Azure foundations for infrastructure Deployment Checklist

# Overview

Welcome to Azure Foundations for Infrastructure. This design pattern represents the culmination of hundreds of customer cloud deployments throughout the past few years. From these deployments, several key patterns emerged, and many best practices were created. The design patterns described here includes all these elements in a simple to understand manner and includes an application to help you get started. The application is named *Foundations Editor* and is available here: <https://github.com/csajeflan/FoundationsEditor/blob/master/FoundationsEditor.zip>

The application is designed to gather the minimum amount of information to create and deploy your base network infrastructure for IaaS deployments in Microsoft Azure. A key design goal of this pattern is to allow for a modular approach to creating your cloud environment. It begins small and can be expanded as your cloud usage increases. The basic pattern begins with two subscriptions in your Server Cloud Enrollment: One for production services and one for pre-production services.

Contents

[Overview 1](#_Toc517255975)

[Azure Enrollment 3](#_Toc517255976)

[Subscriptions 3](#_Toc517255977)

[Subscription Model 3](#_Toc517255978)

[Subscription Names 3](#_Toc517255979)

[Virtual Networks 3](#_Toc517255980)

[Hybrid Connectivity 3](#_Toc517255981)

[Networks 4](#_Toc517255982)

[Subnets 4](#_Toc517255983)

[Administrative Access and Permissions Management 4](#_Toc517255984)

[Administrative Subscription Access 4](#_Toc517255985)

[Role Based Access Controls 5](#_Toc517255986)

[Resource Tagging 5](#_Toc517255987)

# Azure Enrollment

It is a best practice to always utilize an email distribution group address for all email addresses associated with an Azure enrollment. This practice ensures that more than one person in an organization will have access to administer the Enrollment. If an individual users’ email account is utilized, all administrative functions are isolated to that individual which is not ideal if that person is not available. As such, applying a distribution group or service account email address that several people have access to is preferred.

|  |  |  |
| --- | --- | --- |
| ***Field*** | ***Value*** | ***Notes - Examples*** |
| Enrollment Number |  |  |
| Azure Active Directory Namespace |  | contosocitygov.onmicrosoft.com |
| Enrollment Contact Name |  |  |
| Enrollment Contact Phone |  |  |
| Enrollment Contact Email (group or service account) |  | azuregovadmin@contosocity.gov |

# Subscriptions

The organization and determination of your specific Subscription needs will ultimately be based on the governance that you decide. List your desired subscription model and individual Subscription information in this section.

## Subscription Model

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Subscription Model:*** | Services | Prod Pre-prod | Departmental | Custom |

Describe Custom model (if required):

## Subscription Names

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Name*** | ***ID*** | ***Notes - Examples*** |
| Subscription 1  (Primary) |  |  | Production, Services, Department name, etc. |
| Subscription 2 |  |  |  |
| Subscription 3 |  |  |  |
| Subscription 4 |  |  |  |
| Subscription 5 |  |  |  |

# Virtual Networks

## Hybrid Connectivity

Initially you will most likely begin with a VPN connection to Azure. ExpressRoute connections are typically added after the initial creation of your Azure environment as it often takes a long period of time to install a new circuit from your service provider. Fill in the necessary connectivity information here:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Field*** | ***Name*** | ***Resource Group*** | ***Notes – Examples*** |
| VPN Connection Name |  |  | cn-local-az | rg-vnet-prod-az |
| VPN Local Gateway Name |  |  | gw-local | rg-vnet-prod-az |
| VPN Local Gateway IP Address |  | N/A | 61.72.83.94 |
| Local IP Address Range |  | N/A | 10.0.0.0/9 |

## Networks

This list contains the necessary information for all virtual networks that will be required.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Subscription*** | ***Name*** | ***Resource Group*** | ***IP Space*** | ***Region*** | ***Gateway*** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Subnets

The subnet model should be kept similar between all virtual networks if possible. The following names are used by default with the Foundations Editor, but they can be changed if desired (with the exception of the GatewaySubnet). The IP segment sizes will be automatically calculated unless your requirements are different. An ASE must always be a /25 in size.

No changes are required here if you want to accept the defaults.

|  |  |  |
| --- | --- | --- |
| ***Subnet Name*** | ***IP Segment Size*** | ***Notes – Examples*** |
| GatewaySubnet |  | Not editable – do not change |
| dmz |  | Public facing web tier |
| nva |  | Network Virtual Appliance |
| identity |  | Domain Controllers, ADFS |
| ase | /25 | App Services Environment |
| web |  | Internal facing web tier |
| apps |  | Application tier |
| data |  | Data tier |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Administrative Access and Permissions Management

Controlling user access and permissions is necessary in any organization. Separation of workloads and users by department or function is often a requirement of any governance structure. There are a few different ways to accomplish this, and often a combination of these will be used.

## Administrative Subscription Access

Enter your user Subscription access requirements in this table:

|  |  |  |
| --- | --- | --- |
| ***User*** | ***Subscription(s)*** | ***Role (Owner, Contributor, Reader)*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Role Based Access Controls

RBAC allows the partitioning of rights within a desired scope. These are typically applied at the Resource Group level. Individual permissions such as networking, virtual machine creation, specific PaaS services access, etc. can be granted to users or groups as required. This allows for a much more granular level of access than the Subscription level global admin role. The RBAC mechanism can delegate permissions to specific workloads based on the role of an end user. More information about RBAC is located here:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

Enter your desired RBAC permissions in this table:

|  |  |  |
| --- | --- | --- |
| ***User/Groups*** | ***Resource Group*** | ***Roles*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Resource Tagging

Enter your specific resource tagging requirements in this table:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Key*** | ***Value*** | ***Resource*** | ***Notes – Examples*** |
| Department | Central IT | rg-vnet-prod-az | Central IT managed | Production Vnet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |