Microsoft

Project Journey

Azure Migration Enablement Program

8 Sept 2020 – 11 Nov 2020

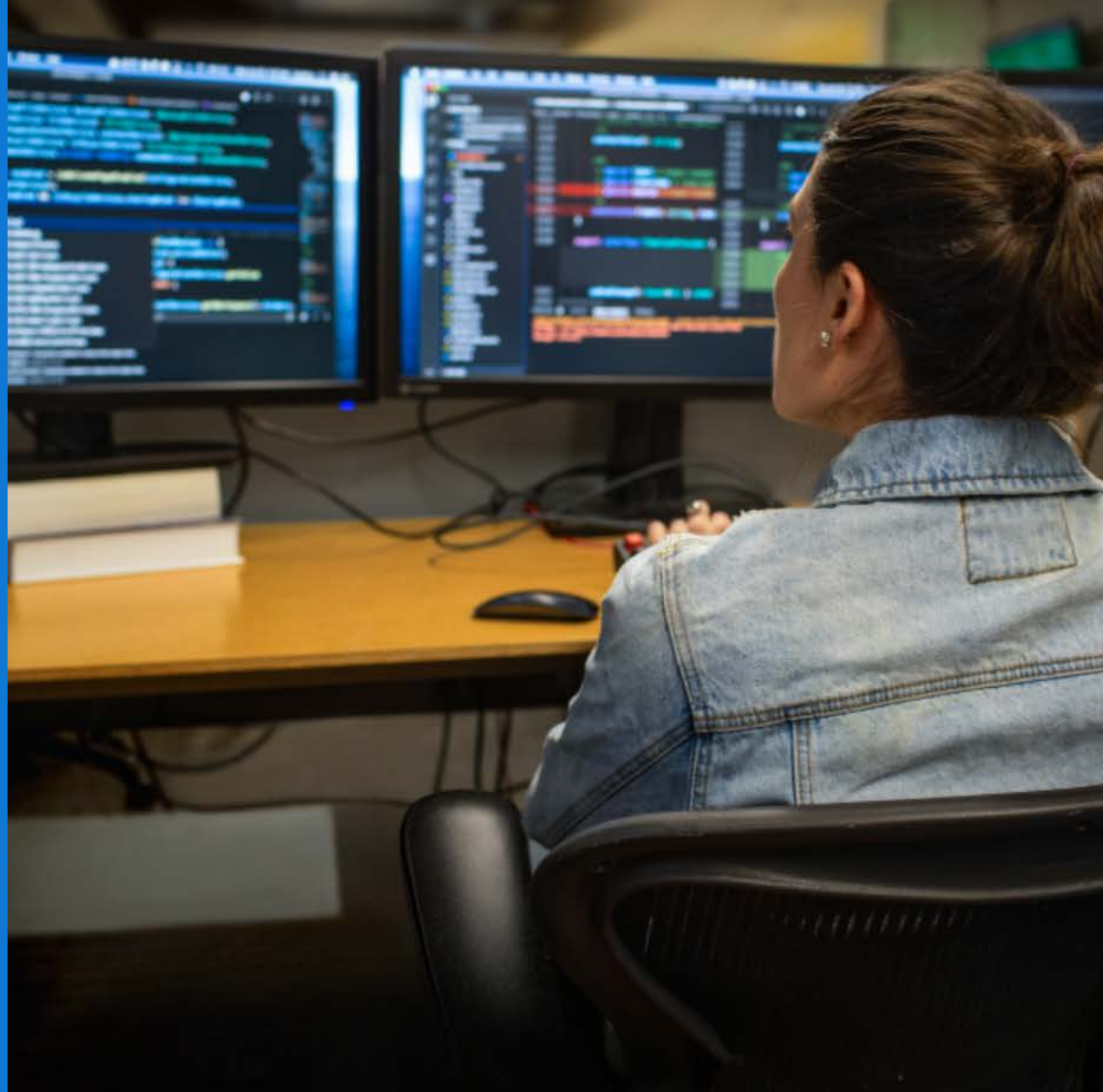
APAC

Today's Session
Module 3 – Tuesday 13 October 2020

Please hold while we get the event ready…
Session will start at 10:15am SGT

IMPORTANT NOTICE:

- If you choose to participate in this session using Microsoft Teams, your name, email address, phone number, and/or title may be viewable by other session participants.
- Please note that the training will not and cannot be recorded in alignment with Microsoft's policies



Microsoft

Azure Migration / Project Journey
Module 3 – Getting Ready

Nicolas Yuen - Cloud Solution Architect

Inseob Kim - Cloud Solution Architect

Azure Migration – Getting Ready

Is the technical skills needed to start a cloud adoption effort and prepare your migration target environment

Agenda

Cloud Adoption Framework: Ready

Azure Setup Guides

First Landing Zone

Azure Terraform Landing Zone

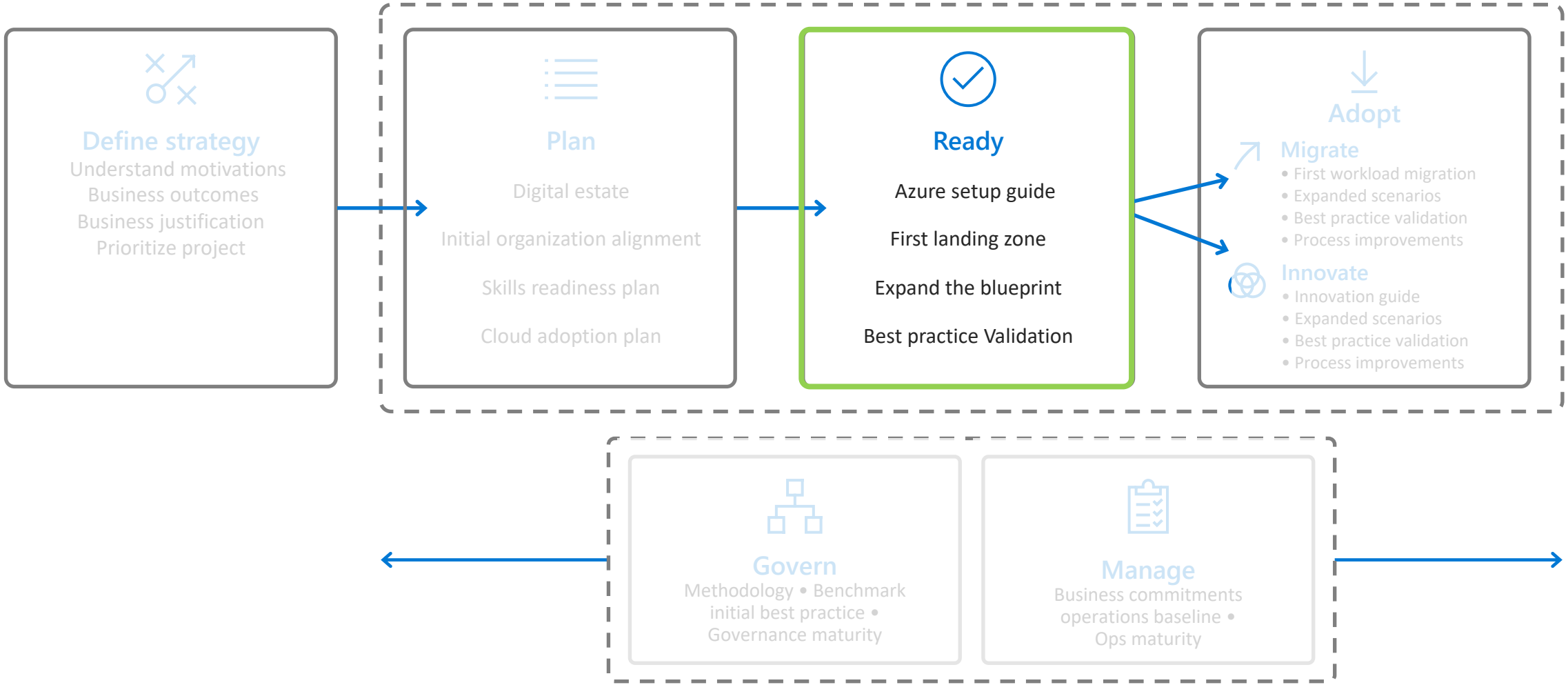
Expand Landing Zones

Enterprise Scale

Ready

Cloud Adoption Framework

Microsoft Cloud Adoption Framework for Azure



Cloud Adoption Framework: Ready

The ‘Ready’ module establishes a cloud foundation or adoption target that can provide hosting for any adoption efforts.

1. **Azure setup guide**
   Azure setup guidance on the tools and approaches you need to create a landing zone
2. **First landing zone**
   Choose the most appropriate landing zone option to establish a code-based starting point for your environment
3. **Expand the landing zone**
   Meet the platform considerations of your cloud adoption plan by expanding your landing zone
4. **Best practices**
   Validate landing zone modifications against best practices

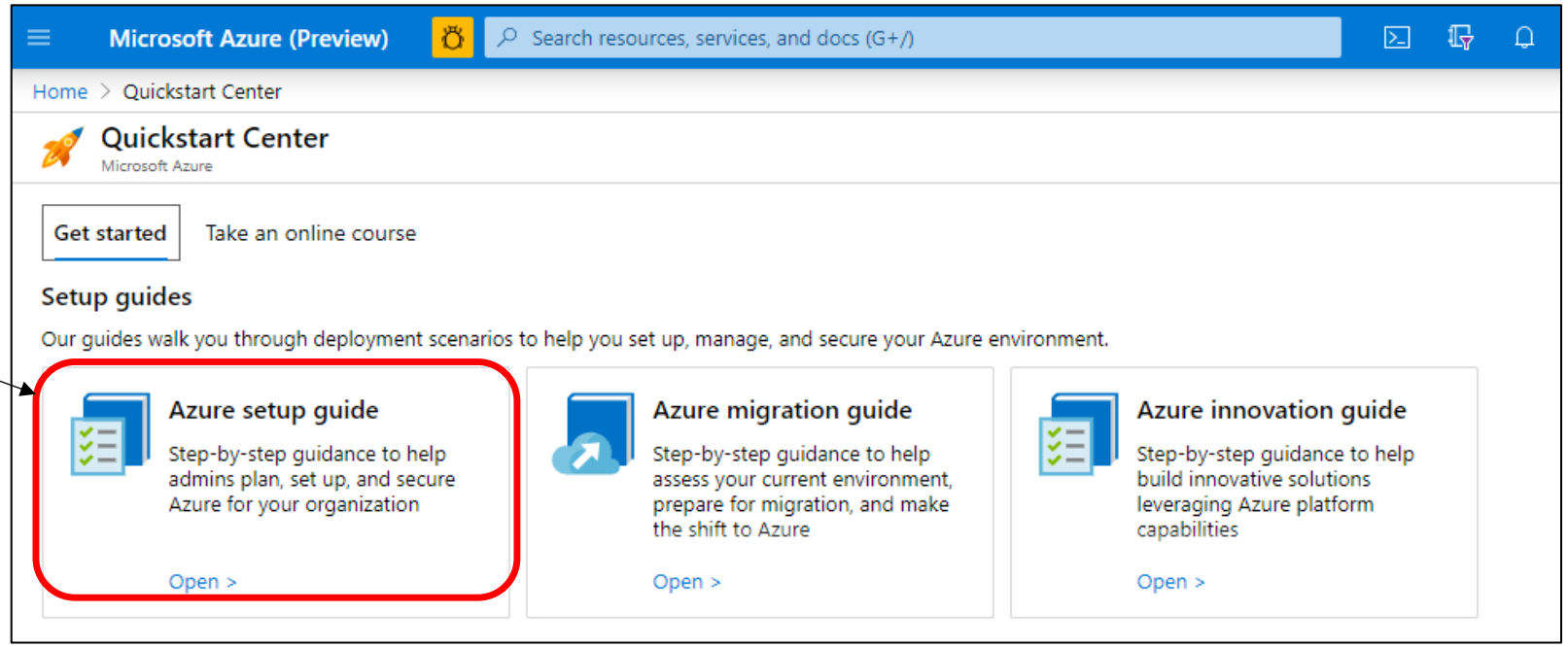
How to prepare Azure environment before you start migration and innovation?

Azure Setup Guides

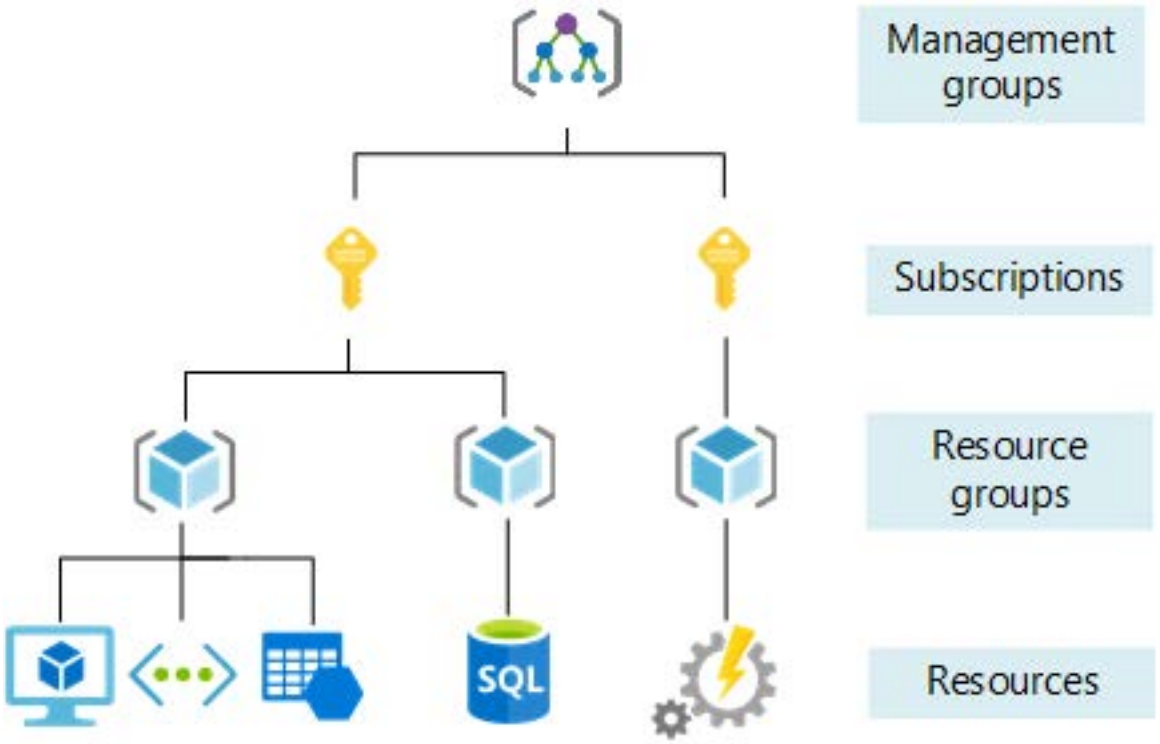
Azure setup guide

- Prepare the cloud environment before building and deploying solutions using Azure services
- The Azure setup guide provides guidance on how to organize resources, control costs, and secure and manage your organization helping you create your landing zone in Azure

The guide is also published in the **Azure Quickstart Center** within the Azure Portal



Organize Azure resources



Management groups: These groups are containers that help you manage access, policy, and compliance for multiple subscriptions.

