PROACT

Azure Landing Zone

Design and Implement

What is it?

This service is a technical consulting service that helps customers with the rollout of an Azure Landing Zone and migration of an existing data center to this environment. Proact will configure and implement an environment that can hold at least virtual machines and enables connectivity It delivers a basic secure and available environment **based on our best-practices and design decisions** with customer parameterization.

The project will deliver the Landing Zone, but also a detailed design, build-as documentation and makes sure there is a basic handover to the customers IT administrators. Out of Scope are administration guides, work instructions and Azure training.

Project Approach

- √ Customer Kick-off
- √ Workshop
- √ Detailed Design
- √ Project Management
- √ Documentation
- √ Configuration of the areas below
- √ Project Evaluation

Monitoring

Monitoring setup, will deliver a standard Monitoring Dashboard, a monitoring agent in each deployed Virtual Machine and a basic alert to the customer IT team for the event a resource goes offline. Out of scope in the basic setup is the integration with 3rd party tools and other advanced alerting and automation functions of Azure.

Optionally advanced monitoring functions can be configured as well. Advanced functions can be (for example) integration with other Microsoft products, custom dashboards or custom alerts. These can be configured as additional work during the project.

Governance

The basic configuration of the Azure infrastructure will consist of two (2) subscriptions, one for Production and one for Test. In this infrastructure we will configure Resource Groups, one for Networking, one for Infrastructure & Backup and one for each workload/application, including basic tagging of resources.

Advanced configuration is available as well around governance All advanced configuration work is additional work and can contain (not limited to):

- √ Advanced tagging of resources
- √ Management group deployment
- √ Automatic identity and access management
- √ Audit trails and Audit reports
- √ Automatic policies

Security

Basic configuration of security in the environment covers the setup of Network Security Groups, the implementation of the principle of Least Privilege and excludes the configuration of Public IP's. Basic configuration also covers the setup of Multi Factor Authentication (MFA) for IT administrators. Last, this setup will cover one Key Vault configuration.

Furthermore, it is also possible to perform advanced security configurations as additional work Advanced configuration can, not limited to, cover the following areas:

- √ Azure Firewall
- √ 3rd party firewalls
- √ Azure VM Disk Encryption (BitLocker)
- √ Privileged Identity Management (PIM)
- √ Privileged Access Management (PAM)

Connectivity

To be able to deliver connectivity from the customers location to the resources in Azure, a basic network configuration will be made. This setup contains the following scope;

- √ Virtual Network (2 x)
- √ Gateways (max. 5)
- √ Subnets (max. 5)
- √ Network Security Group (max. 5)
- √ Bastion Host (1 x)
- √ Site to Site VPN (1 x)

Out of scope for the basic configuration is the on-premise configuration for connectivity and User Defined Routing (UDR).

Advanced configuration options are here available as well and , can be, not limited by;

- √ Additional Virtual Networks
- √ ExpressRoute
- √ BGP configuration
- √ Virtual WAN
- √ SD-WAN connection
- √ Azure Frontdoor Services
- √ Global Load Balancing

Availability

The standard infrastructure will be deployed with a basic set of availability settings, a daily backup with Azure Backup (only Virtual Machines and SQL PaaS) and the configuration of local High Availability (Availability Sets). Out of scope for the basic availability setup is application-aware backups, integration with other tools and Disaster Recovery.

It is possible to perform advanced configuration work, like;

- √ 3rd Party Backup and DR
- √ Proact BaaS and DRaaS
- √ Azure Site Recovery
- √ Geo High Availability
- √ Non-IaaS backup (PaaS, Azure Function, NSG's, ...)

Migration

Once the environment is configured, Proact can assist the customer with the migration of virtual machines to this environment. The migration is based on Time and Material (T&M) as each virtual machine and operating system is different. The migration will require an intake and effort estimation, after which we will be able to deliver a detailed Migration Plan. During the migration we can migrate servers/virtual machines, but also databases (e.g. SQL Server to SQL PaaS) and perform application rationalization. Our advice in the migration strategy is to migrate per application (set).