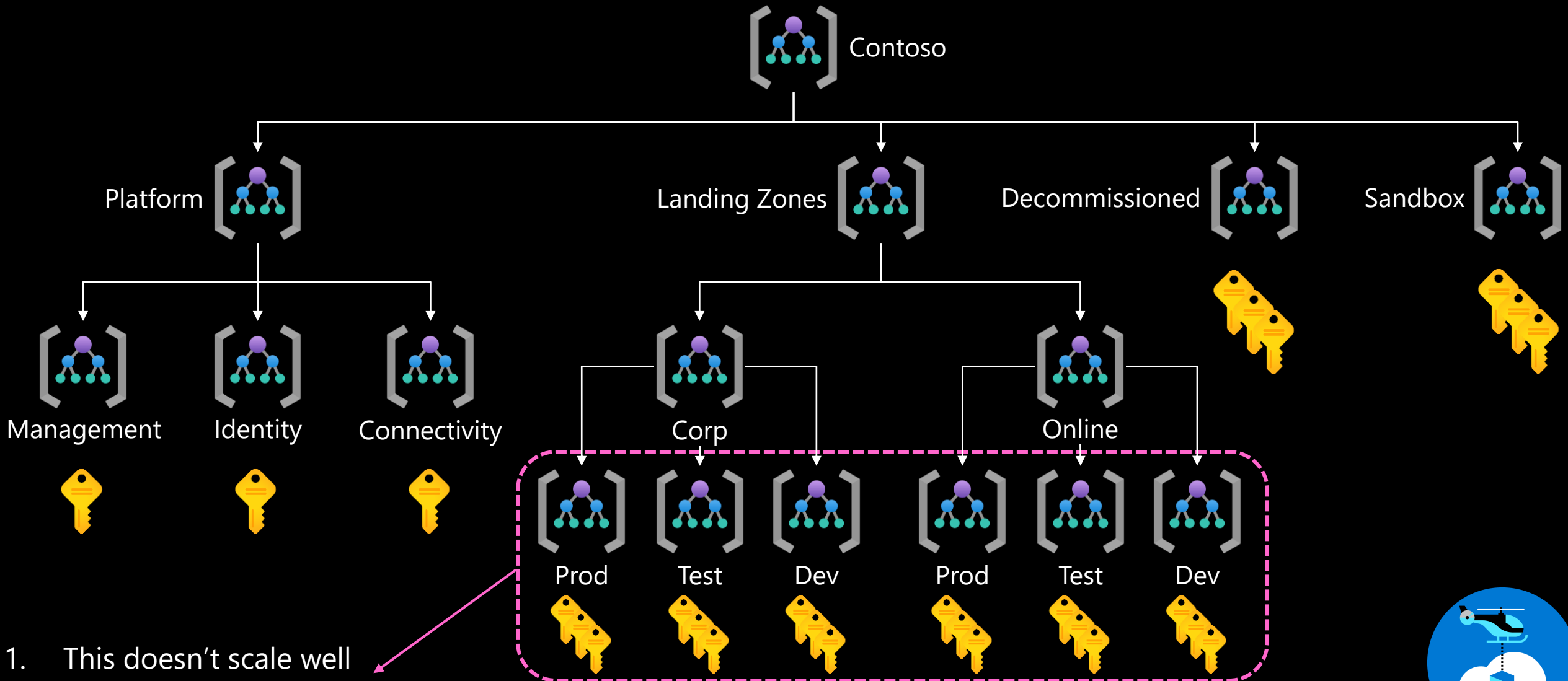
a.k.a. Dev/Test/Prod



Environmental Splitting Design

Handling Workload Environments in ESLZ

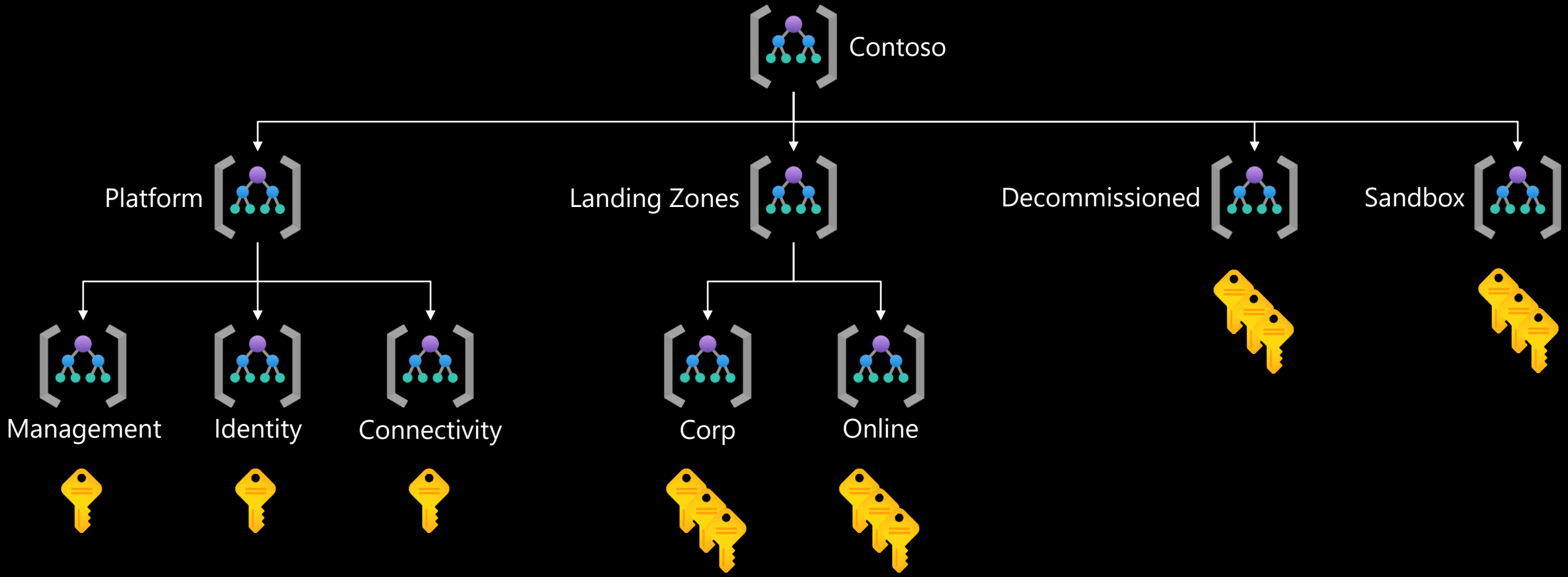
a.k.a. Dev/Test/Prod