Subscriptions: A subscription logically associates user accounts and the resources that were created by those user accounts.

Resource groups: A resource group is a logical container into which Azure resources deployed and managed.

Resources: Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

Management Group & Subscription Organisation

Define Hierarchy, Quota & Capacity, and Manage Cost

Subscription Organization and Governance

- ❑ Use Management Group structure, within an AAD tenant, to support org mapping
- ❑ Must be appropriately considered when planning Azure adoption at-scale

Configure Subscription Quota and Capacity

- ❑ Platform limits and quotas within the Azure platform for services
- ❑ Availability of required SKUs in chosen Azure regions
- ❑ Subscription quotas are not capacity guarantees and are per region

Establish Cost Management

- ❑ Potential need for chargeback models where shared PaaS services are concerned, such as ASE which may need to be shared to achieve higher density
- ❑ Shutdown schedule for non-prod workloads to optimise costs

Tags & Naming standards

Entity	Scope	Length	Casing	Valid characters	Suggested pattern	Example
Resource group	Subscription	1-90	Case insensitive	Alphanumeric, underscore, parentheses, hyphen, period (except at end), and Unicode characters	`<service short name>-<environment>-rg`	`profx-prod-rg`
Availability set	Resource group	1-80	Case insensitive	Alphanumeric, underscore, and hyphen	`<service-short-name>-<context>-as`	`profx-SQL-as`
Tag	Associated entity	512 (Name), 256 (value)	Case insensitive	Alphanumeric	`"Key" : "value"`	`"Department" : "Central IT"`

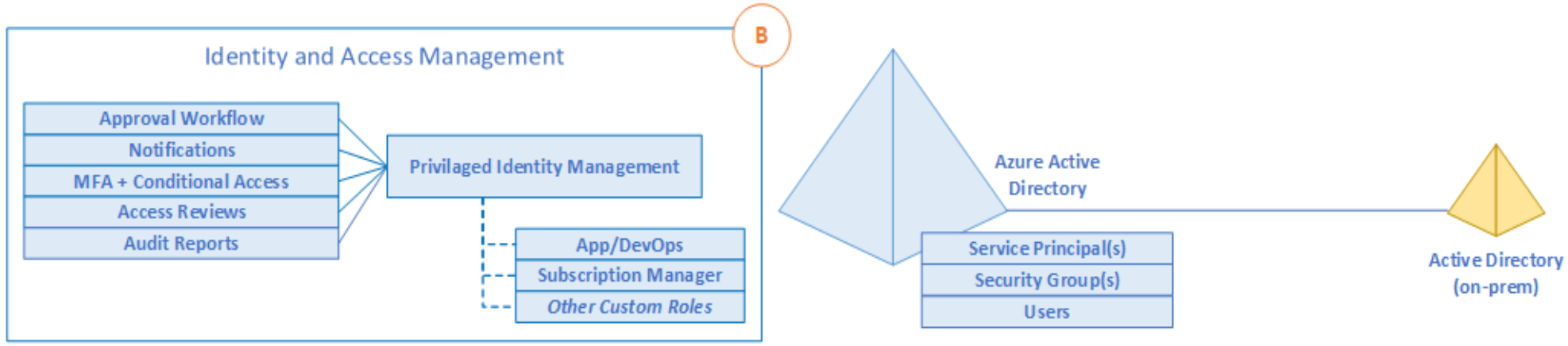
Identity & Access Management

A critical design decision enterprise organization must make when adopting Azure is whether to:

- ❑ **extend** an existing on-premises identity domain into Azure

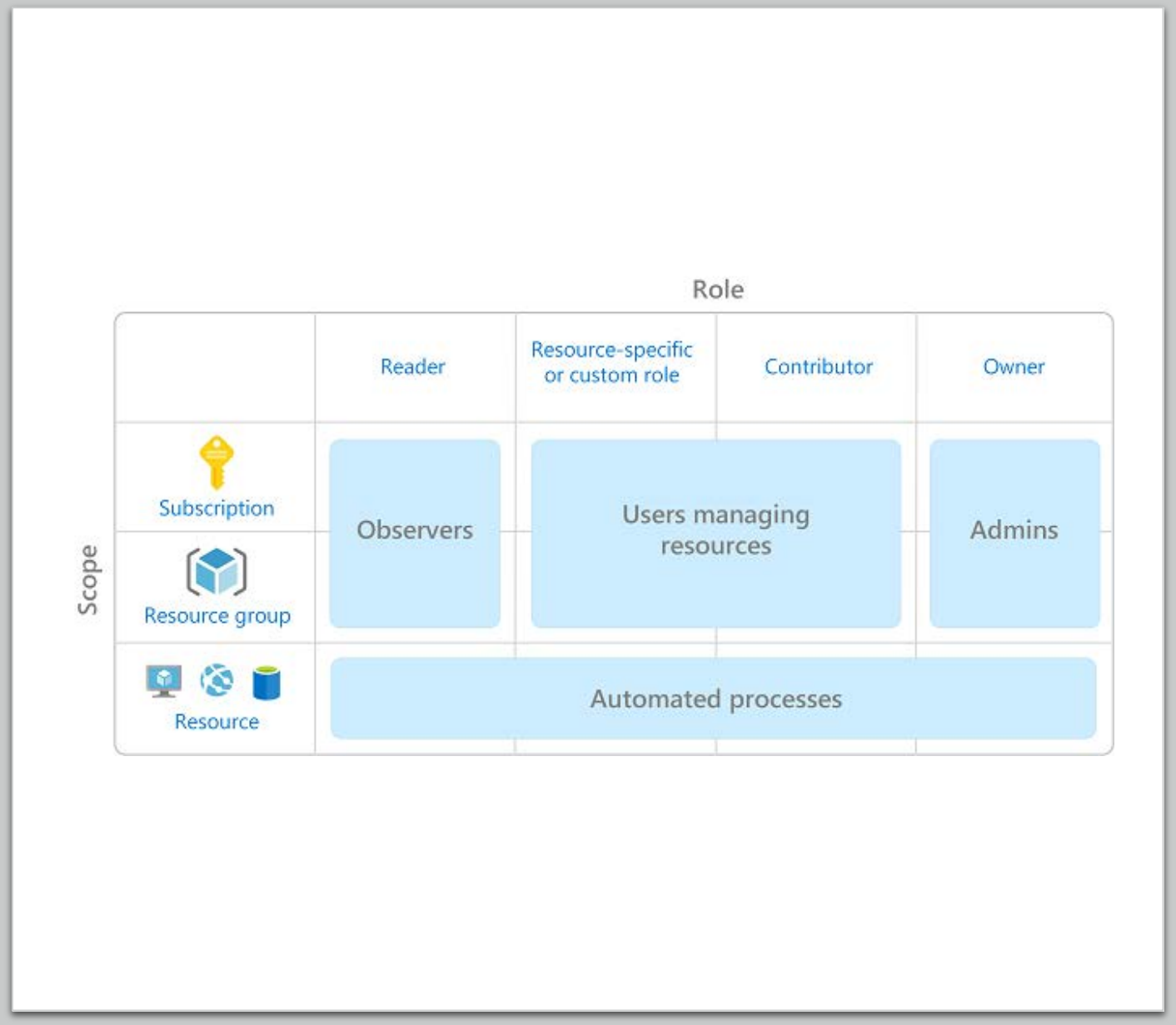
or

- ❑ **create** a brand new one



Access Control

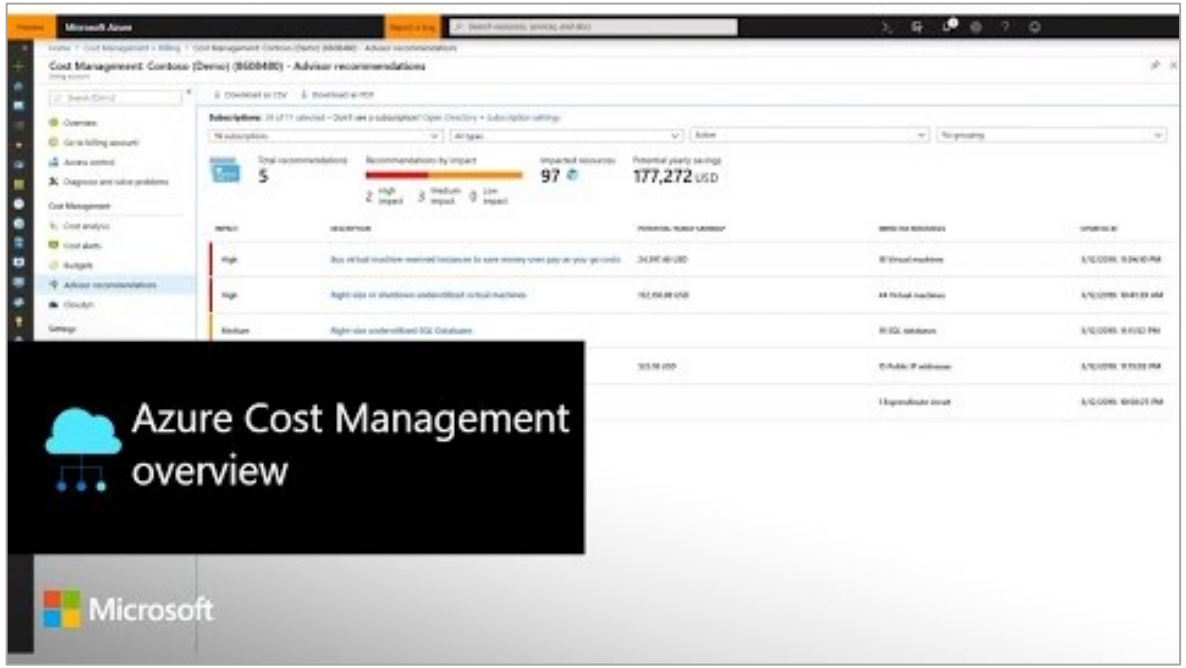
- Azure role-based access control (RBAC) is the primary method of managing access in Azure
- Deal with groups rather than individual users
- Don’t hesitate to create custom roles aligned with your organization
- Avoid creating a new AAD tenant unless there is a strong IAM and JML processes in-place.
- Enforce MFA for all privileged accounts.
- Use AAD PIM for Identity and Access management.



Manage costs and billing

Azure Cost Management helps you predict and manage costs:

- **Analyze cloud costs** helps you explore and analyze your costs. You can view aggregated cost for your account or view accumulated costs over time.
- **Monitor with budgets** allows you to create a budget and then configure alerts to warn you when you're close to exceeding it.
- **Optimize with recommendations** helps identify idle and underused resources so you can take action to reduce waste.
- **Manage invoices and payments** gives you visibility to your cloud investment.



Azure Cost Management overview (video)

How to start deploying an optimized Azure environment?

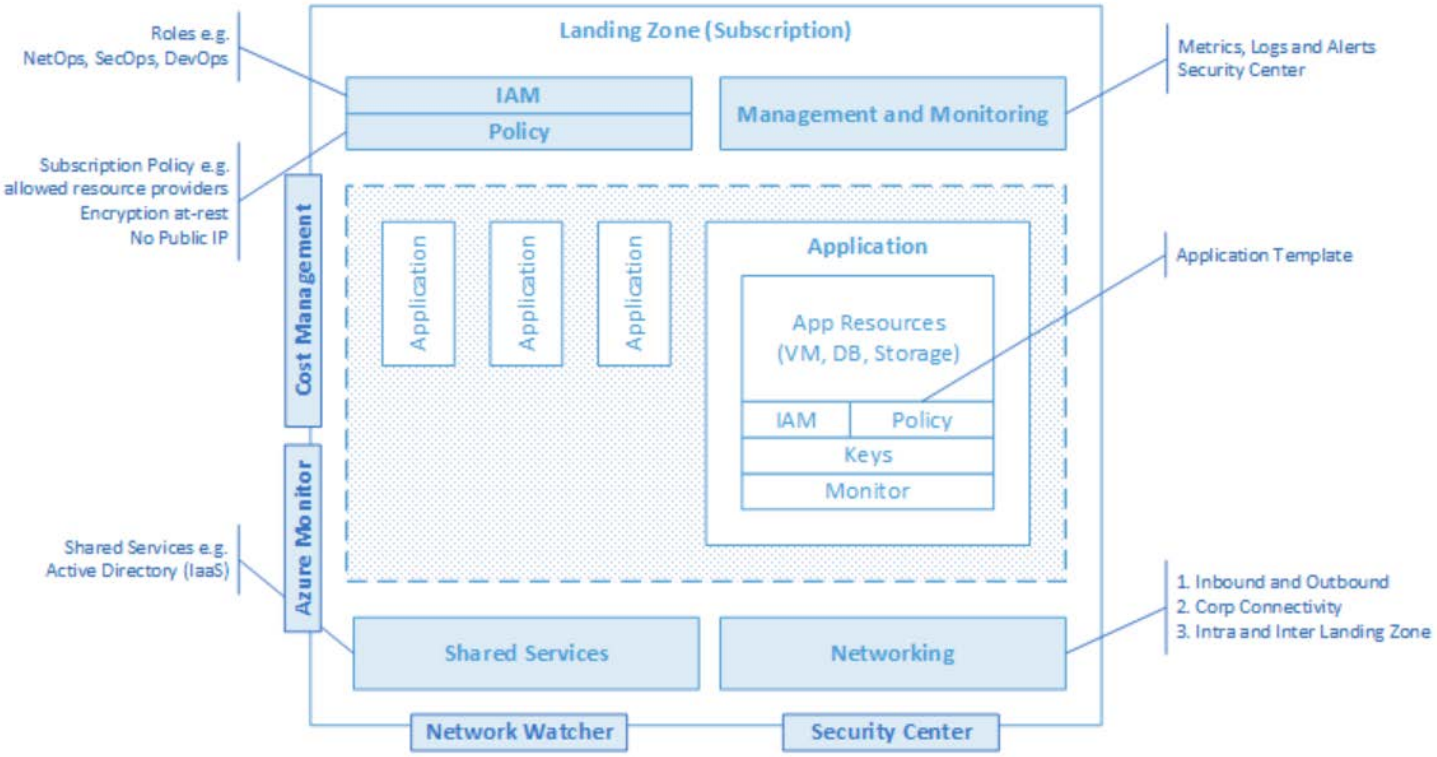
First Landing Zone

Metropolis

*Using an analogy, this is similar to how city utilities such as **water**, **gas**, and **electricity** are accessible before new houses are constructed. In this context, the network, IAM, policies, management, and monitoring are shared '**utility**' services that **must be readily available** to help streamline the application migration process.*

