



# Azure Landingzones

***Cloud architecture for scale, security  
and governance.***

Experts Live 2025, Colin Jochum

# Danke an unsere Sponsoren

PLATINUM



GOLD



Dipl.-Ing.

# Colin Jochum

Graz, Österreich

Lead of Cloud Services, Cloud Solution Architect

ACP IT Solutions GmbH



Web: <https://colinjochum.com>

LinkedIn: <https://linkedin.com/in/colinjochum/>

Sessionize: <https://sessionize.com/colin-jochum/>



# Agenda



Cloud Adoption Framework



Cloud Operating Models



Ressourcen Organisation



Governance, Berechtigungen



**Enterprise Scale Landingzones**

# Wozu Planung?

## Wozu Architektur?

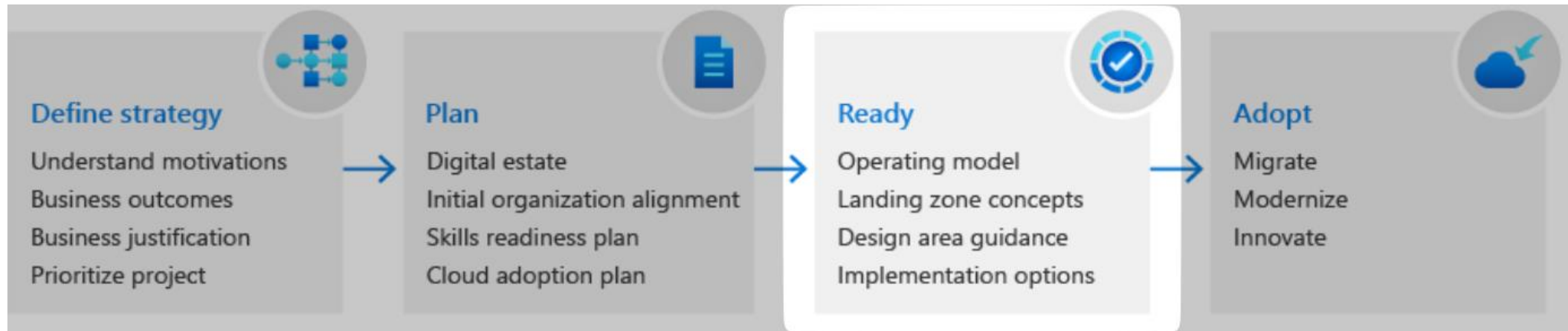






# Antwort von Microsoft: CAF

- Microsoft Cloud Adoption Framework (CAF)
- Best-practices und Guidelines
- Enterprise Scale Architecture



# Enterprise Scale Architecture

## **Definition: Landingzone**

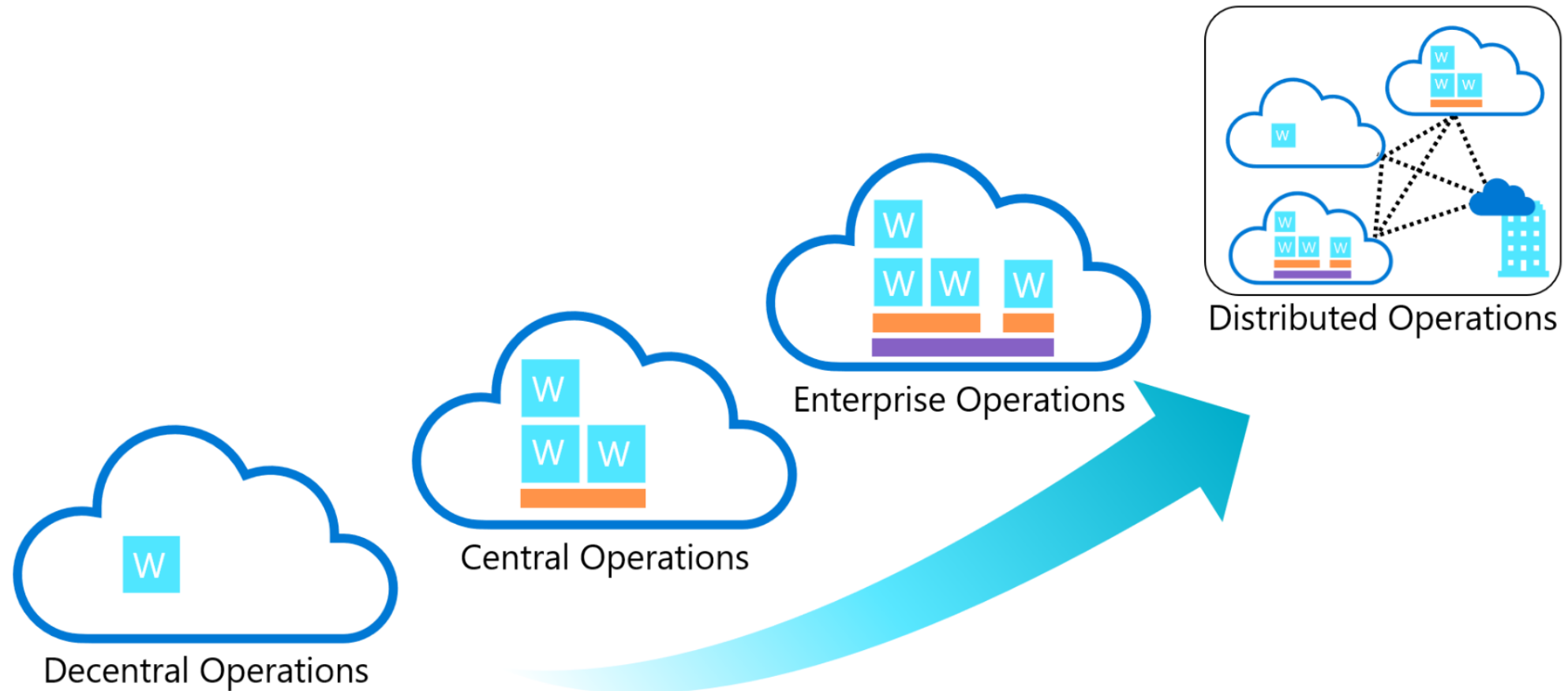
- (1) Azure Umgebung basierend auf Design Prinzipien und Azure Komponenten
- (2) Azure Subscription(s)

## **Ziele**

Skalierbar, Modularer Aufbau, Sicherheit, Governance und Agilität  
Unterstützen der Workload/Applikation Teams



# Cloud Operating Model



# Dezentralisiert

- Vollständige Autonomie der Applikation-Teams
  - Keine zentralisierte Kontrolle und IT-Prozesse
- 
- + Hohe Innovation, Flexibilität, Agilität
  - Fluktuierende Sicherheit, Kontrolle, Governance

# Zentralisiert



- Traditioneller IT Ansatz: Ein zentrales IT-Team
  - IT-Team verwaltet alle Aspekte der Cloud Umgebung
- 
- + Hohe Konsistenz, Standardisierung, Sicherheit
  - Geringe Agilität und Innovation, Langsame Prozesse



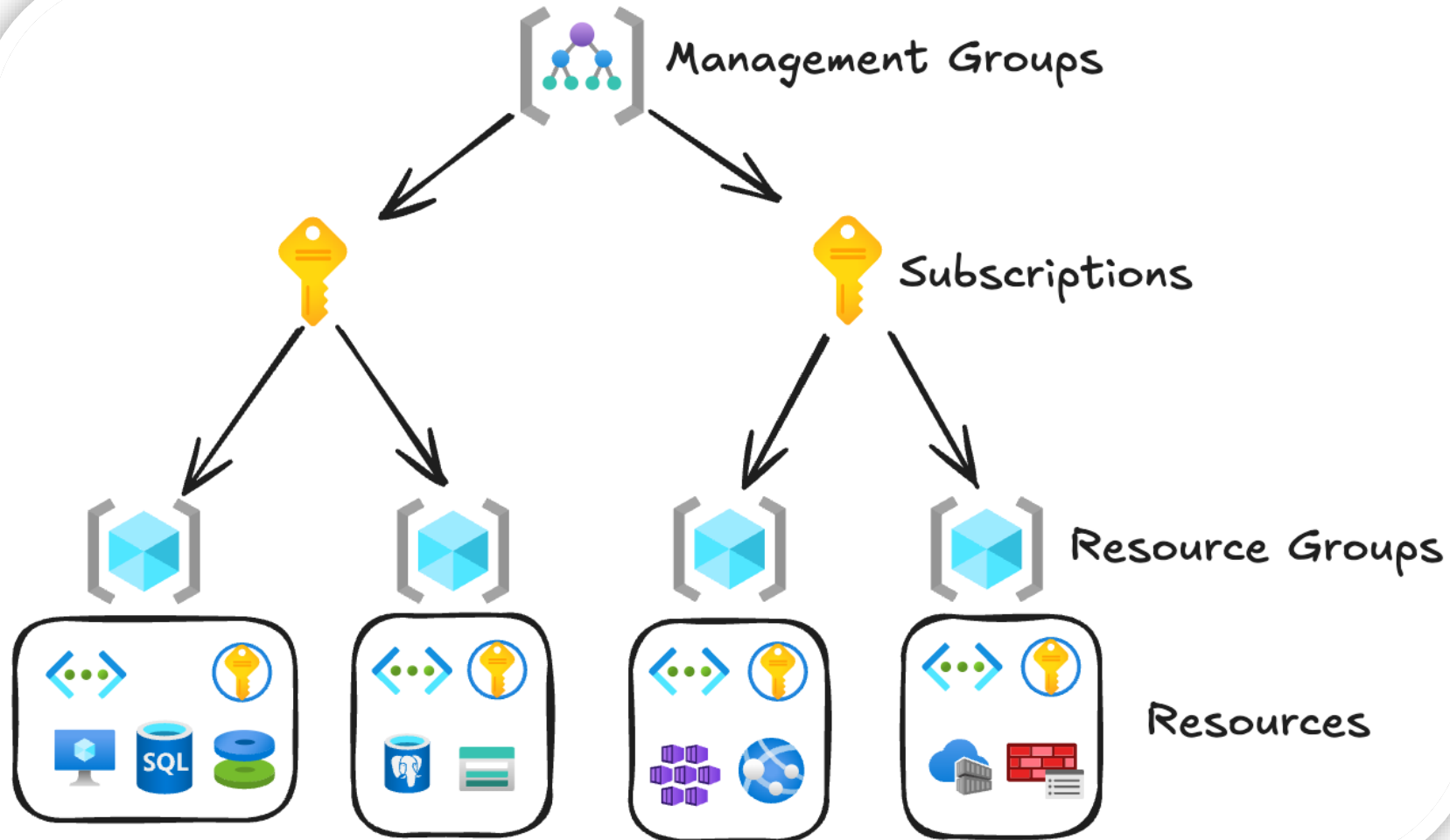


# Enterprise Operations

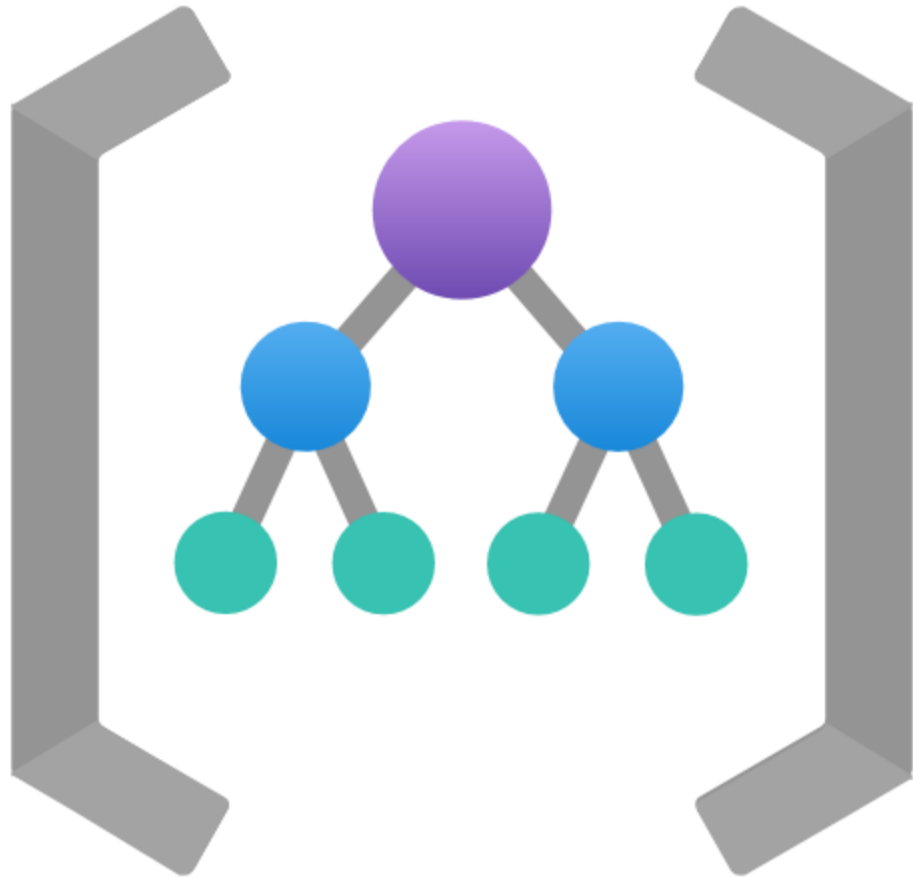
- Balance zwischen Dezentralisiert und Zentralisiert
  - **CCoE Team**  
Cloud Architects & Specialists  
Zentrale Governance, Sicherheit, Plattform Dienste, Innovation und Enablement der Workload Teams
  - **Workload Team(s)**  
Freiraum, Zuständig für ihre Workloads und Applikationen
- 
- + Gute Balance, Innovation
  - CCoE Team Investment (\$), Herausfordernde Umsetzung

