Securing your Privileged Identities & DevOps Pipelines in Microsoft Azure

Thomas Naunheim

glueckkanja-gab AG
Cloud Security Architect

Securing your Privileged Identities and DevOps Pipelines in Microsoft Azure

Thomas Naunheim

Cloud Security Architect, glueckkanja-gab AG
Microsoft MVP

@Thomas_Live

www.cloud-architekt.net

Securing your Privileged Identities and DevOps Pipelines in Microsoft Azure

PRIVILEGED **IDENTITIES**

PRIVILEGED **ACCESS**

PRIVILEGED **PIPELINES**

Level of Isolation and Seperation
= Your Balance of Security, Complexitity and Usability

Privileged Identity

Strong security baseline for high impact accounts

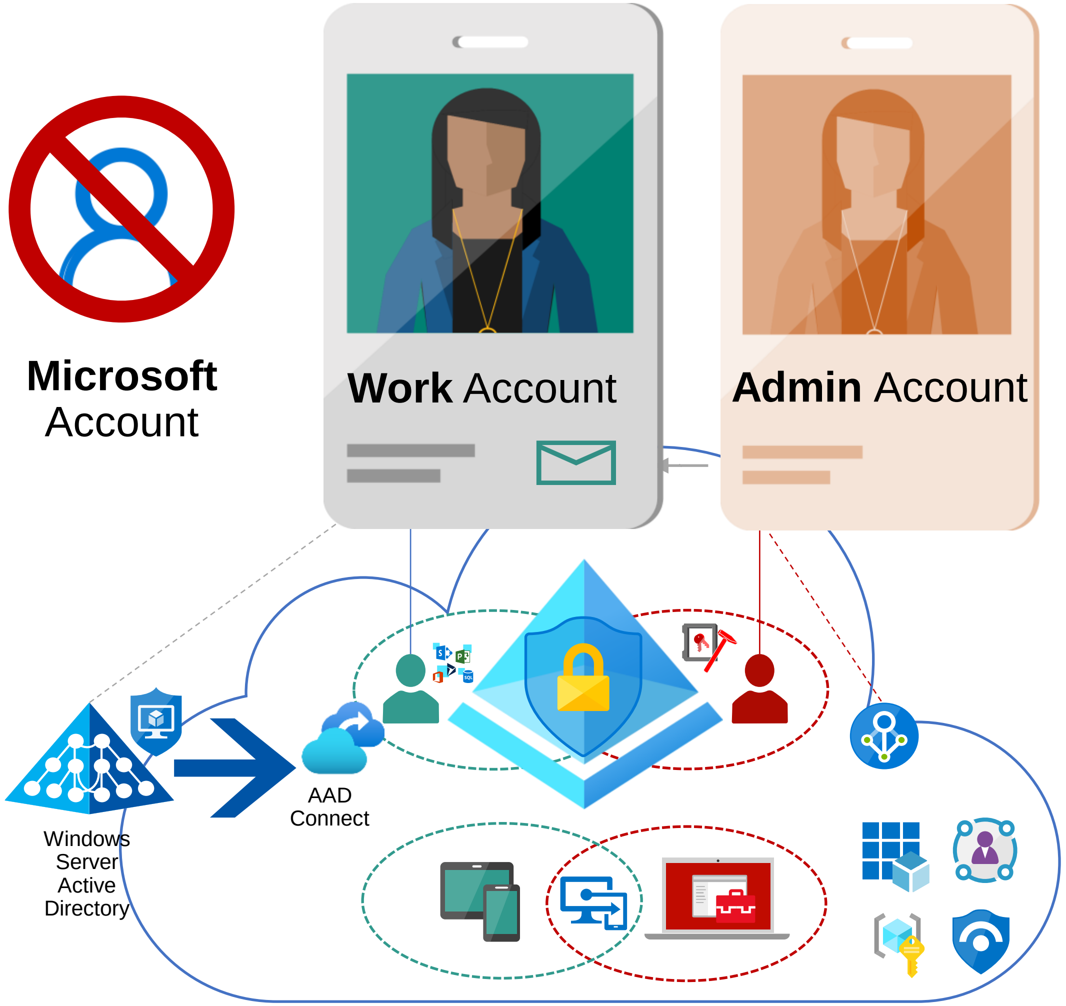
Foundation of Privileged Accounts

Separation of work and privileged accounts

- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Implement identity lifecycle and access review
- ✓ Remove licenses of productivity workloads

Secured and hardened Azure AD Tenant

- ✓ Strong baseline and tenant-level security
- ✓ Active identity security posture management
- ✓ Consider external privileged access by Delegated Access Permissions (DAP) of CSP/MSP or consented (multi-tenant) apps
- ✓ Incident and Response for suspicious activities
- ✓ Isolation of work- and privileged resources



Microsoft Account

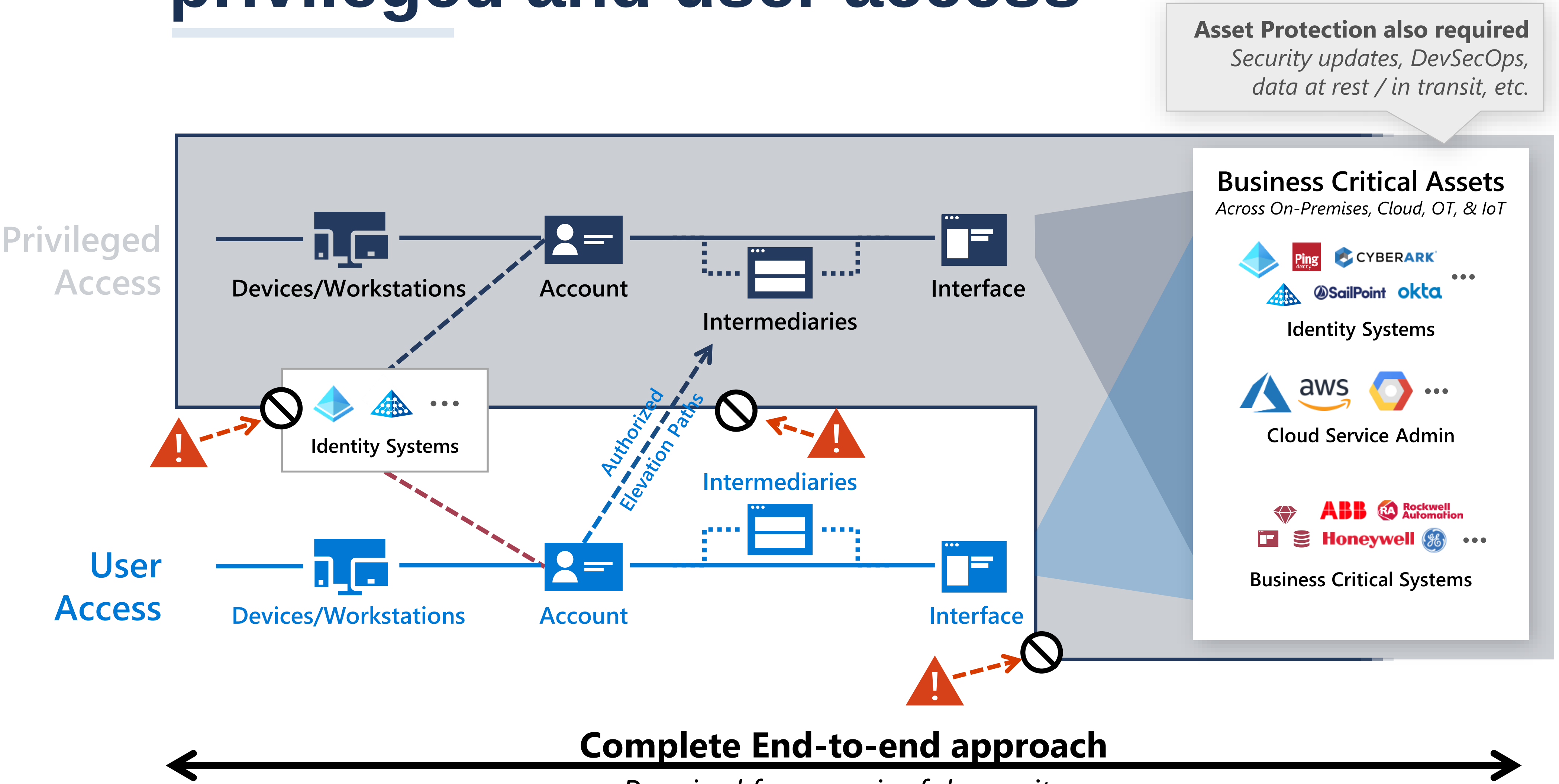
Work Account

Admin Account

Windows Server Active Directory

AAD Connect

Authorized (Elevated) Paths for privileged and user access



"End-to-end Session Security - Establish explicit Zero Trust validation for privileged sessions, user sessions, and authorized elevation paths."

