**Build Azure Landing Zone**

**using ARM Template**

Start small and expand

06/11/2024

**­­Documents Control**

Prepared For:

**Internal Only**

Prepared By:

**Nitin Kansara**

@cobweb.com

Prepared For:

**Internal Only**

Prepared By:

**Nitin Kansara**

@cobweb.com

**Author**

|  |  |
| --- | --- |
| Author Name | Nitin Kansara |
| Email | Nitin.Kansara@cobweb.com |
| Telephone | +97144553135 |
| Web | [www.cobweb.com/ae](http://www.cobweb.com/ae) |
| Address | Cobweb Solutions Limited  Grosvenor Business Tower  Suite 1911  Barsha Heights  Dubai  P.O. Box 500449  United Arab Emirates |

**Document Validity**

|  |
| --- |
| Printed copy uncontrolled |

**Document History**

| **Version** | **Date** | **Revised By** | **Comments** |
| --- | --- | --- | --- |
| 1.0 | 06/11/2023 | Nitin Kansara | First Draft |
| 2.0 | 06/11/2023 | Nitin Kansara | Updated Pre-req. Section |

**Document Distribution**

| **Name** | **Title** | **Date of Issue** | **Version** |
| --- | --- | --- | --- |
|  |  | 06/11/2023 | 1.0 |
|  |  |  |  |

**Copyright & Confidentiality Notice**

*This document is Company Restricted and is not to be copied, distributed, stored, duplicated, or transmitted without the express written permission of Cobweb Solutions Limited Senior Management. All Trademarks are hereby acknowledged. All references to third party products, partners and existing Cobweb Solutions Limited clients should be considered as confidential and may not be distributed without Cobweb Solutions.*

Contents

[Contents 3](#_Toc187149627)

[Introduction 4](#_Toc187149628)

[Customer profile 4](#_Toc187149629)

[How to evolve later 4](#_Toc187149630)

[Prerequisites 4](#_Toc187149631)

[Optionalpre-requisites 4](#_Toc187149632)

[Howto deploy this reference implementation 5](#_Toc187149633)

[Whatwill be deployed? 5](#_Toc187149634)

[Nextsteps 7](#_Toc187149635)

# Introduction

The Enterprise-Scale architecture is modular by design. It allows organizations to start with foundational landing zones, regardless of whether the applications are being migrated or are newly developed and deployed to Azure. The architecture enables organizations to **start as small as needed and scale** alongside their business requirements regardless of scale point.

# Customer profile

This document provides a design path and initial technical state for Small and Medium Enterprises to start with foundational landing zones that support their application portfolios. This reference implementation is meant for organizations that do not have a large IT team and do not require fine grained administration delegation models. Hence, Management, Connectivity and Identity resources are consolidated in a single Platform Subscription.

This reference implementation is also well suited for customers who want to start with Landing Zones for their net new deployment/development in Azure by implementing a network architecture based on the traditional hub and spoke network topology.

Please refer to [Enterprise-Scale Landing Zones User Guide](https://github.com/Azure/Enterprise-Scale/wiki/Deploying-Enterprise-Scale) for detailed information on prerequisites and deployment steps.

# How to evolve later

If the business requirements change over time, the architecture allows for creating additional subscriptions and placing them into the suitable management group and assigning Azure policies. For more details, see the next steps section at the end of this document.

# Prerequisites

To deploy this ARM template, there are a number of prerequisites that must be met. See [here](https://github.com/Azure/Enterprise-Scale/blob/main/docs/wiki/Deploying-ALZ-Pre-requisites.md) for more details.

# Optionalpre-requisites

The deployment experience in Azure portal allows you to bring in an existing (preferably empty) subscription dedicated to host your Platform (Management, Connectivity and Identity) resources. It also allows you to bring existing subscriptions that can be used as the initial landing zones for your applications.