# Ressourcen Organisation

# Management Levels





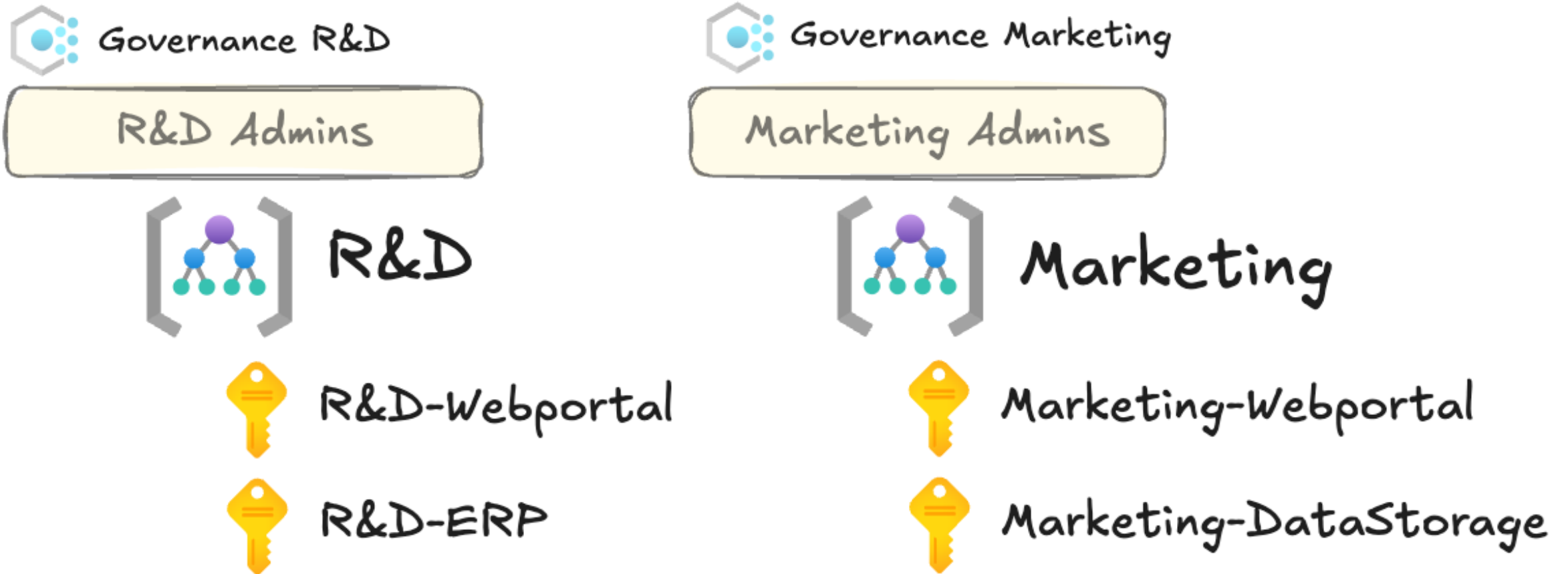


# Management Gruppen

Gruppieren und Strukturieren  
Governance & Berechtigungen

Keep it simple!  
max. 4 Ebenen

# Beispiel: Design von Business Units



# Beispiel: Dev/Prod



App1-Dev  
App2-Dev



App1-Prd  
App2-Prd



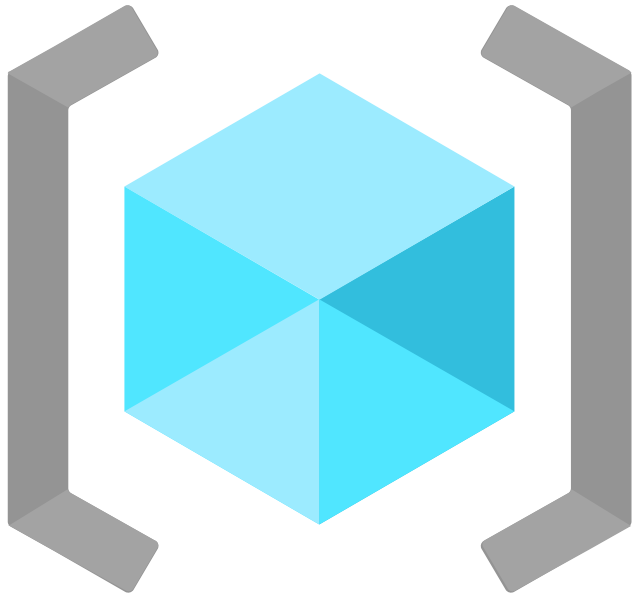
App1-Dev  
App2-Dev  
App1-Prd  
App2-Prd





# Subscriptions

- Landingzone
- Hier "Landen" Workloads  
VMs, Storage, WebApps...
- Abgrenzung  
Kosten, Governance, Berechtigungen,  
Netzwerk
- **Quotas & Limits!**



# Ressourcen Gruppen

- Container für Azure Ressourcen
- Gruppieren von Ressourcen
- Lifecycle Management

# Namensschema

- Ressourcen umbenennen nicht möglich!
- Namensschema erzwingen nur bedingt möglich via Azure Policy

## Empfehlungen

- Standard definieren und dokumentieren
- Ausnahmen und Limitierungen beachten z.B. Storage Accounts, VMs...
- Kleinbuchstaben
- Dynamische Komponenten vermeiden z.B. SKU, (Region), Service Type, Env

Azure Naming Tool





# Tagging

- Zusatzinformationen, Metadaten
- Verbesserte Filterung, Kostenmanagement
- Automation: Backup Onboarding

Subscription ([move](#)) : [SandboxLZ](#)

Deployments : [2 Succeeded](#)

Subscription ID : 2cf5c93e-ca70-4d4f-b785-1dd8ea35a65b

Location : West Europe

Tags ([edit](#)) :

Environment : Sandbox

DateCreatedUTC : 2024-11-27T11:50:14.2237329Z

Owner : Colin Jochum

Description : Test Environment

Criticality : Low



# Governance

# Azure Policy

- Built-In / Custom
- Policy Initiativen  
z.B. ISO27001:2013, MCSB
- Audit, Deny, Modify...
- Non-Compliant Nachricht!

```
Azure Policy Example - SQL DB min. TLS Version 1.2

1 "if": {
2   "allOf": [
3     {
4       "field": "type",
5       "equals": "Microsoft.Sql/servers"
6     },
7     {
8       "anyOf": [
9         {
10          "field": "Microsoft.Sql/servers/minimalTlsVersion",
11          "exists": false
12        },
13        {
14          "field": "Microsoft.Sql/servers/minimalTlsVersion",
15          "less": "1.2"
16        }
17      ]
18    }
19  ]
20 },
21 "then": {
22   "effect": "Audit"
23 }
```

Basics

Parameters

Remediation

Non-compliance messages

Review + c

Non-compliance messages help users understand why a resource is not compliant with the policy. The message will be displayed when a resource is denied and in the evaluation details of any non-compliant resource.

