



# Azure Architects Connect | CAF, ALZ, WAF



# Referentinnen



**Maria Theilemann**  
Cloud Solution Architect  
Azure Infrastruktur



**Sarah Wendel**  
Cloud Solution Architect  
Azure Infrastruktur

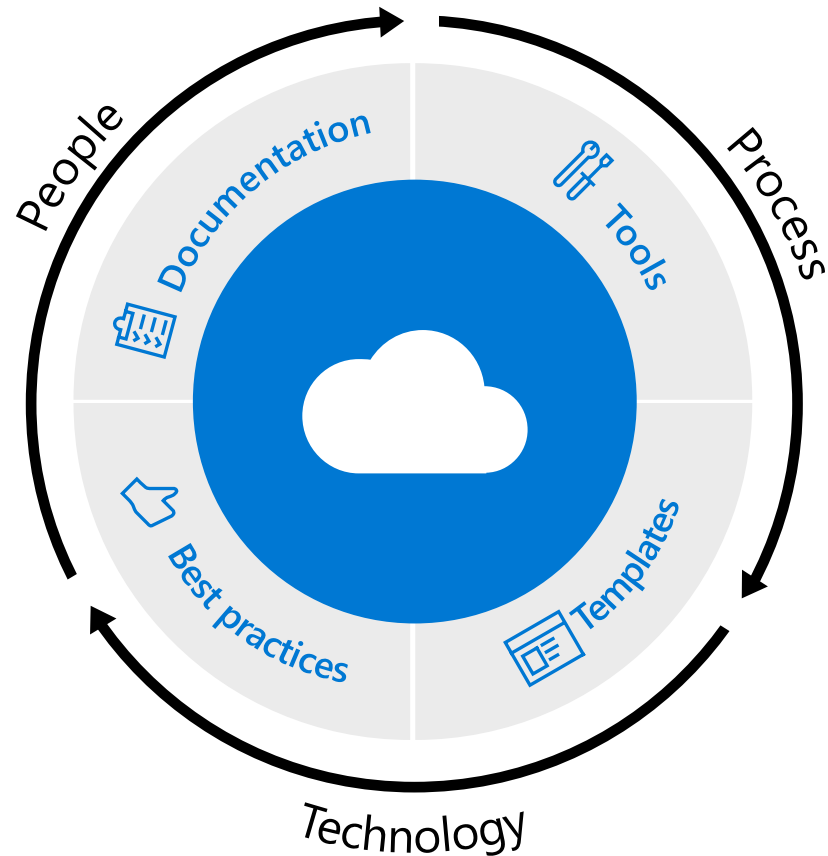
# Agenda:

- 9:00 Begrüßung
- 9:15 Cloud Adoption Framework
- 9:45 Azure Landing Zones
- 11:15 Well-Architected Framework
- 11:45 Q&A

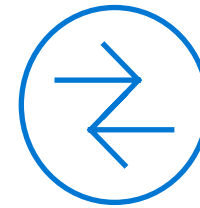


# Cloud Adoption Framework

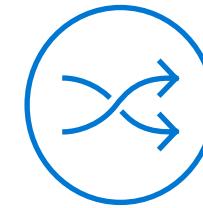
# Microsoft Cloud Adoption Framework for Azure



Kontrolle  
& Stabilität



Geschwindigkeit  
& Ergebnisse



Balance

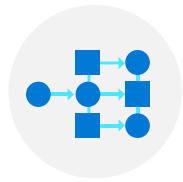
**Anpassen** der Strategie auf das Business, die Menschen und die Technologie.

**Erreichen** der Geschäftsziele anhand einer umsetzbaren, effizienten und verständlichen Anleitung.

**Liefern** schneller Ergebnisse mit Kontrolle & Stabilität.

# Cloud Adoption Framework für Azure

Bewährte Anleitungen für Business und Technologie, um Kunden in Ihrer Cloudreise zu unterstützen



## Strategie

Definieren des Business Case und der erwarteten Ergebnisse



## Planen

Ausrichten eines umsetzbaren Cloud-Adoptionsplans an Geschäftsergebnisse



## Bereit

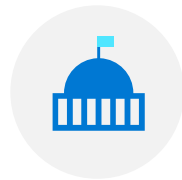
Bereiten der Menschen, Prozesse und Umgebung auf Veränderungen vor



## Cloud Adoption

### **Migration** oder **Innovation**

Implementieren der gewünschten Änderungen über IT- und Geschäftsprozesse hinweg



## Steuern

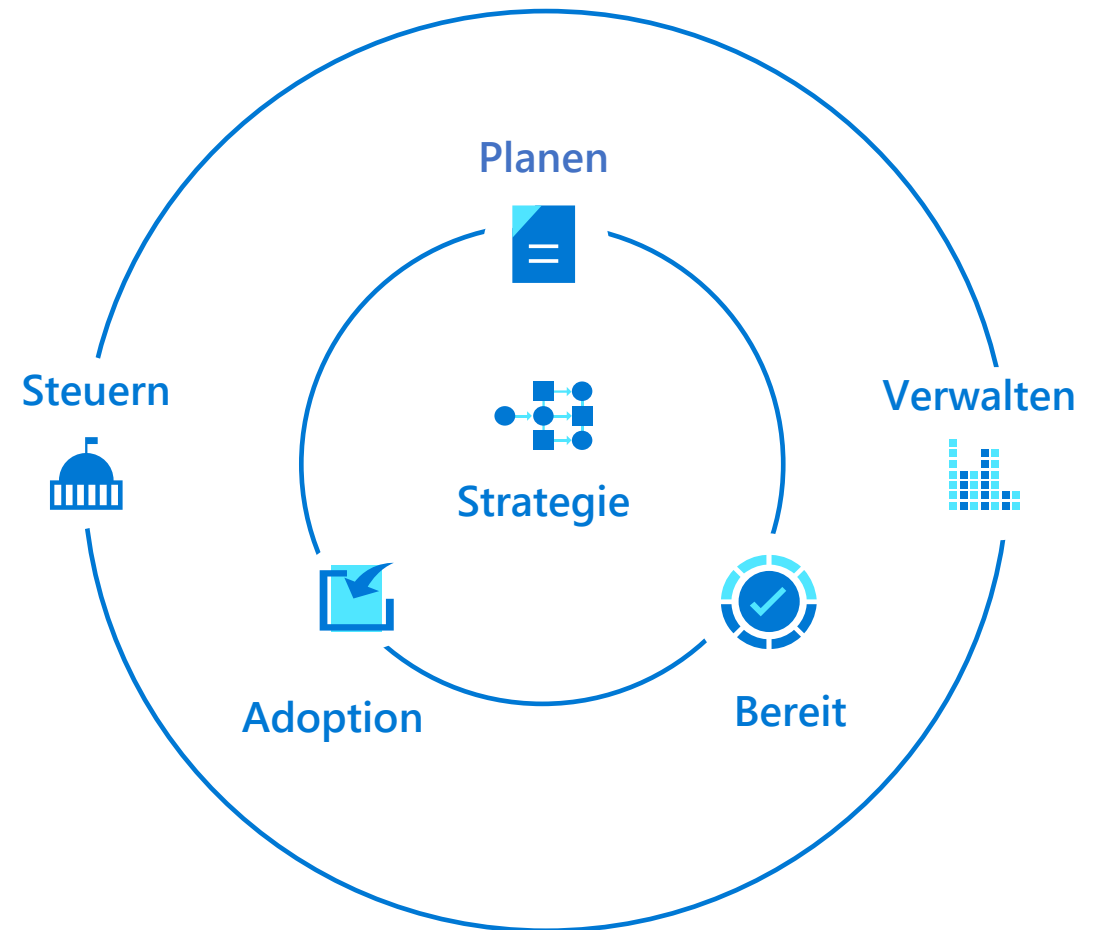
Compliance, Kontrolle und Sicherheit



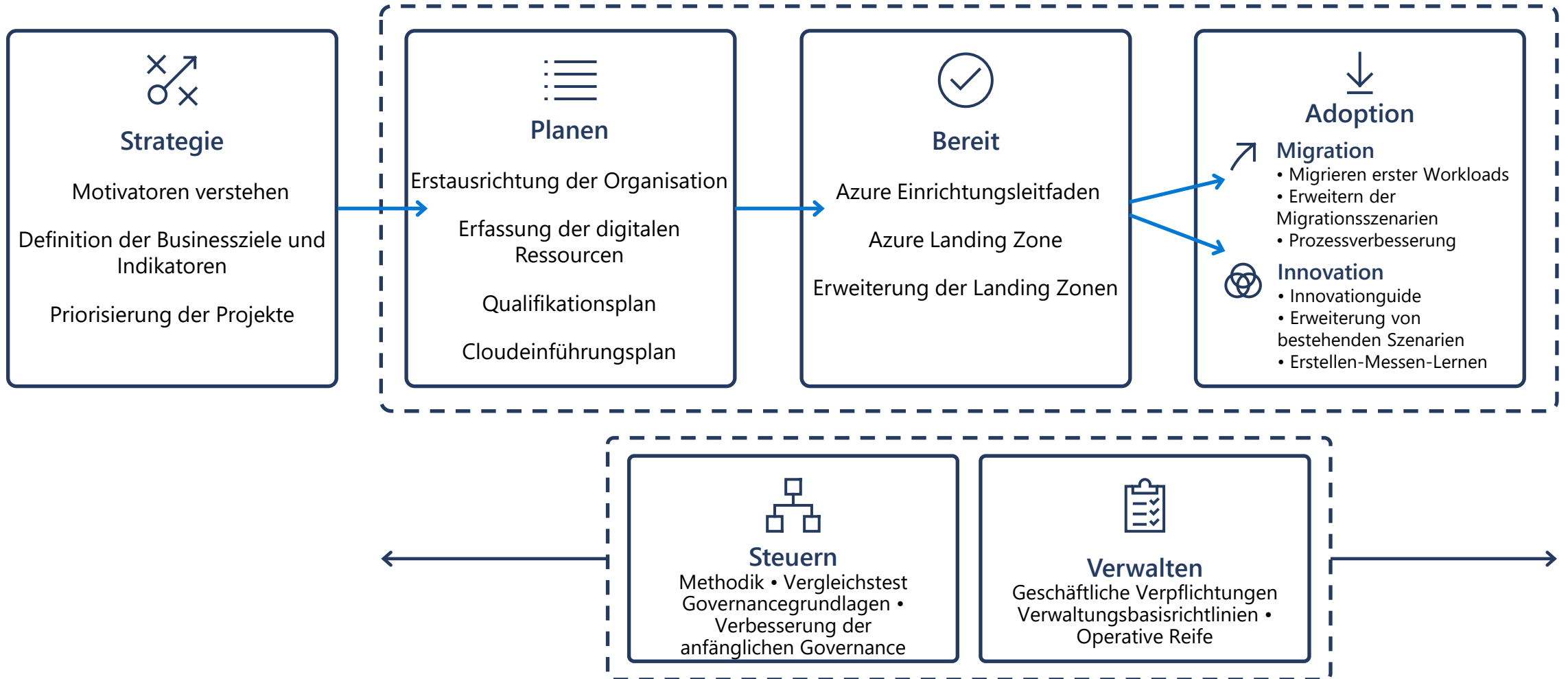
## Verwalten

Betrieb und Optimierung

Ein iterativer Ansatz  
abgestimmt auf  
Geschäftsziele und -  
bedarfe

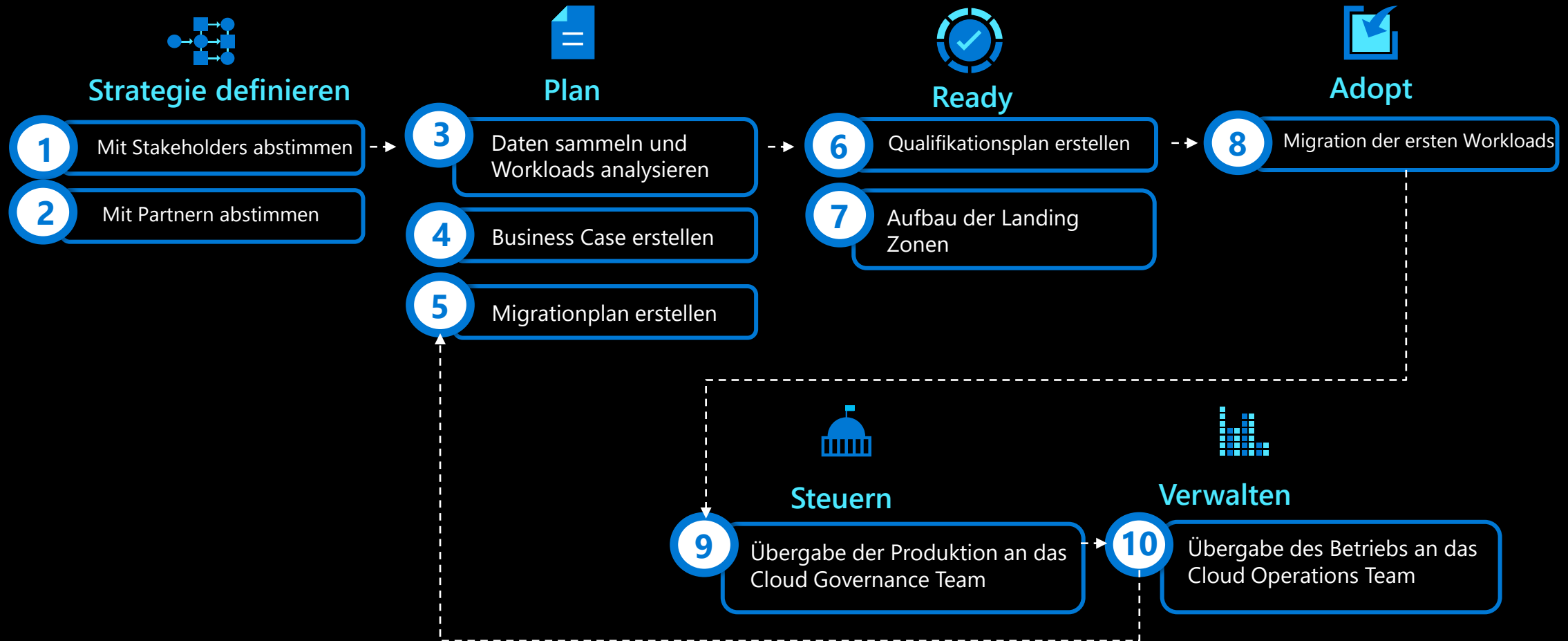


# Microsoft Cloud Adoption Framework for Azure





# Migration bestehender Workloads

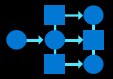


[aka.ms/adopt/getstarted-migrate](https://aka.ms/adopt/getstarted-migrate)



# Tools, Templates, und Assessments

# Tools, templates und Assessments



## Strategie

- [Cloud journey tracker](#)
- [Business outcome template](#)



## Planen

- [Azure DevOps demo generator](#)
- [Cloud adoption plan template](#)



## Bereit

- [Azure setup guide](#)
- [Readiness checklist](#)
- [Naming and tagging tracking template](#)
- [Landing zone blueprints](#)



## Adoption

- [Strategic migration assessment and readiness tool \(SMART\)](#)
- [Azure migration guide](#)
- [Azure innovation guide](#)



## Steuern

- [Governance benchmark](#)
- [Governance process template](#)
- [Cost Management process template](#)
- [Deployment acceleration process template](#)
- [Identity process template](#)
- [Resource consistency process template](#)
- [Security baseline process template](#)




## Verwalten

- [Microsoft Azure Well-Architected Review](#)
- [Best practices source code](#)
- [Operations management workbook](#)

Coffee break...