1. This doesn't scale well
2. Can be even worse if done per app etc.
3. What is the difference between environments?

Handling Workload Environments in ESLZ

a.k.a. Dev/Test/Prod

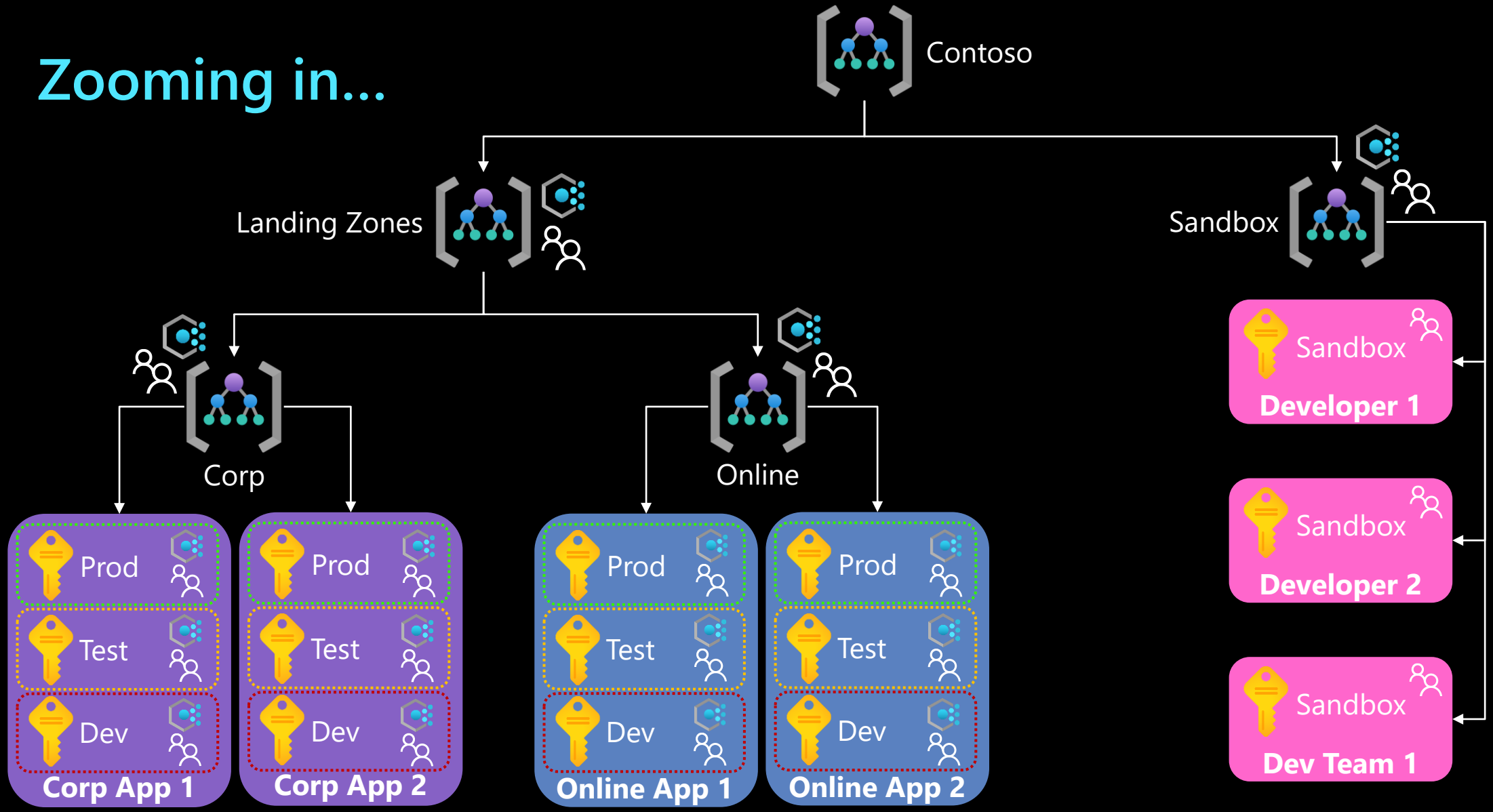


ESLZ Conceptual Architecture

Handling Workload Environments in ESLZ

a.k.a. Dev/Test/Prod

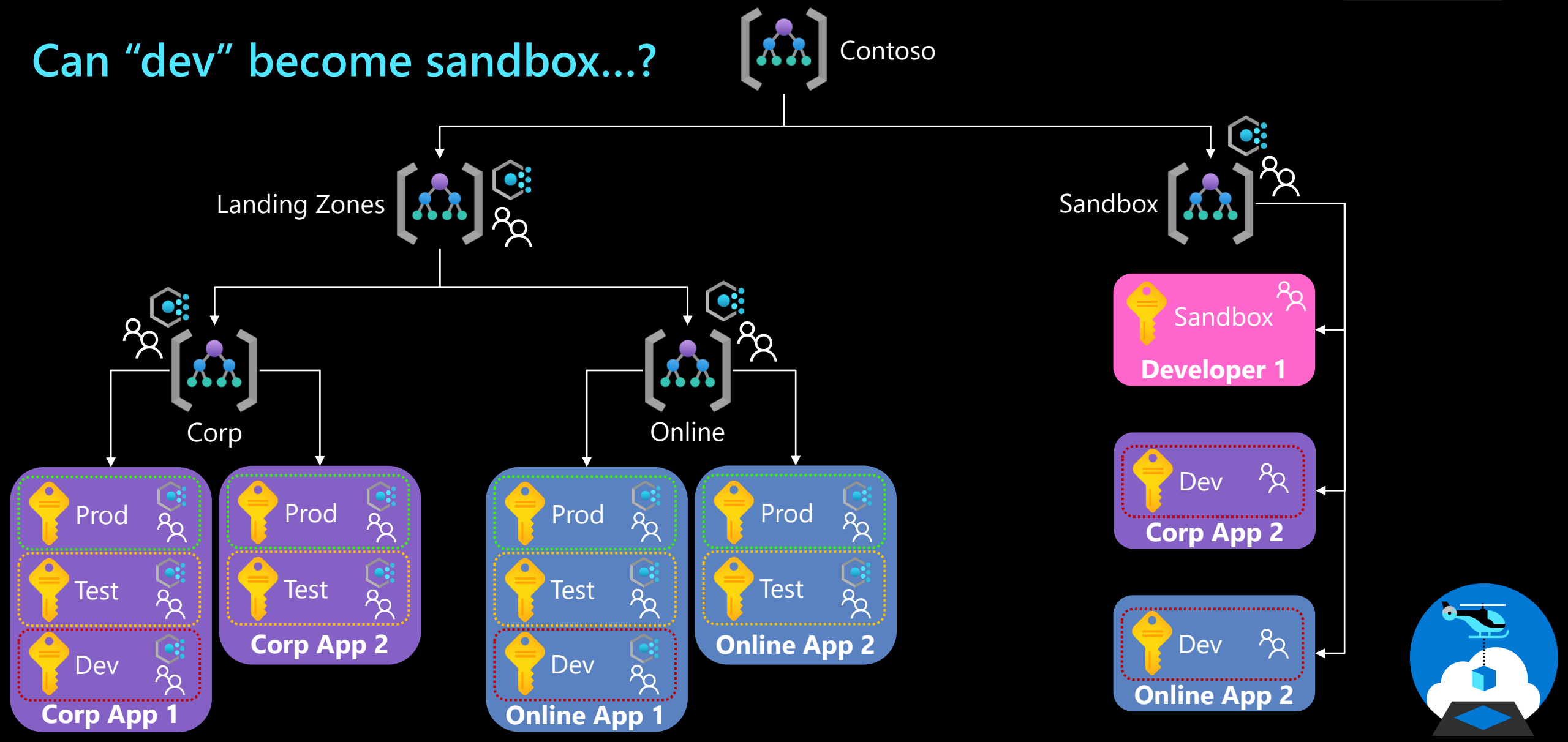
Zooming in...