Non-compliance message

This resource type is not allowed and was blocked by Azure Policy: "Not allowed resource types". Please contact your local administrator or the CCoE team for more information.

# Policy Architektur

- Aufbau und Design eines Baseline-Policy Sets
- Empfehlung: Management Gruppen und Subscriptions

## Microsoft Landingzone Accelerator Policy Set

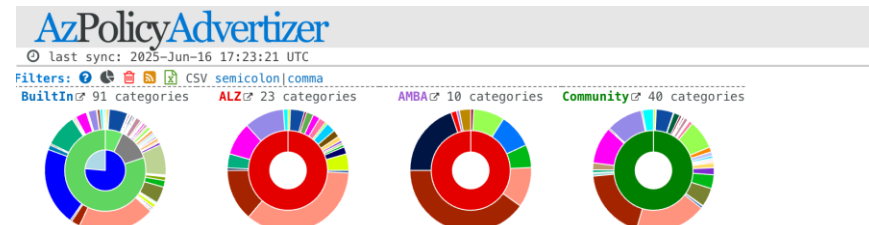
92+ Azure Policies

[Deny-Vnet-Peering](#) (Sandbox), [Deny-MgmtPorts-From-Internet](#),...



## AzPolicyAdvertiser

Übersicht von Azure Policies incl. AZL und Community Policies





# Berechtigungen

# Azure IAM

- Built-In Rollen (über 120) für 99% der Fälle ausreichend
- Control Plane vs Data Plane

```
User Access Administrator

1 // {
2   "id": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
3   "properties": {
4     "roleName": "User Access Administrator",
5     "description": "Lets you manage user access to Azure resources.",
6     "assignableScopes": [
7       "/"
8     ],
9     "permissions": [
10      {
11        "actions": [
12          "*/read",
13          "Microsoft.Authorization/*",
14          "Microsoft.Support/*"
15        ],
16        "notActions": [],
17        "dataActions": [],
18        "notDataActions": []
19      }
20    ]
21  }
22 }
```

Control Plane

Data Plane



# Persönliche Empfehlungen

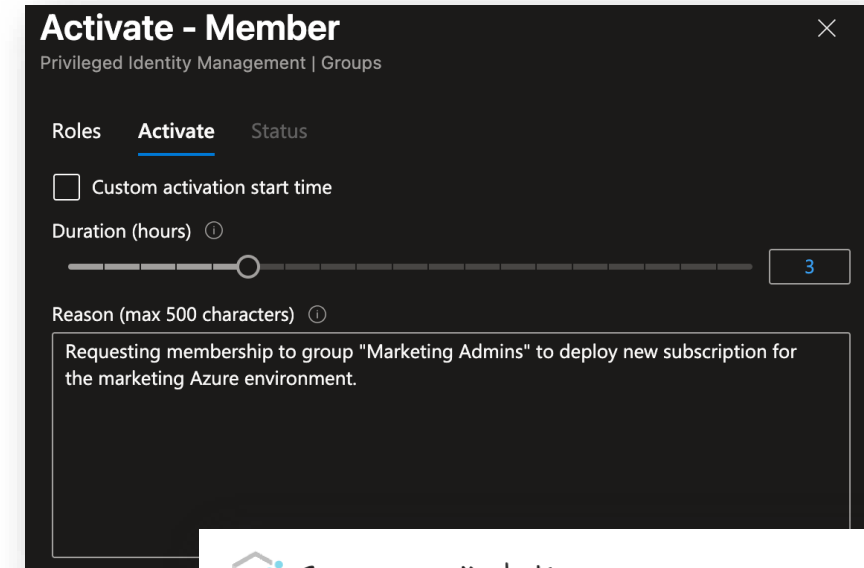
- Principle of Least Privilege - Abwägung Administrativer Aufwand
- Vorsicht mit Admin Rollen: Owner, Contributor, UAM
- Regelmäßiger Audit der Berechtigungen
- Zuweisungsebene berücksichtigen
- Zuweisung mittels Entra/AD Gruppen
- Verwenden von Managed Identities