05:00

mins:  secs:  type:    
 Breaktime for PowerPoint by Flow Simulation Ltd. Pin controls when stopped

# Landing Zones



# Was möchtest du aufbauen?



Haus



Stadion



Brücke

# Das Fundament ist NICHT gleich



Haus



Stadion



Brücke

# Landingzonen

Landingzonen unterstützen Kunden beim **Errichten ihrer Azure-Umgebung** für Skalierung, Sicherheit, Governance, Netzwerk und Identität.



# Überlegungen beim Erstellen einer Landezone

## HOSTING

Compute

Netzwerk

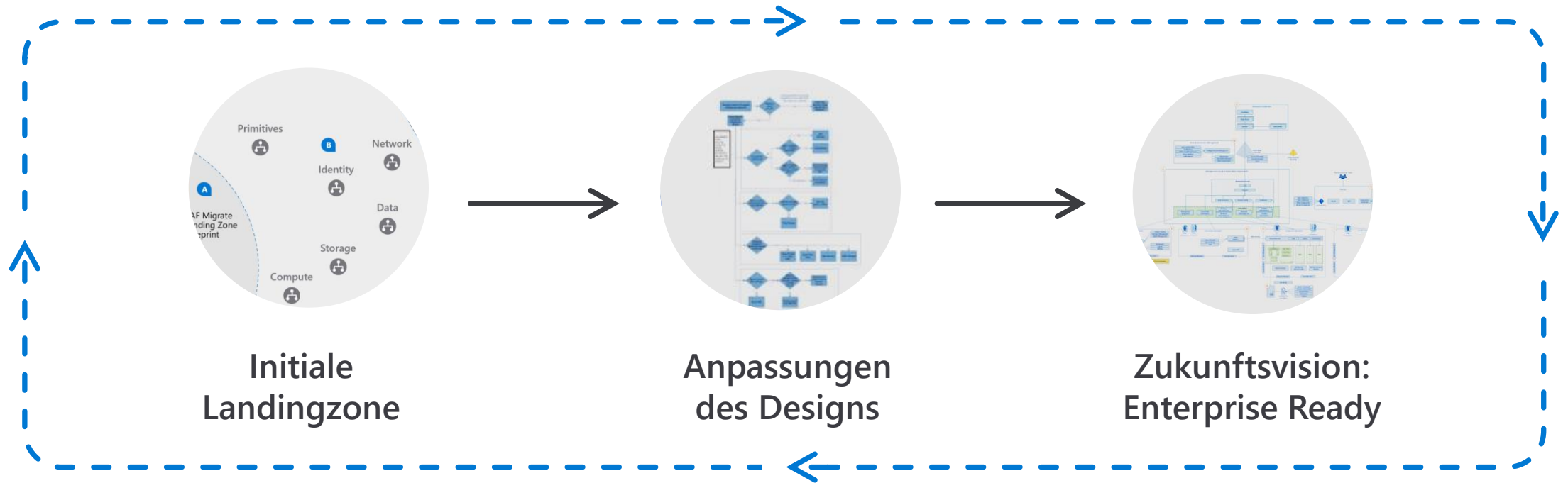
Speicher

Daten

AZURE FUNDAMENT  
Managementgruppen  
Resourcengruppen  
Namensstandards  
Subscriptiondesign

GOVERNANCE  
Kosten  
Monitoring  
Identitäten  
Richtlinien

# Evolution von Landingzonen



# Was sind Azure Landing Zones?

(\*bekannt als Enterprise-Scale Ansatz)

# Metropolis

*In einer Analogie ähnelt dies der Frage, wie Wasser, Gas und Strom zugänglich sind, bevor neue Gebäude erbaut werden. In Azure sind das Netzwerk, IAM, Richtlinien, Management und Monitoring gemeinsam genutzte "Utility"-Dienste, die leicht verfügbar sein müssen, um den Anwendungsmigrationsprozess zu optimieren.*



# Azure Landing Zones?

**ALZ** ist ein **Architektur Approach** und eine **Referenzimplementierung**, die eine effektive **Konstruktion** und **Operationalisierung** von Landezonen in Azure ermöglicht, die skaliert und auf die **Azure Roadmap** und das **Microsoft Cloud Adoption Framework for Azure** abgestimmt ist.

**Maßgebend**

**Bewährt**

**Vorschreibend**

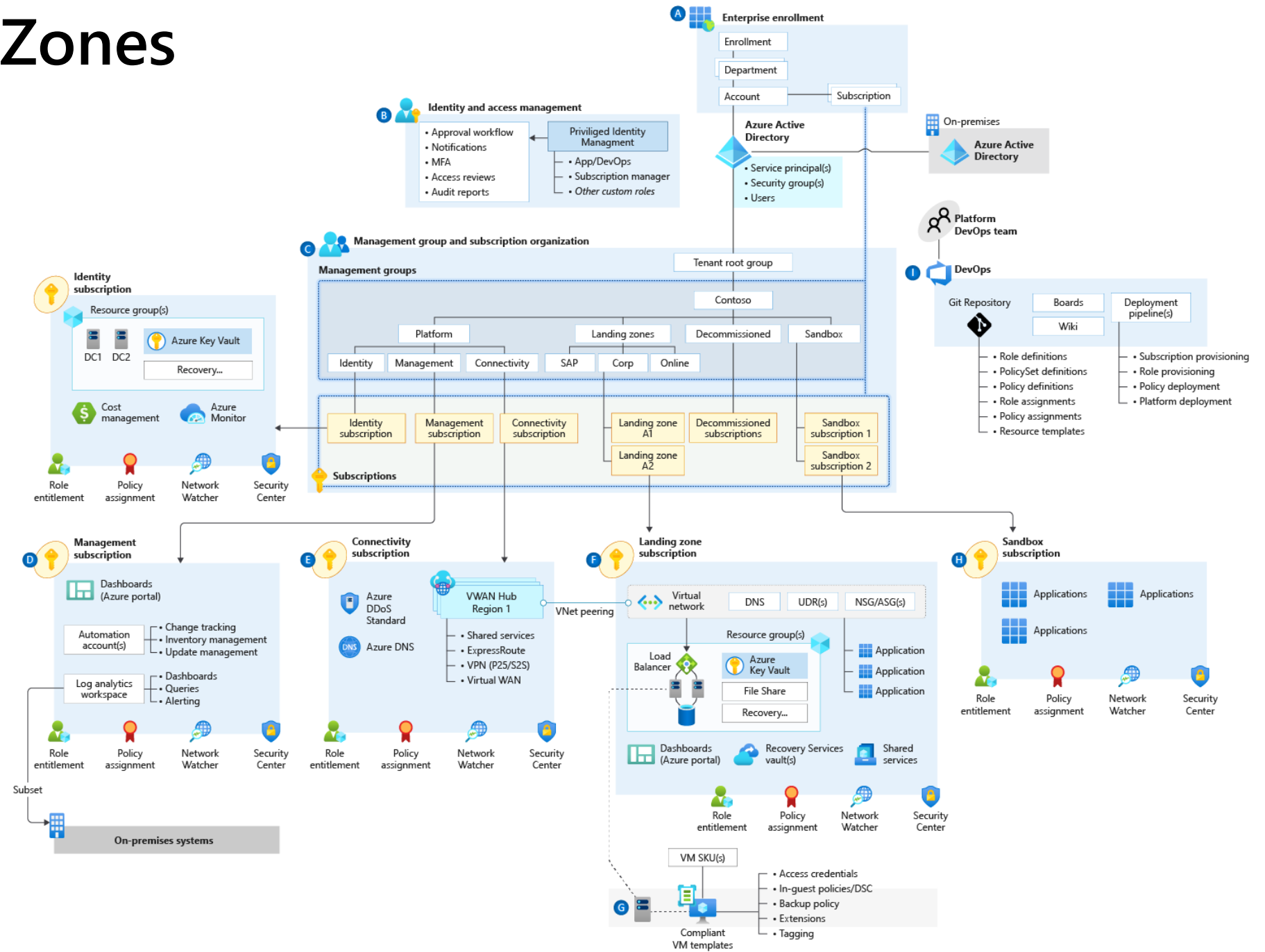
## Architektur:

- Azure Landing Zone Designprinzipien
- Azure Landing Zone Designrichtlinien
- Azure Landing Zone Implementierungsguide

## Referenzimplementierung:

- Azure Landing Zone Grundlagendienste
- Azure Landing Zone Landezonen

# Azure Landing Zones



# Designprinzipien der Azure Landing Zones



Subscription Demokratisierung



Richtliniengestützte Governance



Einheitliche Kontroll- & Verwaltungsebene



Applikationszentrisch & Archetyp-Neutral



Azure Natives Design & Ausrichtung an  
Plattform Roadmap

# Designrichtlinien



# Designrichtlinien der Azure Landing Zones



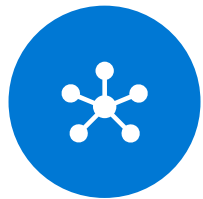
Enterprise Enrollment &  
Azure AD Tenants



Identitäts- &  
Zugriffsverwaltung



Management Group &  
Subscriptionorganisation



Netzwerktopologie &  
Anbindung



Management &  
Monitoring



Businesskontinuität &  
Notfallwiederherstellung



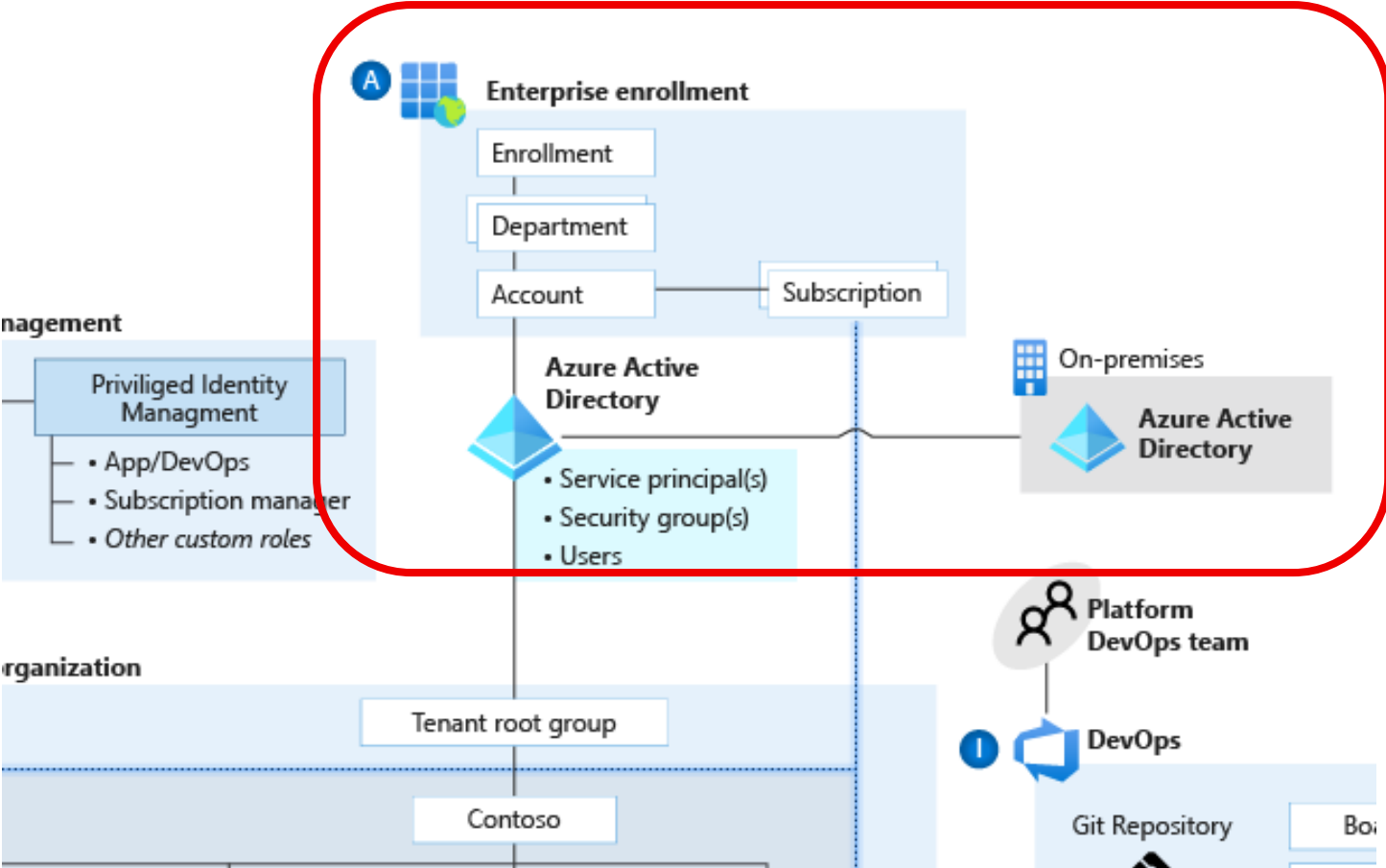
Sicherheit, Governance &  
Compliance



Plattformautomatisierung  
& DevOps



# Definition der Enrollment & Azure AD Struktur





# EA Portal

Enrollment Department Account Subscription

Enrollment Department Account Subscription

Enrollment Department Account Subscription

Enrollment Department Account Subscription

Test Enrollment (Direct) [User Icon]

Test Enrollment (Direct) [User Icon]

Test Enrollment (Direct) [User Icon]

Test Enrollment (Direct) [User Icon]

Subscriptions

All Departments All Accounts  Active Search + Add Subscription Refresh Subscription View My Subscriptions

Subscription Name	Subscription GUID	Start Date	Status	Account	Cost Center
Multi Factor	01302cdf-b781-4136-9996-3a205dab9bbd	3/17/2015	Active	1-MAEP Test3	
Pay-As-You-Go(Converte...	0269cb22-2799-44eb-a410-f1674b4ad47a	3/10/2015	Active	test123	
Azure Promotional Offer...	03107ee0-0754-4b7d-9458-1c4f446d4cc6	2/27/2015	Active	Andrew Hwangbo	
Microsoft Azure Enterprise	03edf0b1-e493-4239-9b52-68ca4a7cbba4	2/18/2015	Active	Open Test	
Microsoft Azure Enterprise	04b1ab26-9889-4dff-8372-adf1a2fba022	9/23/2015	Active	1-MAEP Test3	
Microsoft Azure Enterprise	072ae617-3793-4709-878a-19f9c2bf14ec	9/24/2015	Active	1-MAEP Test3	
Microsoft Azure Enterpris...	09c065c7-910f-4289-af23-7df395135930	4/1/2015	Active	Smoke Test	
Microsoft Azure Enterprise	09c2b1d7-3325-4be2-bfe6-94872bcded1c	9/30/2015	Active	1-MAEP Test3	