Handling Workload Environments in ESLZ

a.k.a. Dev/Test/Prod

Can “dev” become sandbox…?

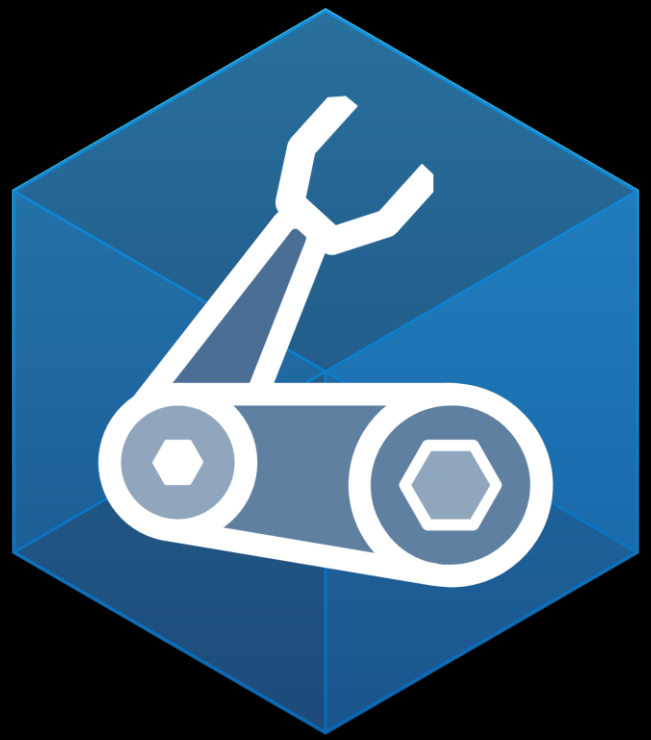


Handling Workload Environments in ESLZ

a.k.a. Dev/Test/Prod – Key Takeaways

- Management groups should align to workloads/archetypes
- There should be no difference in policies between environment type
  - Why create something that works in dev that then won't work in production?
- Splitting by environment does not scale well
  - Do you then group by application as well?
    - N x 3 at least for each app! = 20 apps = 60 Management Groups!
- Sandbox should be utilised for true "dev" purposes
- Empower application owners via subscription democratisation
  - With empowerment comes responsibility for the app owners for things like cost, SKU usage etc.

