# Landing zones

As a cloud provider, we provide infrastructure to the client

A client needs to migrate the resources from on-prem to the cloud, like - application servers. We need do have an architecture, using that we move the work load to the cloud.

that infrastructure that includes all the concepts of monitoring, security, and many other services that azure provides.

Landing zone is a Microsoft recommended service which we do in collaboration and put in-front of a customer to move the work load.

before moving the resources to the cloud, we need to have a good architecture, Microsoft provides many guidelines to create architectures.



high

If we create an infrastructure from the recommended guidance of Microsoft, we can achieve

security, and



high scalable



cost effective

# Landing zone

As we prepare for cloud migration, we want to move workloads securely. Its also crutial to scale and innovate.

Scalable migration starts with a landing zone.

A landing zone is a place where you host your workloads pre provisioned through code. It provides all cloud services and best practices to add foundational capabilities.

It provides a stable place for your work to run and a framework to scale. To provide scalability, we follow



5 principles of landing zone

##### networking services.

which enable you to add or remove workloads without any disruption.

##### set identity rules.

so only trusted users can access the data

addressing the first 2 principles enables you to start migrating low risk workloads.

##### Govern environment.

can done with integrated compliant policies to ensure the workloads meet industry regulations

##### Use security controls.

to create a safe place for your workloads

##### manage your environment.

by monitoring performance and creating a resilient base for your workload.

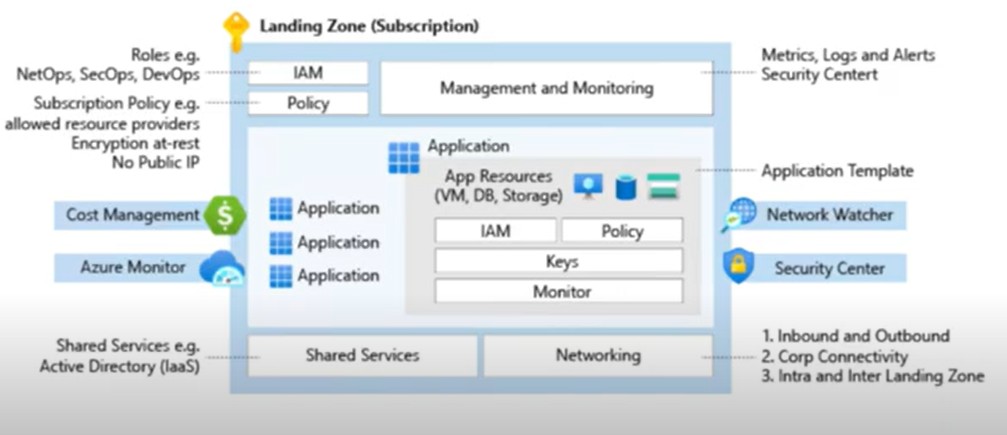
These 5 principles can be used to create a robust landing zone that offers *increased speed*, *better security and performance* leading to faster and secure and efficient cloud migration.

# Fields

*greenfield* when you are complete beginner and starting the cloud journey from the scratch. If you have an existing environment, this is referred to as *brownfield*

It depends on the customer’s level to recommend same level of architecture.

# Foundational landing zone



This is the Microsoft recommended architecture for a client with a single subscription and we provide bare minimum resources in this architecture.

If you have a single subscription and have a normal workload, which can be deployed in a single subscription.

Start small and expand.

can choose foundational level infrastructure and expand it to an enterprise level architecture.

## what are the bare min resources we provide

### IAM and Policy

#### policy

we can manage the security posture using policies.

We enable audit level policies for the customers.

#### IAM

IAM are the RBAC rules.

What kind of access you can give to a specific user or group.

### Cost Management

Analyzing the costs of the created resources

### Azure Monitor

The resources we create in Azure have a matrix which is automatically enabled in the background. We can *configure Alerts* based on those matrix.

### Shared Services

#### AD

extending on-prem AD to the Cloud.

### Networking

connectivity between on-prem to azure.

resources like Vnets,

subnets, NSG’s,

connectivity to on-prem,

connectivity to the internet comes under this subscription.

### Management and Monitoring

How are we setting monitoring the managed resources in Azure, like log analytics

alerts

### Security Center

default enabled

Checking compatibility and compliance of the created infrastructure. Gives a compliance score

Gives recommendations based on your security posture. Security Center can be enabled in standard SKU.

### Network Watcher

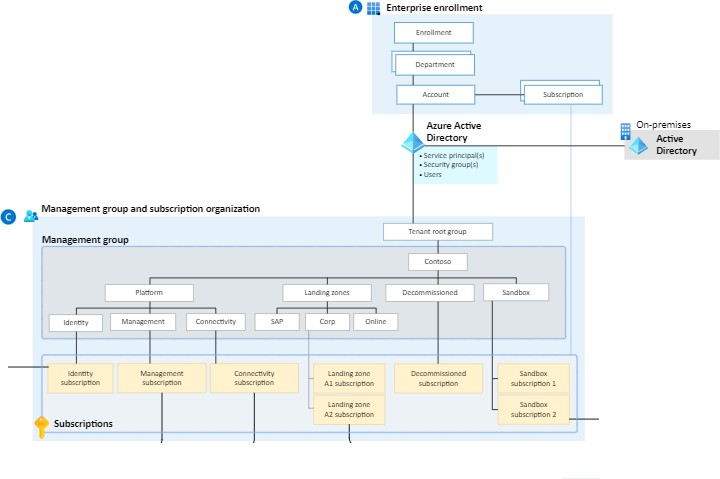
When Traffic flows from source to destination, can take a look which port is open and which is closed, which port has an allow access and deny access.