Complete End-to-end approach

Required for meaningful security

Source: "Privileged access Strategy" (Microsoft)

Live Demo

- Conditional Access for Privileged Identities
- Cloud-managed SAW
- Security Monitoring and Posture Management

Privileged Access

Least privileged and tiered RBAC design

Foundation of Privileged Access

Granular Task/ Scoped Access (Just Enough)

Just in Time Access

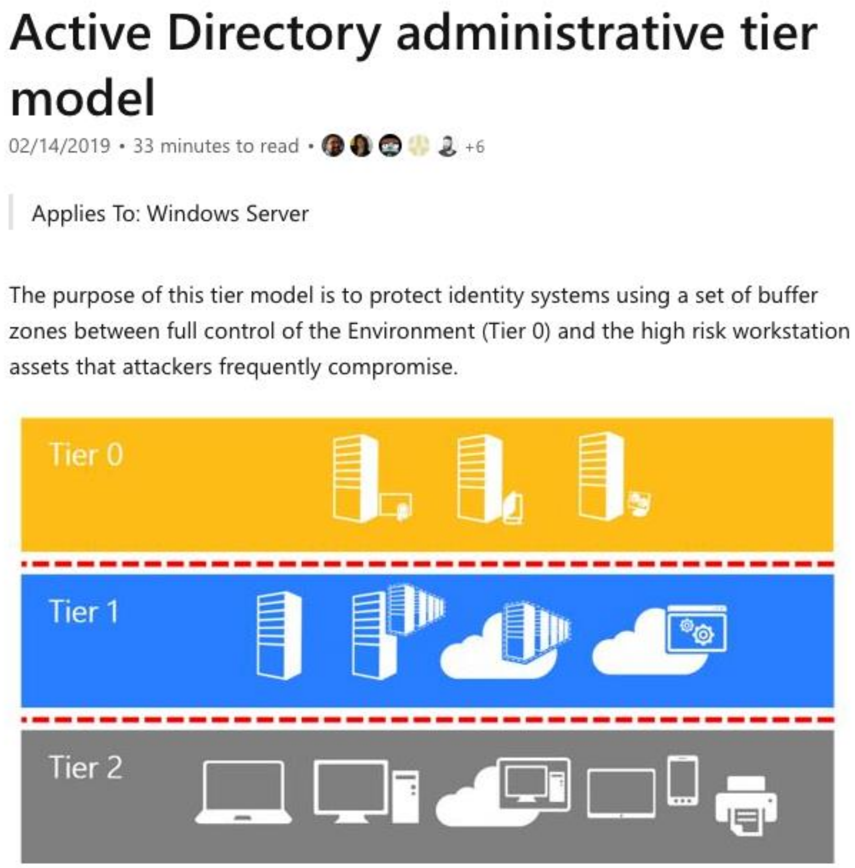
Privileged Admin Workflow

Audit and Access Review

Administrative Tier Model in Azure AD?

„To mitigate risk of identity compromise, or bad actors, implement **tiered administration** and ensure that you **follow principles of least privilege for Azure AD Administrator Roles**.“

Source: „Securing Azure Environments with Azure AD (Architecture and Design Guide)“



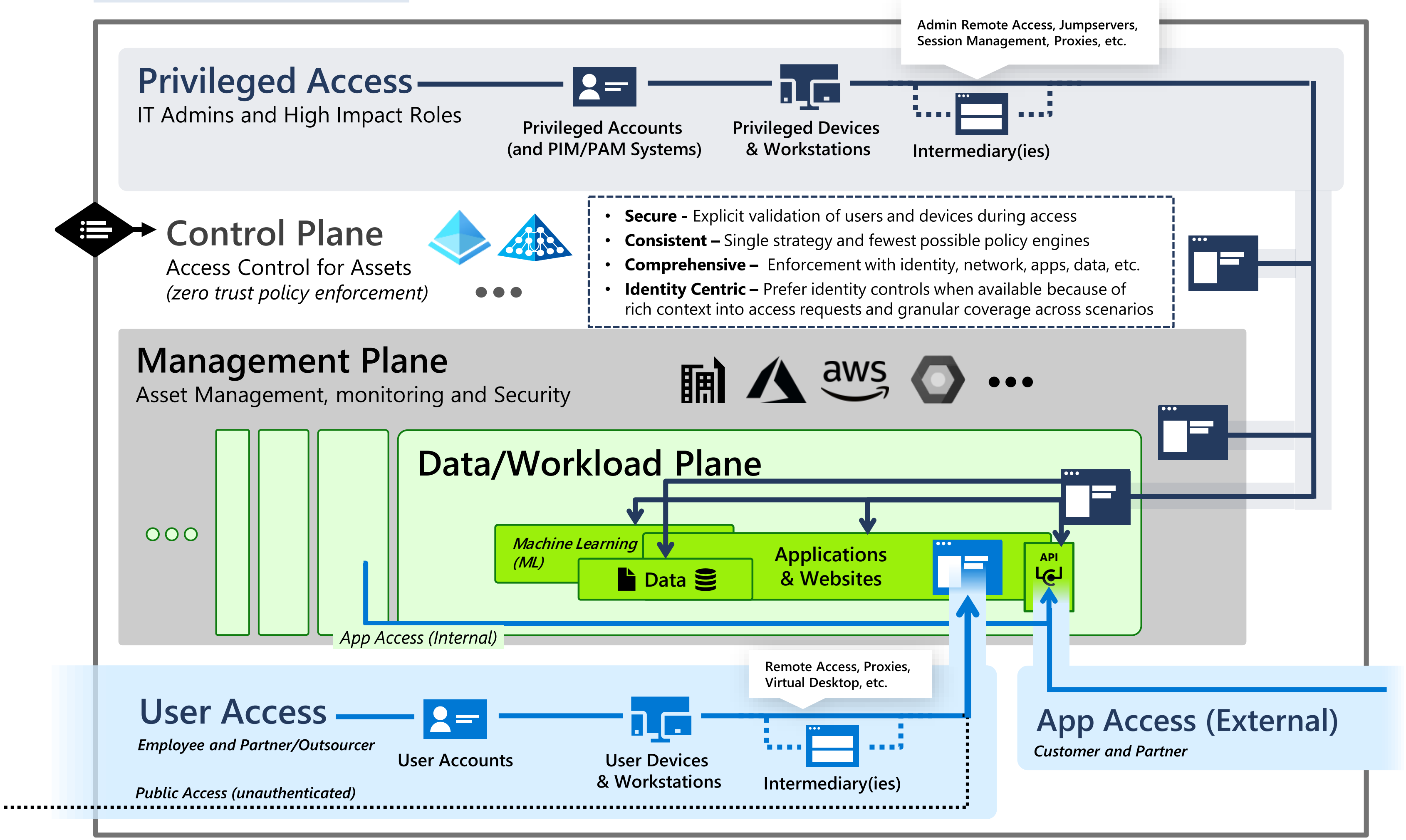
Active Directory administrative tier model

02/14/2019 • 33 minutes to read • +6

Applies To: Windows Server

The purpose of this tier model is to protect identity systems using a set of buffer zones between full control of the Environment (Tier 0) and the high risk workstation assets that attackers frequently compromise.

Enterprise Access Model by Microsoft



Admin Remote Access, Jumpservers, Session Management, Proxies, etc.

Privileged Access

IT Admins and High Impact Roles

Privileged Accounts (and PIM/PAM Systems)

Privileged Devices & Workstations

Intermediary(ies)

Control Plane

Access Control for Assets

(zero trust policy enforcement)

- **Secure -** Explicit validation of users and devices during access
- **Consistent –** Single strategy and fewest possible policy engines
- **Comprehensive –** Enforcement with identity, network, apps, data, etc.
- **Identity Centric –** Prefer identity controls when available because of rich context into access requests and granular coverage across scenarios

Management Plane

Asset Management, monitoring and Security

Data/Workload Plane

Machine Learning (ML)

Data

Applications & Websites

API

App Access (Internal)

Remote Access, Proxies, Virtual Desktop, etc.

User Access

Employee and Partner/Outsourcer

User Accounts

User Devices & Workstations

Intermediary(ies)

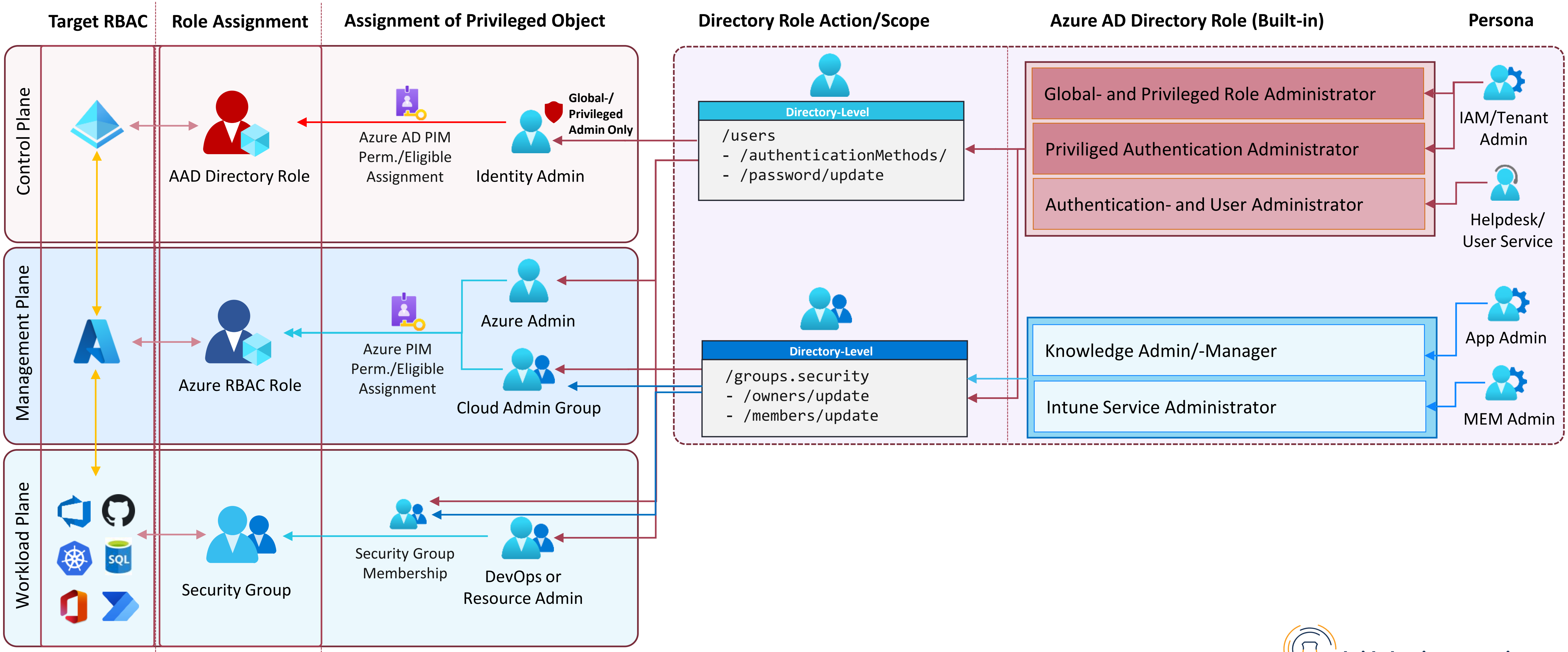
Public Access (unauthenticated)