# Azure Privileged Identity Management (PIM)

- Time-Based Access
- Audit, Approval, MFA, Monitoring
- Entra ID P2 Lizenz

Für großflächig Administrative Berechtigungen

- Vorsicht mit Genehmigungsprozess

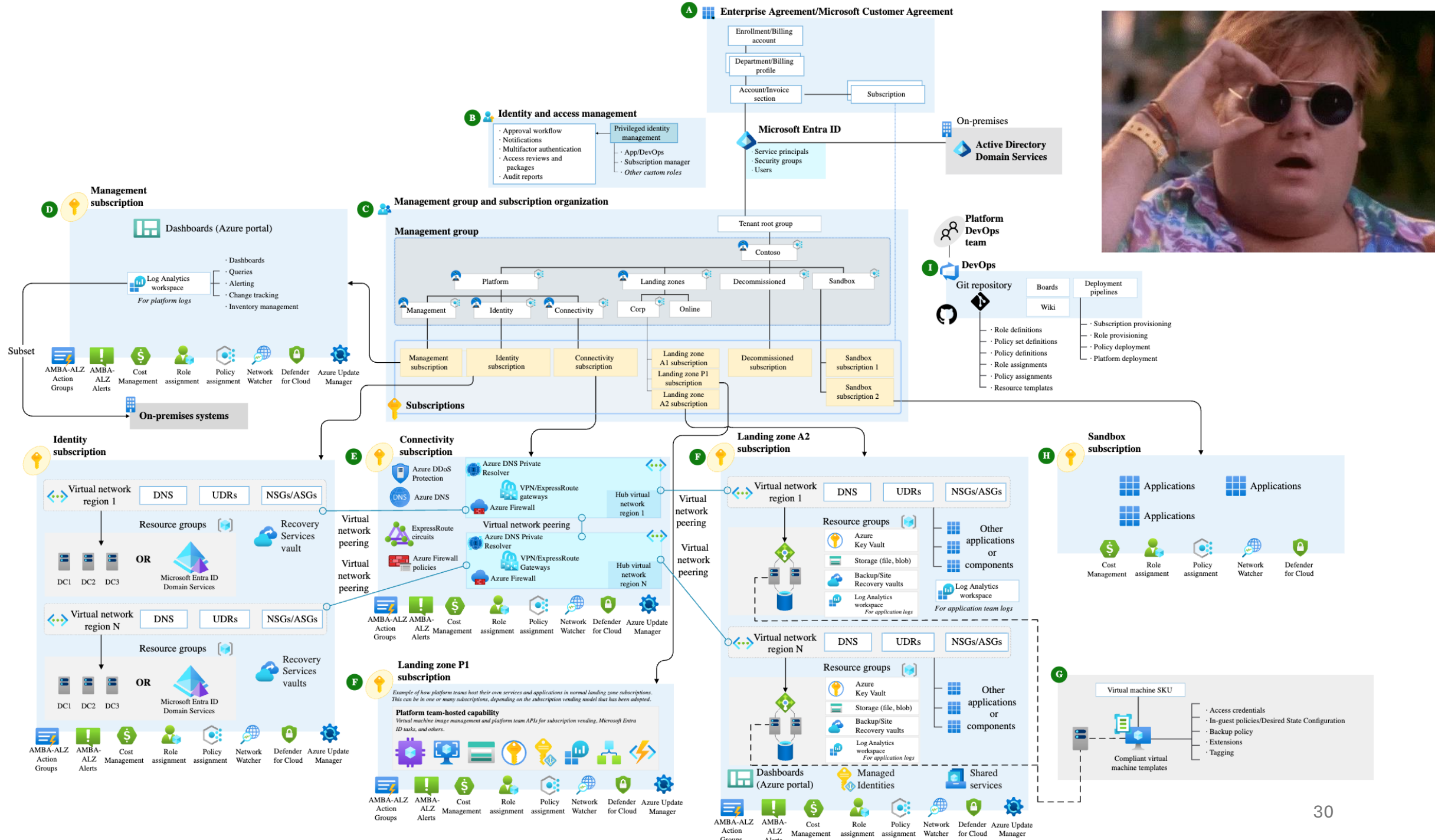


The screenshot shows the 'Activate - Member' window in the Azure Privileged Identity Management console. It has tabs for 'Roles', 'Activate', and 'Status'. Under the 'Activate' tab, there is a checkbox for 'Custom activation start time'. Below that is a 'Duration (hours)' slider set to 3 hours. A text box for 'Reason (max 500 characters)' contains the text: 'Requesting membership to group "Marketing Admins" to deploy new subscription for the marketing Azure environment.'