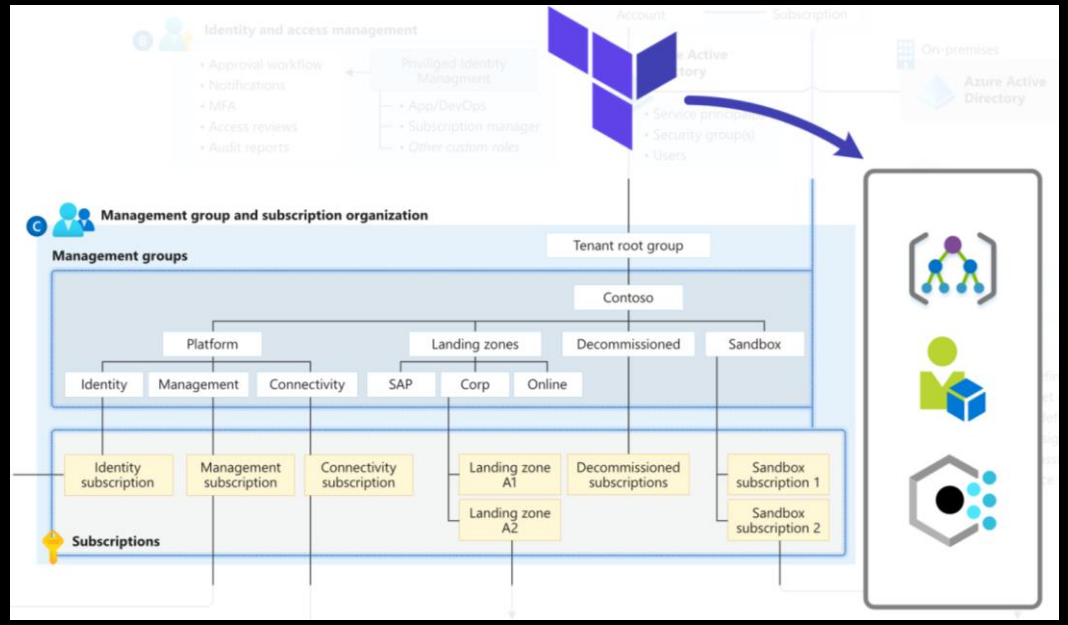
ESLZ Bicep Options



- Coming soon! – currently tracking for October 2021
- Using the latest bicep features available in v0.4+
- Will initially deliver a Hub & Spoke topology (a.k.a. Adventure Works)
  - Will look to add others soon after
- Will be modular from the start
- Instructions on how to sequence and deploy will be provided
  - Will also provide orchestration template to sequence for you like the “Deploy To Azure” button today
- Some Policy elements, likely to stay in JSON for reusability