App Access (External)

Customer and Partner

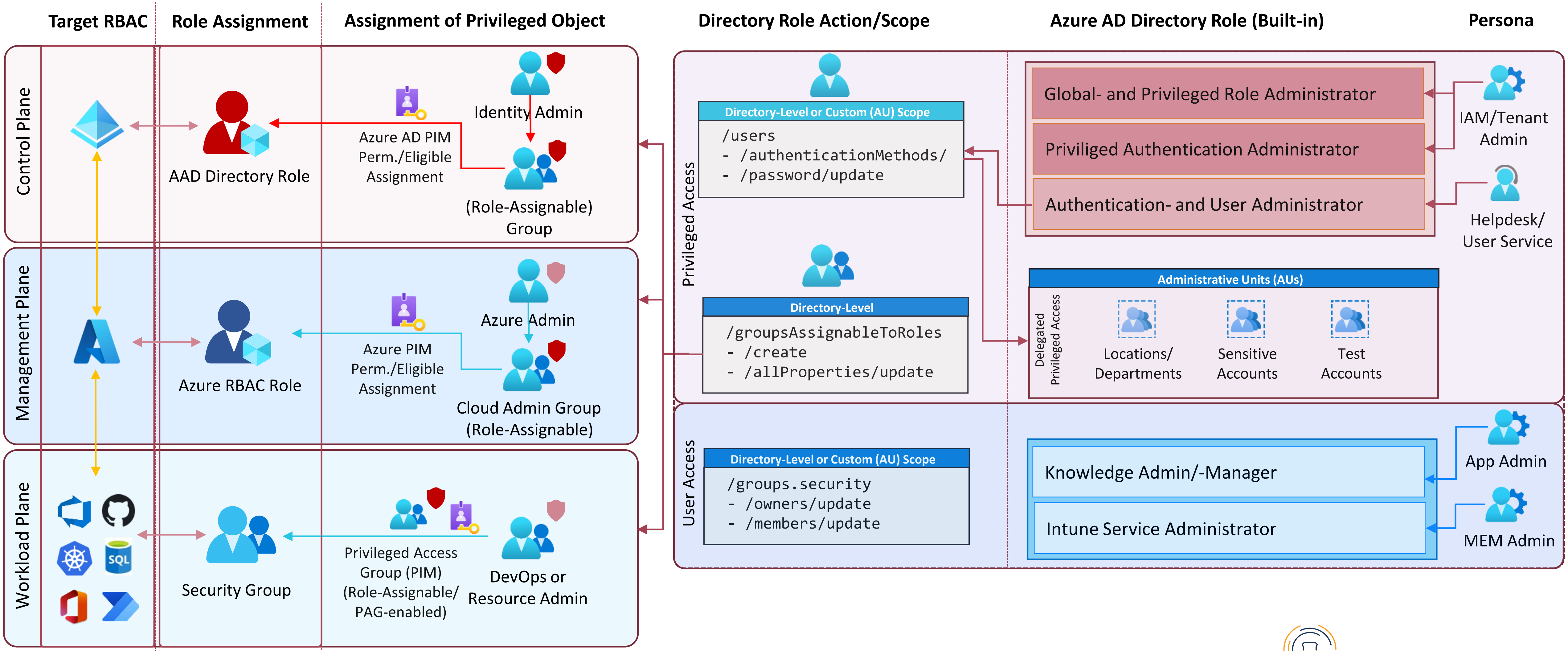
Source: "Enterprise Access Model" (Microsoft Docs)

Privileged Access in Microsoft Cloud Services



Hybrid Identity Protection

Privileged Access and Scoped Azure AD Roles



Target RBAC | Role Assignment | Assignment of Privileged Object | Directory Role Action/Scope | Azure AD Directory Role (Built-in) | Persona

Control Plane

AAD Directory Role

Azure AD PIM Perm./Eligible Assignment

Identity Admin

(Role-Assignable) Group

Management Plane

Azure RBAC Role

Azure PIM Perm./Eligible Assignment

Azure Admin

Cloud Admin Group (Role-Assignable)

Workload Plane

Security Group

Privileged Access Group (PIM) (Role-Assignable/ PAG-enabled)

DevOps or Resource Admin

Privileged Access

Directory-Level or Custom (AU) Scope

```
/users
- /authenticationMethods/
- /password/update
```

Directory-Level

```
/groupsAssignableToRoles
- /create
- /allProperties/update
```

Global- and Privileged Role Administrator

Priviliged Authentication Administrator

Authentication- and User Administrator

IAM/Tenant Admin

Helpdesk/ User Service

Administrative Units (AUs)

Delegated Privileged Access

Locations/ Departments

Sensitive Accounts

Test Accounts

User Access

Directory-Level or Custom (AU) Scope

```
/groups.security
- /owners/update
- /members/update
```

Knowledge Admin/-Manager

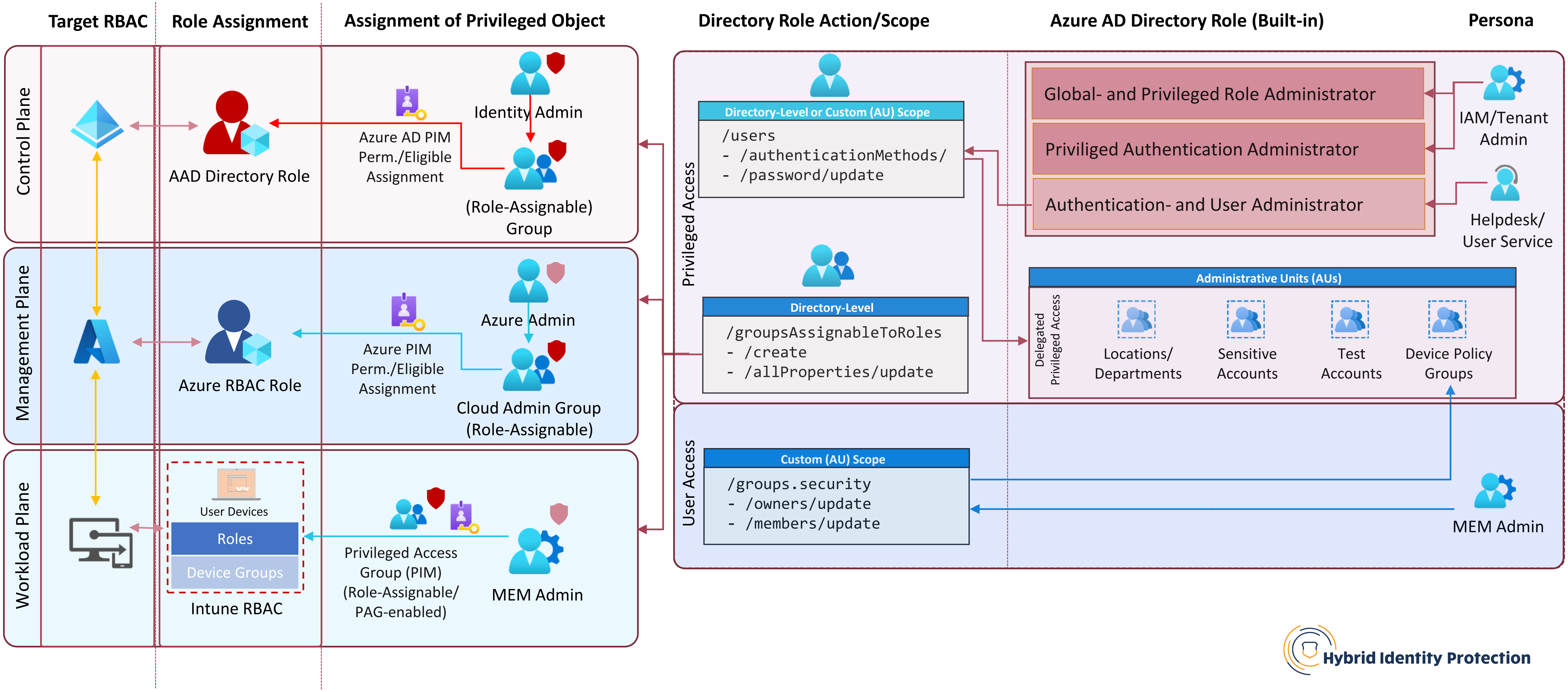
Intune Service Administrator

App Admin

MEM Admin

Hybrid Identity Protection

Privileged Access and Service-Specific Roles



Target RBAC

Role Assignment

Assignment of Privileged Object

Directory Role Action/Scope

Azure AD Directory Role (Built-in)

Persona

Control Plane

AAD Directory Role

Azure AD PIM Perm./Eligible Assignment

Identity Admin

(Role-Assignable) Group

Management Plane

Azure RBAC Role

Azure PIM Perm./Eligible Assignment

Azure Admin

Cloud Admin Group (Role-Assignable)

Workload Plane

User Devices

Roles

Device Groups

Intune RBAC

Privileged Access Group (PIM) (Role-Assignable/ PAG-enabled)

MEM Admin

Privileged Access

Directory-Level or Custom (AU) Scope

```
/users
- /authenticationMethods/
- /password/update
```