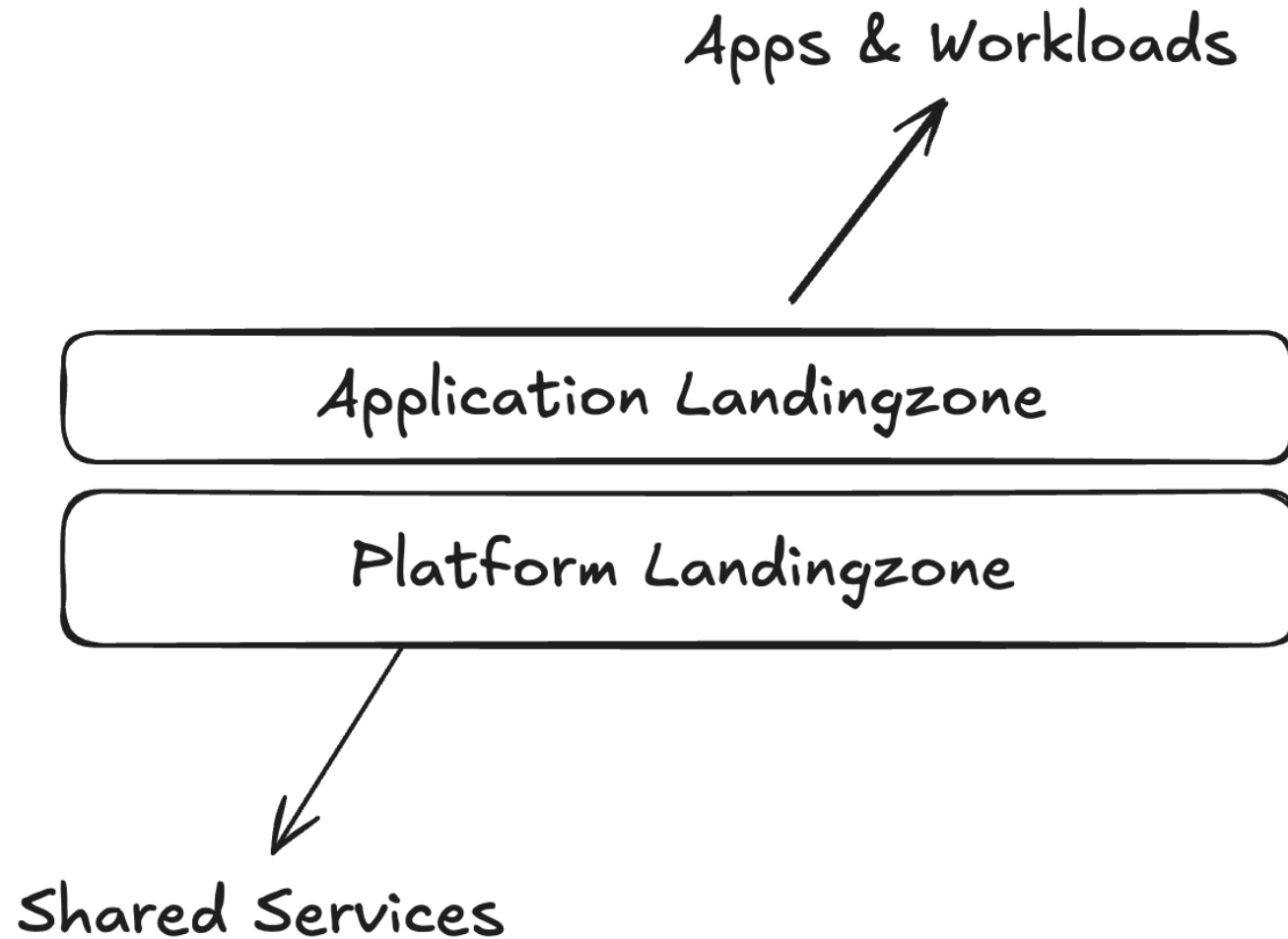


# Enterprise Scale Landingzones

## Architekturdesign

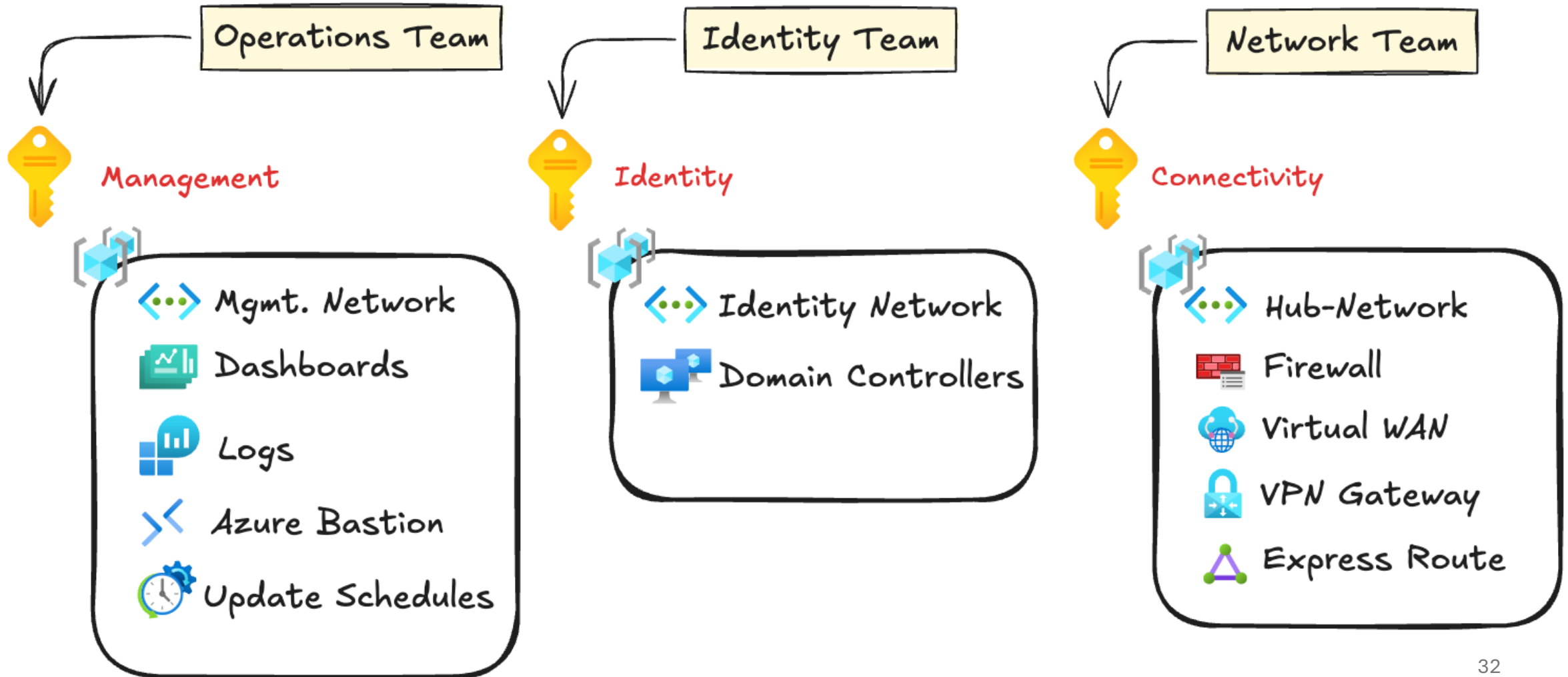


# Landingzone Typen



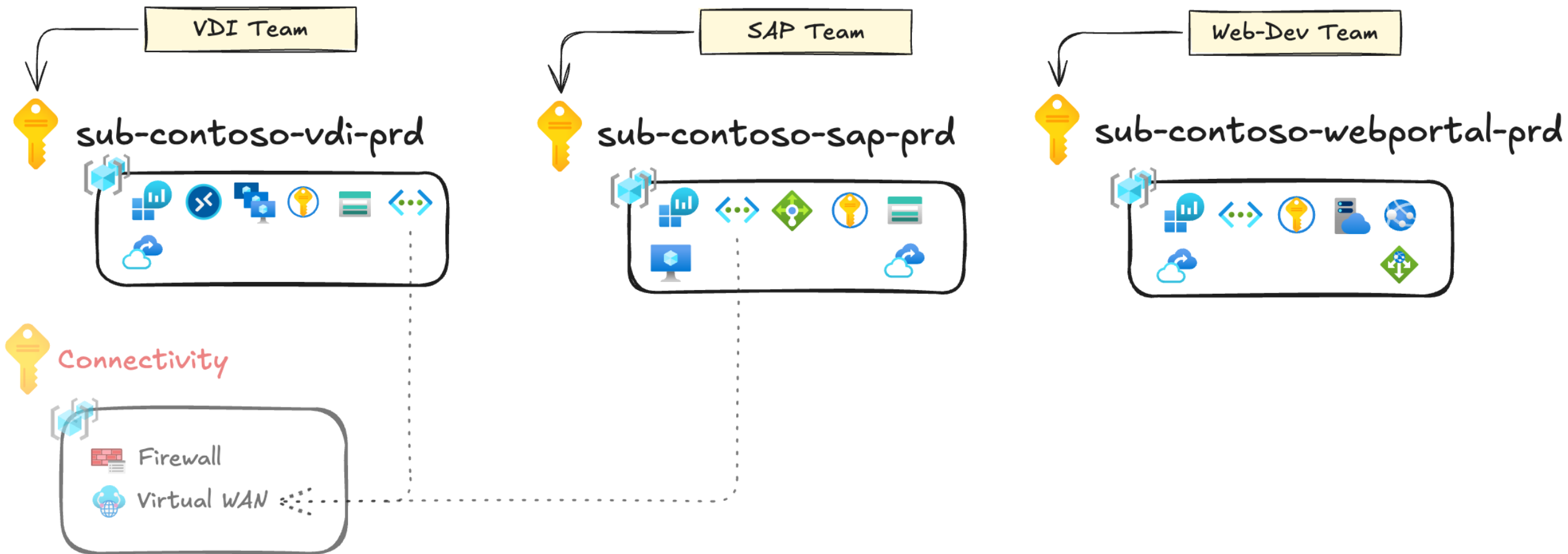
# Platform Landingzones

## Shared Services

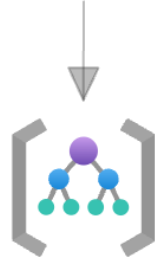




# Application Landingzones



Tenant Root /



Tenant Root Group



Contoso



Default



New Subscription(s)



Platform



Landingzones



Sandbox



Sandbox



Decomissioned



Legacy Subscription(s)



Management



Management



Identity



Identity



Connectivity



Connectivity



SAP App



VDI App



WebPortal



...



# Ansatz: Eine Subscription

## Vorteile

- Kontrolle durch zentrales Team

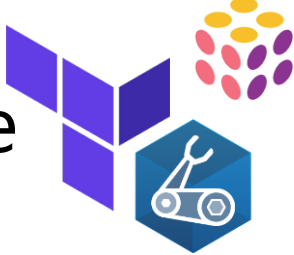
## Nachteile

- Subscription Quotas und Limits
- Berechtigungen, Flexibilität, Skalierung, Modularität
- Governance & Kostenstruktur
- Defender for Cloud

## Einsatzszenarien

Startups, Test-Tenant, App Team = Platform Team

# AZL Deployment

Infrastructure-as-Code  Pulumi

## Deployment Frameworks & Produkte

Azure Landingzone Accelerator (Portal, Terraform, Bicep)

ACP Azure Basis Landing Zone





Vielen Dank Experts Live 2025