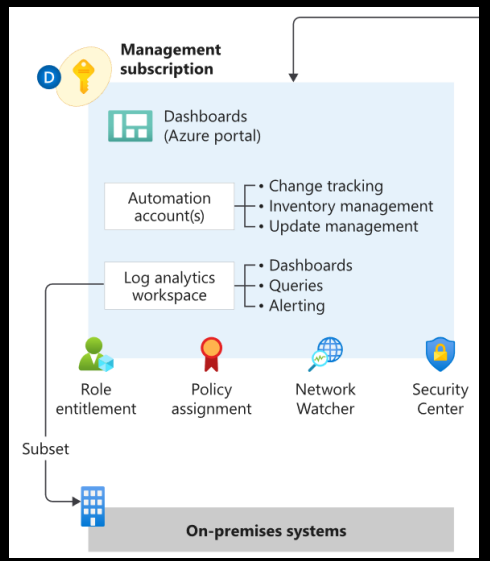
Terraform Modules

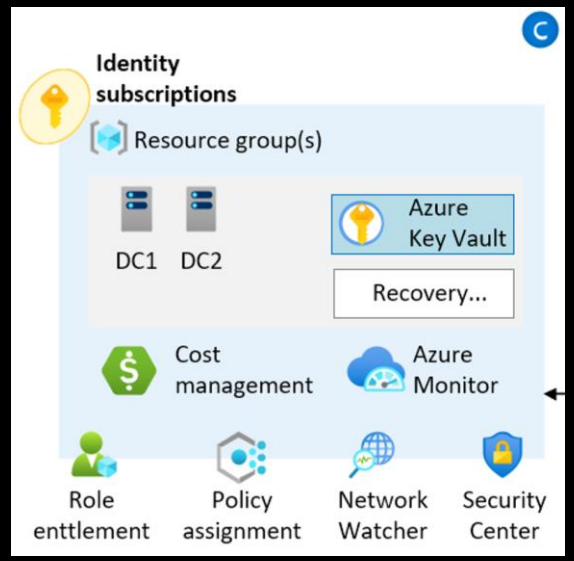
CAF-Enterprise-Scale

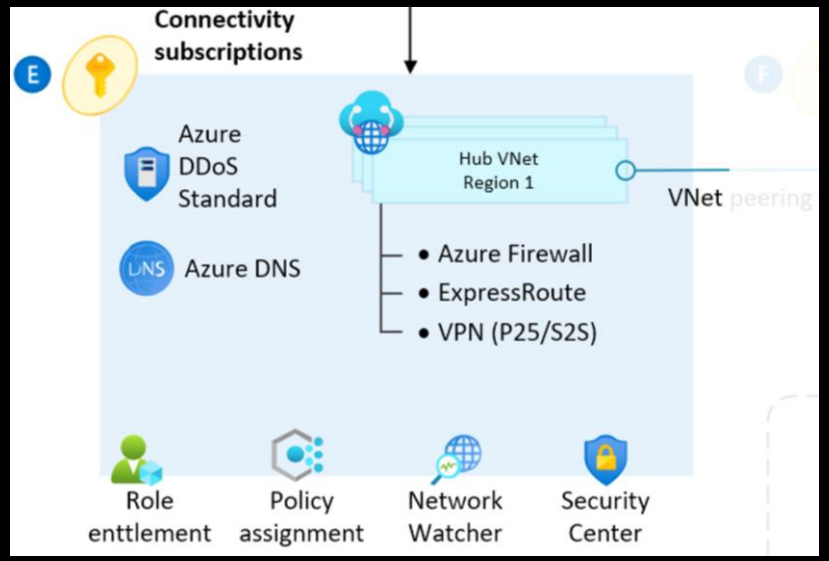


CAF-Enterprise-Scale

- Official module authored and maintained by the Enterprise Scale team
- Delivers the components included in Enterprise Scale
- Native Terraform and can be run anywhere Terraform can be
- Parity with other Enterprise Scale implementation options and features
- Simple to use, fully customisable if desired
- Useable in any operational approach