Directory-Level

```
/groupsAssignableToRoles
- /create
- /allProperties/update
```

Global- and Privileged Role Administrator

Priviliged Authentication Administrator

Authentication- and User Administrator

IAM/Tenant Admin

Helpdesk/ User Service

Administrative Units (AUs)

Delegated Privileged Access

Locations/ Departments

Sensitive Accounts

Test Accounts

Device Policy Groups

User Access

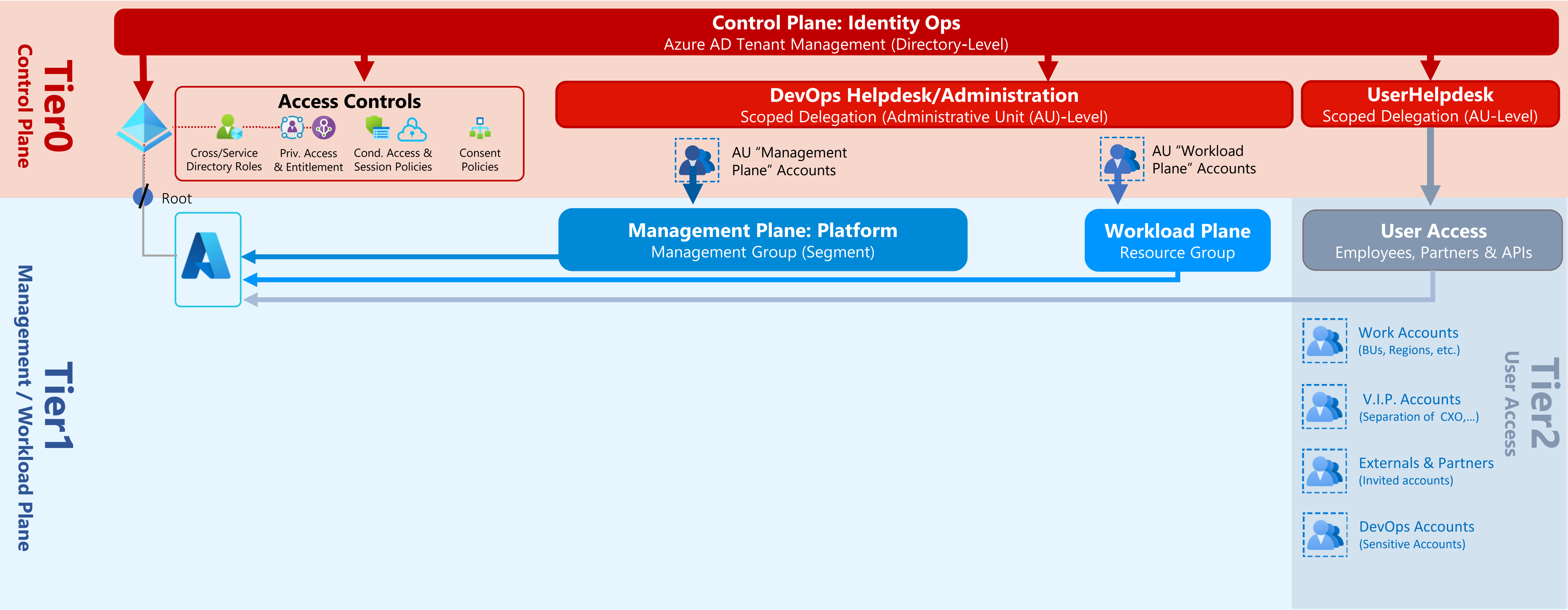
Custom (AU) Scope

```
/groups.security
- /owners/update
- /members/update
```

MEM Admin

Hybrid Identity Protection

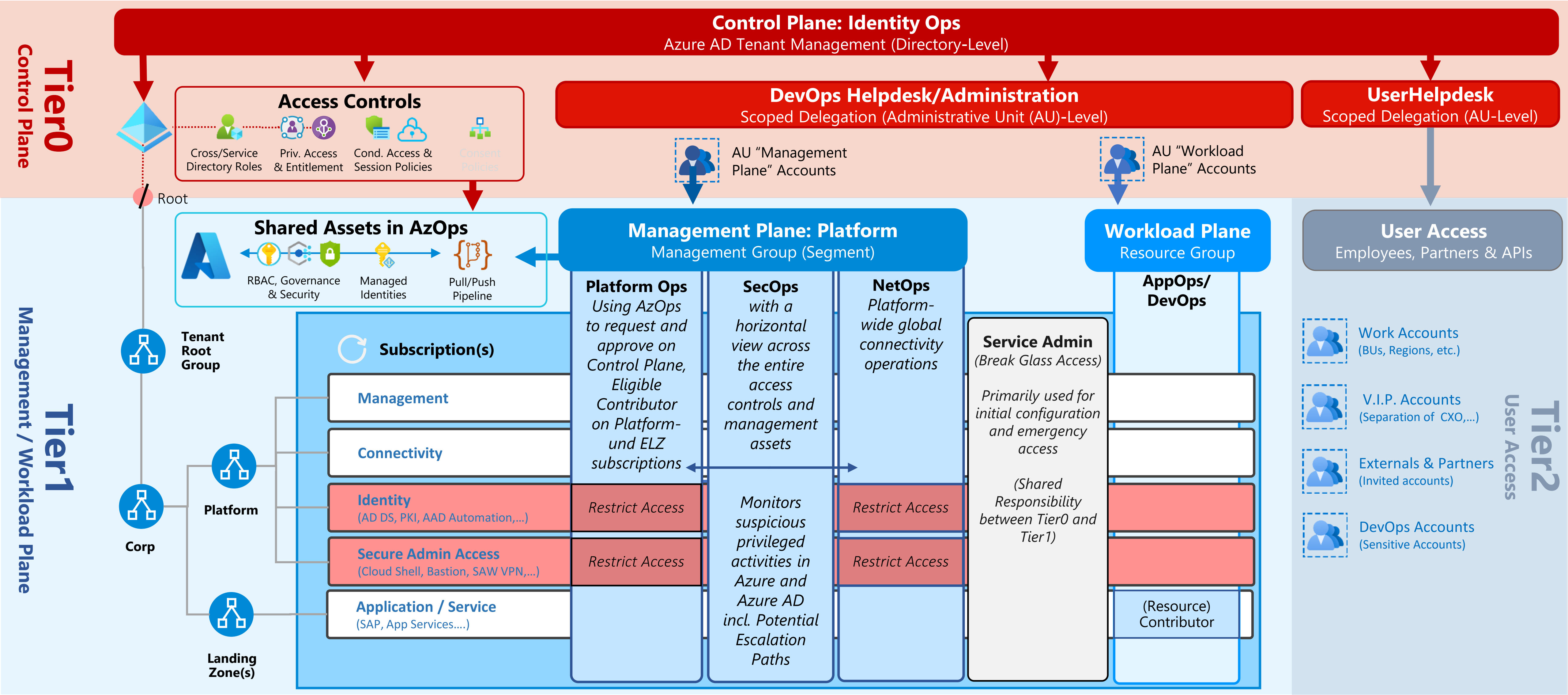
My implementation of Enterprise Access Model


Tier0
Control Plane
Control Plane: Identity Ops
Azure AD Tenant Management (Directory-Level)
Access Controls
Cross/Service Directory Roles
Priv. Access & Entitlement
Cond. Access & Session Policies
Consent Policies
DevOps Helpdesk/Administration
Scoped Delegation (Administrative Unit (AU)-Level)
UserHelpdesk
Scoped Delegation (AU-Level)
AU "Management Plane" Accounts
AU "Workload Plane" Accounts
Root
Tier1
Management / Workload Plane
Management Plane: Platform
Management Group (Segment)
Workload Plane
Resource Group
User Access
Employees, Partners & APIs
Tier2
User Access
Work Accounts
(BUs, Regions, etc.)
V.I.P. Accounts
(Separation of CXO,...)
Externals & Partners
(Invited accounts)
DevOps Accounts
(Sensitive Accounts)

Live Demo

- Administrative Accounts
- Privileged Access Groups
- Administrative Units and Scoped Delegation of Tasks
- Identity Governance

My implementation of Enterprise Access Model



Tier0 Control Plane

Control Plane: Identity Ops
Azure AD Tenant Management (Directory-Level)

Access Controls

- Cross/Service Directory Roles
- Priv. Access & Entitlement
- Cond. Access & Session Policies
- Consent Policies

DevOps Helpdesk/Administration
Scoped Delegation (Administrative Unit (AU)-Level)

AU "Management Plane" Accounts

AU "Workload Plane" Accounts

UserHelpdesk
Scoped Delegation (AU-Level)

Root

Shared Assets in AzOps

- RBAC, Governance & Security
- Managed Identities
- Pull/Push Pipeline

Tier1 Management / Workload Plane

- Tenant Root Group
- Corp
- Platform
- Landing Zone(s)

Subscription(s)

- **Management**
- **Connectivity**
- **Identity** (AD DS, PKI, AAD Automation,...)
- **Secure Admin Access** (Cloud Shell, Bastion, SAW VPN,...)
- **Application / Service** (SAP, App Services....)