Landing Zones

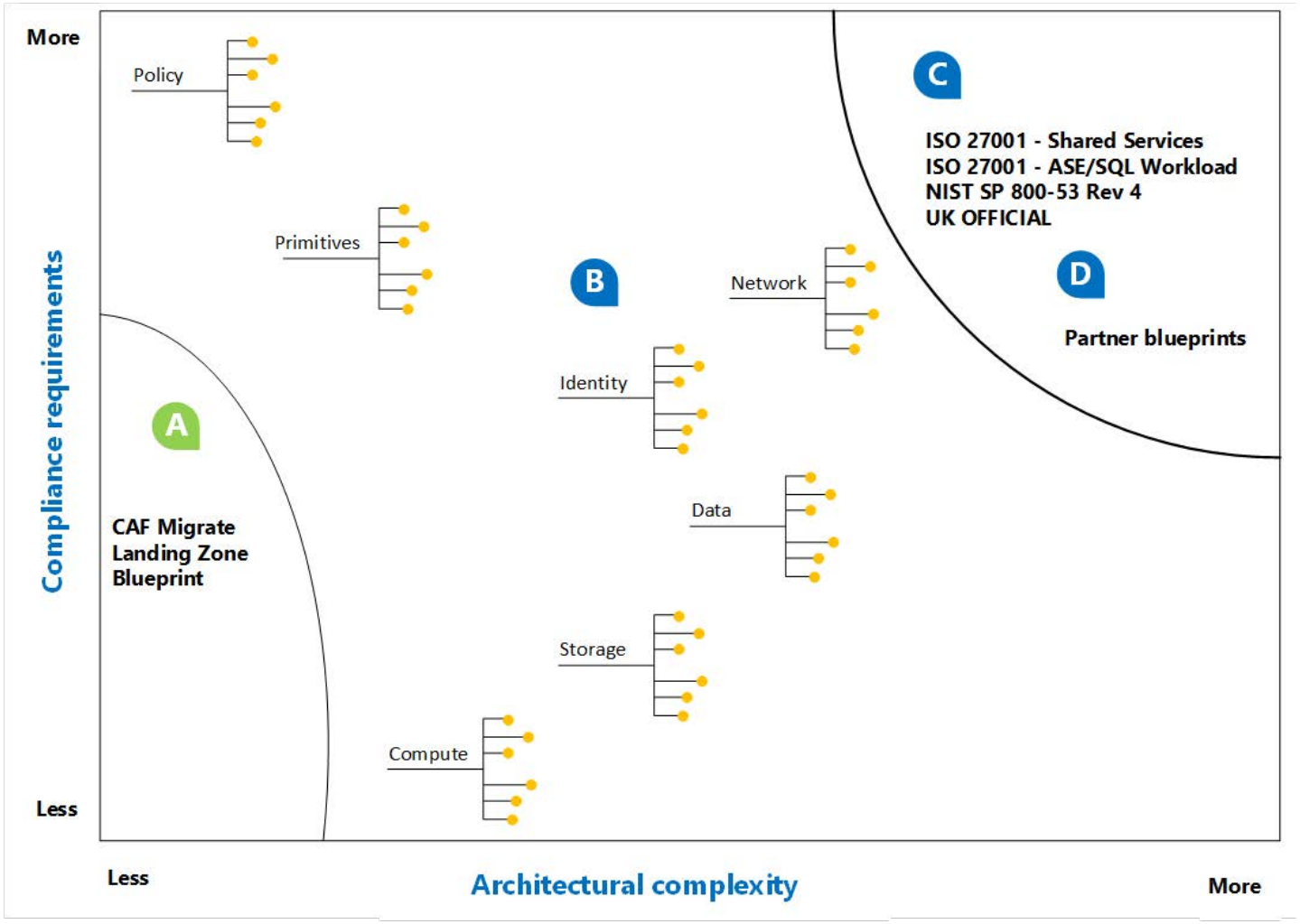
The principle purpose of the "Landing Zone" is to ensure that when a workload lands on Azure, the required "**plumbing**" is already in place, providing greater agility and compliance with enterprise security and governance requirements.



First landing zone

- A landing zone is a pre-provisioned environment for hosting your workloads. It uses a defined set of cloud services and best practices to add foundational capabilities that set you up for success.

- If you're unsure where to begin, the Cloud Adoption Framework migration landing zone blueprint creates a landing zone which can be updated to meet your specific needs.



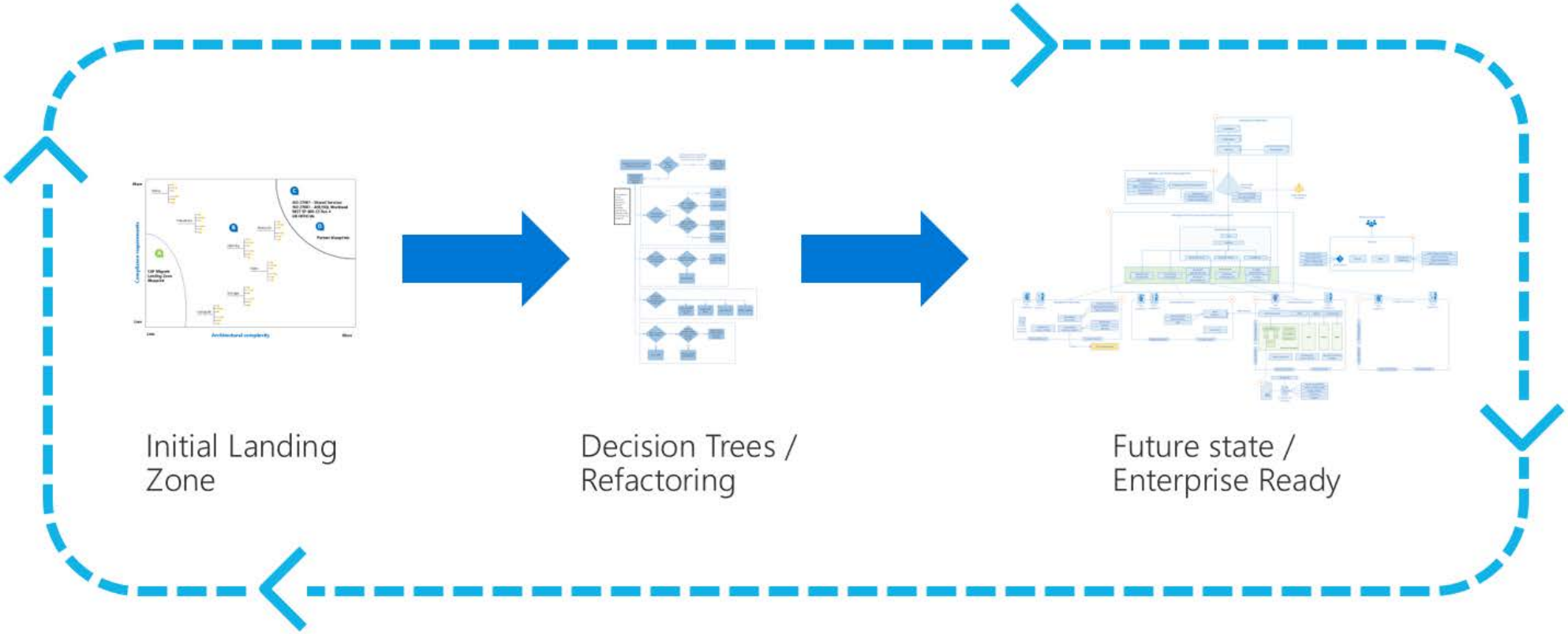
Key Challenges

Architecture Complexity: Customers lack the required level of understanding and experience on Azure. The mismatch between on-premises infrastructure and cloud-design considerations creates dissonance and friction with respect to defining architectures and standards for their migration to the cloud. They are struggling with the translation of their requirements to Azure concepts, capabilities, constructs and security model.

Operating Compatibility: Existing approaches and functions for the traditional delivery and management of IT services are not compatible with the Azure platform and cloud operating models. When combined with a lack of skills and experience, customers are struggling to define and therefore transform their operating model to manage and support large-scale cloud infrastructure.

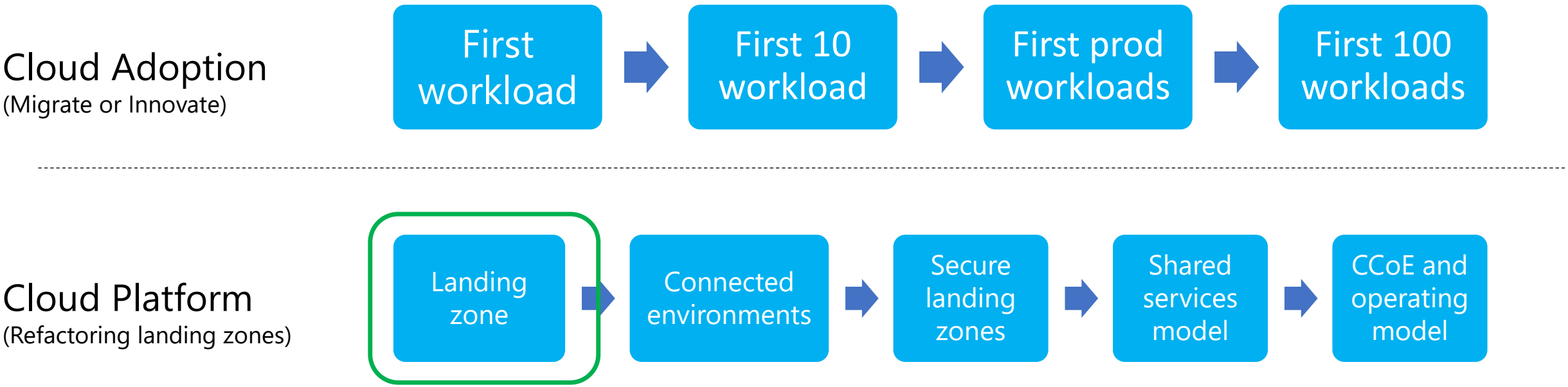
Lack of Trust and Desire for Control: The absence of a precise and detailed cloud architecture that is compliant with their requirements, and the lack of a well-defined operating model to support such a platform, leads IT not to trust Azure and instead strive to maintain full control. This often involves building ‘walls’ and complicated processes which ultimately get in the way of business lines adopting Azure.

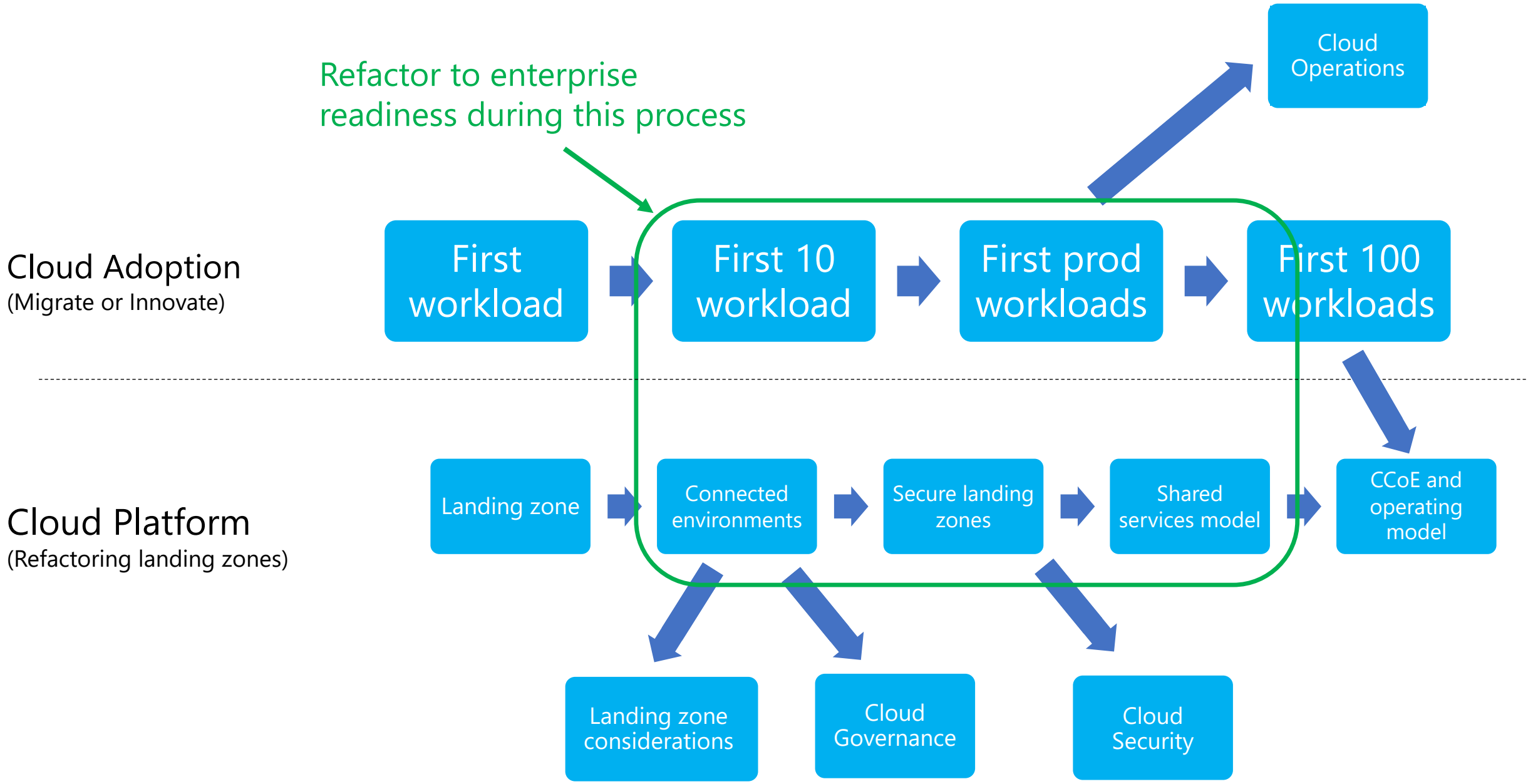
Refactoring landing zones



Since landing zone infrastructure is defined in code, it can be refactored similar to any other codebase. Refactoring is the process of modifying or restructuring source code to optimize the output of that code without changing its purpose or core function.

