Microsoft

Swiss Post
Cybersecurity

Introduction to Microsoft Azure

Microsoft
Solutions Partner

Security

Specialist
Threat Protection

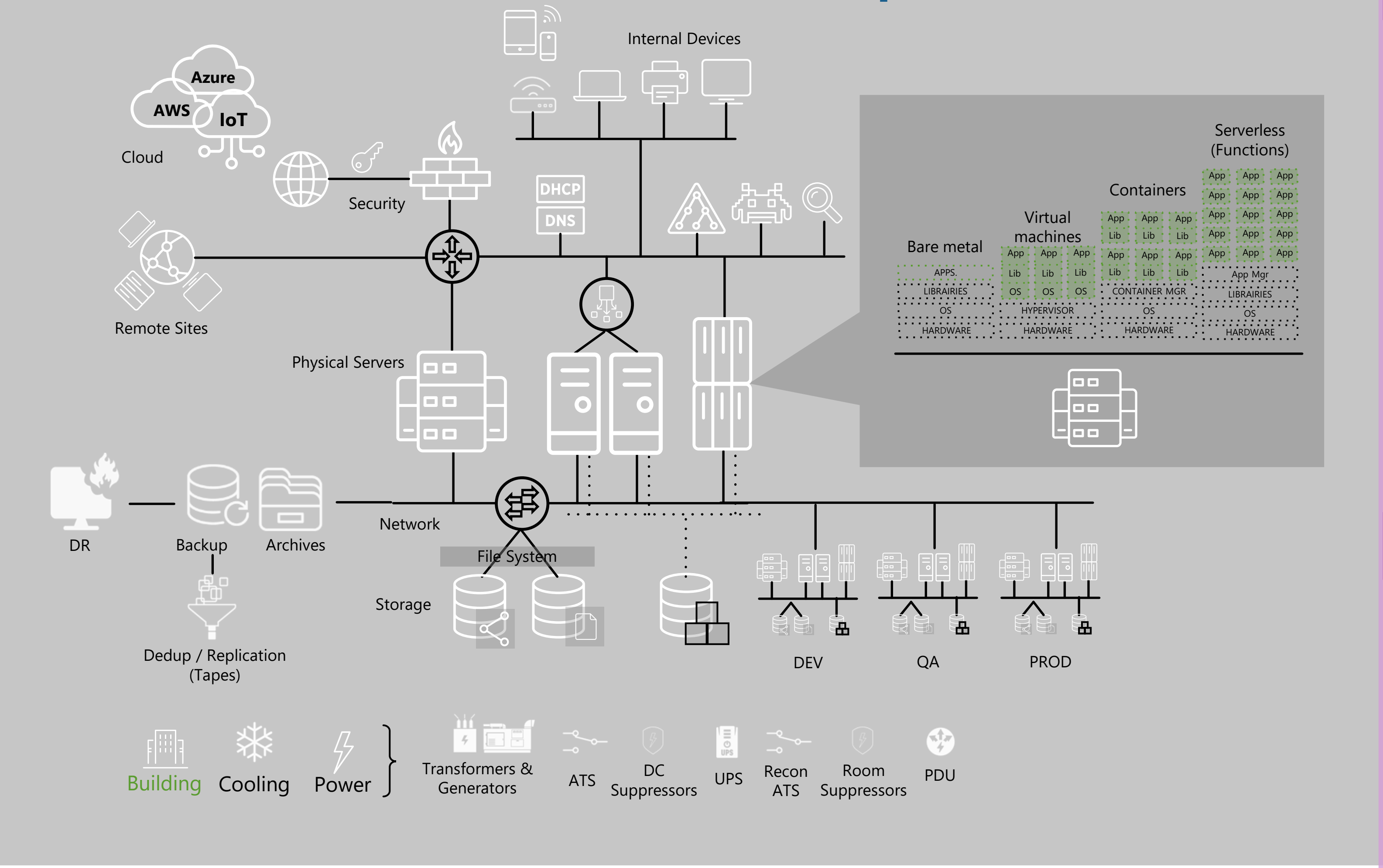
Learning path agenda

- Describe the Azure Architecture
- Describe the Roles
- Understand the licences and products
- Describe Security products and Defender products