Management Plane: Platform
Management Group (Segment)

Platform Ops
Using AzOps to request and approve on Control Plane, Eligible Contributor on Platform- und ELZ subscriptions

Restrict Access

Restrict Access

SecOps
with a horizontal view across the entire access controls and management assets

Monitors suspicious privileged activities in Azure and Azure AD incl. Potential Escalation Paths

NetOps
Platform-wide global connectivity operations

Restrict Access

Restrict Access

Service Admin
(Break Glass Access)

Primarily used for initial configuration and emergency access

(Shared Responsibility between Tier0 and Tier1)

Workload Plane
Resource Group

AppOps/ DevOps

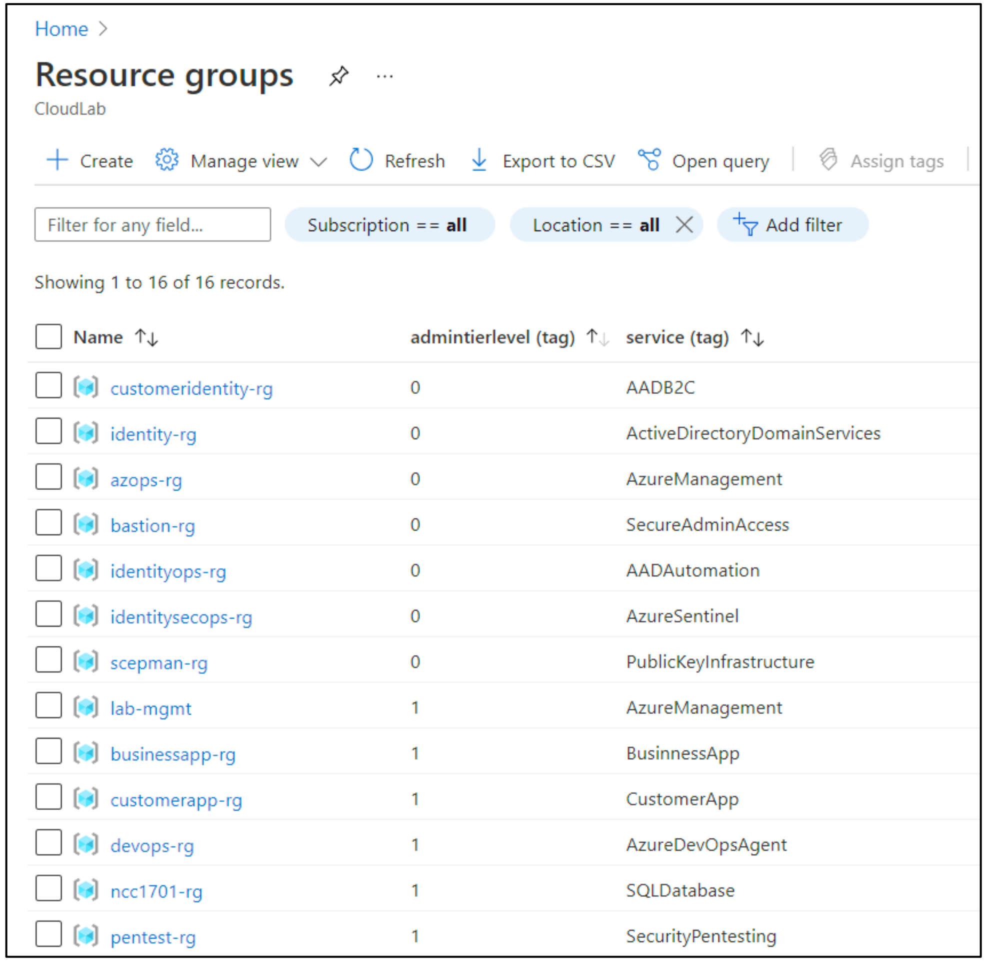
(Resource) Contributor

User Access
Employees, Partners & APIs

Tier2 User Access

- Work Accounts (BUs, Regions, etc.)
- V.I.P. Accounts (Separation of CXO,...)
- Externals & Partners (Invited accounts)
- DevOps Accounts (Sensitive Accounts)

Classification of all Azure Resources by Tags



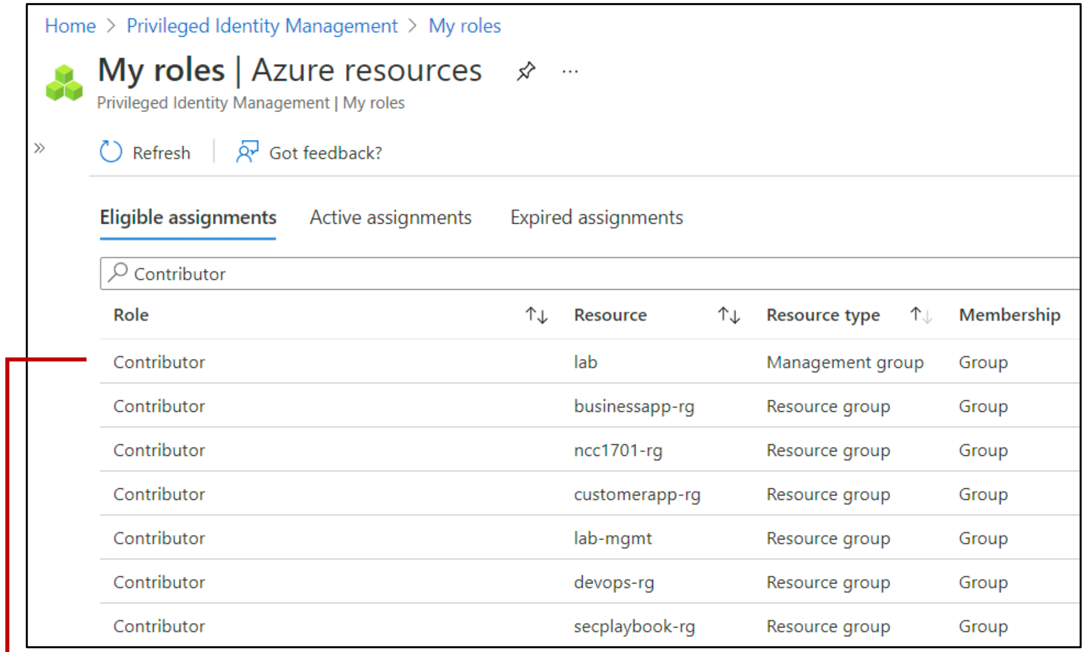
Home >

Resource groups

CloudLab

Showing 1 to 16 of 16 records.

□ Name ↑↓	admintierlevel (tag) ↑↓	service (tag) ↑↓
□ customeridentity-rg	0	AADB2C
□ identity-rg	0	ActiveDirectoryDomainServices
□ azops-rg	0	AzureManagement
□ bastion-rg	0	SecureAdminAccess
□ identityops-rg	0	AADAutomation
□ identitysecops-rg	0	AzureSentinel
□ scepman-rg	0	PublicKeyInfrastructure
□ lab-mgmt	1	AzureManagement
□ businessapp-rg	1	BusinessApp
□ customerapp-rg	1	CustomerApp
□ devops-rg	1	AzureDevOpsAgent
□ ncc1701-rg	1	SQLDatabase
□ pentest-rg	1	SecurityPentesting



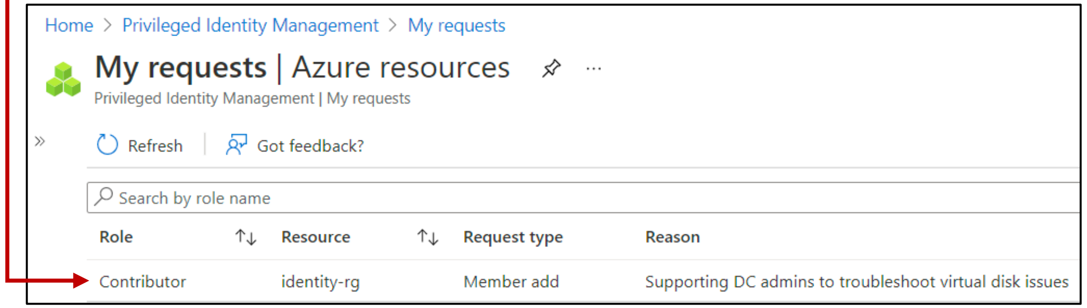
Home > Privileged Identity Management > My roles

My roles | Azure resources

Privileged Identity Management | My roles

Contributor

Role ↑↓	Resource ↑↓	Resource type ↑↓	Membership
Contributor	lab	Management group	Group
Contributor	businessapp-rg	Resource group	Group
Contributor	ncc1701-rg	Resource group	Group
Contributor	customerapp-rg	Resource group	Group
Contributor	lab-mgmt	Resource group	Group
Contributor	devops-rg	Resource group	Group
Contributor	secplaybook-rg	Resource group	Group