Development approach




Refactor to enterprise readiness during this process
Cloud Operations
Cloud Adoption
(Migrate or Innovate)
First workload
First 10 workload
First prod workloads
First 100 workloads
Cloud Platform
(Refactoring landing zones)
Landing zone
Connected environments
Secure landing zones
Shared services model
CCoE and operating model
Landing zone considerations
Cloud Governance
Cloud Security

Design areas of a well-architected landing zone

Enterprise Enrolment & Azure AD Tenants

Identity & Access Management

Management Group & Subscription Organization

Network Topology & Connectivity

Management & Monitoring

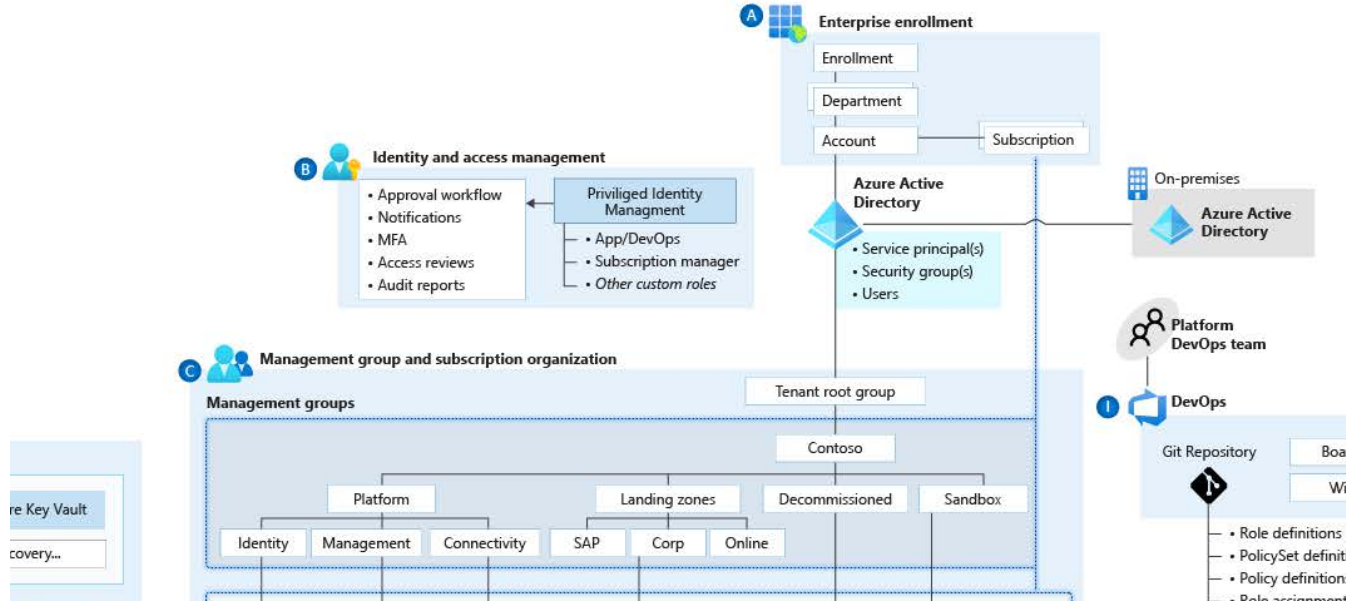
Business Continuity & Disaster Recovery

Security, Governance & Compliance

Platform Automation & DevOps

Identity & Access Management

Planning for Authentication Inside the Landing Zone



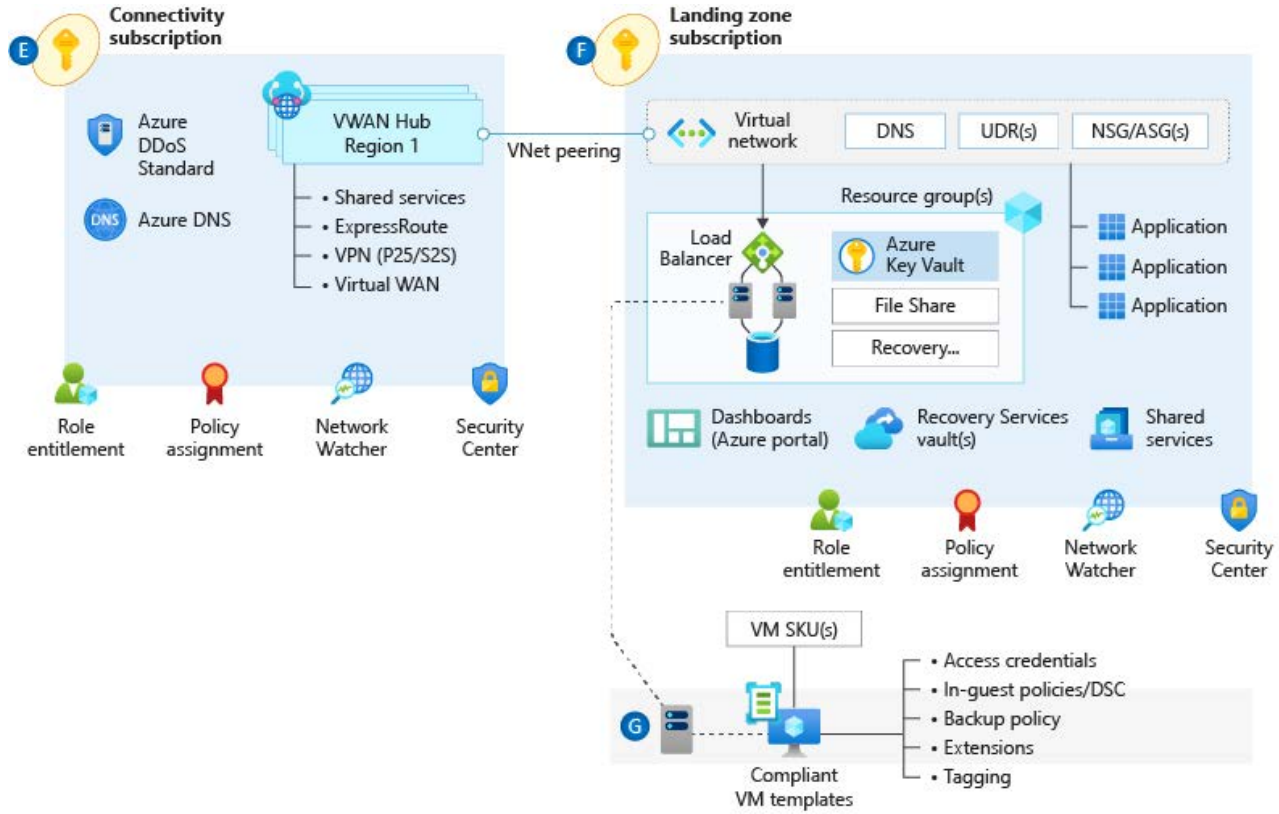
A critical design decision enterprise organization must make when adopting Azure is whether to:

- ❑ **extend** an existing on-premises identity domain into Azure

or

- ❑ **create** a brand new one

Network Topology & Connectivity

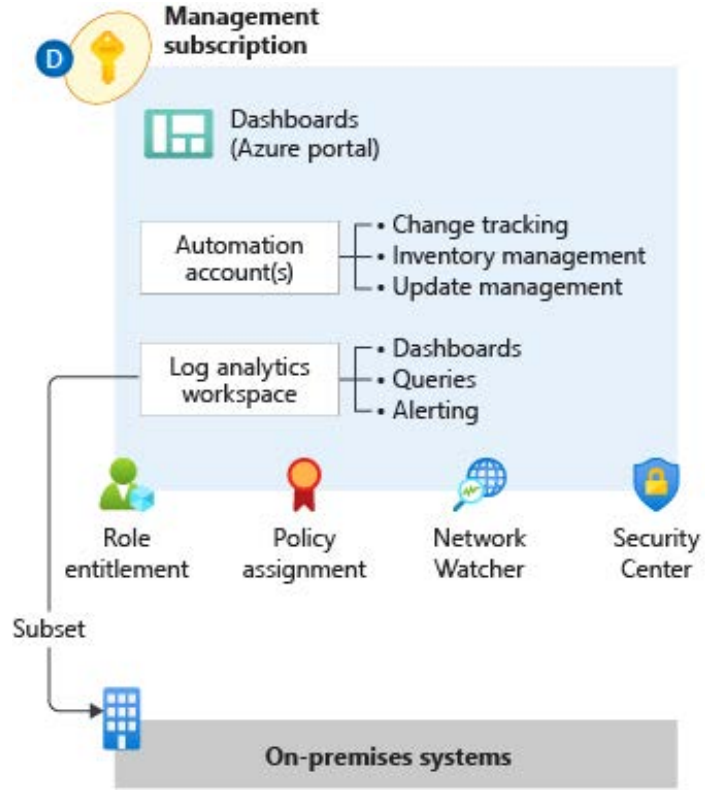


Consider the following design elements:

- ❑ Planning for IP Addressing
- ❑ Configure DNS
- ❑ Define an Azure Networking Topology
- ❑ Azure VWAN (Microsoft Managed)
- ❑ Traditional Azure networking (Customer Managed)
- ❑ Walkthrough – Enterprise-scale network topology (VWAN-based)
- ❑ Connectivity to Azure

Management & Monitoring

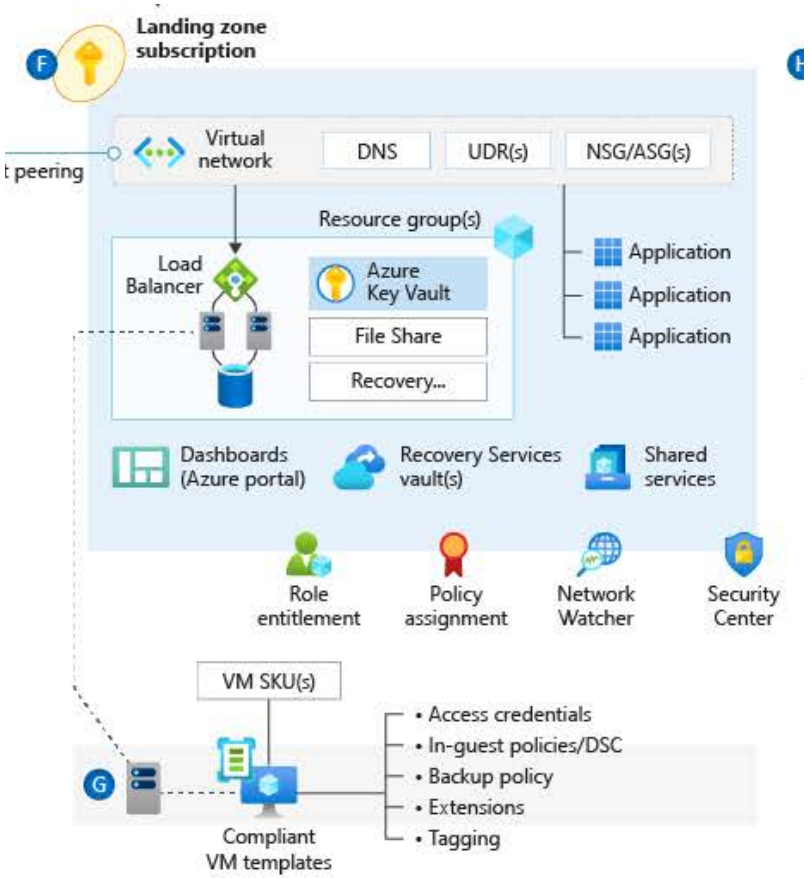
Planning for Platform & Application Management and Monitoring



- **Log Analytics workspace** is an administrative boundary Security audit logging and achieving a horizontal security lens across the entire customer Azure estate
- **Azure data retention thresholds** and requirements for archiving

Business Continuity & Disaster Recovery

Planning for BCDR

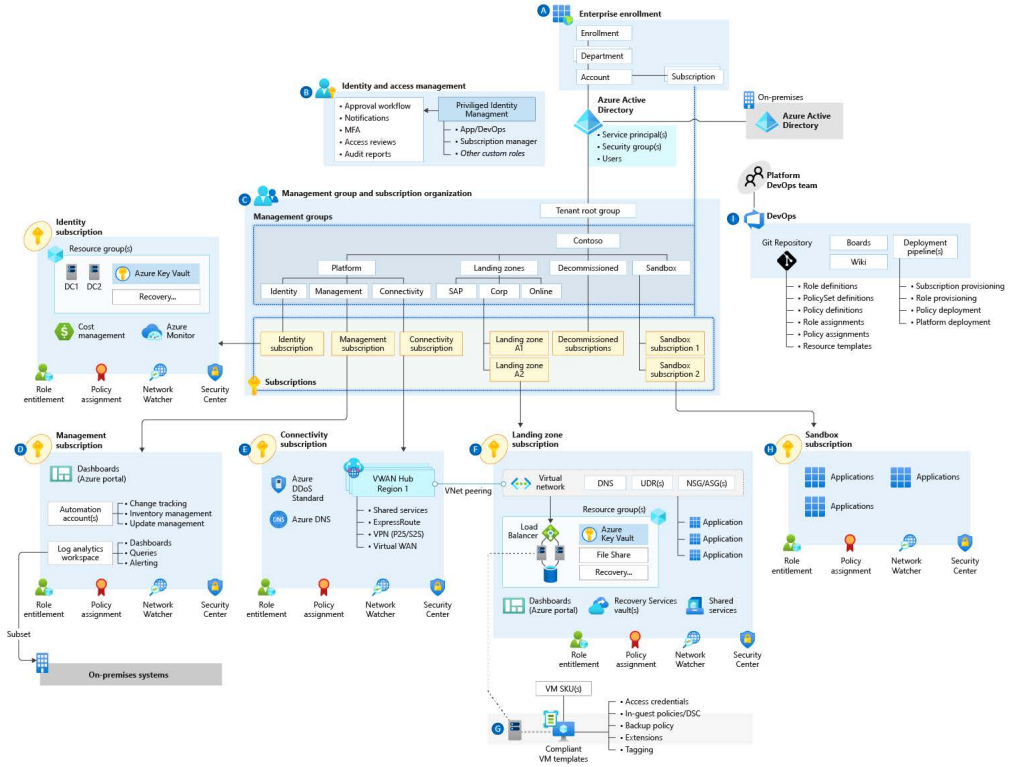


Application and data availability requirements:

- ❑ **BCDR for PaaS** services and the availability of native DR and HA features
- ❑ Support for **multi-region deployments** for failover purposes
- ❑ Application operations with **reduced functionality or degraded performance** in the presence of an outage

Security, Governance & Compliance

Define Encryption & Key Management



Subscription and scale limits as they apply to Key Vault

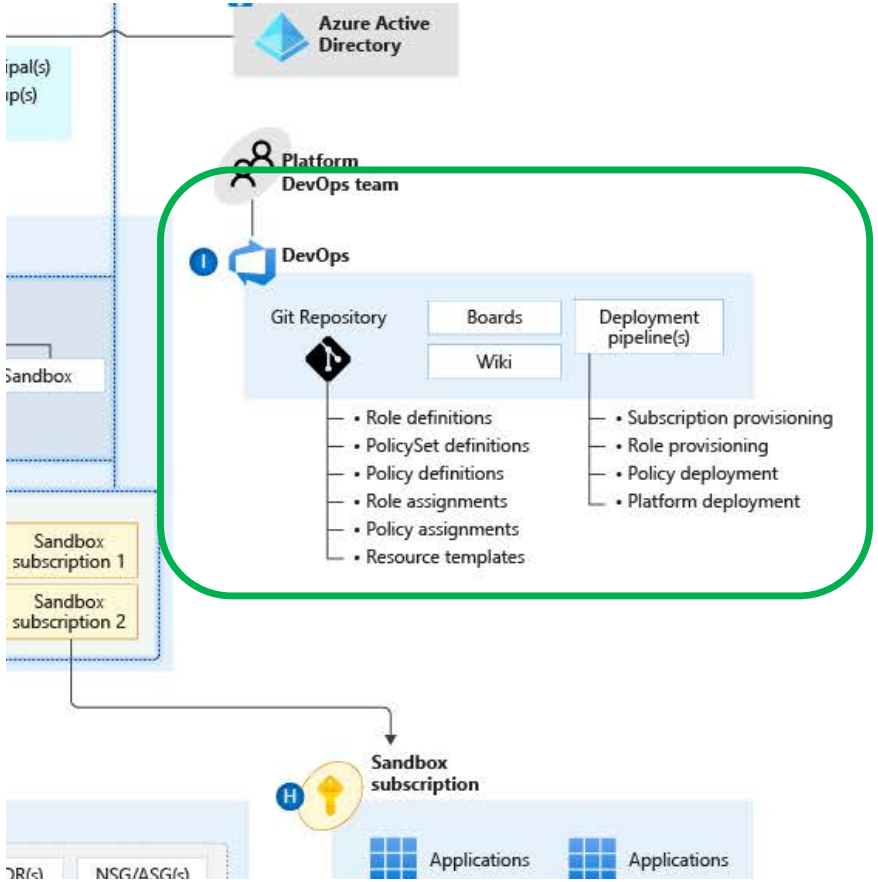
- ❑ Key Vault serves a security boundary since access permissions for keys, secrets and certificates are at the vault level
- ❑ Premium SKU can be leveraged where HSM protected keys are required

Key rotation and secret expiration

- ❑ Use a federated Key Vault model to avoid transaction scale limits
- ❑ Establish an automated process for key and certificate rotation

Platform Automation & DevOps

Planning for a DevOps Approach



- ❑ Where central teams are concerned, CI/CD pipelines should be used to manage policy definitions, role-definitions, policy assignments, and template galleries

The blanket application of a DevOps model will not miraculously establish capable DevOps teams.