Cost Center

Save Cancel

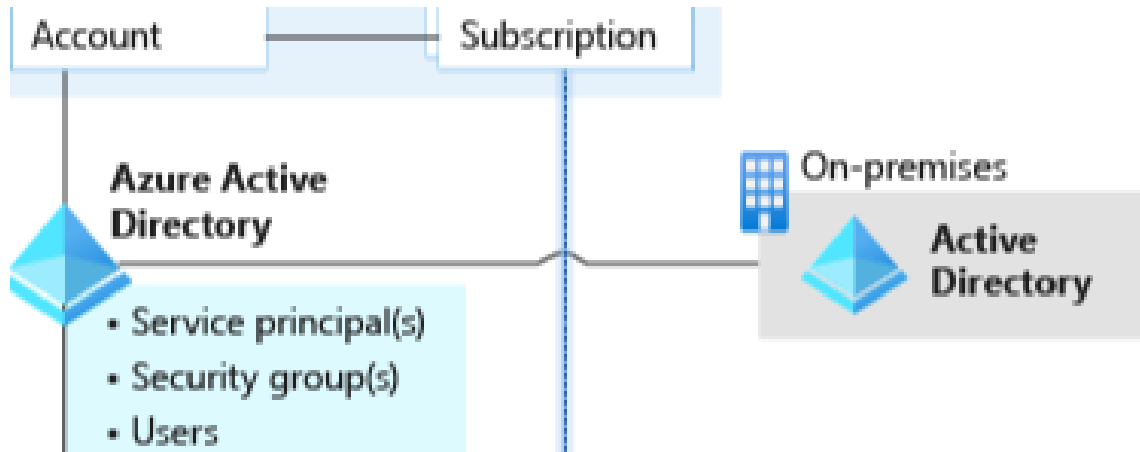
Support English © 2015 Microsoft Trademarks Privacy & Cookies Terms of Use Microsoft

+ Add Administrator

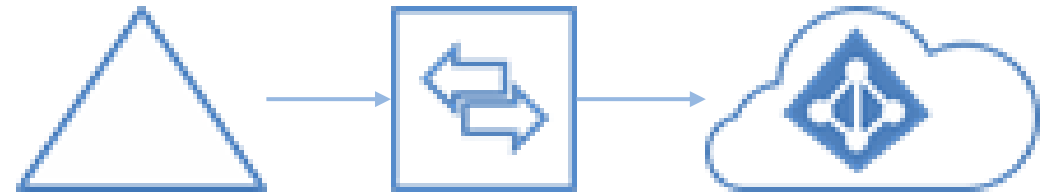
ookies Terms of Use Microsoft



# Tenants



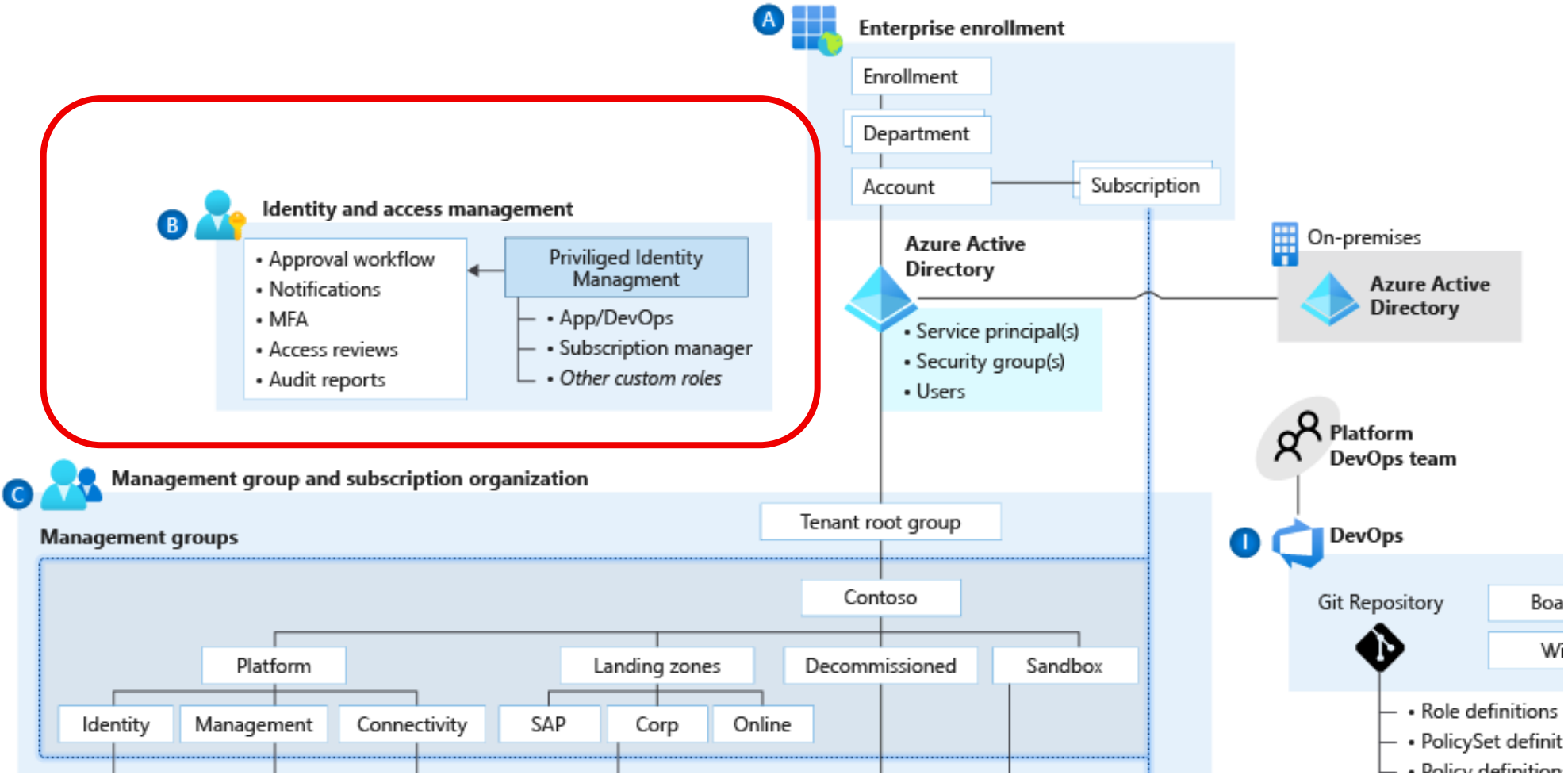
Cloud-only strategy – only one AAD



Hybrid strategy – On-prem and AAD

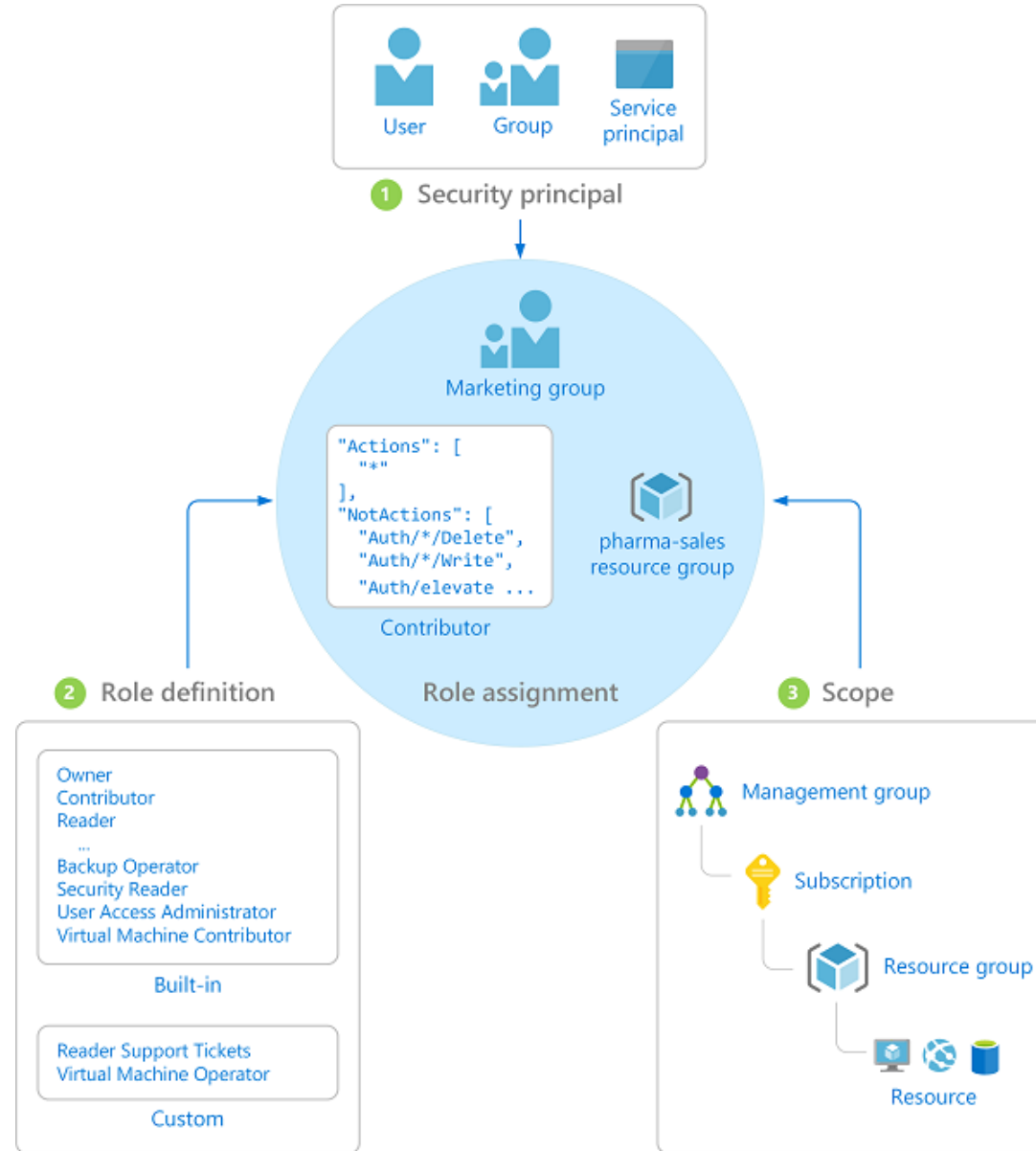


# Identitäts- & Zugriffs- Management





# Rollenzuweisung über RBAC





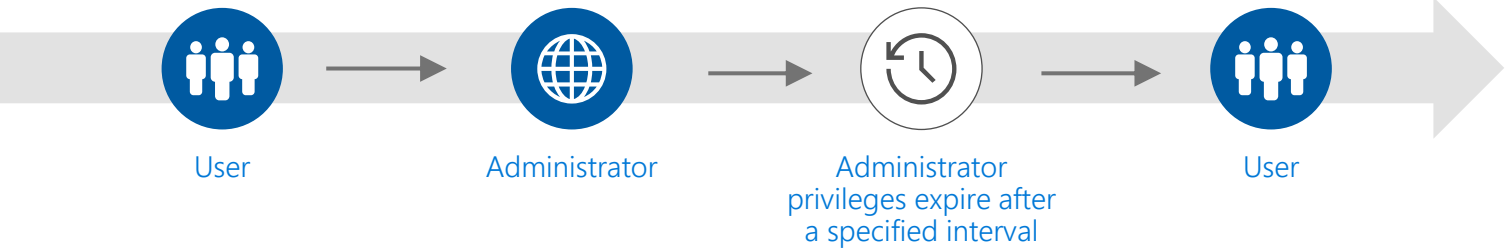
# IAM – Autorisierung Rollendefinitionen:

Rolle	Nutzung	Actions	Not Actions
<b>Azure platform owner</b>	Management group and subscription lifecycle management	*	
<b>Network management (NetOps)</b>	Platform-wide global connectivity management: Virtual networks, UDRs, NSGs, NVAs, VPN, Azure ExpressRoute, and others	*/read, Microsoft.Network/vpnGateways/*, Microsoft.Network/expressRouteCircuits/*, Microsoft.Network/routeTables/write, Microsoft.Network/vpnSites/*	
<b>Security operations (SecOps)</b>	Security administrator role with a horizontal view across the entire Azure estate and the Azure Key Vault purge policy	*/read, */register/action, Microsoft.KeyVault/locations/deletedVaults/purge/action, Microsoft.Insights/alertRules/*, Microsoft.Authorization/policyDefinitions/*, Microsoft.Authorization/policyAssignments/*, Microsoft.Authorization/policySetDefinitions/*, Microsoft.PolicyInsights/*, Microsoft.Security/*	
<b>Subscription owner</b>	Delegated role for subscription owner derived from subscription Owner role	*	Microsoft.Authorization/*/*write, Microsoft.Network/vpnGateways/*, Microsoft.Network/expressRouteCircuits/*, Microsoft.Network/routeTables/write, Microsoft.Network/vpnSites/*
<b>Application owners (DevOps/AppOps)</b>	Contributor role granted for application/operations team at resource group level	*	Microsoft.Authorization/*/*write, Microsoft.Network/publicIPAddresses/write, Microsoft.Network/virtualNetworks/write, Microsoft.KeyVault/locations/deletedVaults/purge/action