Module 1: Describe Azure

The Complexity of IT Infrastructure

Automation – DevSecOps - AI



DEV/APPS

CLOUD

OFFICE

BACKUP/DR

REMOTE

SECURITY

STORAGE

NETWORK

SERVERS

BUILDING

Complex

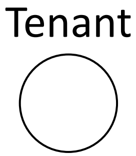
Opaque

Unstable

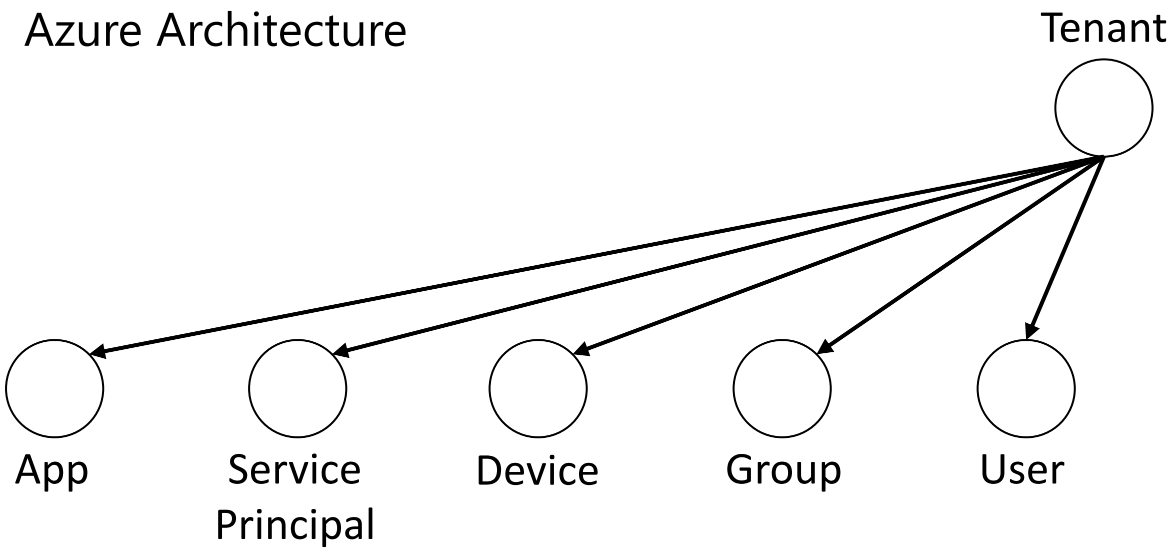
Cyber Security - Governance

Azure Basics

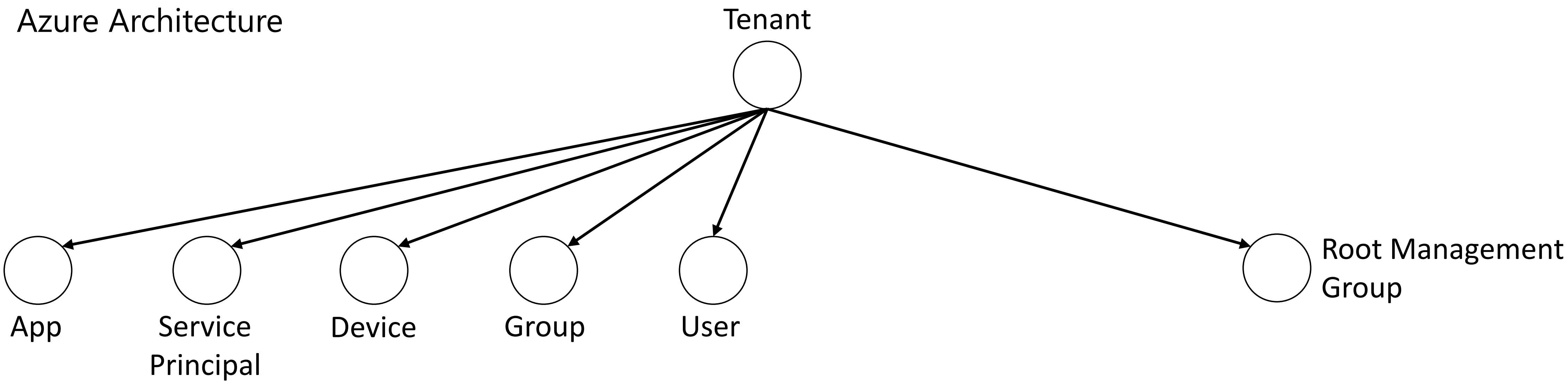
- Understand Azure Architecture
- Understand Roles and Privileges
- Understand Authentication methods