# Howto deploy this reference implementation

Enterprise-Scale landing zones offers a single experience to deploy the different reference implementations. To deploy Enterprise-Scale for Small Enterprises, click on the Deploy to Azure button and ensure you select the following options:

[A blue rectangle with white text

Description automatically generated](https://portal.azure.com/#blade/Microsoft_Azure_CreateUIDef/CustomDeploymentBlade/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2FEnterprise-Scale%2Fmain%2FeslzArm%2FeslzArm.json/uiFormDefinitionUri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2FEnterprise-Scale%2Fmain%2FeslzArm%2Feslz-portal.json)

<https://portal.azure.com/#blade/Microsoft_Azure_CreateUIDef/CustomDeploymentBlade/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2FEnterprise-Scale%2Fmain%2FeslzArm%2FeslzArm.json/uiFormDefinitionUri/https%3A%2F%2Fraw.githubusercontent.com%2FAzure%2FEnterprise-Scale%2Fmain%2FeslzArm%2Feslz-portal.json>

* In the **Enterprise-Scale core setup** blade, select the option for **Single** subscription to host your Platform resources.
* In the **Network topology and connectivity** blade, select either **Hub and spoke with Azure Firewall**.

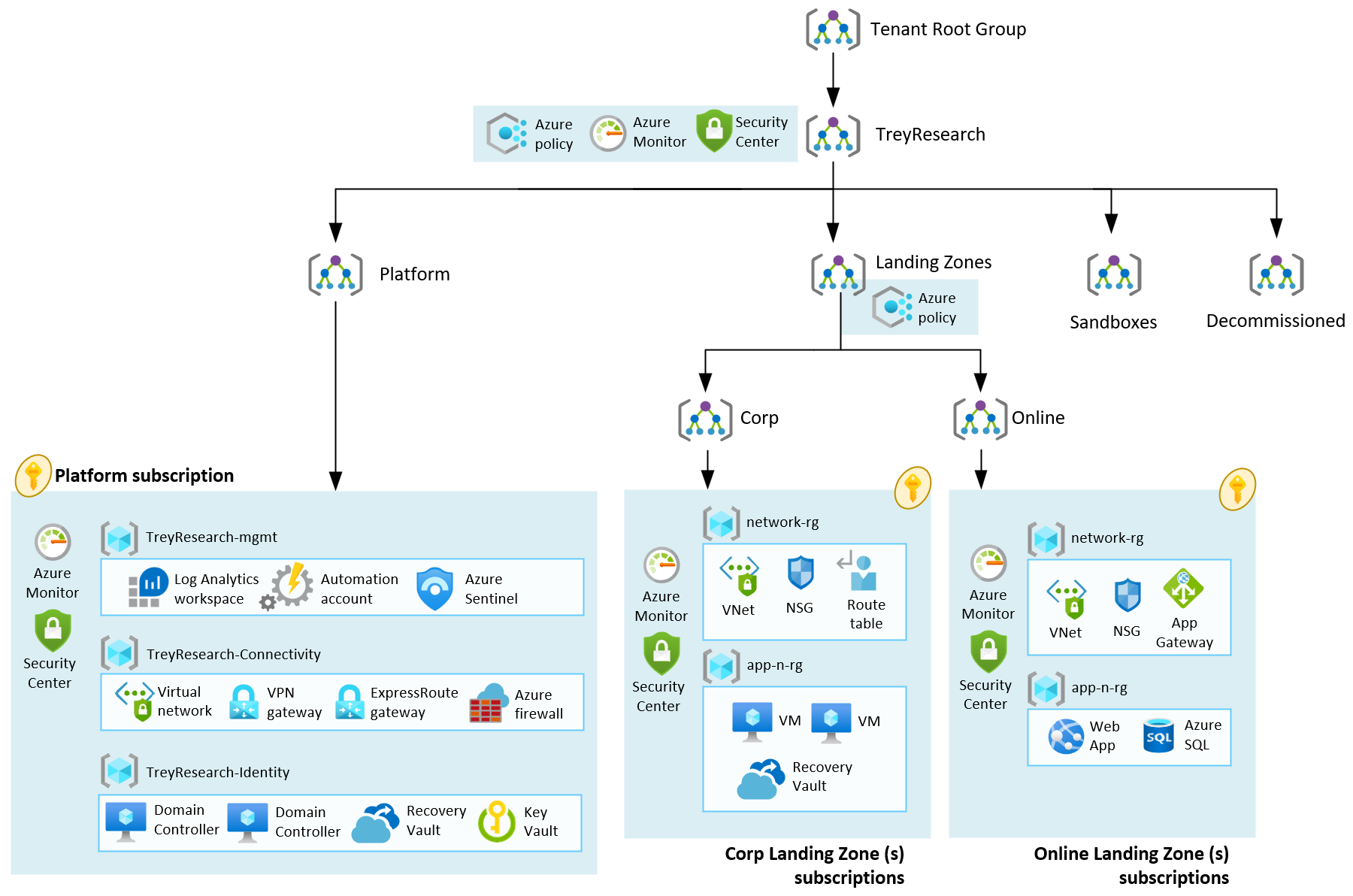
The rest of the options across the different blades will depend on your environment and desired deployment settings. For detailed instructions for each of the deployment steps, refer to the [Enterprise-Scale Landing Zones Deployment Guide](https://github.com/Azure/Enterprise-Scale/wiki/Deploying-Enterprise-Scale-BasicSetup).