- ❑ Establish a cross functional **DevOps Platform Team** to build, manage and maintain your Enterprise Scale architecture.

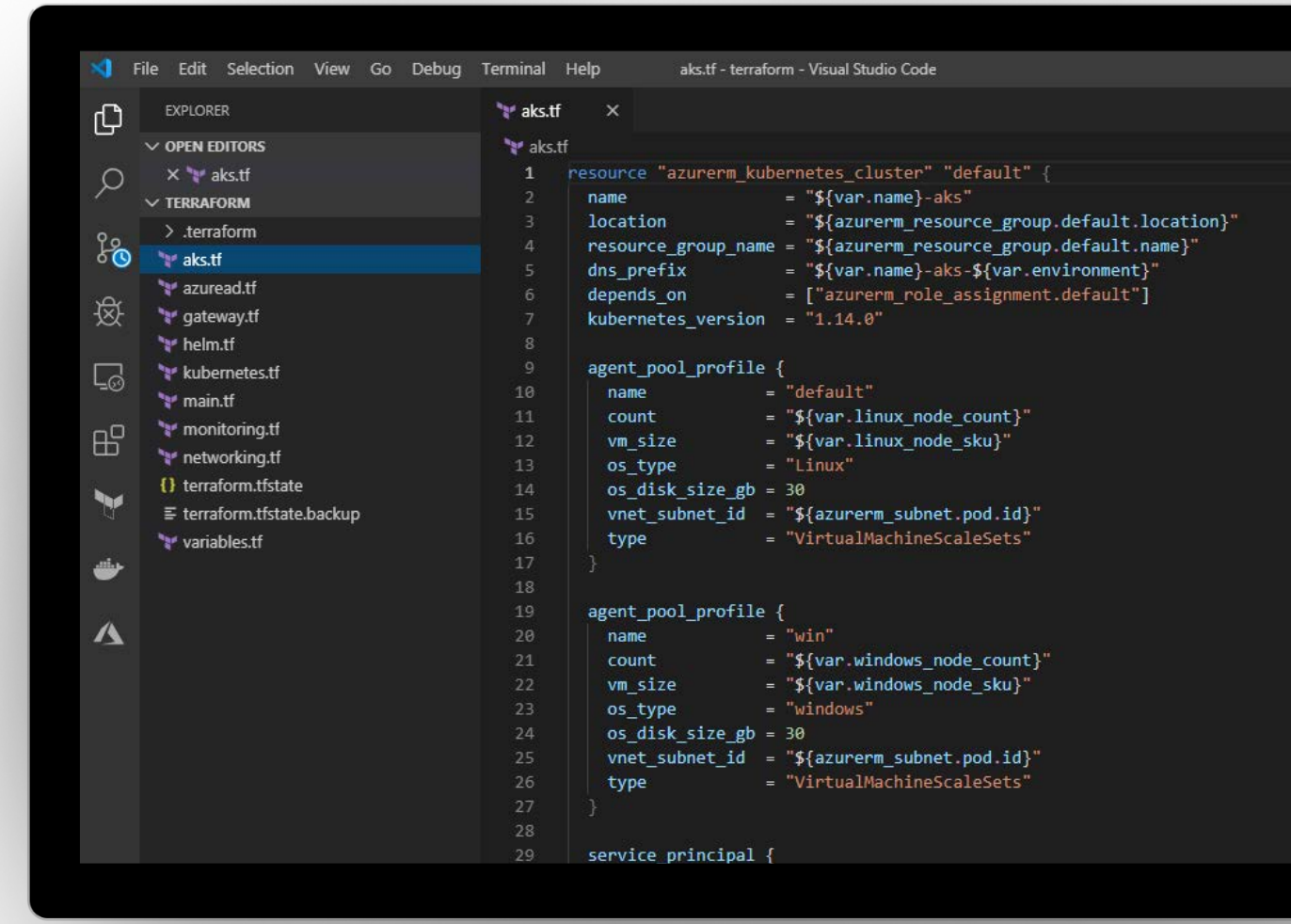
Infrastructure as code

Stand up environments in the fastest means possible.

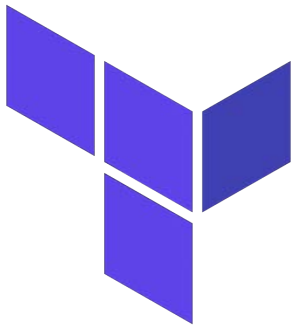
Remove the human element and reliably and repeatable deploy every time.

Improve environment visibility and improve developer efficiency

Store your infrastructure definitions alongside your application code.



Landing zone options

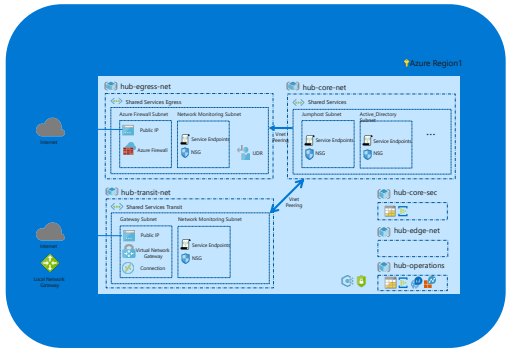


Terraform Landing Zone

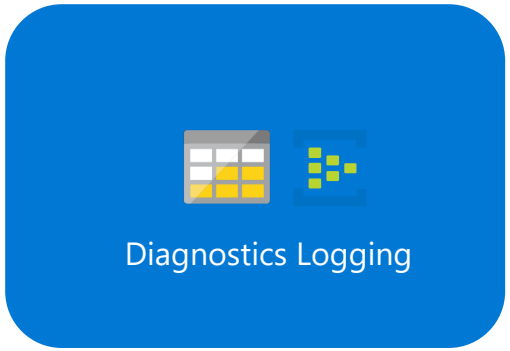
ARM Templates / Blueprints

Azure Terraform Landing Zone

Components of the solution

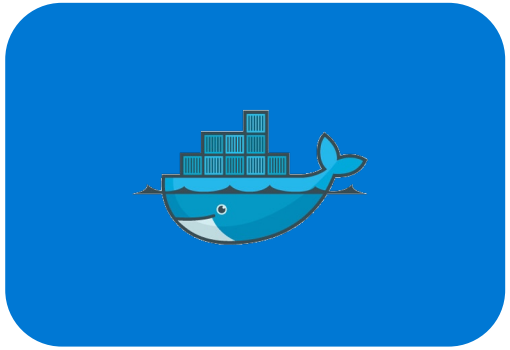


Set of Terraform landing zones



Set of Terraform modules

Terraform CAF provider

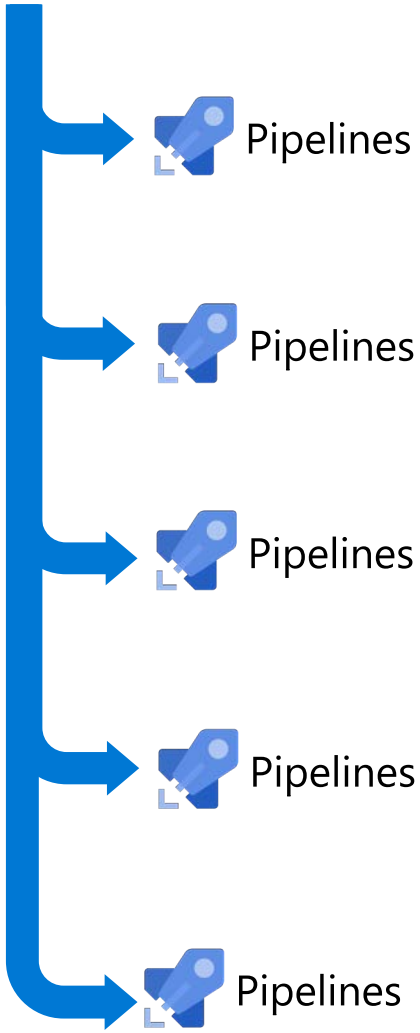


Deployment rover and open source state management

https://aka.ms/tf-landingzones

Inner-source and innovation in the enterprise

Composition from proven components



Solutions and Applications

Applications that you own, you wrote, on IaaS, PaaS, any framework. Extended with Terraform providers ecosystem

AKS

SAP

Image gallery

Data and AI

Your solutions

Any COTS

Core enterprise-scale landing zones and infrastructure

Dynamic infrastructure, always tested, verified, compliant.