Can check the traffic coming to azure/from azure using IP’s which needs a source and destination IP and port number.

The Migration of the Application comes after the setup and can be deployed in a separate subscription landing zone called “*Application landing zone*”.

Monitoring and policies can be created again at this level to the subscription.

# Enterprise Landing Zone



We create a Tenet and integrate on-prem AD to Azure AD. departments are created which are called *management groups*.

Subscriptions will increase and each department have an owner who owns the subscriptions and if need of more subscriptions, That owner will be creating one.

## B

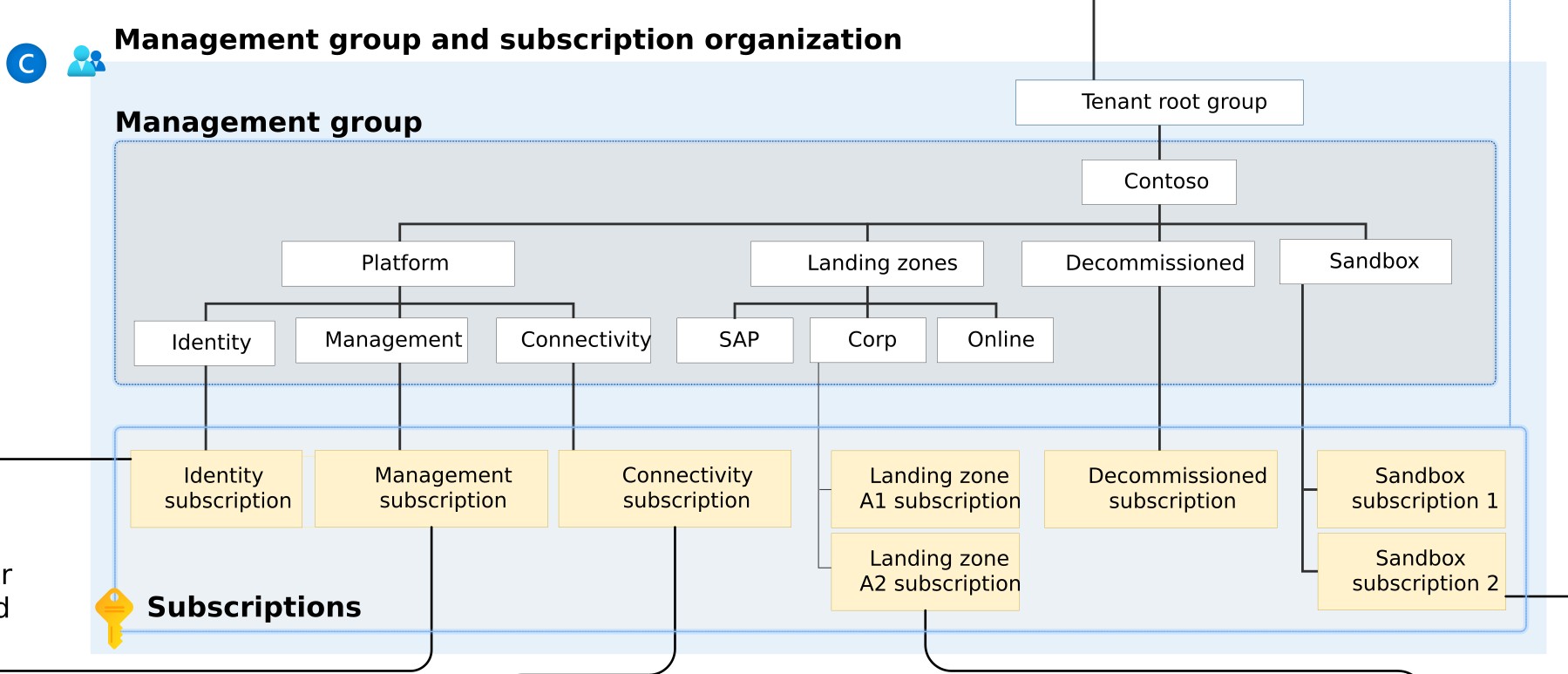
## 

In the *identity and access management*, owners can manage MFA

Notifications audit reports

cost optimization plans

## C



### Platform Landing Zone

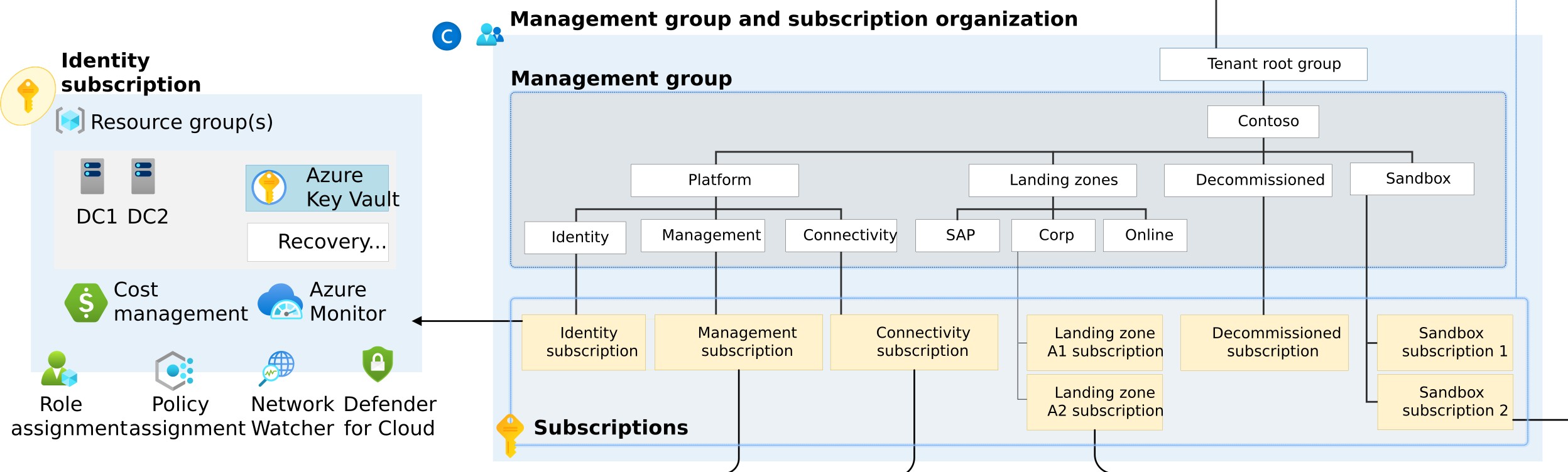
Three subscriptions which provides *shared services*.

identity subscription

connectivity subscription

management subscription

**Identity subscription**



# Platform Landing Zone

Is a subscription which provides shared services *identity, connectivity, management* to apps in application landing zones.

these services often improves operational efficiency. One or more central teams manage the PLZ.



**Enterprise enrollment**

**Identity and access management**

On-premises

**Active Directory**

**Management group and subscription organization**

**Identity**

**subscription**

Resource group(s)

**Management group**

**Platform**

**DevOps team**

**DevOps**

DC1 DC2

n

Cost

management

Azure

Monitor

Role

Policy

Network Defender

* Role definitions
* PolicySet definitions
* Policy definitions
* Role assignments
* Policy assignments
* Resource templates
* Subscription provisioning
* Role provisioning
* Policy deployment
* Platform deployment

assignment assignment Watcher for Cloud