Home > Privileged Identity Management > My requests

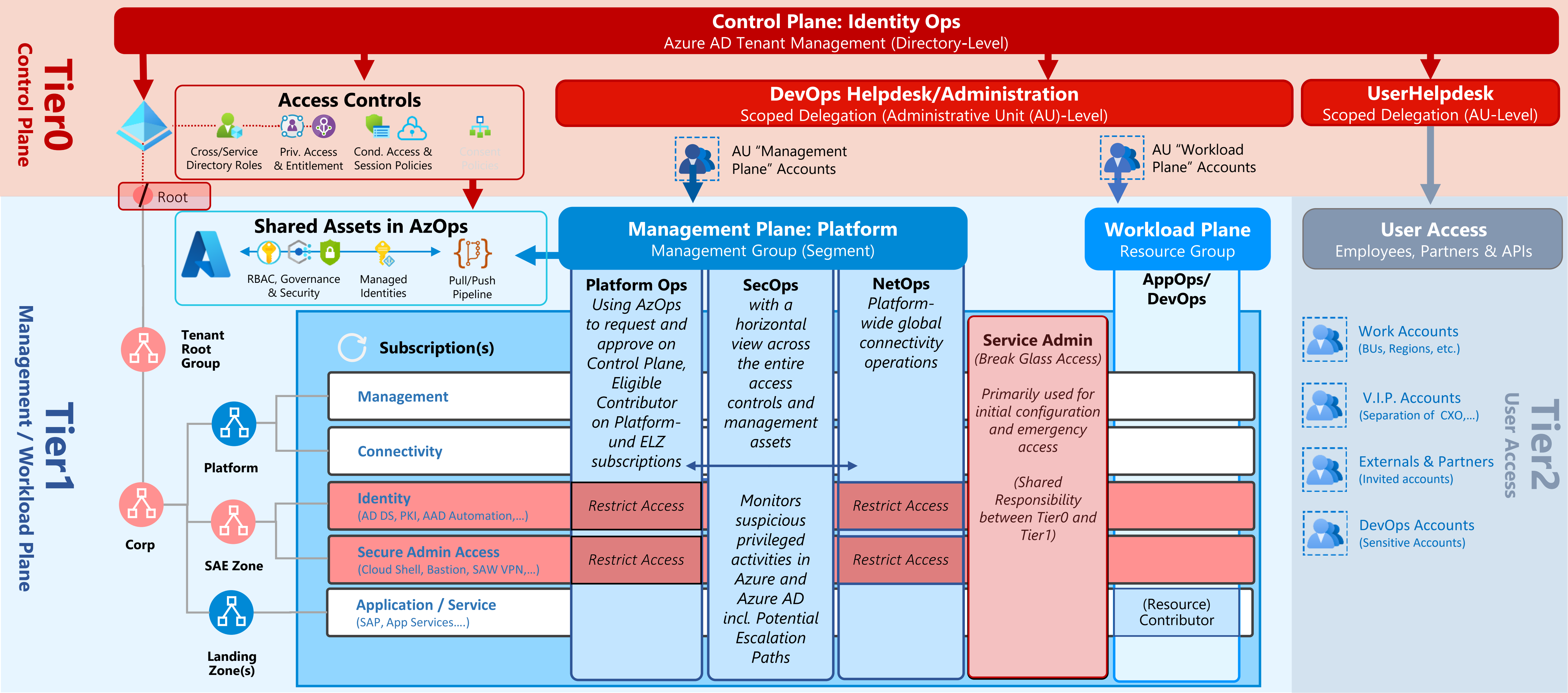
My requests | Azure resources

Privileged Identity Management | My requests

Role ↑↓	Resource ↑↓	Request type	Reason
Contributor	identity-rg	Member add	Supporting DC admins to troubleshoot virtual disk issues

Monitoring RBAC and review PIM requests to restrict privilege escalation

My implementation of Enterprise Access Model



Tier0
Control Plane

Control Plane: Identity Ops
Azure AD Tenant Management (Directory-Level)

Access Controls
Cross/Service Directory Roles
Priv. Access & Entitlement
Cond. Access & Session Policies
Consent Policies

DevOps Helpdesk/Administration
Scoped Delegation (Administrative Unit (AU)-Level)

AU "Management Plane" Accounts

AU "Workload Plane" Accounts

UserHelpdesk
Scoped Delegation (AU-Level)

Root

Tier1
Management / Workload Plane

Shared Assets in AzOps
RBAC, Governance & Security
Managed Identities
Pull/Push Pipeline

Tenant Root Group

Platform

Corp

SAE Zone

Landing Zone(s)

Subscription(s)

Management

Connectivity

Identity
(AD DS, PKI, AAD Automation,…)

Secure Admin Access
(Cloud Shell, Bastion, SAW VPN,…)

Application / Service
(SAP, App Services….)

Management Plane: Platform
Management Group (Segment)

Platform Ops
Using AzOps to request and approve on Control Plane, Eligible Contributor on Platform- und ELZ subscriptions

Restrict Access

Restrict Access

SecOps
with a horizontal view across the entire access controls and management assets

Monitors suspicious privileged activities in Azure and Azure AD incl. Potential Escalation Paths

NetOps
Platform-wide global connectivity operations

Restrict Access

Restrict Access

Service Admin
(Break Glass Access)

Primarily used for initial configuration and emergency access

(Shared Responsibility between Tier0 and Tier1)

Workload Plane
Resource Group

AppOps/ DevOps

(Resource) Contributor

User Access
Employees, Partners & APIs

Work Accounts
(BUs, Regions, etc.)

V.I.P. Accounts
(Separation of CXO,…)

Externals & Partners
(Invited accounts)

DevOps Accounts
(Sensitive Accounts)

Tier2
User Access

Live Demo

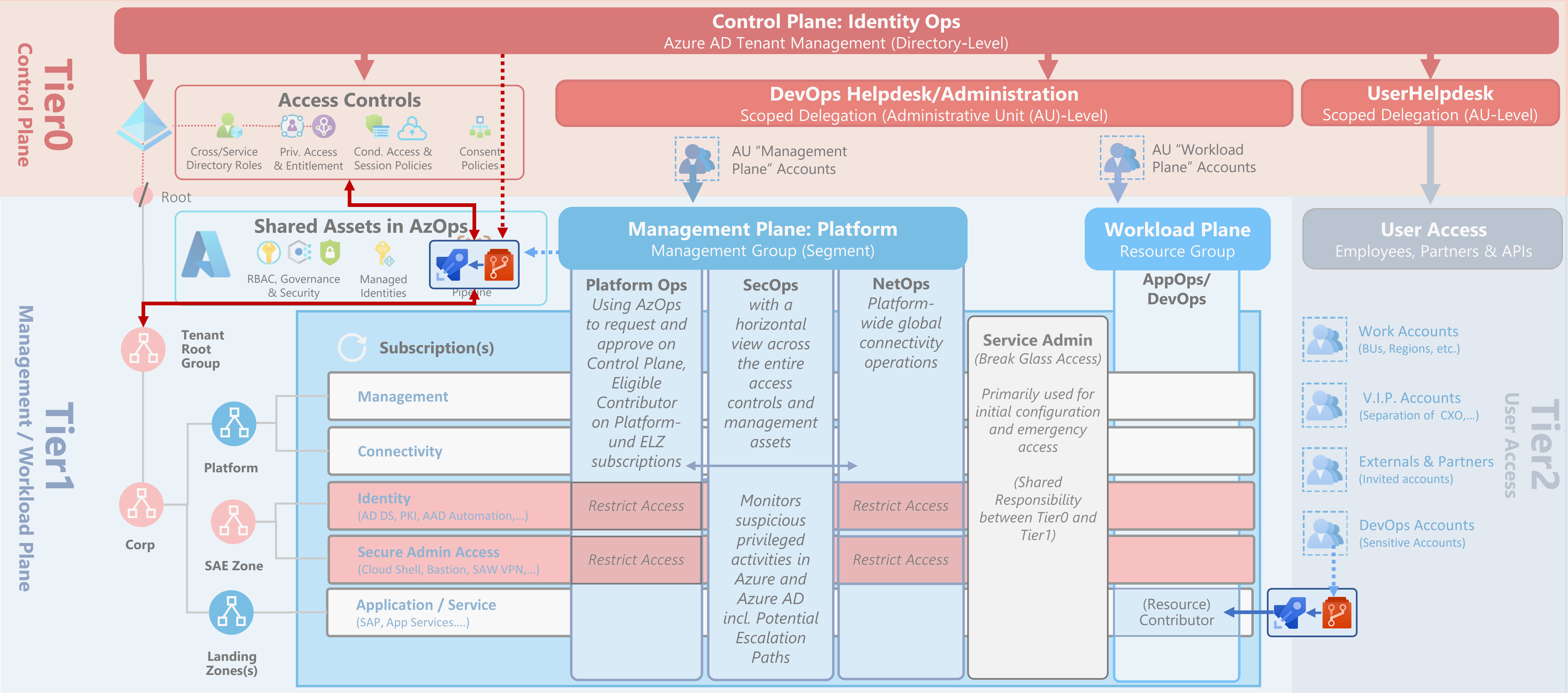
- Azure RBAC considerations
- Control Plane-Roles
  and -Assets in Azure
- AzOps for Operationalization

Hybrid Identity Protection

Poll #2

Do you already manage your Azure or Azure AD resources “as code”?

My implementation of Enterprise Access Model



Tier0
Control Plane

Control Plane: Identity Ops
Azure AD Tenant Management (Directory-Level)

Access Controls
Cross/Service Directory Roles
Priv. Access & Entitlement
Cond. Access & Session Policies
Consent Policies

DevOps Helpdesk/Administration
Scoped Delegation (Administrative Unit (AU)-Level)

AU "Management Plane" Accounts

AU "Workload Plane" Accounts

UserHelpdesk
Scoped Delegation (AU-Level)

Root

Shared Assets in AzOps
RBAC, Governance & Security
Managed Identities
Pipeline

Management Plane: Platform
Management Group (Segment)

Workload Plane
Resource Group

User Access
Employees, Partners & APIs

Tier1
Management / Workload Plane

Tenant Root Group

Platform

Corp

SAE Zone

Landing Zones(s)

Subscription(s)

Management

Connectivity

Identity
(AD DS, PKI, AAD Automation,...)

Secure Admin Access
(Cloud Shell, Bastion, SAW VPN,...)

Application / Service
(SAP, App Services....)

Platform Ops
Using AzOps to request and approve on Control Plane, Eligible Contributor on Platform- und ELZ subscriptions

Restrict Access

Restrict Access

SecOps
with a horizontal view across the entire access controls and management assets

Monitors suspicious privileged activities in Azure and Azure AD incl. Potential Escalation Paths

NetOps
Platform-wide global connectivity operations

Restrict Access

Restrict Access

Service Admin
(Break Glass Access)

Primarily used for initial configuration and emergency access

(Shared Responsibility between Tier0 and Tier1)

AppOps/ DevOps

(Resource) Contributor

Tier2
User Access

Work Accounts
(BUs, Regions, etc.)

V.I.P. Accounts
(Separation of CXO,...)