# IAM – Autorisierung Privileged Identity Management:

Discover, restrict, and monitor privileged identities

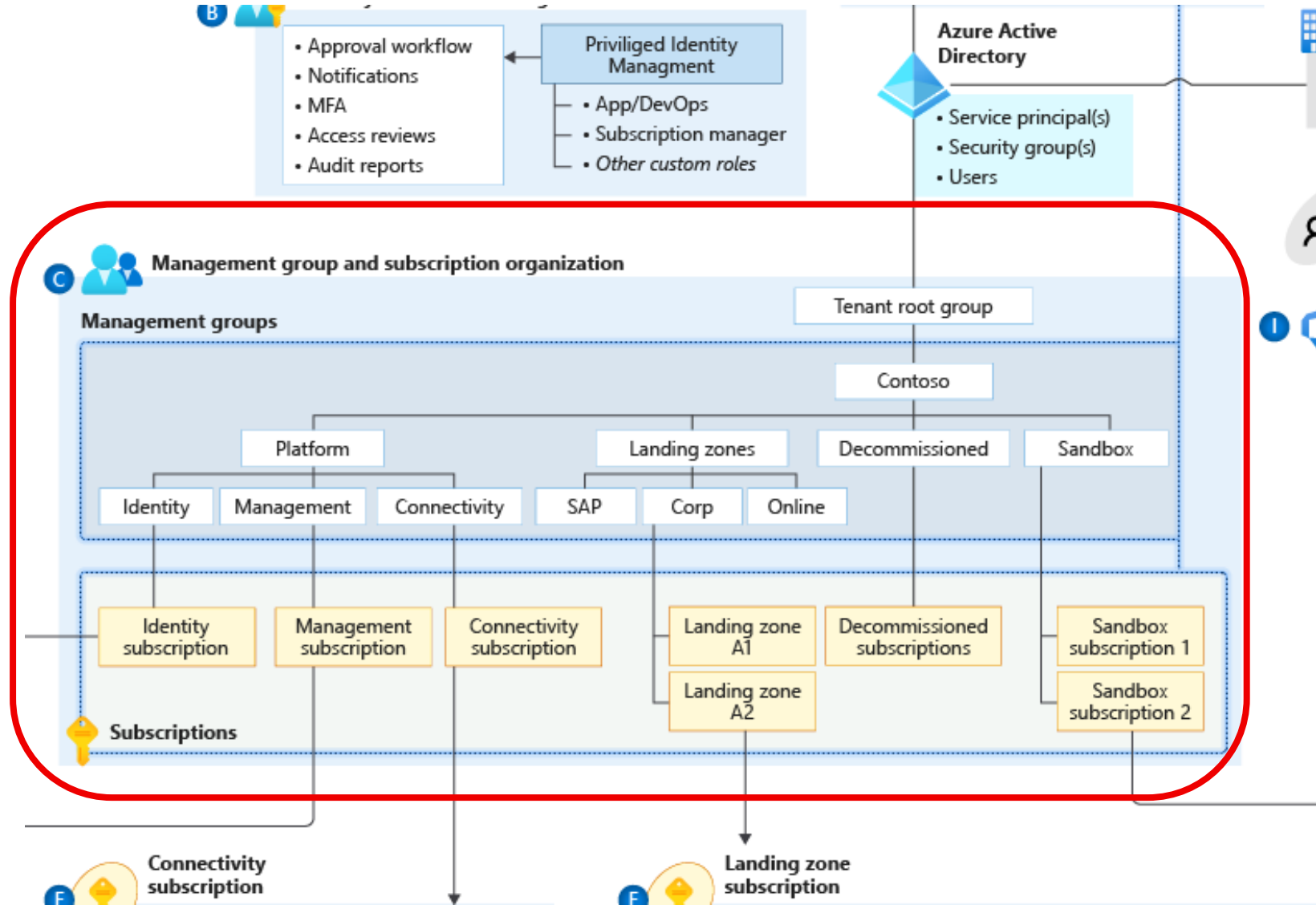


A large magnifying glass graphic is positioned over a dashboard screenshot. The dashboard includes a 'Refresh' button at the top. Below it is an 'Activity' section with 'Security alerts' and 'ACTIVE ALERTS'. A prominent '3 Alerts' indicator is shown with a warning icon. Two alert messages are visible: 'Weak authentication is configured for role activ...' and 'Redundant administrators increase your attack...'. Below the alerts is a 'Role summary' section and a 'Roles' section with a link 'VIEW ALL USER...'. The magnifying glass is surrounded by a shield icon on the left, an open padlock icon at the top right, and a magnifying glass icon at the bottom right.



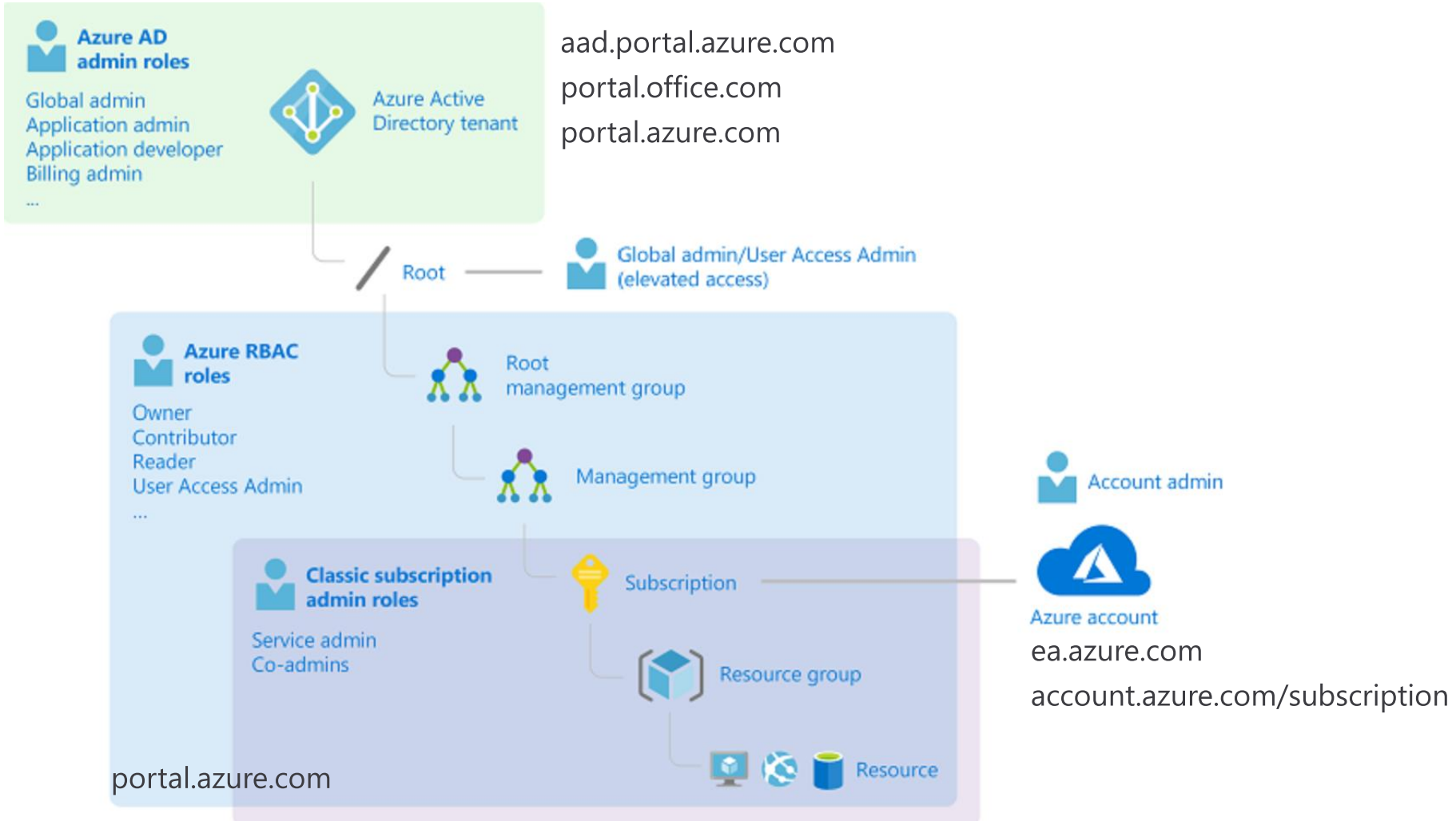


# Management Group & Subscription- organisation





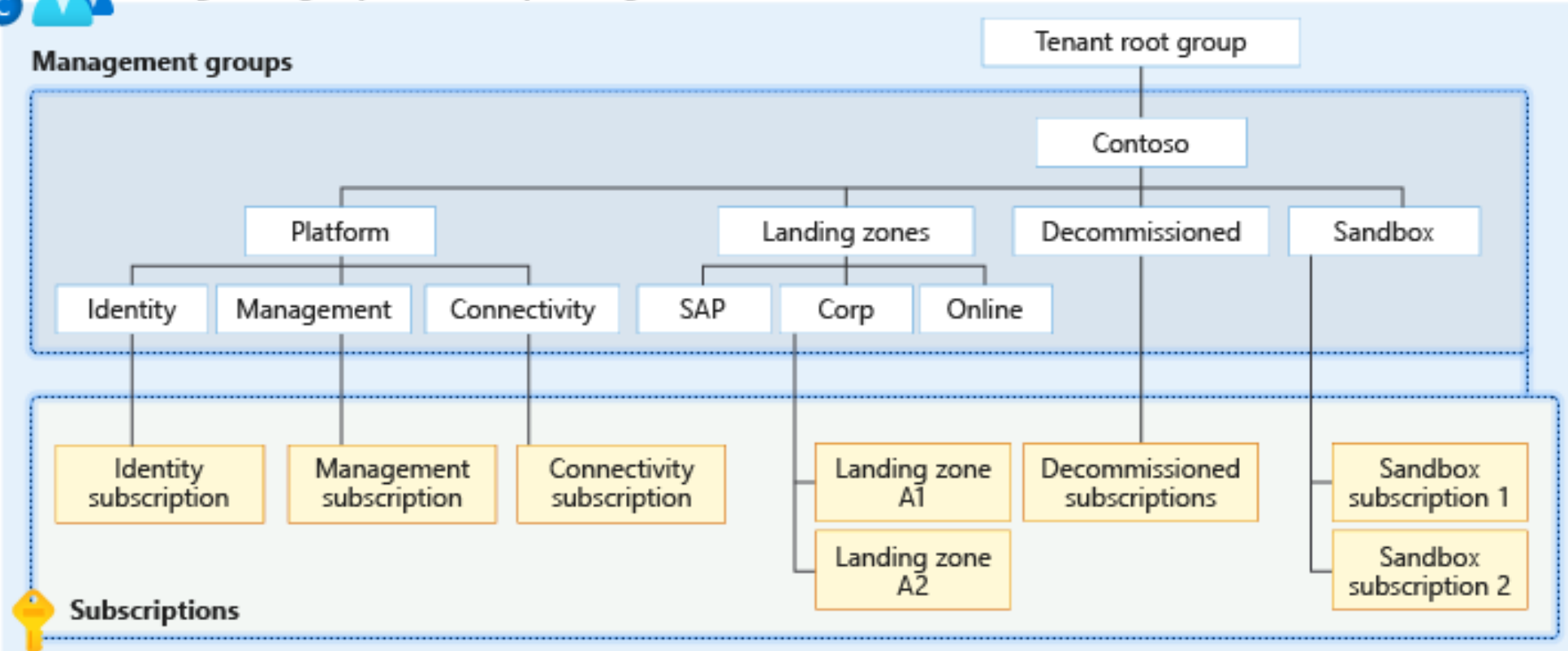
# Management Group & Azure Active Directory





# Management Group Hierarchy

## Management group and subscription organization



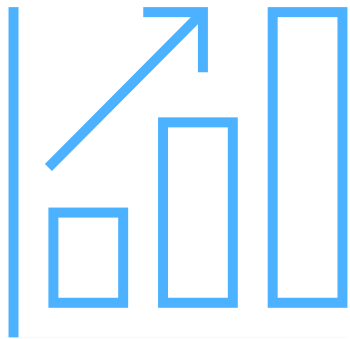
Tenant Root Group [\(details\)](#) → Settings

- Hierarchy settings
- Deployments

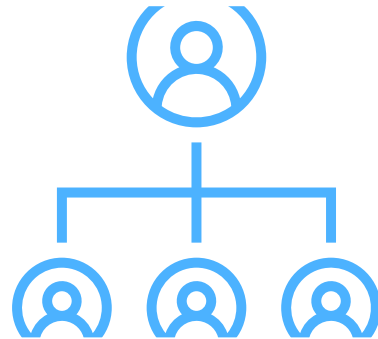


# Subscription Organization & Governance Empfehlungen

## Wann soll eine neue Subscription angelegt werden?



Scale Limits



Management boundary



Policy boundary



Networking Topology

## Wer ist Verantwortlich?

Subscription Owner: Kosten, Nutzung der Ressourcen, Policy Compliance & Betrieb



## Subscription Limits

Resource	Limit
Subscriptions per Azure Active Directory tenant	Unlimited
<a href="#">Resource groups</a> per subscription	980
Tags per subscription	50
Unique tag calculations per subscription	10,000
<a href="#">Subscription-level deployments</a> per location	800
Number of storage accounts per region per subscription, including standard, and premium storage accounts.	250
Maximum storage account capacity	5 PiB
Load balancers	1,000
VM total cores per <a href="#">subscription</a> for Enterprise Agreement	350 per region. Contact support to increase limit.
... there are a lot more!	

[Azure subscription limits and quotas - Azure Resource Manager | Microsoft Docs](#)



# Subscription Quota & Capacity – Verbrauch im Portal

Events

## Cost Management

Cost analysis

Cost alerts

Budgets

Advisor recommendations

## Billing

Invoices

Partner information

## Settings

Programmatic deployment

Resource groups

Resources

Preview features

**Usage + quotas**

Request Quota Increase Refresh

You can use each Microsoft Azure resource up to its quota. Each subscription has separate quotas and usage is tracked per subscription. If you reach a quota cap, you can request an increase via Help + Support. [Learn more](#)

Request

Search All service quotas All providers All locations Show all

Showing 1 to 100 of 4227 records.

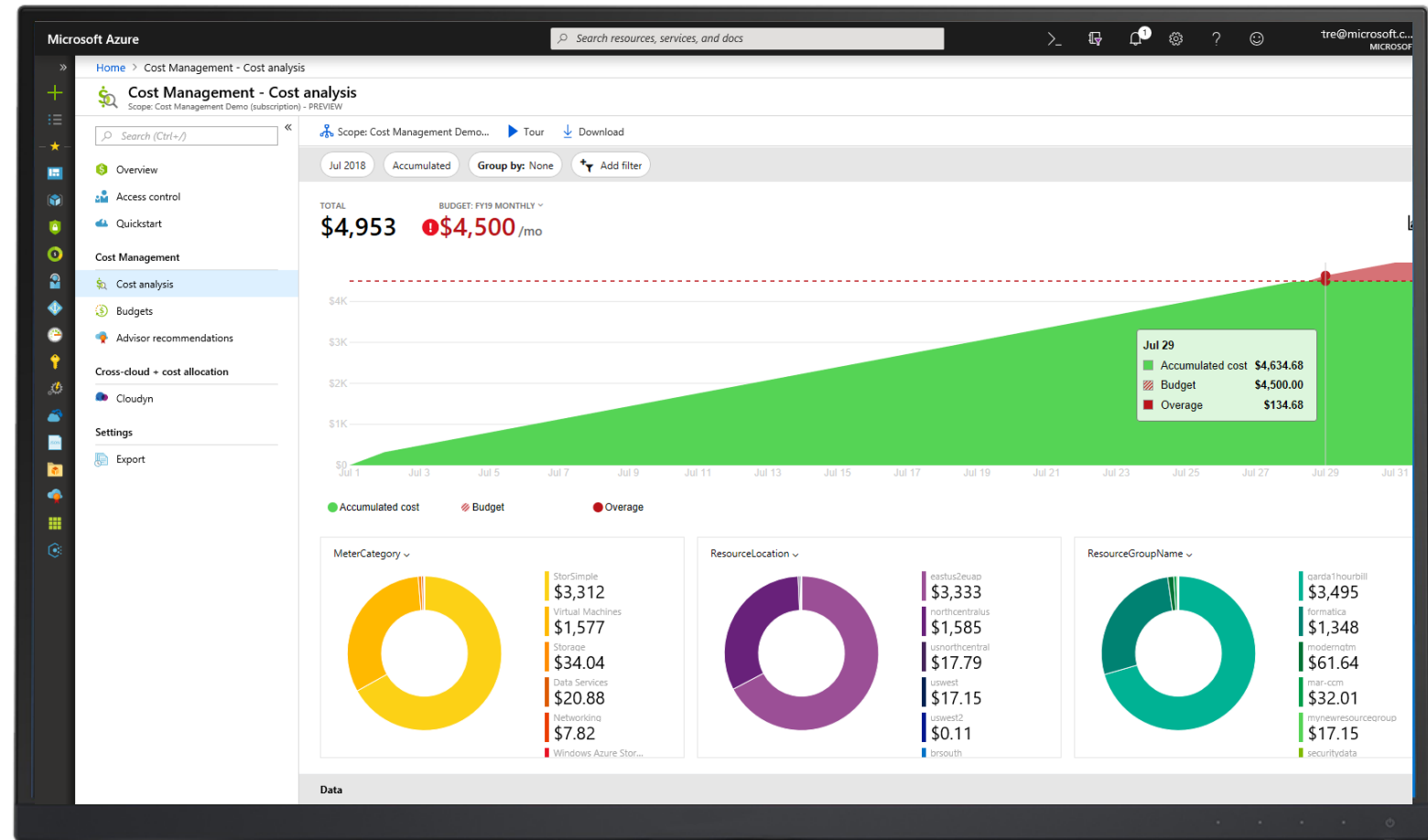
No grouping

Quota ↑↓	Provider ↑↓	Location ↑↓	Usage ↑↓
Network Watchers	Microsoft.Network	West Europe	100%
Total Regional vCPUs	Microsoft.Compute	West Europe	2%
Standard Dsv3 Family vCPUs	Microsoft.Compute	West Europe	2%
Storage Accounts	Microsoft.Storage	West Europe	0%
Virtual Networks	Microsoft.Network	West Europe	0%
Public IP Addresses	Microsoft.Network	West Europe	0%
Network Security Groups	Microsoft.Network	West Europe	0%
Virtual Machines	Microsoft.Compute	West Europe	0%
Network Interfaces	Microsoft.Network	West Europe	0%
StandardSSDStorageDisk	Microsoft.Compute	West Europe	0%