Hub and spoke

Hub and mesh

DMZ and other topologies, NVA

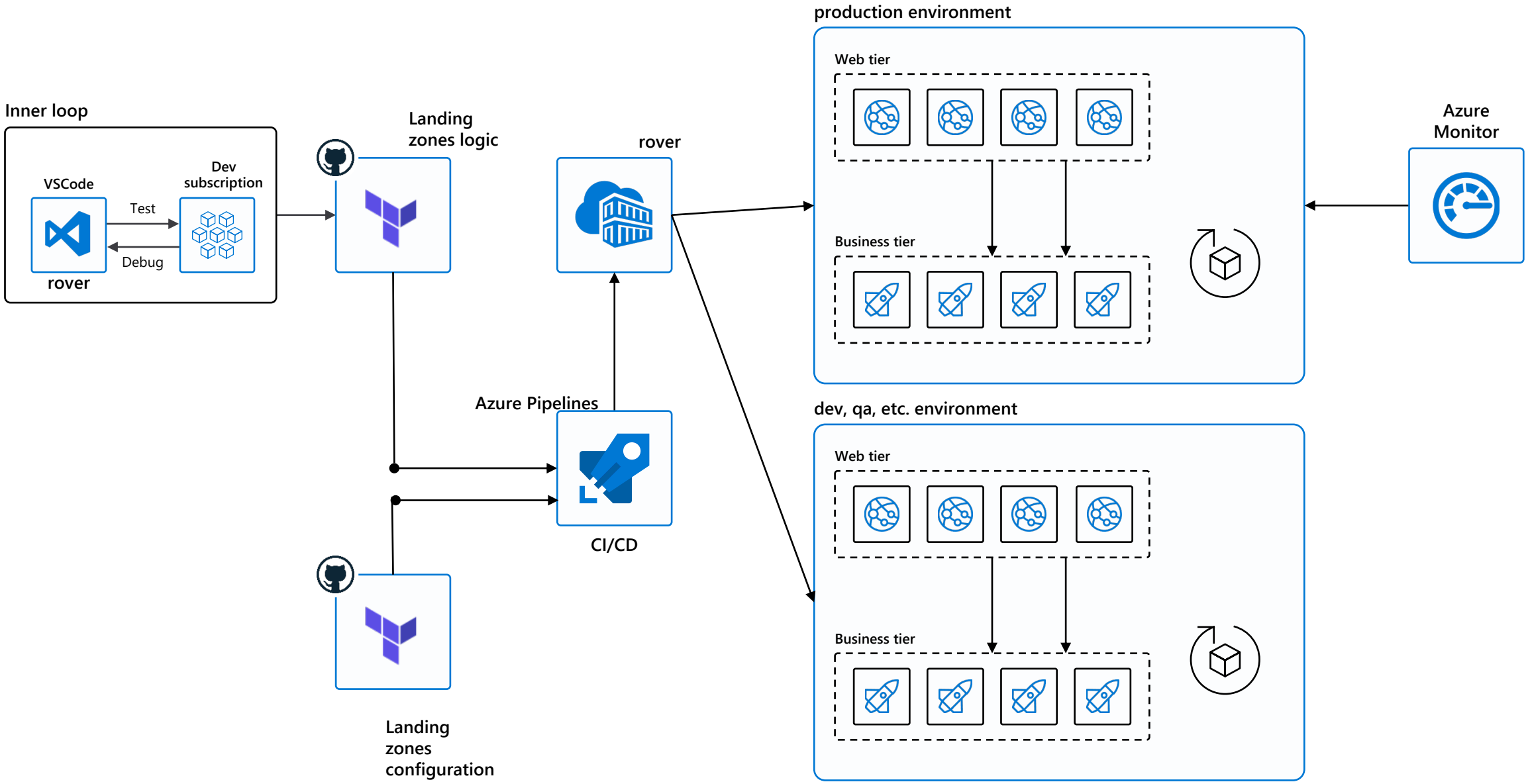
Multi-subscription management

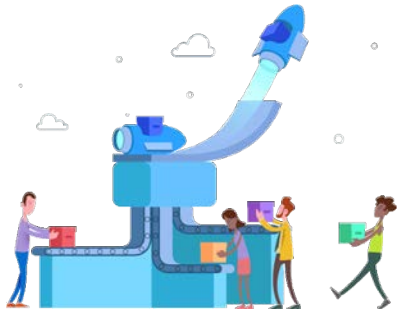
Compliance and governance

DevOps GitOps Fundamentals

Security controls and auditing

Operating IaC - CI/CD Pipeline

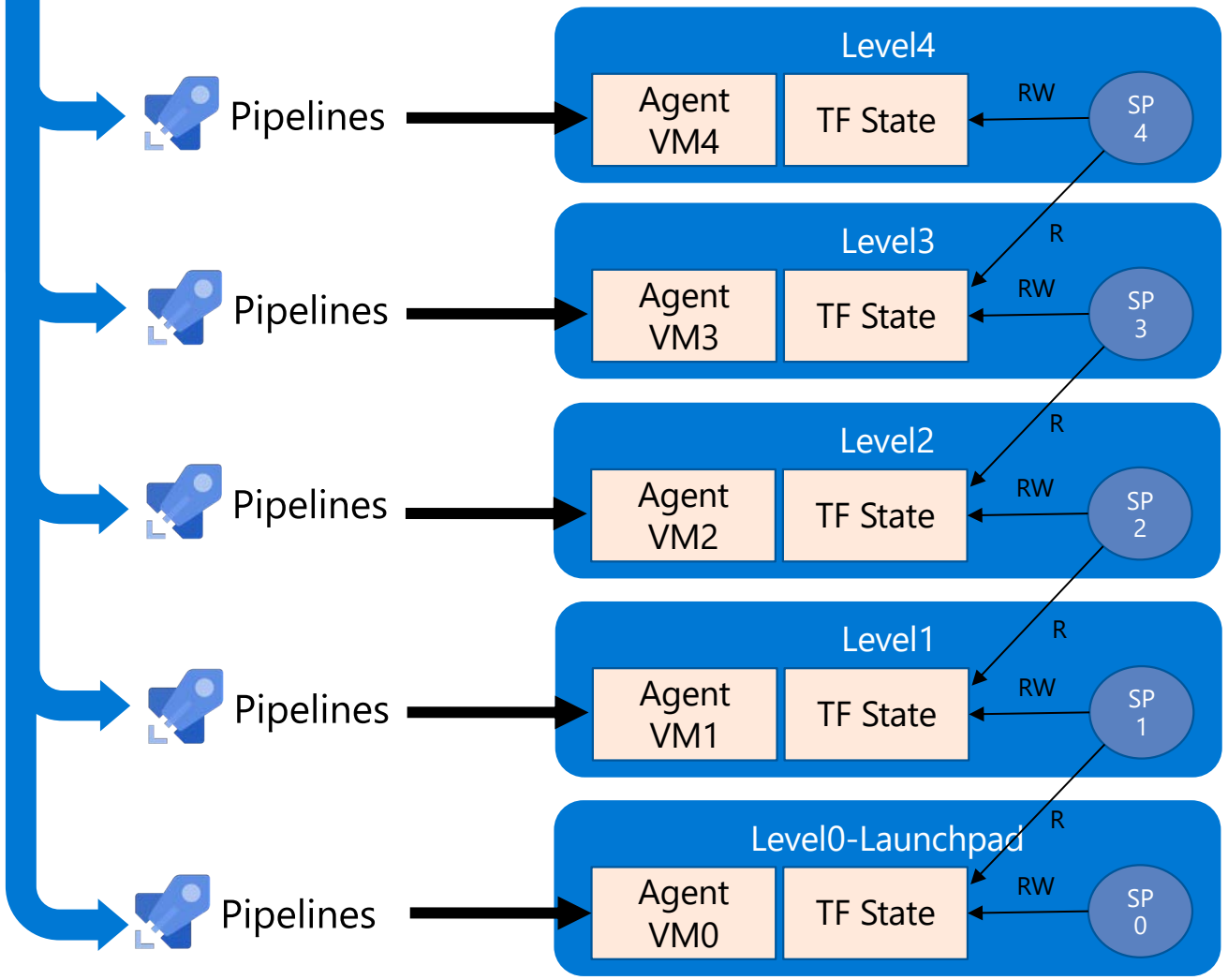




Azure Pipelines

Continuously build, test, and deploy to any platform and cloud

Landing zones structuring example



Manage the deployment of an **application itself / ML model** in the application's landing zone e.g (Springboot microservices, dotnet core…)

Manage the deployment of an **application's landing zone** in a spoke environment (e.g AKS Cluster + WAF)

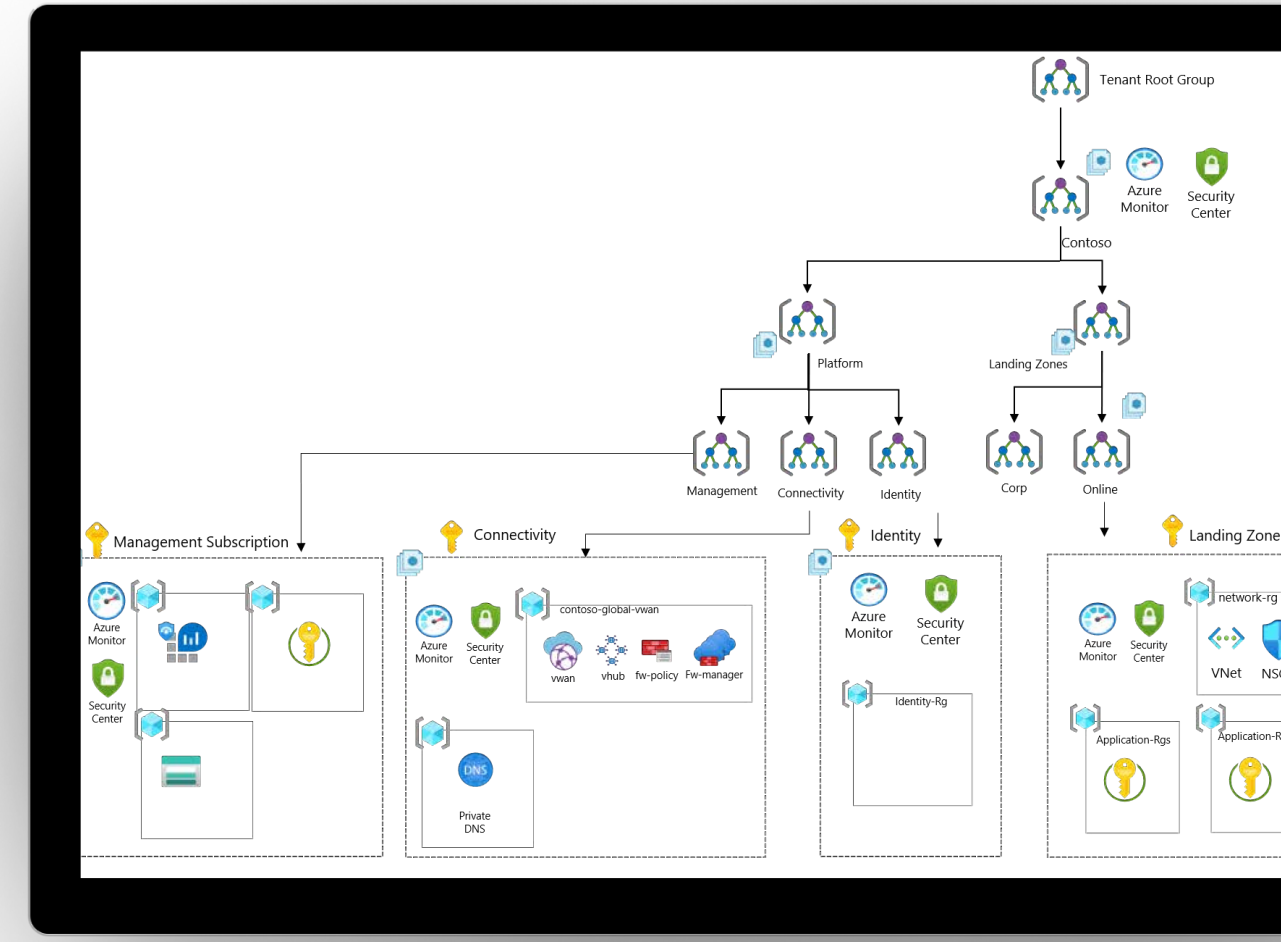
Manage the **hub and spokes** and **shared services** of each environments, as described in the design document (backup, DR, Azure monitor, patch management…)

Manage the **security and compliance** (RBAC, Policies, OMS monitoring, shared security services, including event hub collector for SIEM, preventive and reactive controls…)

Transition from manual to automation. Create the subscriptions (for level 0 to level 4) + terraform state repository, privileged access workstation, service principals

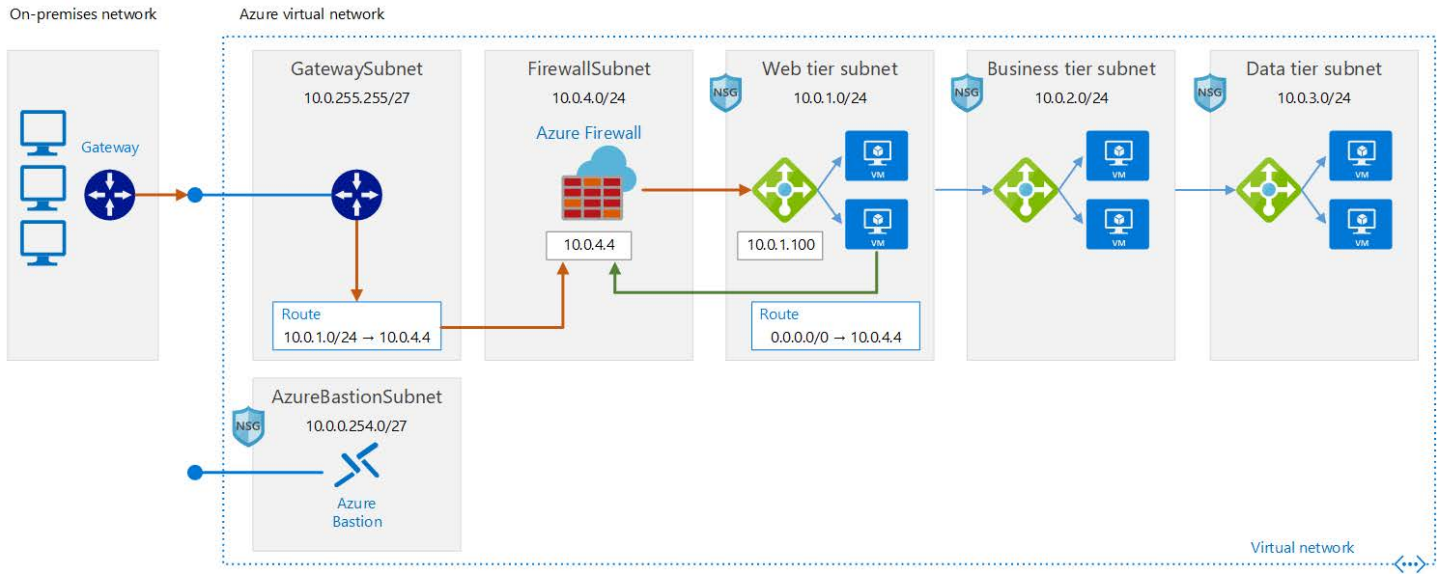
Azure Terraform landing zones - Summary

- Open Source and community driven
- Enterprise-scale approach for IaC
- Part of Cloud Adoption Framework
- Lower entry cost to Infrastructure as Code
- Best practices in a-box