# Whatwill be deployed?

By default, all recommendations are enabled. You must explicitly disable them if you do not want them 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.
* An Azure subscription dedicated for **management, connectivity, and identity**. This subscription hosts core platform capabilities such as:
  + A Log Analytics workspace and an Automation account.
  + Azure Sentinel.
  + A hub virtual network
  + VPN Gateway (optional - deployment across Availability Zones)
  + ExpressRoute Gateway (optional - deployment across Availability Zones)
  + Azure Firewall (optional - deployment across Availability Zones)
* 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.
* **Azure Policies** that will enable autonomy for the platform and the landing zones:
  + The following Azure Policies are applied at the root of the Enterprise Scale Management Group hierarchy enabling core platform capabilities at scale:
    - Azure Security monitoring
    - Azure Security Center (Azure Defender OFF (free) and Azure Defender ON)
    - Diagnostics settings for Activity Logs, VMs, and PaaS resources sent to Log Analytics
  + On the other hand, Azure Policies that will apply to all your landing zones. That includes Online, Corp and additional Landing Zone's types you may add in the future:
    - Enforce VM in-guest monitoring (Windows & Linux)
    - Enforce Backup for all virtual machines (Windows & Linux) by deploying a recovery services vault in the same location and resource group as the virtual machine
    - Ensure encryption in transit is enabled for PaaS services
    - Prevent inbound RDP from Internet
    - Ensure subnets are associated with NSG
    - Prevent IP forwarding
    - Enforce encryption for Azure SQL
    - Enforce auditing for Azure SQL
    - Enforce secure access (HTTPS) to storage accounts

**Note:** You may notice the creation of different *managed identities* after deploying the policies described above. This is because a policy with effect *deployIfNotExists (DINE) or modify* will be enforced when enabling a recommendation. These kind of policy effects use managed identities in order to remediate resources that are not compliant. To learn more about what policies are included in ALZ reference implementations, refer to [ALZ Policies](https://github.com/Azure/Enterprise-Scale/wiki/ALZ-Policies).

[](https://github.com/Azure/Enterprise-Scale/blob/main/docs/reference/treyresearch/media/es-lite.png)

# Nextsteps

**From an application perspective**

**Configure security roles for your Azure resources**

Assign Azure RBAC permissions to the groups/users who should use the landing zones (subscriptions) so they can start deploying their workloads.

Azure role-based access control (Azure RBAC) is a system that provides fine-grained access management of Azure resources. Using Azure RBAC, you can segregate your team's duties and grant only the amount of access to users that they need to perform their jobs. See more about security roles at [Microsoft Docs](https://learn.microsoft.com/azure/role-based-access-control/).

**Manage your Landing Zones**

Once you have deployed the reference implementation, you can create new subscriptions or move an existing subscription to the **Landing Zones** > **Online** or **Corp** management group, and finally assign RBAC to the groups/users who should use the landing zones (subscriptions) so they can start deploying their workloads.

**About Cobweb**

Cobweb is one of Europe’s largest cloud solutions providers. Founded in 1996, the company draws on in-depth expertise and decades of experience in what is now known as cloud, empowering organisations of all sizes to grow into flexible, agile businesses through the deployment of best-of-breed cloud technologies.

A member of the Cloud Industry Forum and a Microsoft Gold Certified Partner, Cobweb was the first provider in Europe to deliver Microsoft cloud services through the Microsoft Cloud Solution Provider programme. The company prides itself on innovation and liberating its customers and partners through technology. This is backed up by UK support and advice 24 hours a day, 365 days per year. Based in London and Dubai, with an operations centre on the south coast, Cobweb is a British company with a global outlook.

sales.uae@cobweb.com | +971-4-455-3100 | www.cobweb.com/ae