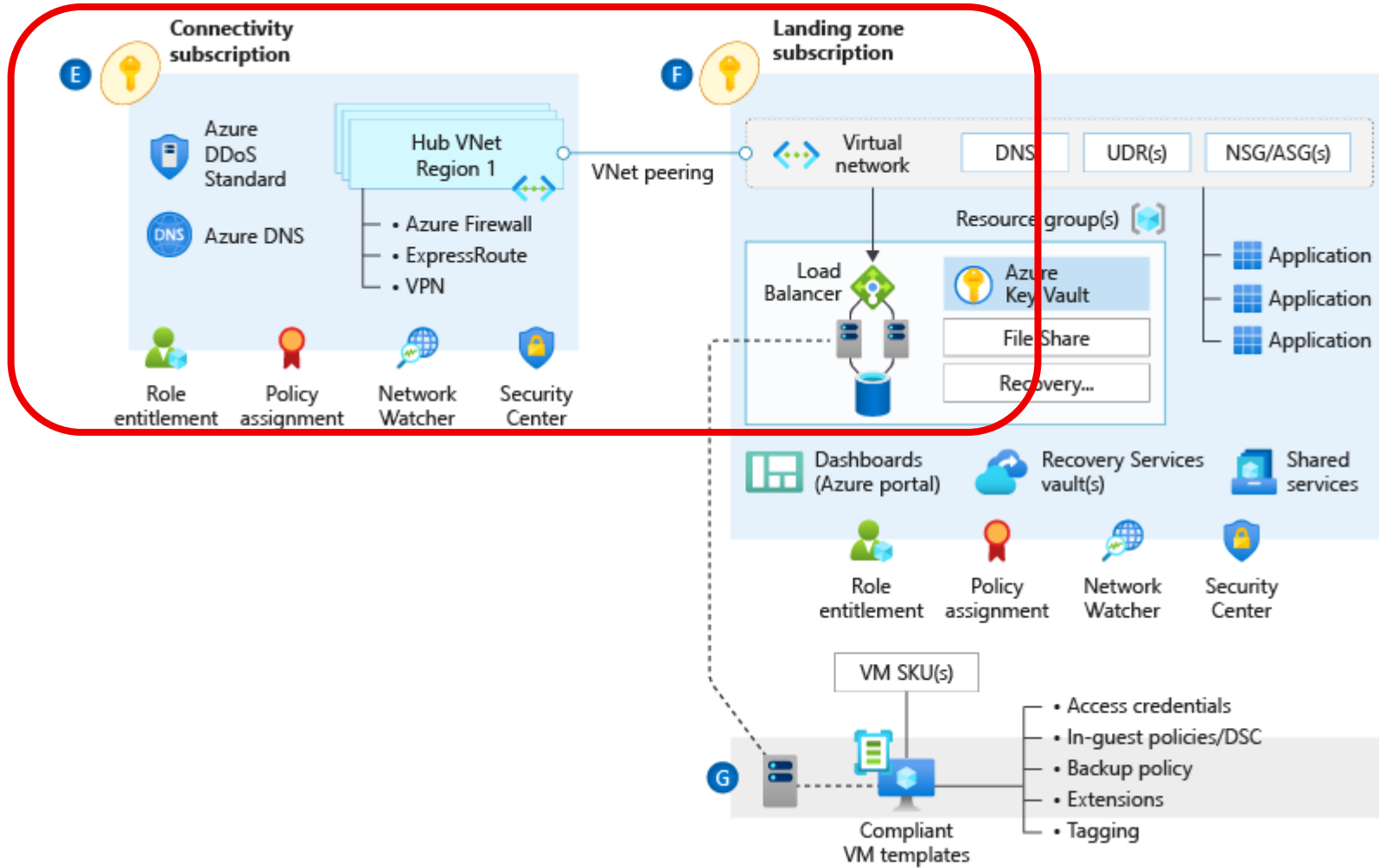
# Cost Management

## Wie schaffe ich Kostentransparenz & Kostenverrechnung?





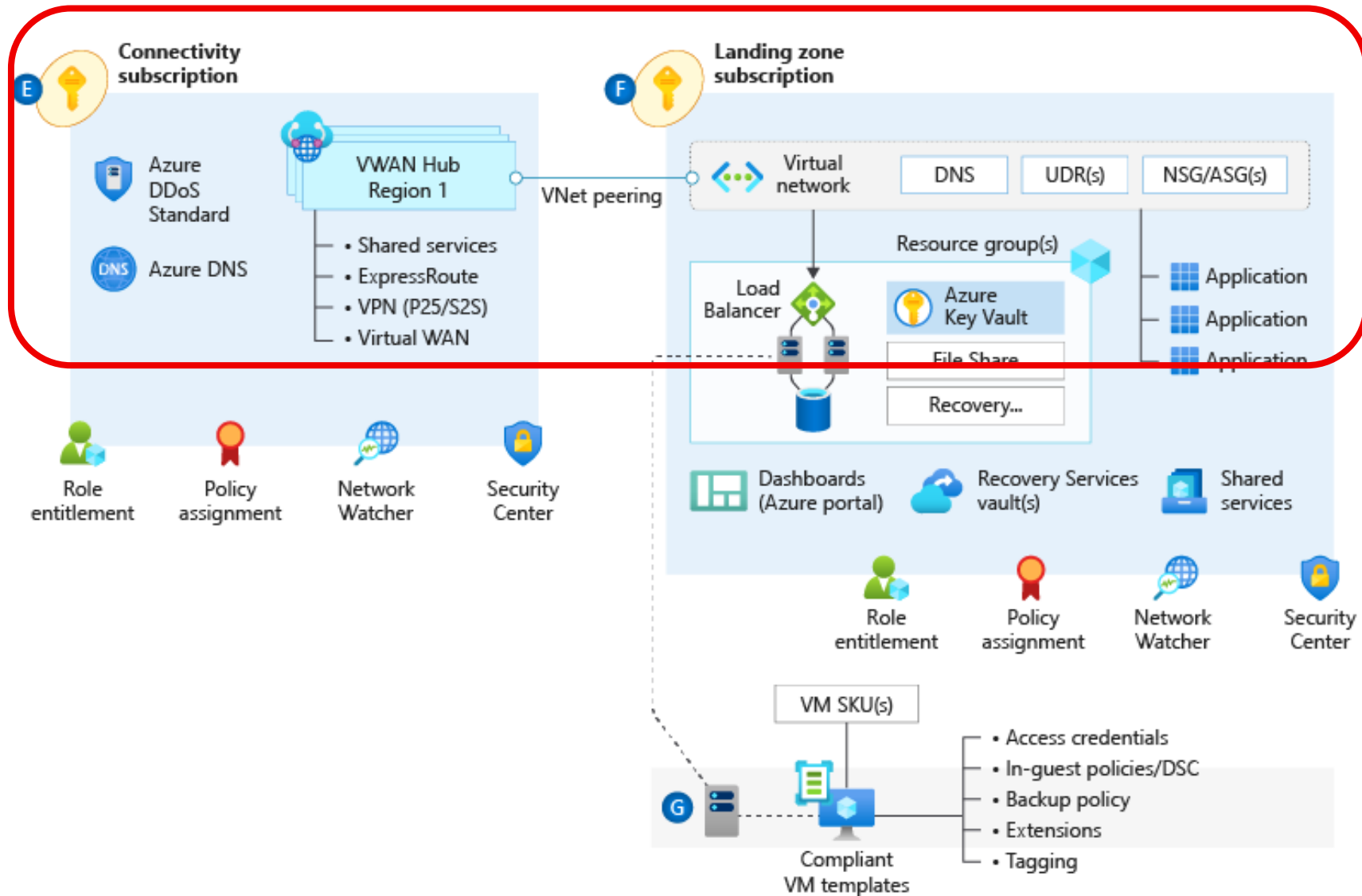
# Netzwerktopologie – Hub and Spoke

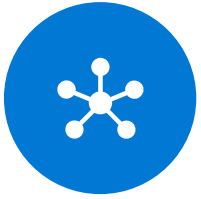




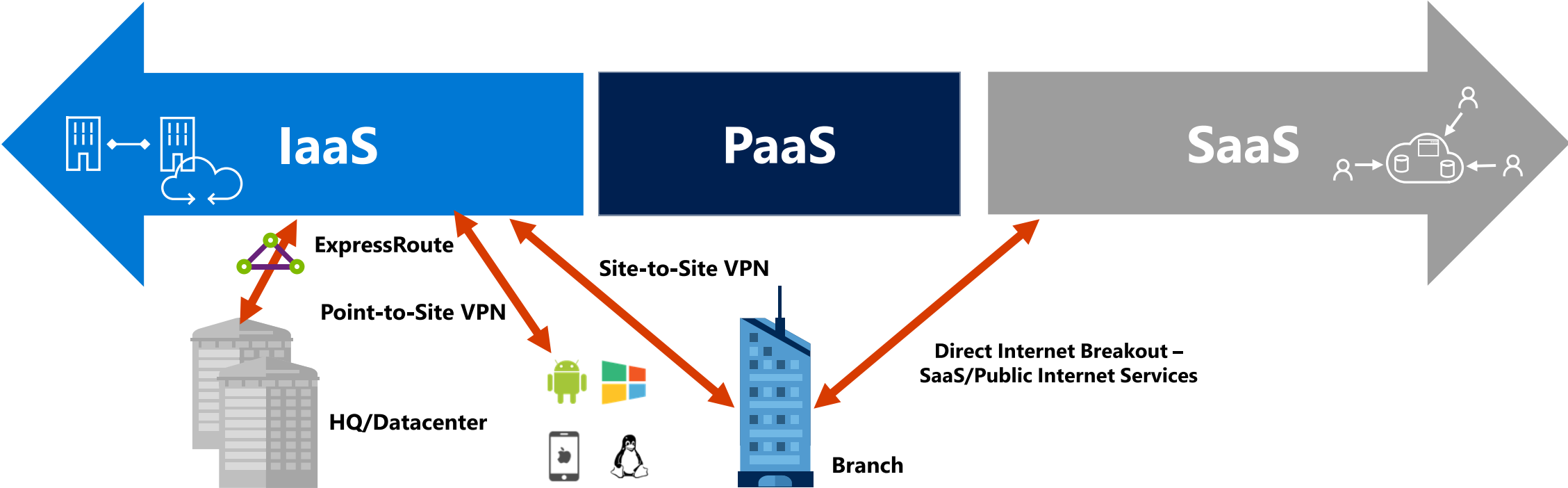


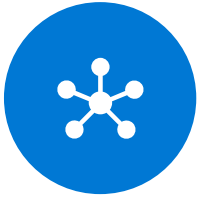
# Netzwerktopologie – virtual WAN





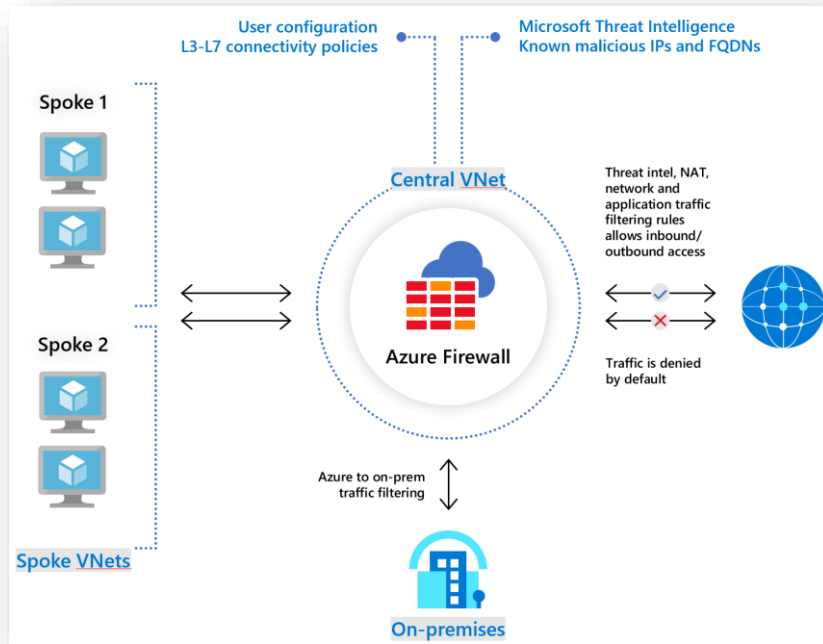
# Netzwerkanbindung



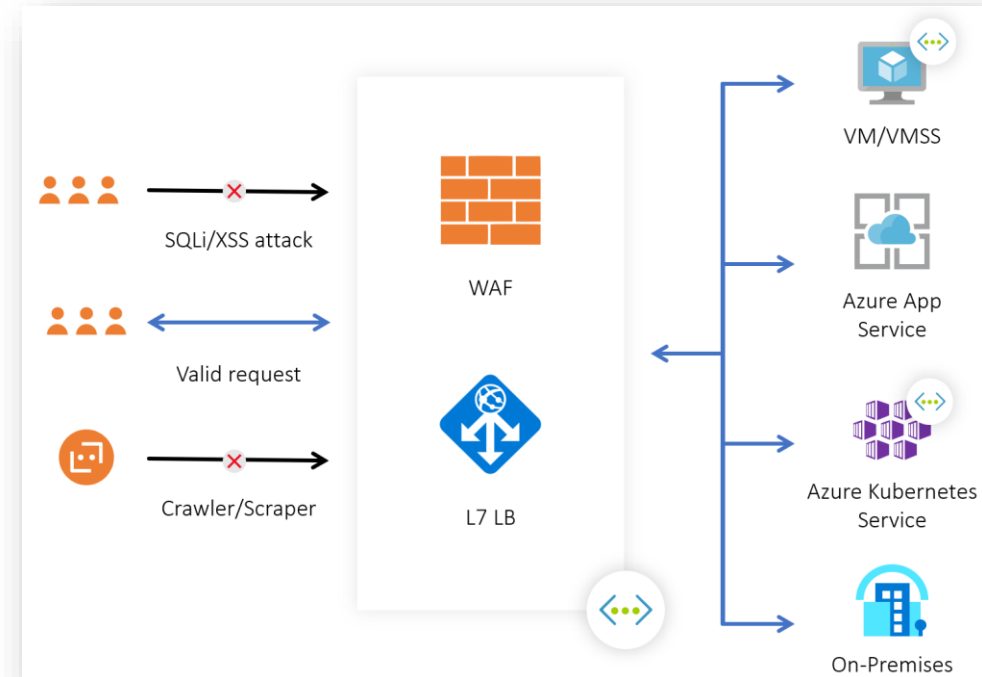


# Netzwerkabsicherung

## Azure Firewall

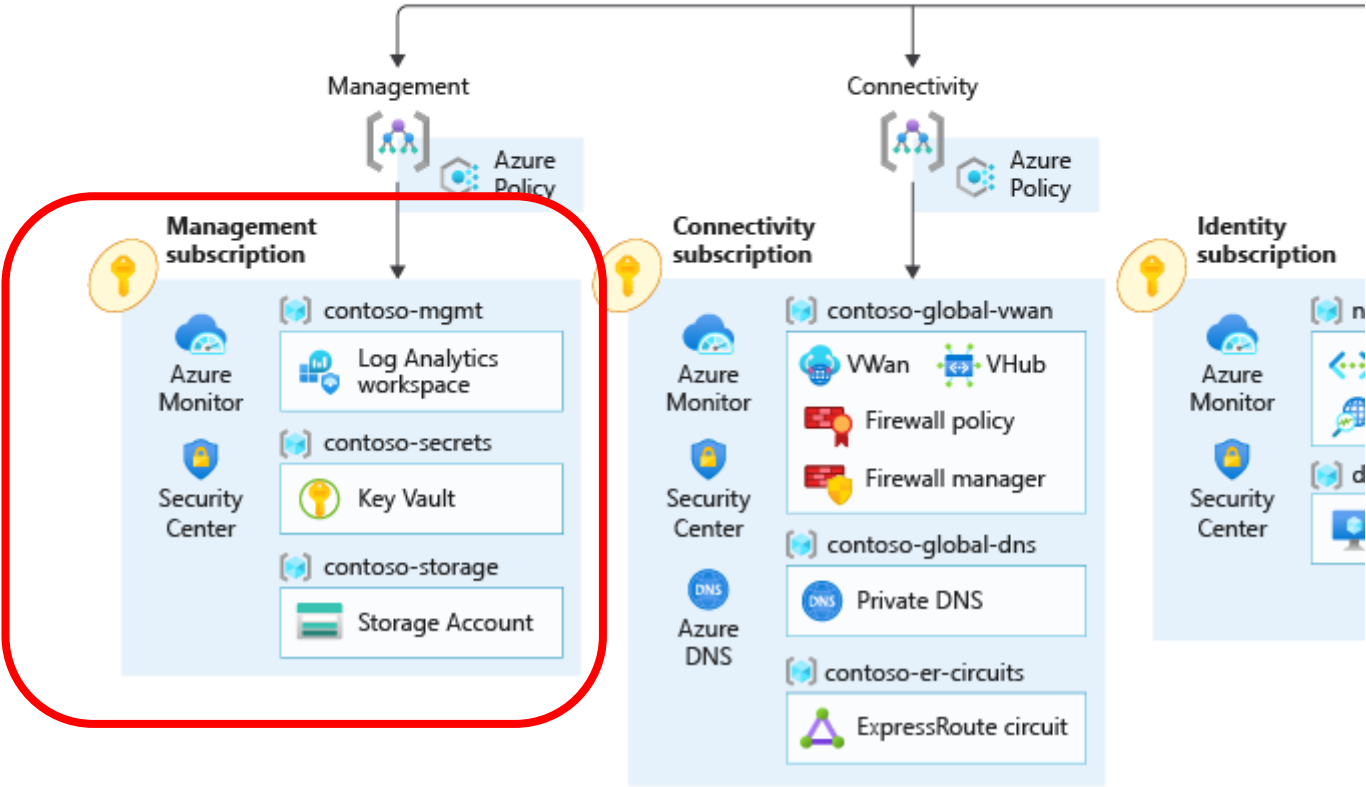


## Web Application Firewall





# Management & Monitoring





# Azure Policies

Home > Management groups > ES1 > ES1-platform > ES1-management >

## Policy | Definitions

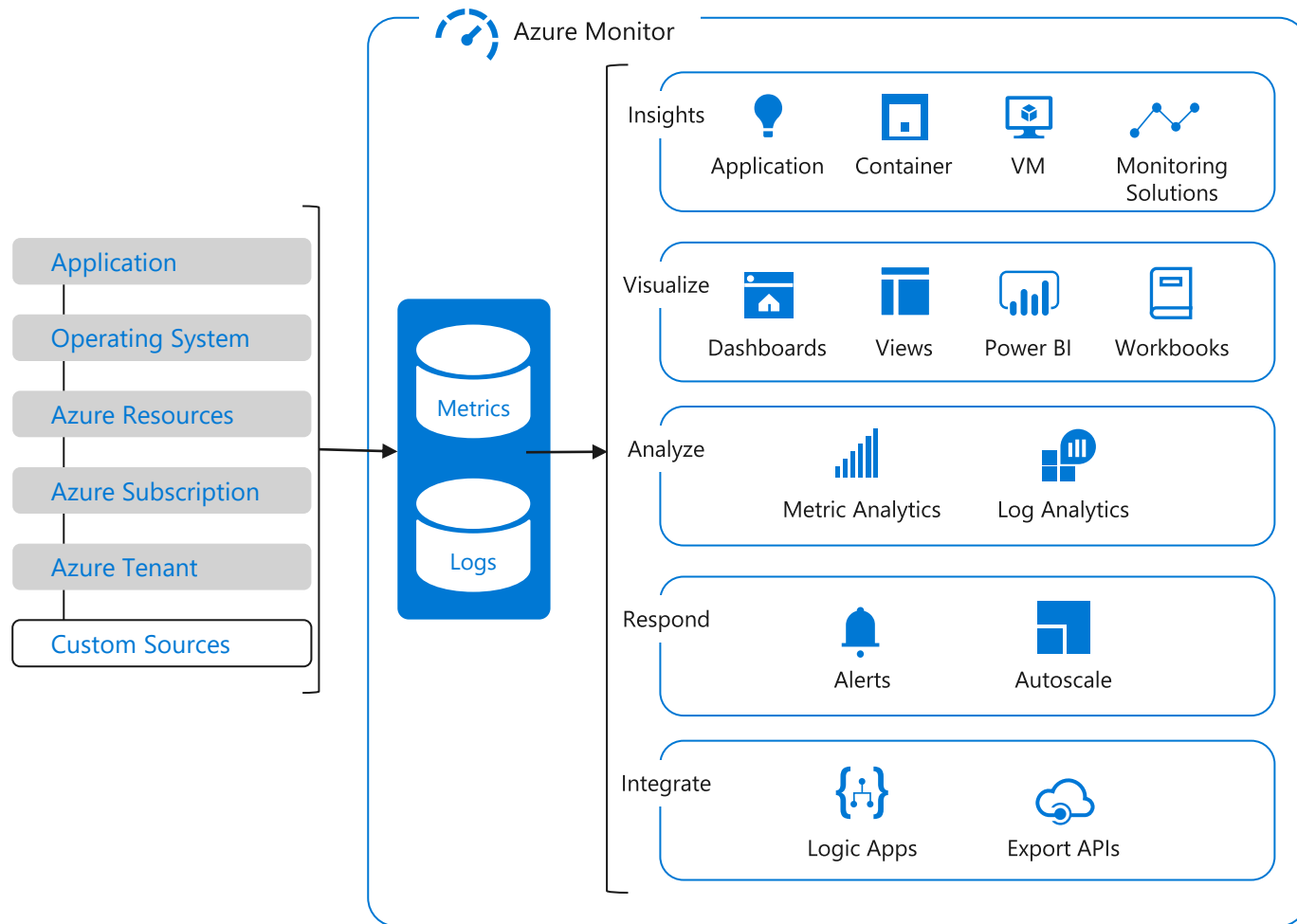
Search (Ctrl+/) << + Initiative definition + Policy definition Refresh

Scope: ES1-management Definition type: All definition types Type: All types Category: All categories

Name	↑↓ Definition location	↑↓ Policies	↑↓ Type	↑↓ Definition type
<a href="#">Deny-Public-Endpoints-for-PaaS-Services</a>	ES1	8	Custom	Initiative
<a href="#">Deploy-Diag-LogAnalytics</a>	ES1	49	Custom	Initiative
<a href="#">Deploy-Sql-Security</a>	ES1	4	Custom	Initiative
<a href="#">Append-KV-SoftDelete</a>	ES1		Custom	Policy
<a href="#">Deny-AppGW-Without-WAF</a>	ES1		Custom	Policy
<a href="#">Deny-ERPeeing</a>	ES1		Custom	Policy
<a href="#">Deny-PublicEndpoint-Aks</a>	ES1		Custom	Policy
<a href="#">Deny-PublicEndpoint-CosmosDB</a>	ES1		Custom	Policy
<a href="#">Deny-PublicEndpoint-KeyVault</a>	ES1		Custom	Policy
<a href="#">Deny-PublicEndpoint-MariaDB</a>	ES1		Custom	Policy