**Subscriptions**

**Management**

**subscription**

**Connectivity**

**subscription**

**Landing zone A2**

**subscription**

**Sandbox**

**subscription**

Dashboards (Azure portal)

Azure

DDoS

Standard

VNet

peering

Virtual

network

Applications Applications

* Change tracking
* Inventory management
* Update management

Azure DNS

* Dashboards
* Queries
* Alerting
* Azure Firewall
* ExpressRoute
* VPN (P25/S2S)

Resource groups(s)

Applications

Application

Application Application

Cost

Role

Policy

management assignment assignment

Network Defender

Watcher for Cloud

Subset Cost

Role

Policy Network

Cost

Role

Policy Network

management assignment assignment Watcher

Defender

for Cloud

Defender

management assignment assignment Watcher for Cloud

Dashboards

(Azure portal)

Recovery Services

vault(s)

Shared

services

**On-premises systems**

Cost

Role

Policy Network Defender

management assignment assignment Watcher for Cloud

* Access credentials
* In-guest policies/DSC
* Backup policy
* Extensions

Compliant  Tagging

VM templates

VM SKU(s)

Hub VNet Region 1

Log analytics workspace

Automation account(s)

Wiki

Deployment pipeline(s)

Boards

Git Repository

Recovery...

Azure

Key Vault

Sandbox subscription 2

Landing zone A2 subscription

Sandbox subscription 1

Decommissioned subscription

Landing zone A1 subscription

Connectivity subscription

Management subscription

Identity subscription

line

O

Corp

SAP

ctivity

Conne

ment

Manage

tity

Iden

Sandbox

Decommissioned

Landing zones

orm

Platf

Contoso

enant root group

T

* Service principal(s)
* Security group(s)
* Users

**Azure Active Directory**

Subscription

Account

Department

Enrollment

* App/DevOps
* Subscription manager
* *Other custom roles*

Privileged Identity Management

* Approval workﬂow
* Notifications
* MFA
* Access reviews
* Audit reports

Recovery...

File Share

Azure

Key Vault

NSG/ASG(s)

UDR(s)

DNS