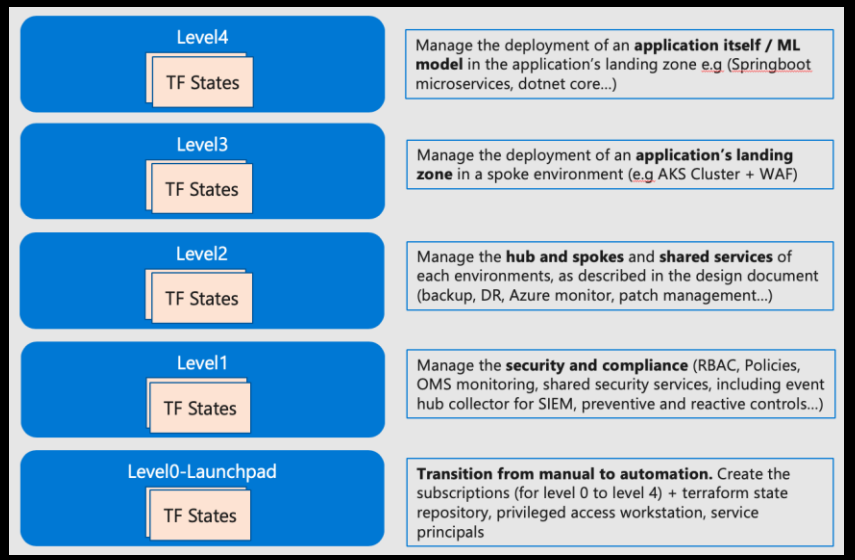


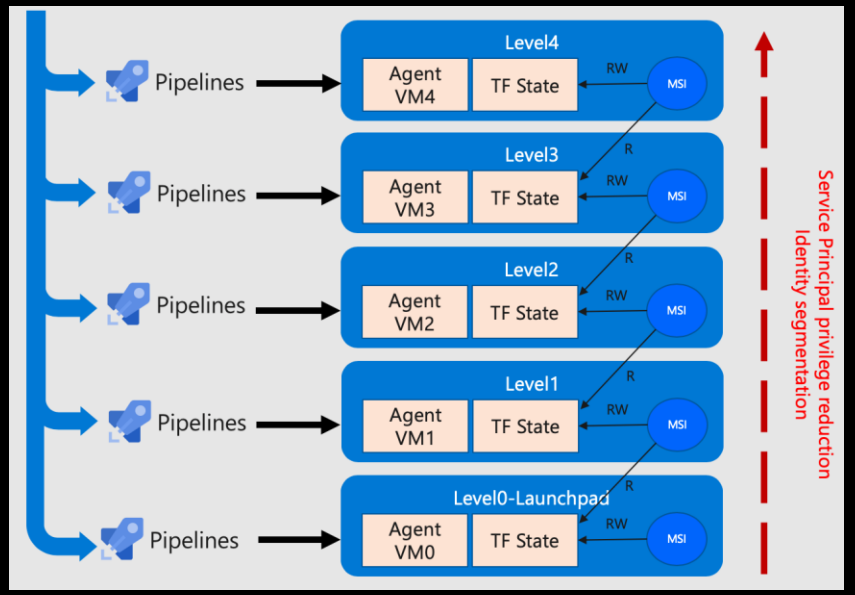




Terraform Modules

CAF-Terraform-LandingZones





CAF-Terraform-LandingZones

- Module created by Microsoft CSAs in Singapore (Arnaud & Laurent)
- Uses a custom container called "Rover" for deployment
- Has various "Levels" (0 to 4)
  - Separate state file and pipeline for each level
- Focus is towards workloads and services that live in Landing Zones (see currently supported list here)
  - Uses the CAF-Enterprise-Scale Module to deploy Enterprise Scale components
- Leans towards a centralised operational approach
- More info on the docs here

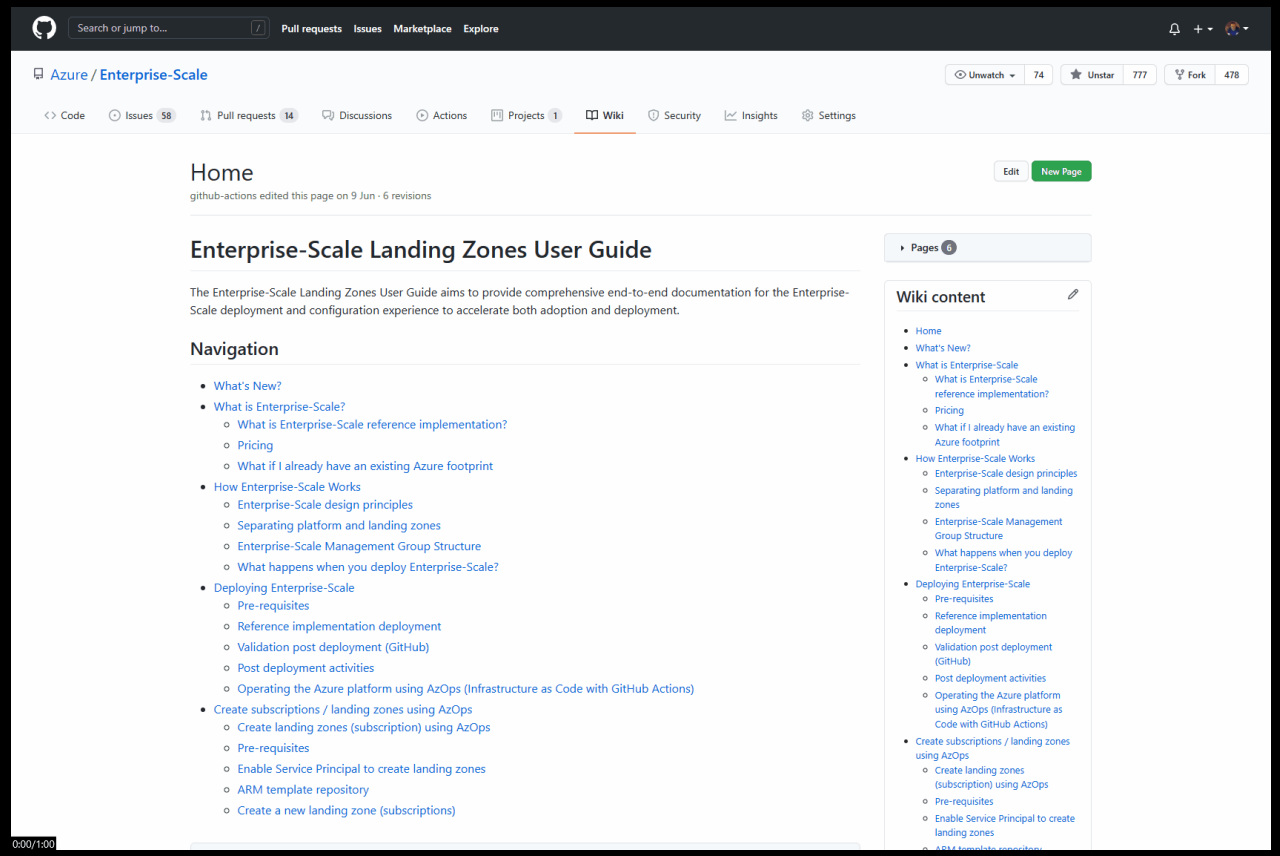
We Want You!