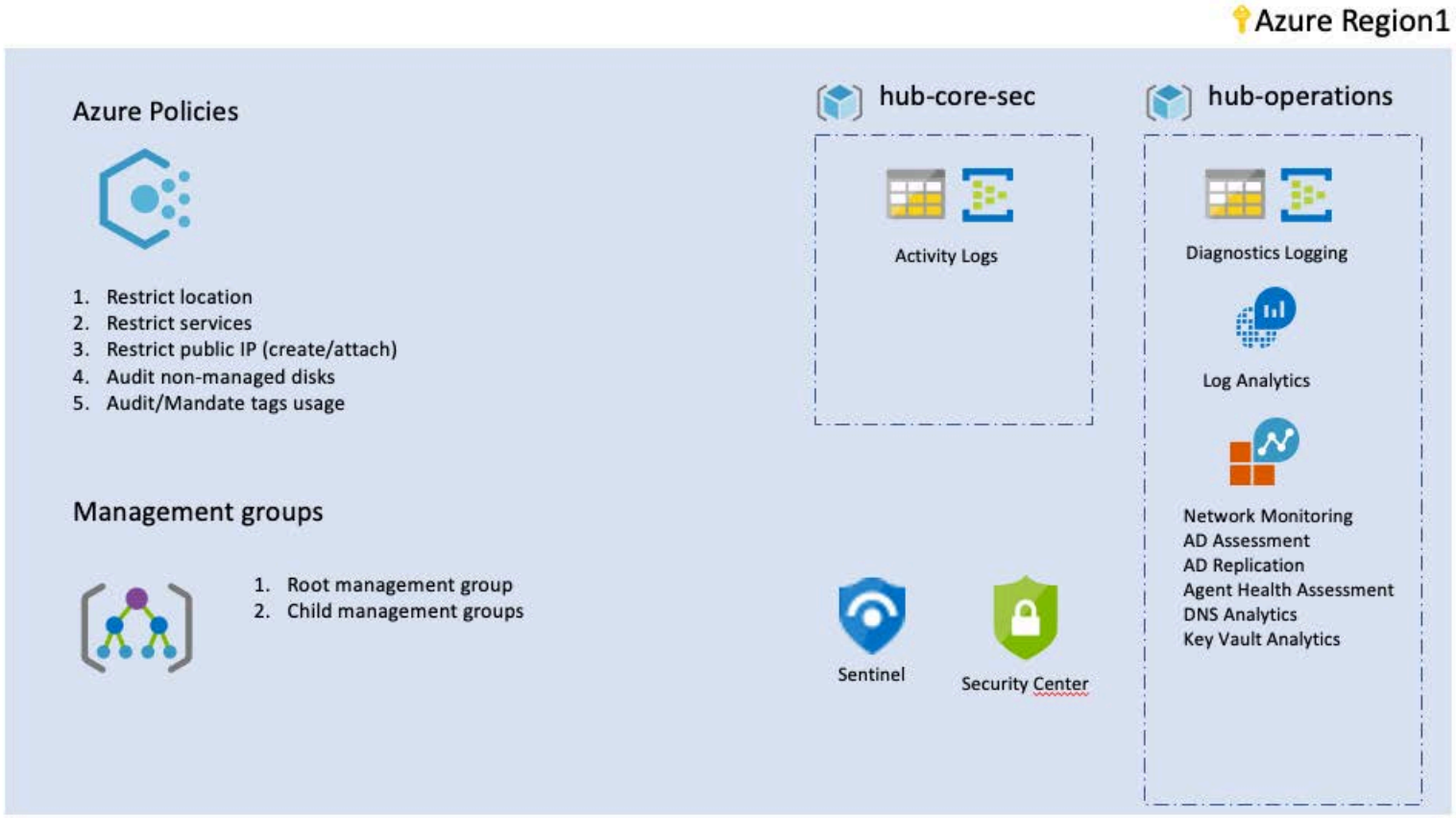
How to create your landing zone

Step 1. Start with the diagram



How to create your landing zone

Step 2. Identify non functional requirements



How to create your landing zone

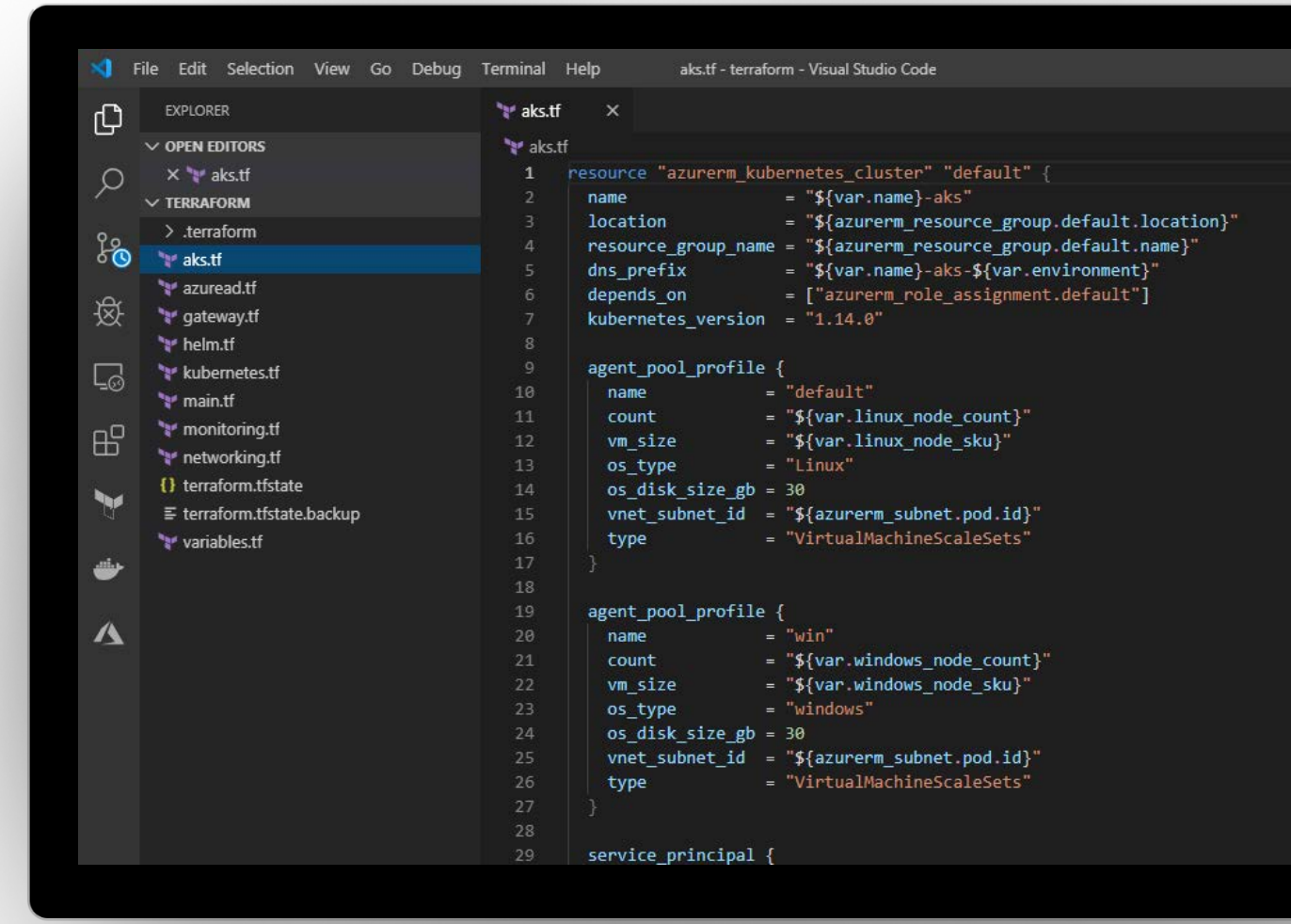
- **Step 3. Do the parts inventory**

·public ip
·site-to-site gateway
·route objects
·azure firewall
·virtual network
·nsg
·subnets
·internal load balancer
·VM
·resource groups
·Azure Bastion (as a replacement of the management subnet, maybe)

How to create your landing zone

- **Step 4. Write your prototype and test**

- **Step 5. Refactor / Structure your code and variables**

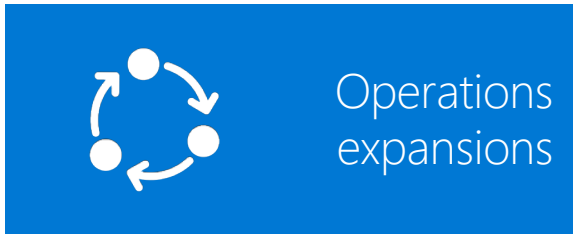


Expand Lading Zone

Expand the landing zone

Expanding your landing zone provides a code-first approach to embedding the following principles into the landing zone and more broadly into your overall cloud environment.

Refactor landing zone to refine **foundational** elements

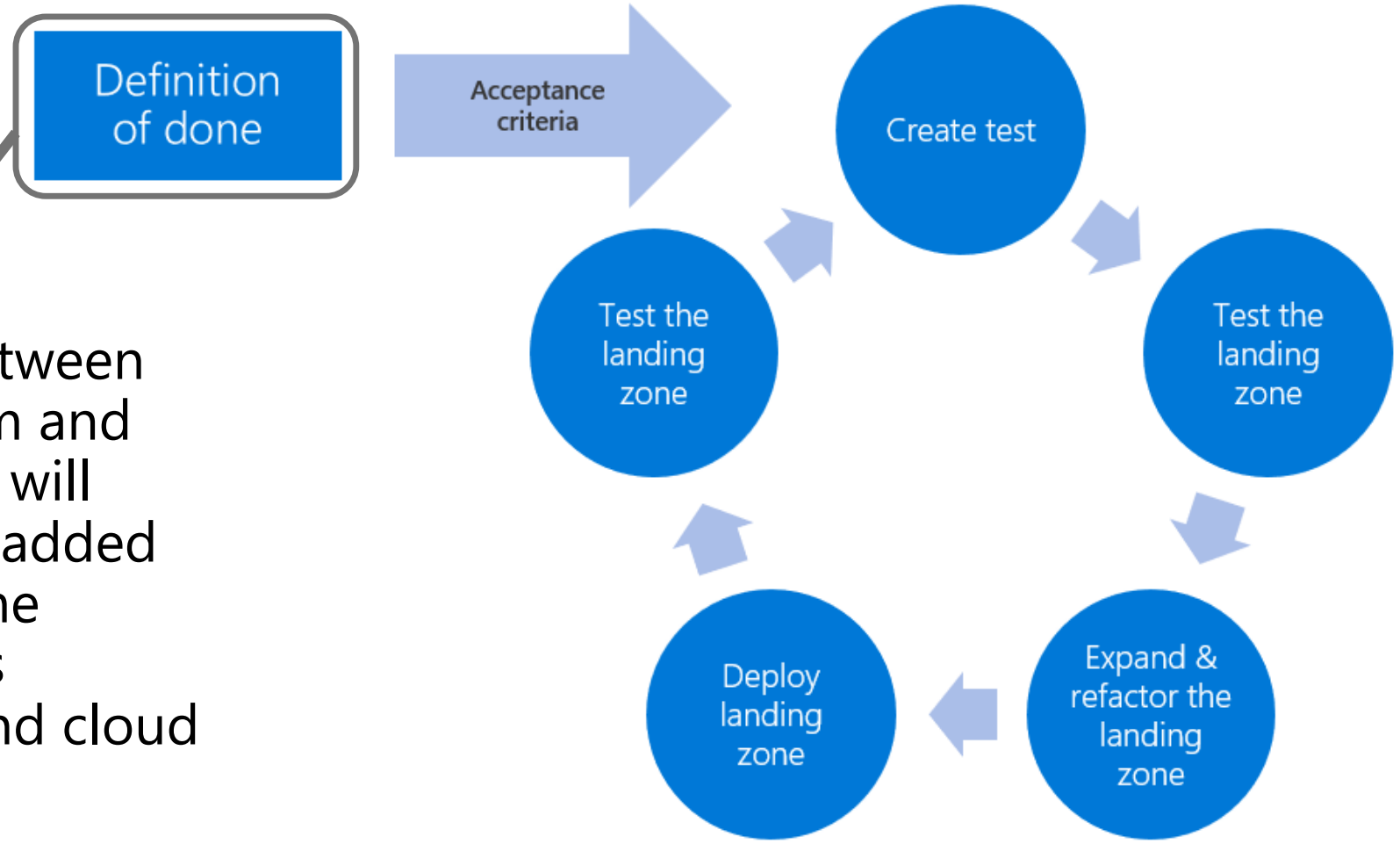


Add configurations to improve **performance, reliability and ops excellence** of your workloads

Add configurations to improve **cost, reliability and security** of your workloads

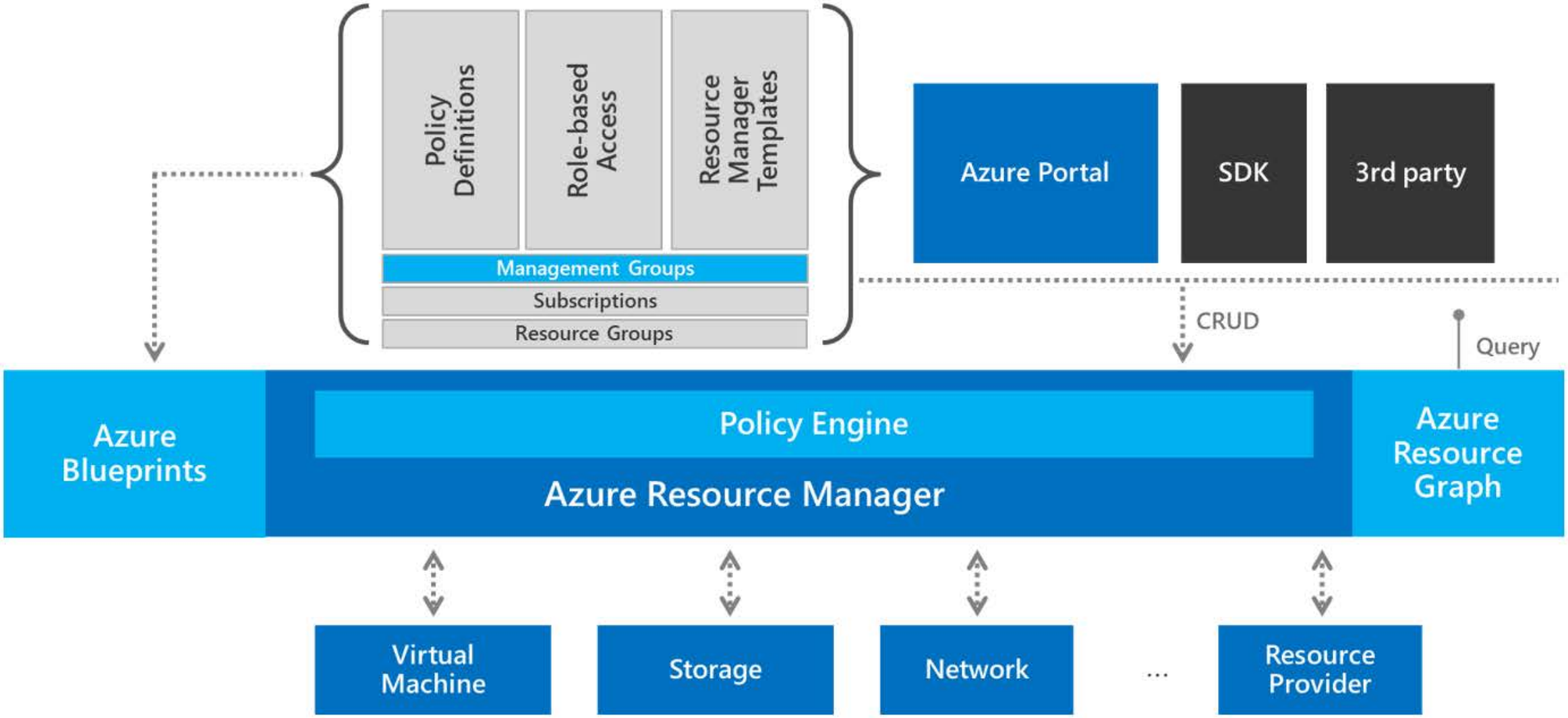
Add configurations to improve security of **sensitive data and critical systems** in your workloads

Test-driven development (TDD)



A simple agreement between the cloud platform team and other affected teams. It will outline expected value-added features and will become increasingly complex as additional workloads and cloud features are adopted.

Azure tools to support landing zone TDD cycles



Starting with enterprise scale

The enterprise-scale architecture is modular by design and allow 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.

Enterprise-Scale?

Enterprise-scale is an **architecture approach and reference implementation** that enables effective **construction** and **operationalization** of landing zones on Azure, at scale and **aligned** with **Azure Roadmap** and **Cloud Adoption Framework**.

Authoritative
Provides holistic design decision framework for Azure Platform.

Proven
Based on success of large-scale migration projects at-scale.

Prescriptive
Apply this on "Monday Morning" in customer environment.

Enterprise-scale Architecture:
• **Enterprise-scale design principles**: Principles to help/guide you customize the design. • **Enterprise-scale design guidelines**: Guidelines (decisions and recommendations) for the 8 components of the enterprise-scale architecture • **Enterprise-scale Implementation guide**: The way you create those things using reference implementation in GitHub and the deployment pipeline

Enterprise-scale reference Implementation:
• **Enterprise-scale foundation:** A reference implementation of shared services containing network, security, identity, governance services required to construct and operationalize an enterprise-scale landing zone • **Enterprise-scale landing zone(s):** A reference implementation of a workload environment conforming to the enterprise-scale architecture (opinionated way to implement, code)

Enterprise-scale Design Principles

- Enable Autonomy for Innovation and Transformation
- Security and Compliance By-Default
- Governance At-Scale with Sustainable Cloud Engineering