Externals & Partners
(Invited accounts)

DevOps Accounts
(Sensitive Accounts)

Privileged Pipelines

Secured DevOps platform and protected Workload identities

Foundation of Pipelines in Dev(Sec)Ops

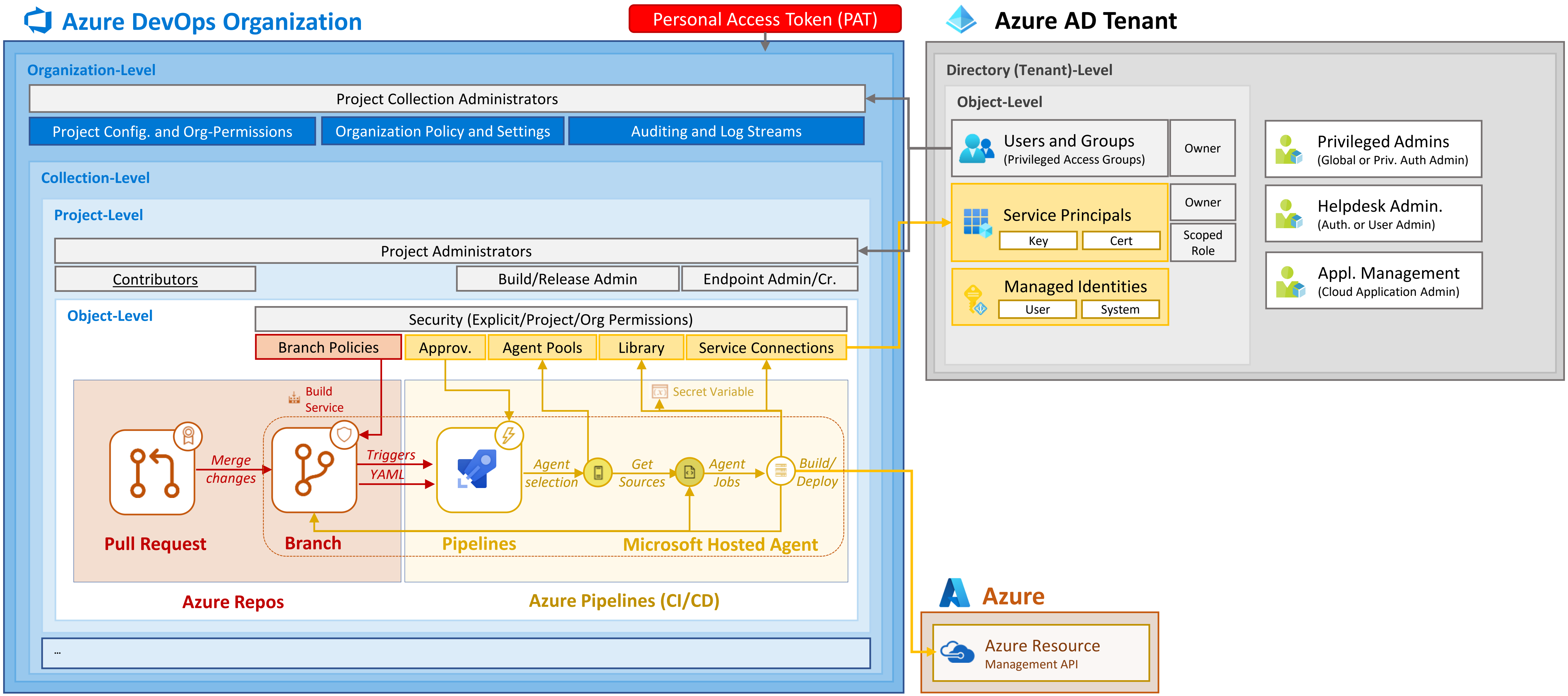
Security Posture and RBAC Management of DevOps Platform

Repository Protection and Compliance Policies

Restricted and audited pipelines on secured agents

Protection and Monitoring of Workload Identity

Overview of Azure DevOps and Security



Azure DevOps Organization

Personal Access Token (PAT)

Organization-Level

Project Collection Administrators

Project Config. and Org-Permissions

Organization Policy and Settings

Auditing and Log Streams

Collection-Level

Project-Level

Project Administrators

Contributors

Build/Release Admin

Endpoint Admin/Cr.

Object-Level

Security (Explicit/Project/Org Permissions)

Branch Policies

Approv.

Agent Pools

Library

Service Connections

Build Service

Secret Variable

Merge changes

Triggers YAML

Agent selection

Get Sources

Agent Jobs

Build/ Deploy

Pull Request

Branch

Pipelines

Microsoft Hosted Agent

Azure Repos

Azure Pipelines (CI/CD)

...

Azure AD Tenant

Directory (Tenant)-Level

Object-Level

Users and Groups (Privileged Access Groups)

Owner

Service Principals

Key

Cert

Owner

Scoped Role

Managed Identities

User

System

Privileged Admins (Global or Priv. Auth Admin)

Helpdesk Admin. (Auth. or User Admin)

Appl. Management (Cloud Application Admin)

Azure

Azure Resource Management API

Live Demo

- Security Configuration of Azure DevOps Org/Projects
- Azure Sentinel Analytics to detect suspicious DevOps activities

Foundation of Pipelines in Dev(Sec)Ops

Security Posture and RBAC Management of DevOps Platform

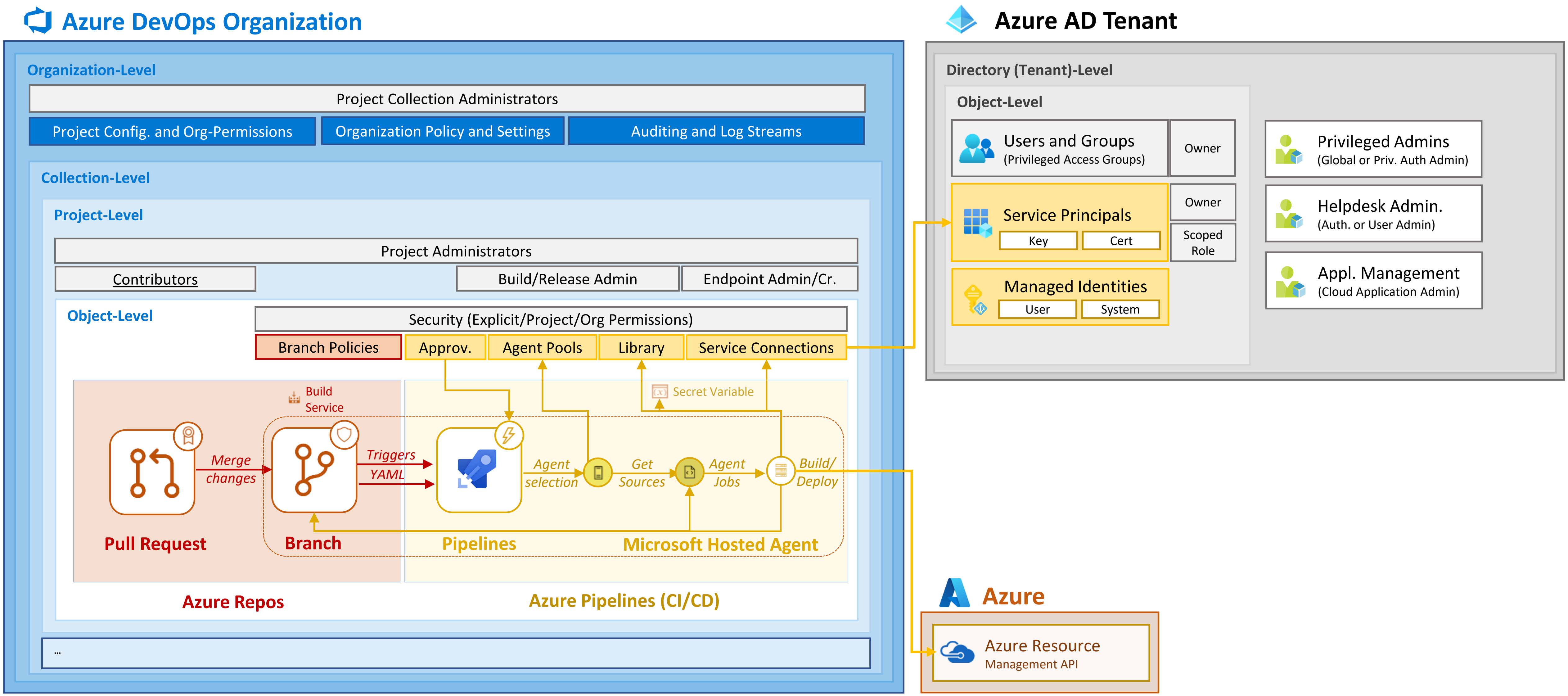
Repository Protection and Compliance Policies

Restricted and audited pipelines on secured agents

Protection and Monitoring of Workload Identity

→ [Azure Security Benchmark v3 (DevOps Security)]()

Overview of Azure DevOps and Azure Pipelines



Azure DevOps Organization

Organization-Level

Project Collection Administrators

Project Config. and Org-Permissions

Organization Policy and Settings

Auditing and Log Streams

Collection-Level

Project-Level

Project Administrators

Contributors

Build/Release Admin

Endpoint Admin/Cr.

Object-Level

Security (Explicit/Project/Org Permissions)

Branch Policies

Approv.

Agent Pools

Library

Service Connections

Build Service

Secret Variable

Merge changes

Triggers YAML

Agent selection

Get Sources

Agent Jobs

Build/ Deploy

Pull Request

Branch

Pipelines

Microsoft Hosted Agent

Azure Repos

Azure Pipelines (CI/CD)

...