https://aka.ms/EnterpriseScale

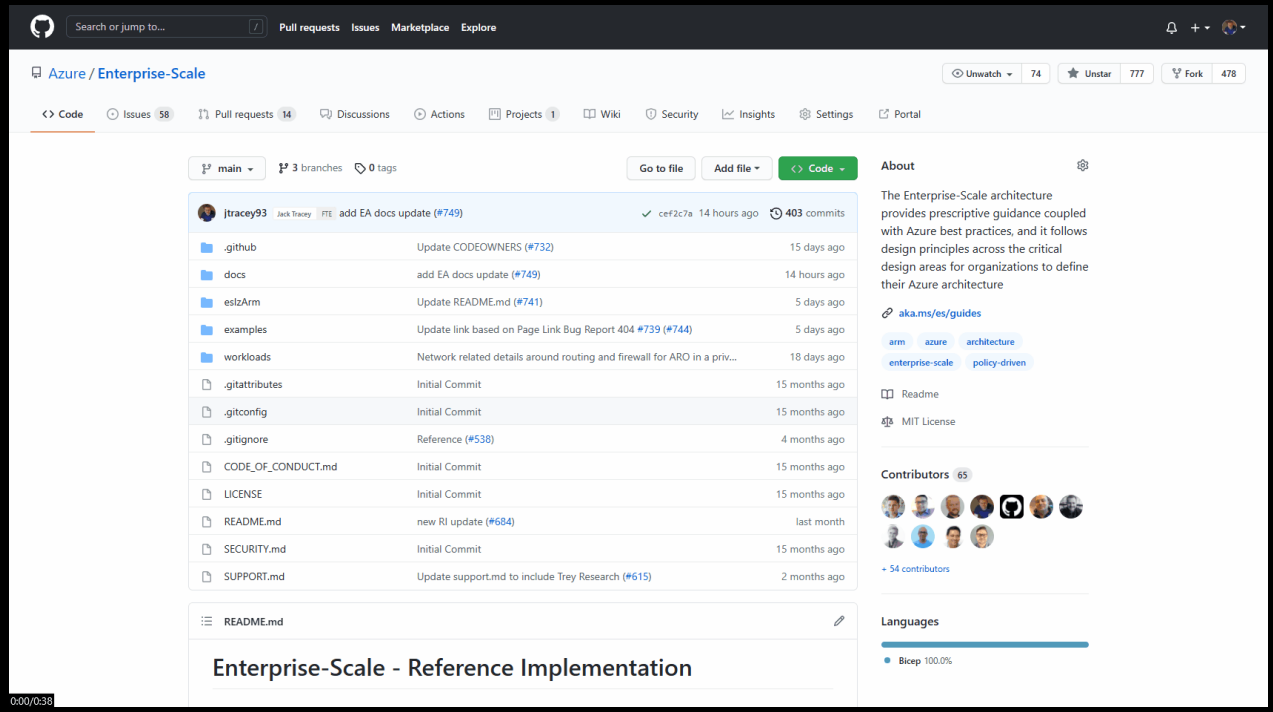
To contribute to ESLZ

- Create issues, bugs and feature requests
- Tell us where we can improve existing guidance or provide new guidance

Update docs/wiki:



Create an issue/feature request:



Microsoft

Q & A

Microsoft

Thank You!

https://aka.ms/ESLZCommunitySurvey