Subscription Democratisation

Policy Driven Governance

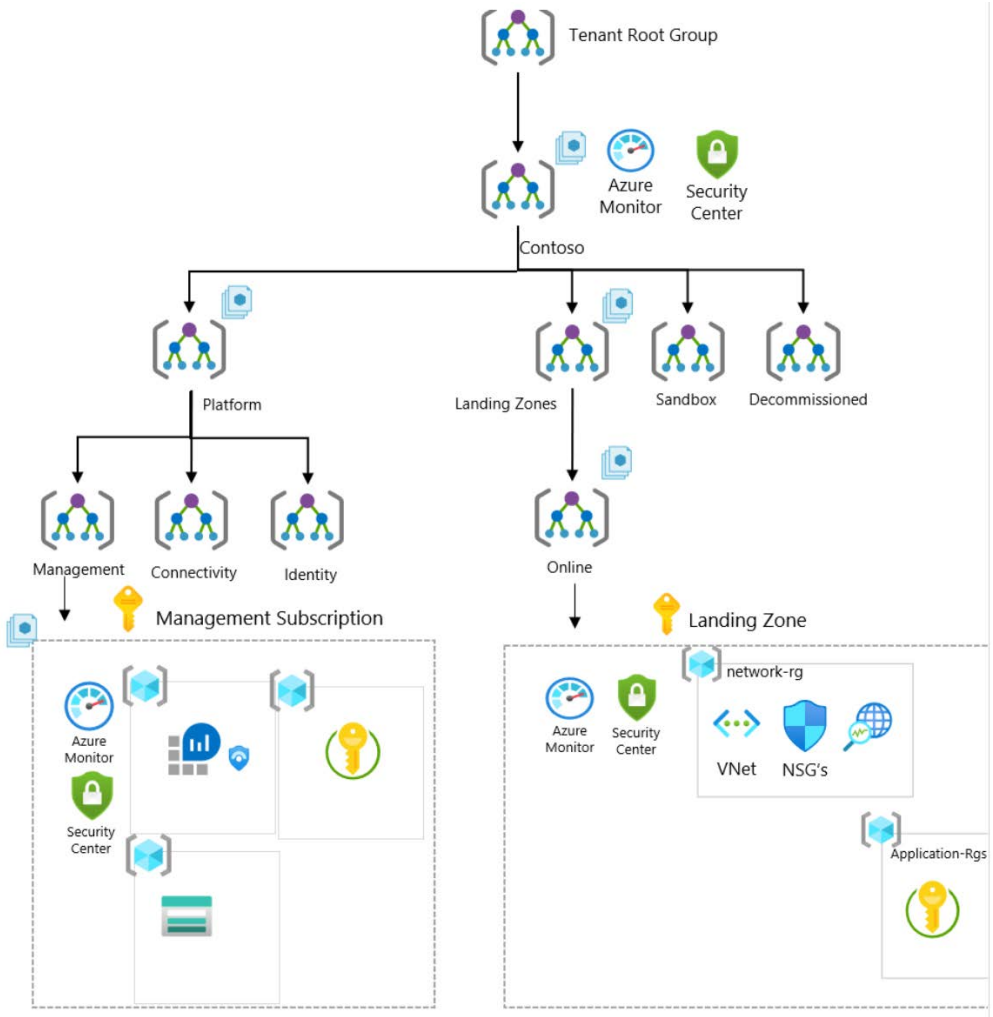
Single Control and Management Plane

Application Centric and Archetype-Neutral

Azure Native Design and Platform Roadmap Alignment

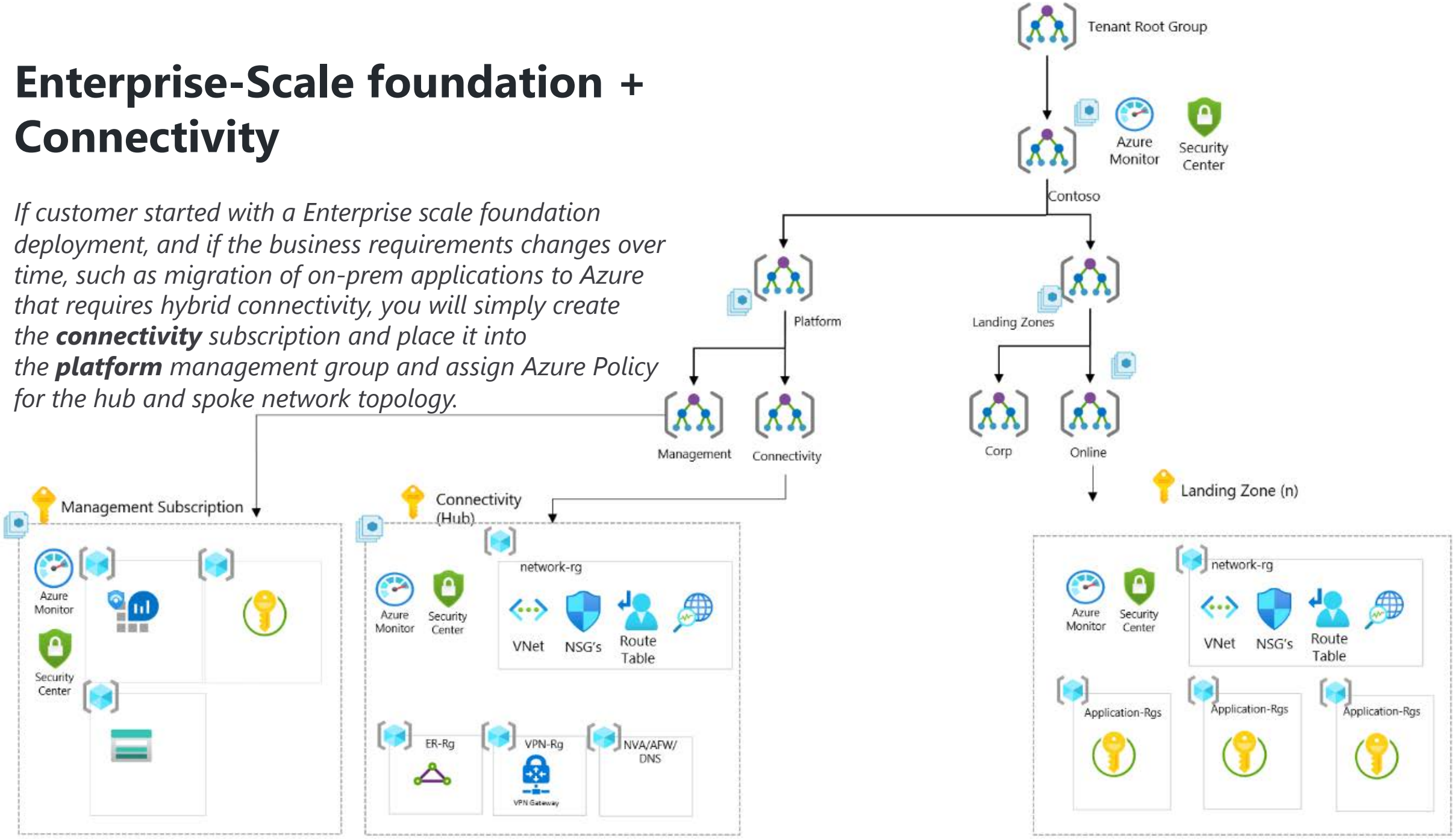
Enterprise-Scale foundation

If the business requirements changes over time, such as migration of on-prem applications to Azure that requires hybrid connectivity, the architecture allows you to expand and implement networking without any refactoring of the architecture nor implications to the runtime state of existing applications. You will simply create the connectivity subscription and place it into the platform management group and assign Azure Policy for the networking topology you desire.



Enterprise-Scale foundation + Connectivity

*If customer started with a Enterprise scale foundation deployment, and if the business requirements changes over time, such as migration of on-prem applications to Azure that requires hybrid connectivity, you will simply create the **connectivity** subscription and place it into the **platform** management group and assign Azure Policy for the hub and spoke network topology.*



Qualifiers: Should I start with enterprise scale?

- Scale and speed
- Security, compliance, and culture
- All-in on the cloud
- Skill requirements

Example implementation

The following table lists example modular implementations.

Example deployment	Description	GitHub repo	Deploy to Azure
Enterprise-scale foundation	This is the suggested foundation for enterprise-scale adoption.	Example in GitHub	Deploy example to Azure
Enterprise-scale Virtual WAN	Add a Virtual WAN network module to the enterprise-scale foundation.	Example in GitHub	Deploy example to Azure
Enterprise-scale hub and spoke	Add a hub-and-spoke network module to the enterprise-scale foundation.	Example in GitHub	Deploy example to Azure

3400 XP

Create an enterprise-scale architecture in Azure

2 hr 46 min • Learning Path • 4 Modules

Beginner | Solutions Architect | Azure

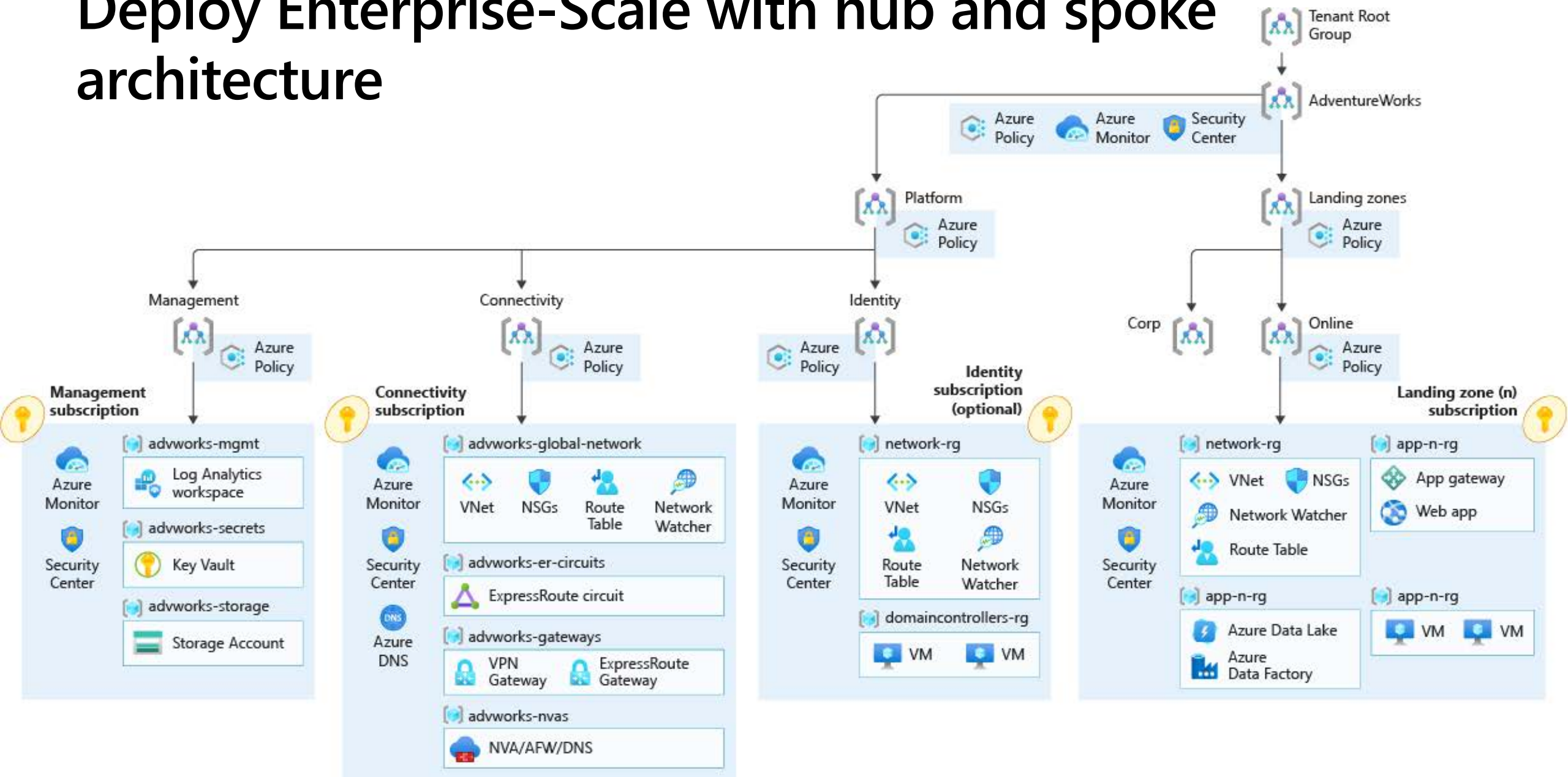
Learn how Microsoft Cloud Adoption Framework for Azure enterprise-scale landing zones can help your organization to accelerate cloud adoption from months to weeks. We will explore how to create Azure landing zone architecture at enterprise-scale. Learn about landing zone critical design areas to build and operationalize your Azure environment.

Prerequisites

None

Start > Bookmark Add to collection

Deploy Enterprise-Scale with hub and spoke architecture



Project Journey

Homework

Homework

Topic		Link
Create an enterprise scale architecture		https://docs.microsoft.com/en-us/learn/paths/enterprise-scale-architecture/
Enterprise scale bootstrap		https://github.com/Azure/Enterprise-Scale
Terraform landing zone : Deploy a level100 landing zone		https://github.com/Azure/caf-terraform-landingzones/
Terraform Landing zone: Introduction to Terraform Landing Zone		https://www.youtube.com/watch?v=w0W90bqZaWA Cloud Adoption Framework: Introduction landing zones for Terraform
Azure Security Best practices		https://info.microsoft.com/AP-HCSAzureHybridInfra-WBNR-FY21-09Sep-14-AzureSecurityLiveEvent-SRDEM37260_LP01Registration-ForminBody.html
Azure Design and Architecture Best Practices		https://info.microsoft.com/AP-HCSAzureHybridInfra-WBNR-FY21-09Sep-29-AzureDesignandArchitectureBestPractices-SRDEM37046_LP02OnDemandRegistration-ForminBody.html

Q&A

Contact us – projectjourney@microsoft.com

Your feedback is important

Nick Westbrook

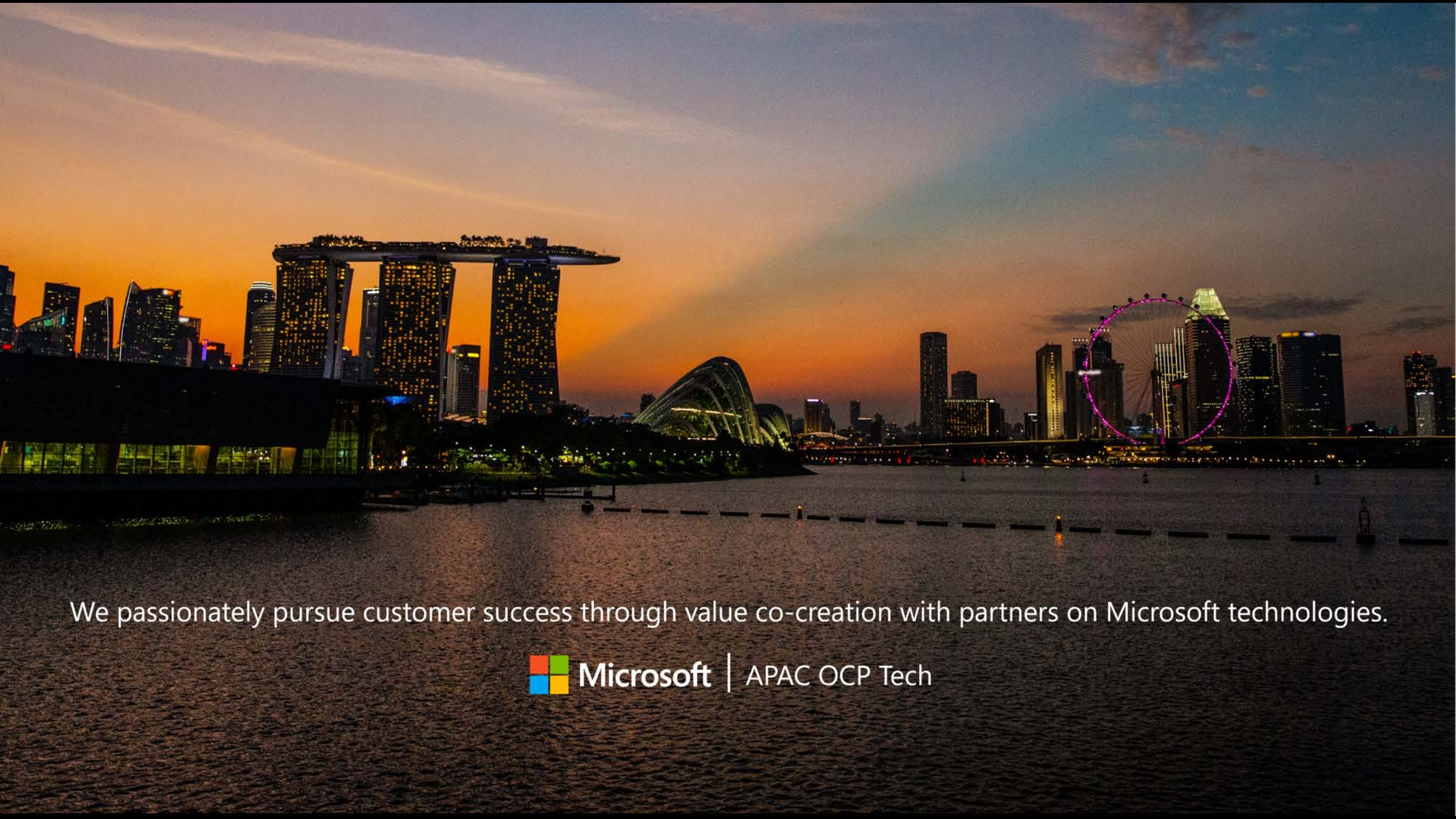
Jenzus Hsu

Nicolas Yuen

Inseob Kim

Tell us what you think

https://aka.ms/JourneySurvey3


We passionately pursue customer success through value co-creation with partners on Microsoft technologies.
Microsoft | APAC OCP Tech