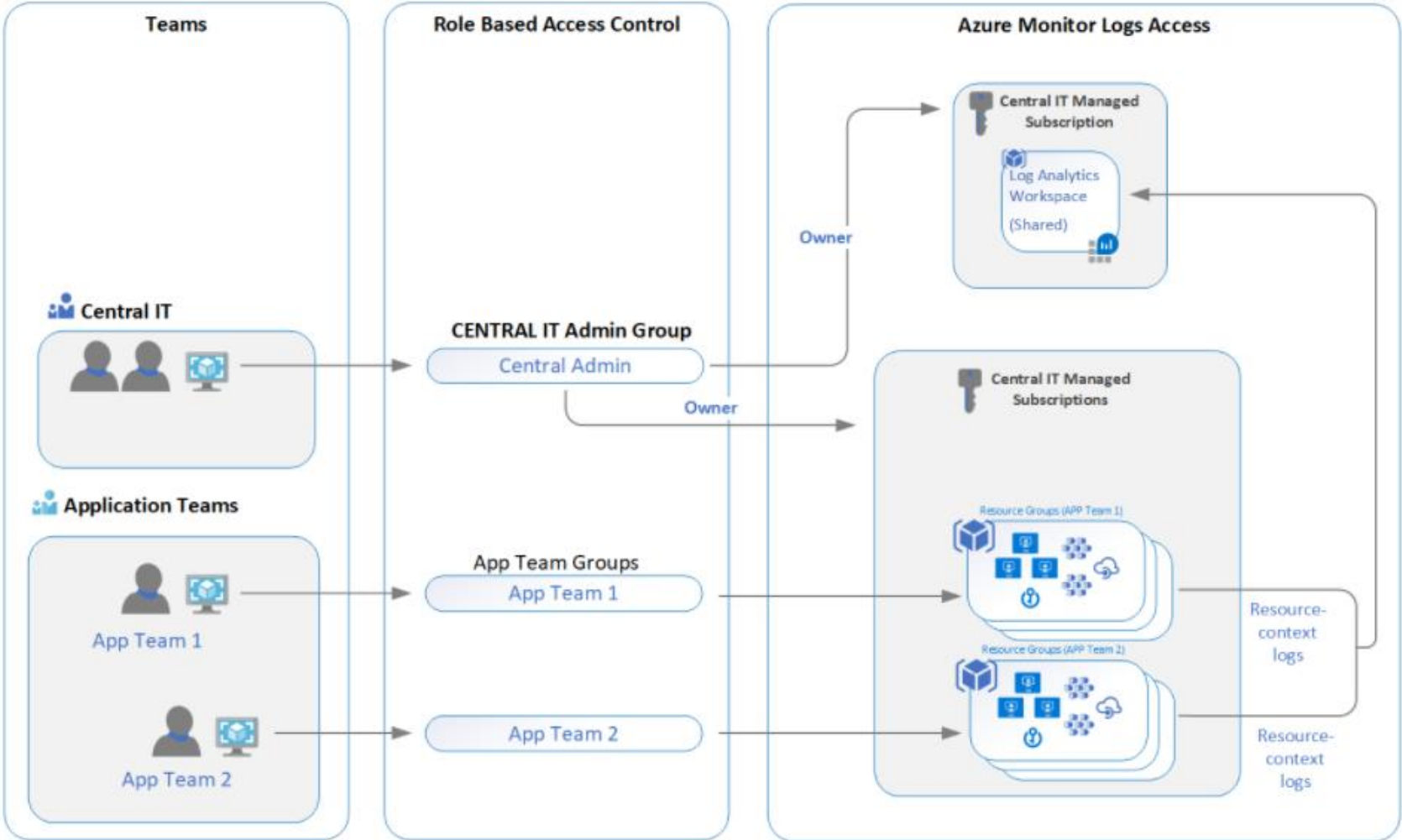


# Azure Monitor



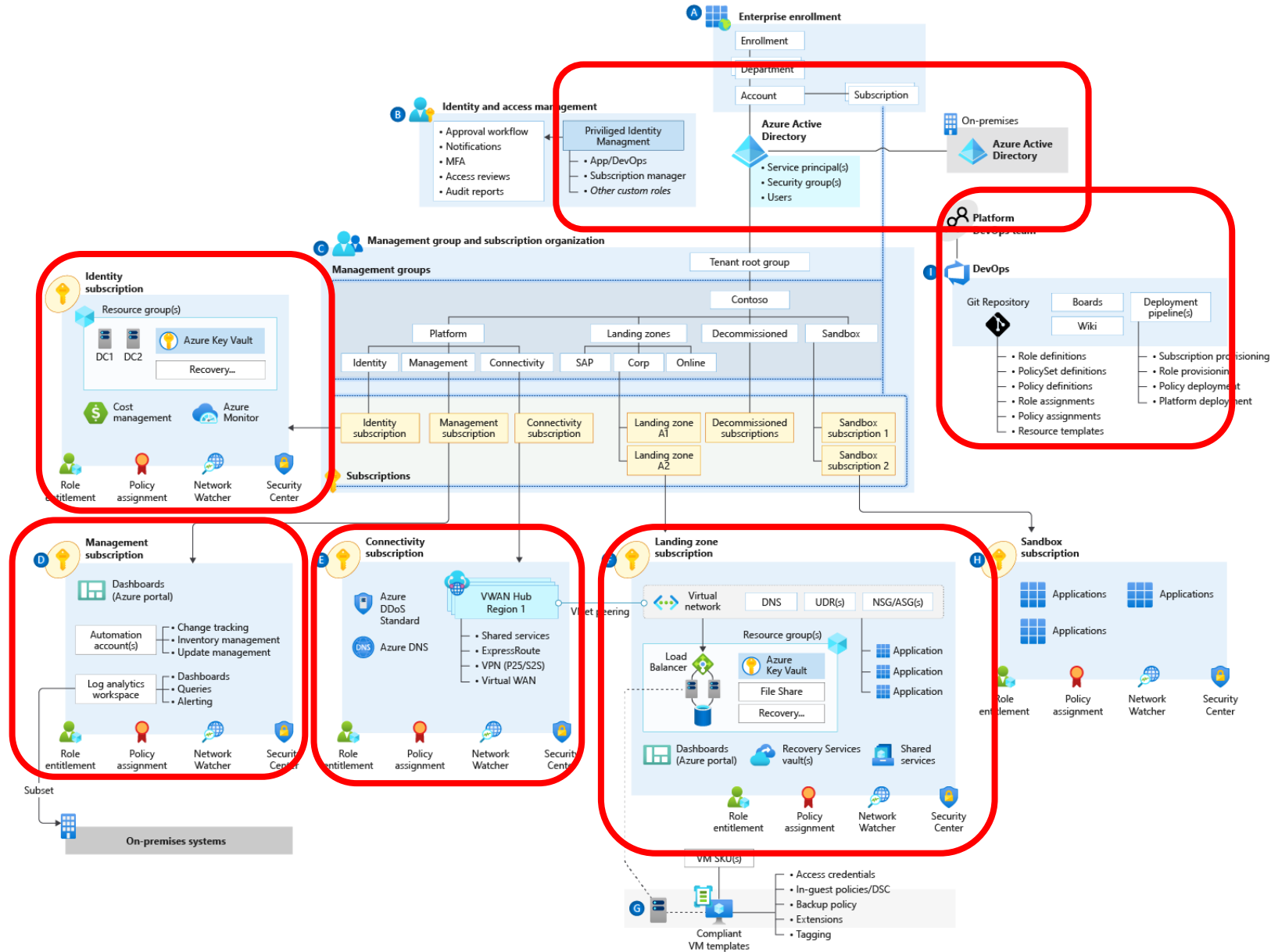


# Log Analytics Workspace





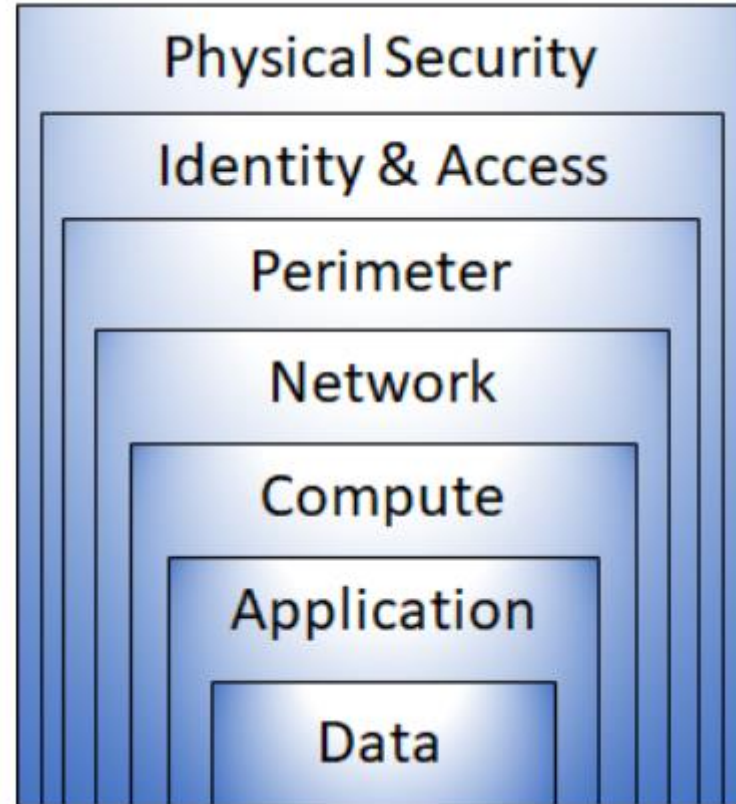
# Sicherheit, Governance & Compliance







# Sicherheit





# Geteilte Verantwortung zwischen Cloudanbieter & Kunde

Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Customer	Customer	Shared	Shared
Application	Customer	Customer	Shared	Microsoft
Network controls	Customer	Customer	Shared	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

■ Microsoft   ■ Customer



# Security Benchmark & regulatorische Compliance

## Azure Security Center



Strengthen multi cloud  
security posture

Secure  
Score

Policies and  
compliance

Improved  
automation



Leveraging  
Azure Arc



Protect your hybrid cloud  
with Azure Defender

For  
servers

For cloud native  
workloads

For databases  
and storage

For Azure  
service layers

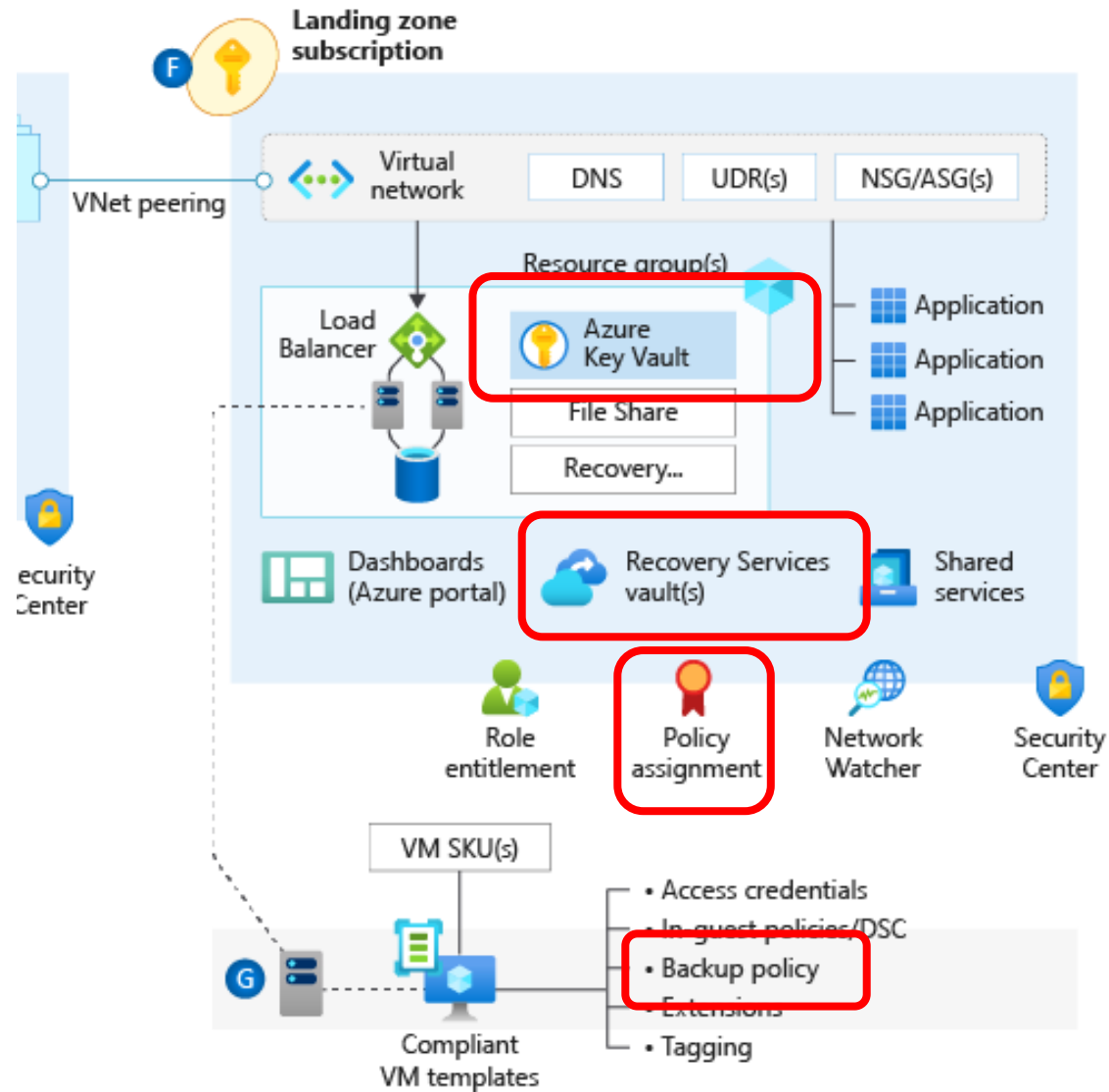
For IoT  
devices



Streamline security management



# Businesskontinuität & Notfallwiederherstellung





# Workload RTO und RPO Anforderungen

**RTO** – Recover Time Objective

Wie schnell muss der Service wieder verfügbar sein?

**RPO** – Recover Point Objective

Wie viel Datenverlust ist akzeptabel?

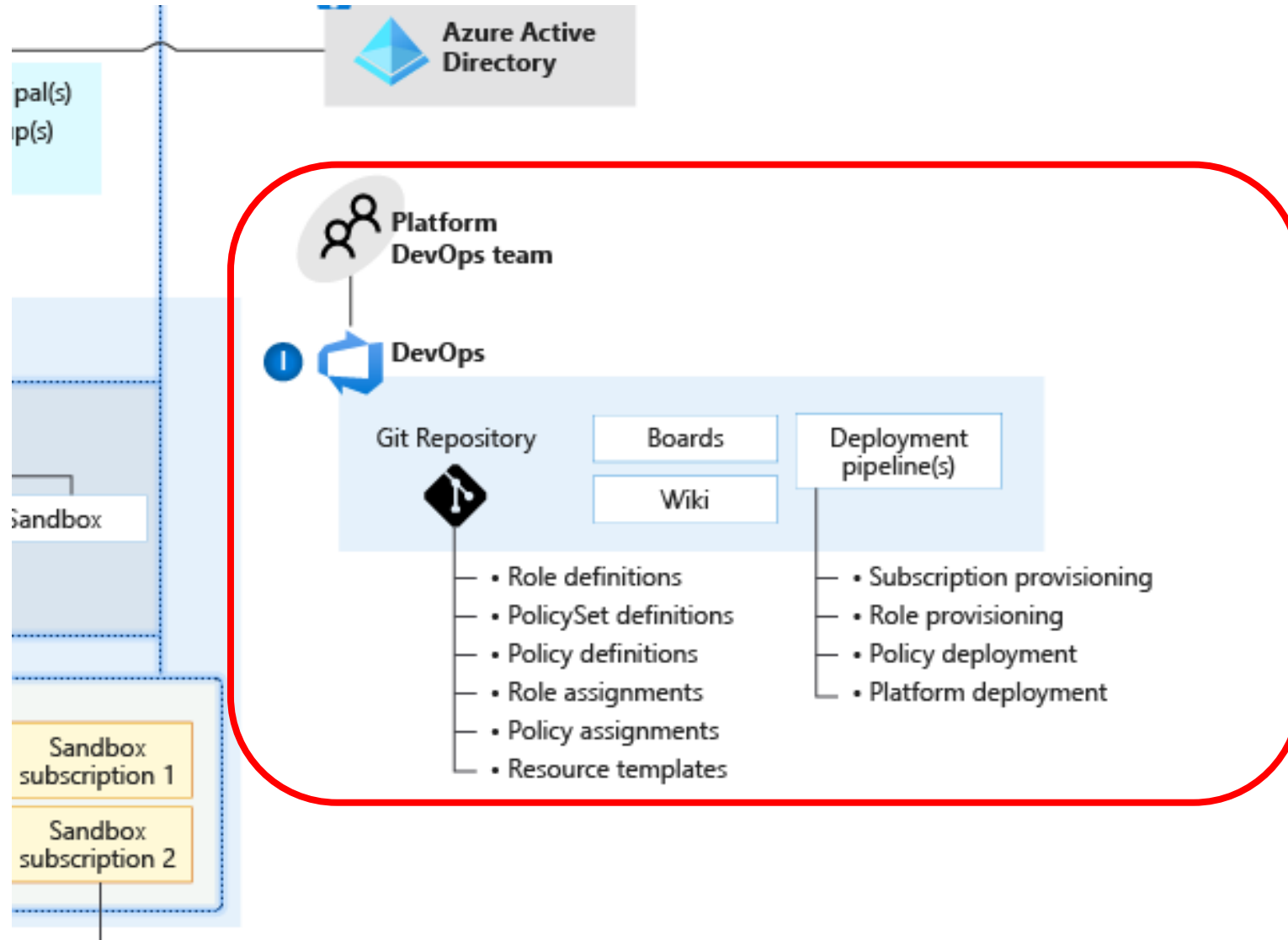


## Workload Überlegungen?

- Kann meine Applikation mit [Availability Zones](#) oder [Availability Sets](#) umgehen?
- Wie stelle ich die [Netzwerkonnktivität](#) her, wenn ein Failover auftritt?
  - Planung der Bandbreitenkapazität für [Azure ExpressRoute](#).
  - Traffic-Routing, wenn ein regionaler, zonaler oder Netzwerkausfall auftritt.
- Wie stelle ich ein [konsistentes Backup](#) von Applikationen und Daten sicher?  
VM Snapshots im [Recovery Services Vault](#)
- Wie bereite ich [geplante](#) und [ungeplante Failover](#)?  
Notfallwiederherstellungsplan