Azure AD Tenant

Directory (Tenant)-Level

Object-Level

Users and Groups (Privileged Access Groups)

Owner

Service Principals

Key

Cert

Owner

Scoped Role

Managed Identities

User

System

Privileged Admins (Global or Priv. Auth Admin)

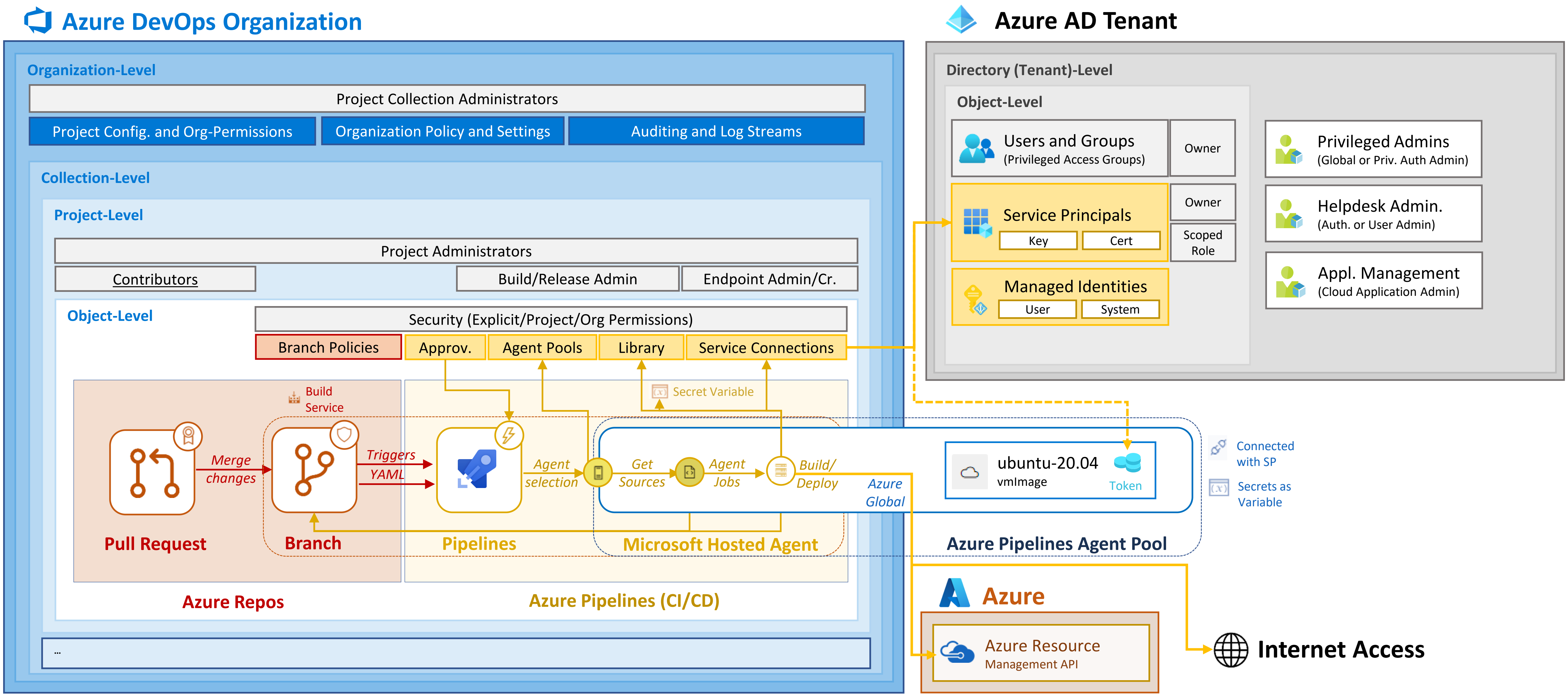
Helpdesk Admin. (Auth. or User Admin)

Appl. Management (Cloud Application Admin)

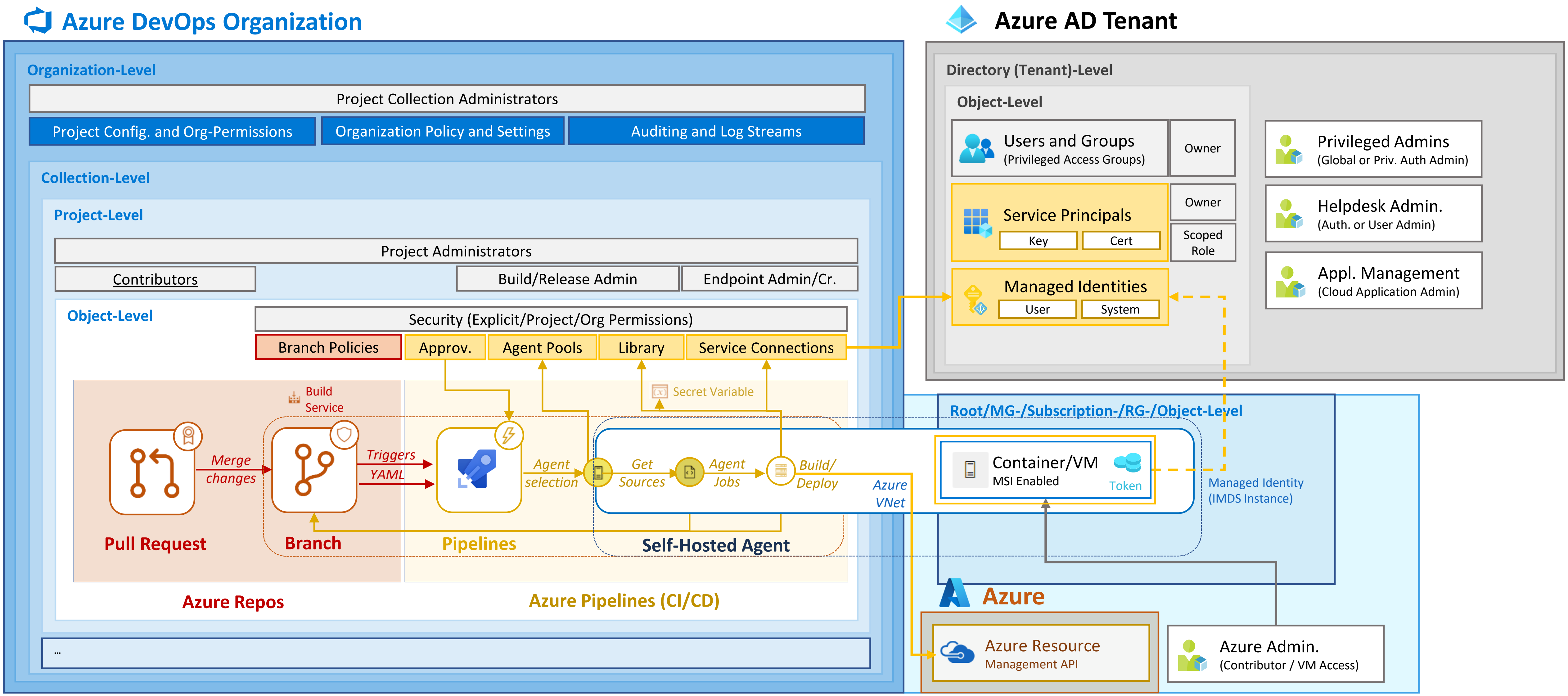
Azure

Azure Resource Management API

Azure Pipelines with Microsoft Hosted Agents



Azure Pipelines with Self Hosted Agents



Live Demo

- Exfiltration of Access Token
- Protection and Isolation of high-priv. Pipeline & Agents
- Monitoring of Abuse usage

Questions?

@Thomas_Live

www.cloud-architekt.net

Key takeaways
“Securing Privileged IAM in Microsoft Azure”

	Foundation	Enterprise, regulatory or sensitive environment
Privileged Identities	• Separation of work and privileged accounts • Password-less authentication • CA Policies to limit access from specific devices, protect and restrict authorization paths to interfaces • Microsoft Sentinel+MDCA to detect suspicious events, monitor and audit privileged identities & access	• Additional separation of Privileged Identities and Access on Control- and Management Plane • Privileged access on Control (Identity) and Management (Platform) Plane from Secure Admin Workstation (SAW) or secured Pipelines only
Privileged Access	• Design of least privileged RBAC • Just-in-Time Access to privileged user by Azure PIM • Approval, assignment and review privileged roles by Identity Governance • Protection of critical privileged objects by role-assignable/privileged access groups • Configuration in Portal UI • Export as Code for Documentation & Track Changes	• Tiered Admin model on scope of AU- and Service RBAC (avoid Directory-Level Roles) • Reduce numbers of direct assignment of privileged roles (part of privileged pipelines) • RBAC-/Policy-As-Code • Pre-Staged & Adv. QA (Tenant/Test Subscription)
Privileged Pipelines	• Inventory and monitoring of all MSI/Service Principals • Lifecycle Process (Key/Cert Rotation, Access Review) • Auditing, restricted RBAC secure configuration of DevOps Platform and pipelines (incl. branch policies) • Secured certificate-based auth. of Service Principals	• Isolated DevOps management between pipelines of Control-, Management and Workload Plane • Active Monitoring of Token Exfiltration • Self-Hosted/Runner Agents on secured container instances with audited “Managed Identities”

Learn more…
Resources

Privileged Identities

- CA Policies for Privileged Interfaces and Azure-managed Secure Admin Workstation (SAW)
- Workbook of "Azure Security Benchmark" and "M365 Secure Score" in Microsoft Sentinel
- User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel
- Security Operations (Guide) for Privileged Accounts

Privileged Access

- Management capabilities for Privileged Access groups
- Privileged Access Groups: Manage privileged access outside of Aad admin roles with Azure PIM
- Azure AD Administrative Units - Use cases, considerations and limitations
- Security considerations of Azure EA management and potential privilege escalation
- How to operationalize Enterprise-Scale with Infrastructure-as-Code via AzOps

Privileged Pipelines

- ADO Security Scanner and ADOPipelinesSecInfo
- Securing Azure Pipelines
- Azure AD Attack & Defense Playbook: Service Principals in Azure DevOps

Thank You

Hybrid
Identity
Protection