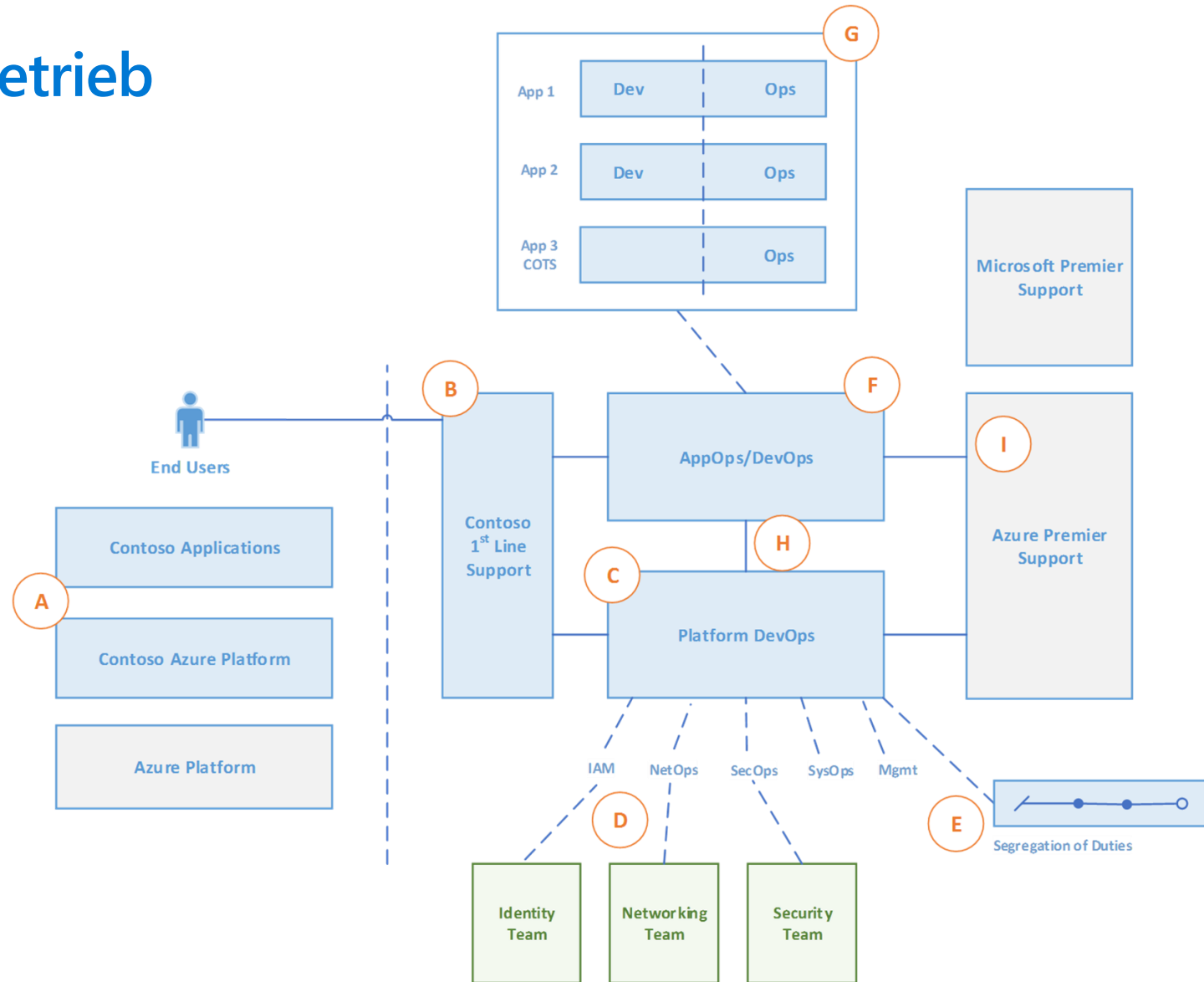


# Plattformautomatisierung & DevOps





# DevOps Betrieb







# Planung des DevOps Betriebs

Erstelle ein **Cross-funktionales DevOps Plattform Team**:

- **PlatformOps** (platform operations)
- **SecOps** (security operations)
- **NetOps** (network operations)
- **AppDevOps**



# AppDevOps

- Konsistente Konfiguration wird durch Policies und RBAC sichergestellt
- Applikationsteams können flexibel innerhalb des Rahmens Applikationen erstellen und verwalten
- Applikationsteams sollen deren DevOps Pipeline nutzen, und nicht von zentralen Prozessen abhängen
- Zentrales Team stellt Set an Templates bereit zum Beispiel für Migrationen



# Definition von zentralen und dezentralen Verantwortlichkeiten

## Zentrales Team

- Governance der Architektur
- Subscription Management
- Platform as code (Management von Templates, Scripts, ...).
- Policy Management
- Platform Management und Monitoring
- Azure RBAC
- Key Management (der zentralen Dienste).
- Network management
- Security Monitoring
- Cost management

## Application Teams

- Applikationsmigration und Transformation.
- Applicationsmanagement und Monitoring (application resources).
- Key management (application keys).
- Azure RBAC (application resources).
- Security Monitoring (application resources).
- Cost management (application resources).
- Network management (application resources).

<https://aka.ms/es-videoseries>

Demo



# Soll ich Enterprise-Scale innerhalb meiner Azure Umgebung nutzen?



**Skalierung &  
Geschwindigkeit**



**Sicherheit &  
Compliance**




**Cloud-First Strategie**



**Cloudskills im  
Plattform Team**

Coffee break...

05:00

mins:  secs:  type:    
 Breaktime for PowerPoint by Flow Simulation Ltd. Pin controls when stopped

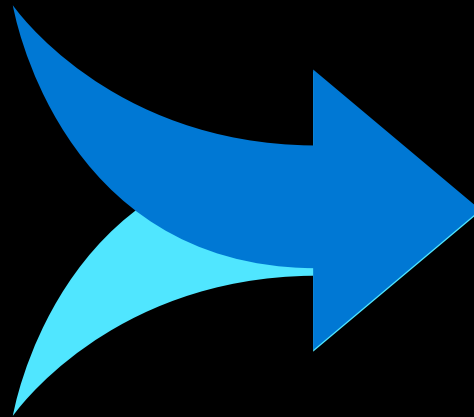
# Microsoft Azure Well-Architected





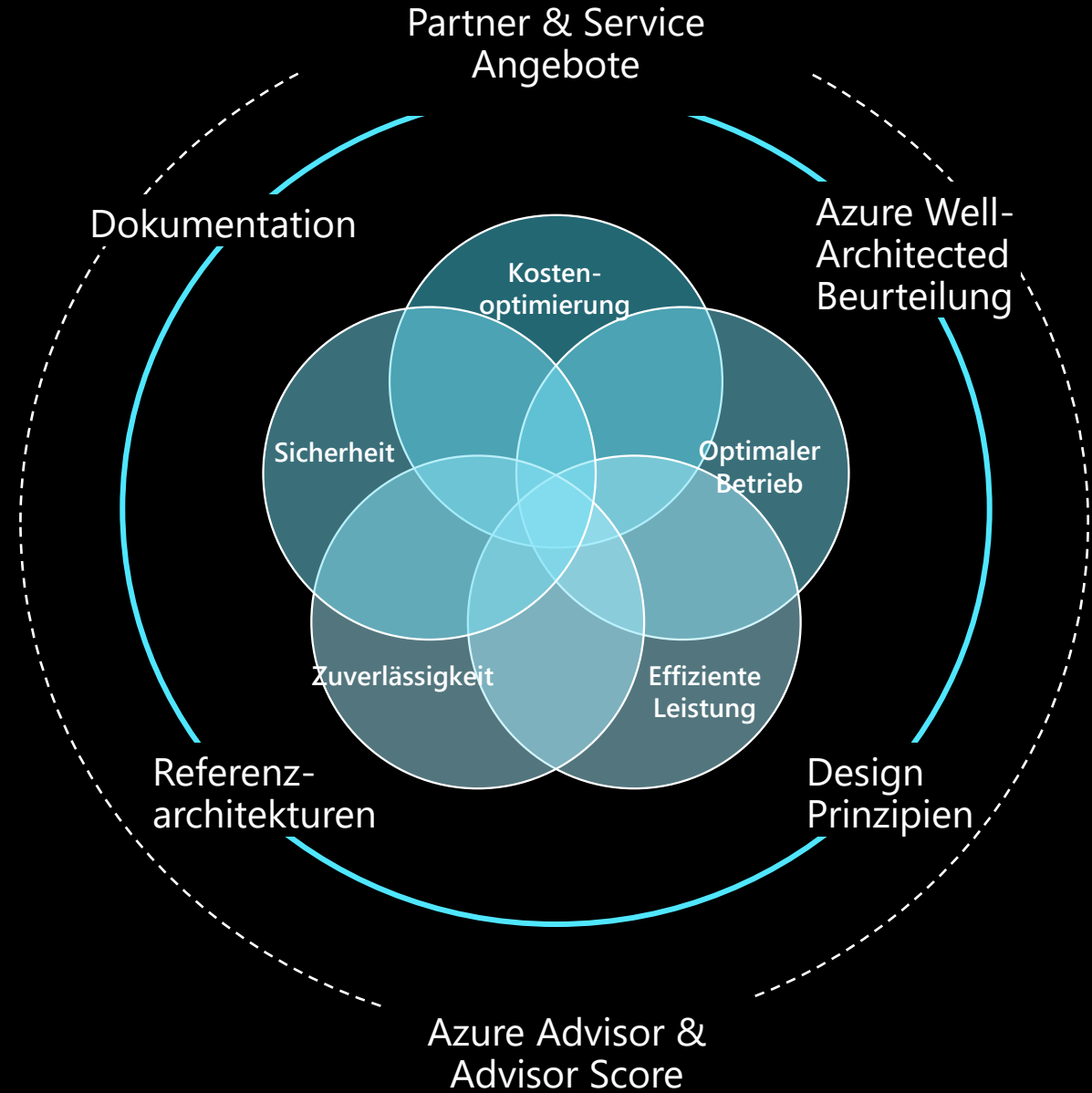
# Warum müssen wir auf die "richtige" Cloud-Architektur achten?

- ✓ Einhaltung des Budgets
- ✓ Verbesserung der Sicherheit
- ✓ Incident Beantwortung
- ✓ Streamline internal processes
- ✓ Fehlervermeidung
- ✓ Effiziente Performance



-  Ausgaben & Verluste
-  Vertrauen
-  Incidents

# Microsoft Azure Well-Architected



# Microsoft Azure Well-Architected Framework

Architektur, Guidance und Best Practices für Cloud Architekten, Entwickler und Lösungsverantwortliche um die Qualität der Workloads zu verbessern anhand dieser Säulen:

**Kosten-  
optimierung**



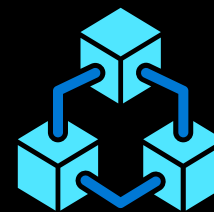
**Optimaler  
Betrieb**



**Effiziente  
Leistung**



**Zuverlässigkeit**



**Sicherheit**



# Kostenoptimierung



Kosten verstehen  
und vorhersagen



Optimierung  
durch Rightsizing



Kostenkontrolle

Learn more: [aka.ms/costoptimization](https://aka.ms/costoptimization)

# Optimaler Betrieb



Agile und akkurate  
Prozesse



Fokussiertes und  
passendes  
Applicationsmonitoring



Kontinuierliche  
Verbesserung

# Effiziente Leistung



Auslastungsprobleme  
erkennen und beheben



Optimale Ausführung  
des Services



Trade-offs abgestimmt auf  
Applikationsanforderungen

# Zuverlässigkeit



Definition der  
Verfügbarkeits- und  
Wiederherstellungs-  
anforderungen



Simulation des  
Ausfallsszenarios



Überwachung der  
Applicationsgesundheit



Ausfall- und  
Fehlerreaktion

# Sicherheit



Aufbau einer  
sicheren Grundlage



Proaktive Sicherung durch  
native Kontrollen



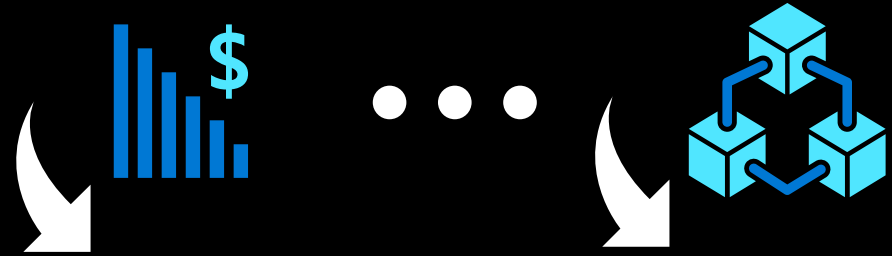
Erkenne Bedrohungen  
frühzeitig



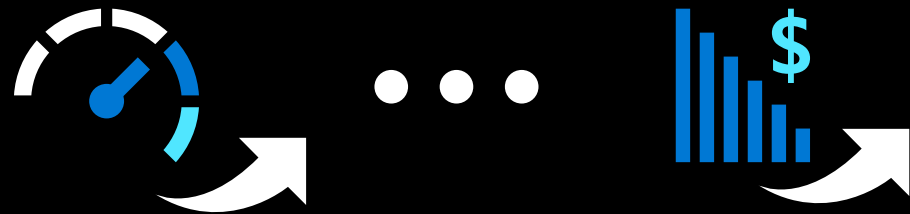
# Kompromiss- bildung

Businessanforderungen  
beeinflussen  
Architekturentscheidungen

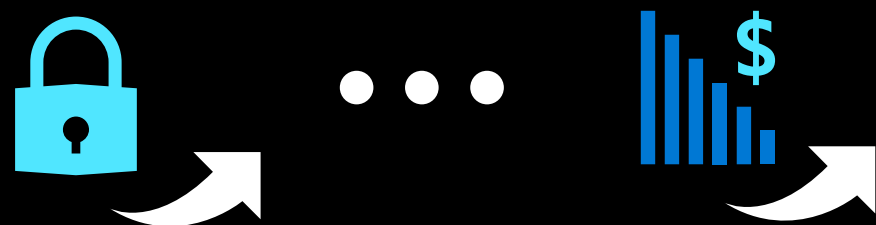
## ENTWICKLUNGS - UND TEST WORKLOADS



## UNTERNEHMENSKRITISCHE WORKLOADS



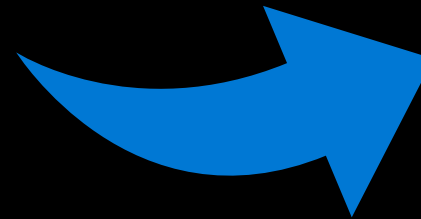
## ABSICHERUNG ALLER WORKLOADS



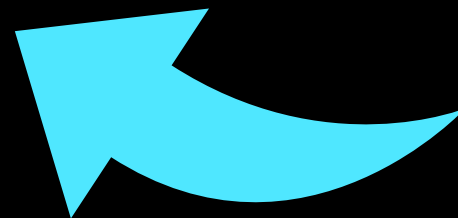
# Wie soll man nun starten?

- ☑ Nutze den **Azure Advisor Score** um Optimierungspotenziale zu erkennen
- ☑ Erkenne, wenn **Veränderungen benötigt werden oder Incidents** auftreten
- ☑ Ziehe Architektur **Trade Offs** in Betracht, um Business Ziele zu erreichen

DESIGN & AUFBAU  
**NEUER** WORKLOADS



- ☑ Passe die Architektur an **Geschäftsprioritäten** an
- ☑ Nutze das **Azure Well-Architected Review** um die geplante Architektur zu beurteilen
- ☑ Ziehe beim Design **Trade Offs** in Betracht, um Business Ziele zu erreichen

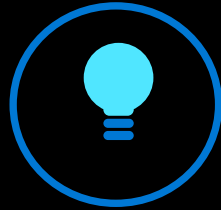


OPTIMIERUNG **BESTEHENDER**  
WORKLOADS

# Nächste Schritte:



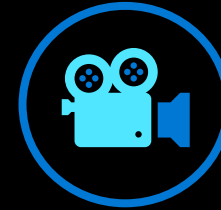
[Azure Well-Architected Review](#)  
([aka.ms/wellarchitected/review](#))



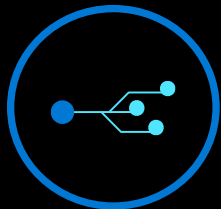
[Well-Architected Learning Path](#)  
([aka.ms/wellarchitected/learn](#))



[Azure Architectures](#)  
([aka.ms/wellarchitected/referencearch](#))



[Channel 9 Show](#)  
([aka.ms/azenable](#))



[Well-Architected Design Principles](#)  
([aka.ms/wellarchitected/designprinciples](#))



[Azure Well-Architected Framework](#)  
([aka.ms/wellarchitected/framework](#))



Partner Offers



MS Consulting Services  
([aka.ms/WAFServices](#))

Q&A

<https://aka.ms/aac-de-connect>



**Dankeschön!**