Tenant

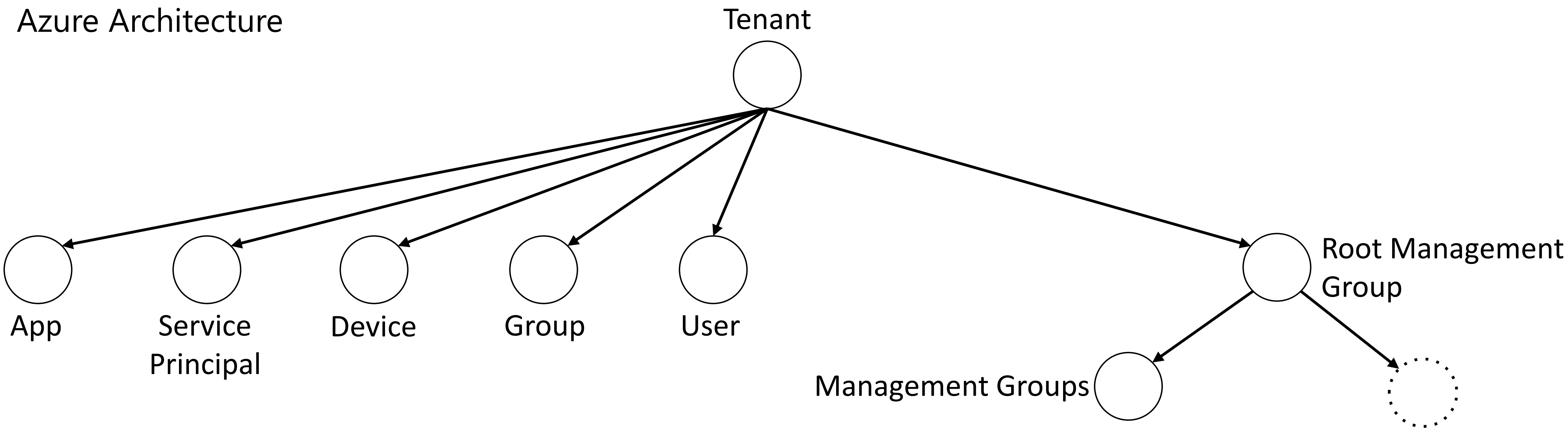
Azure Architecture



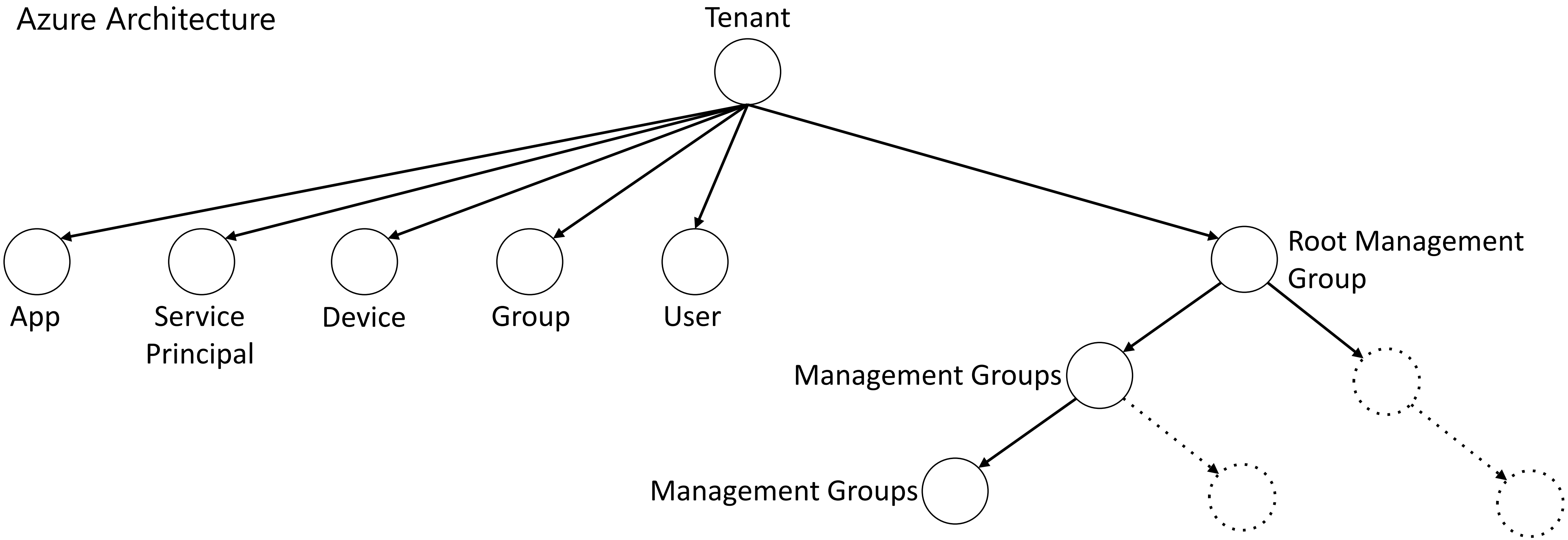
Azure Architecture



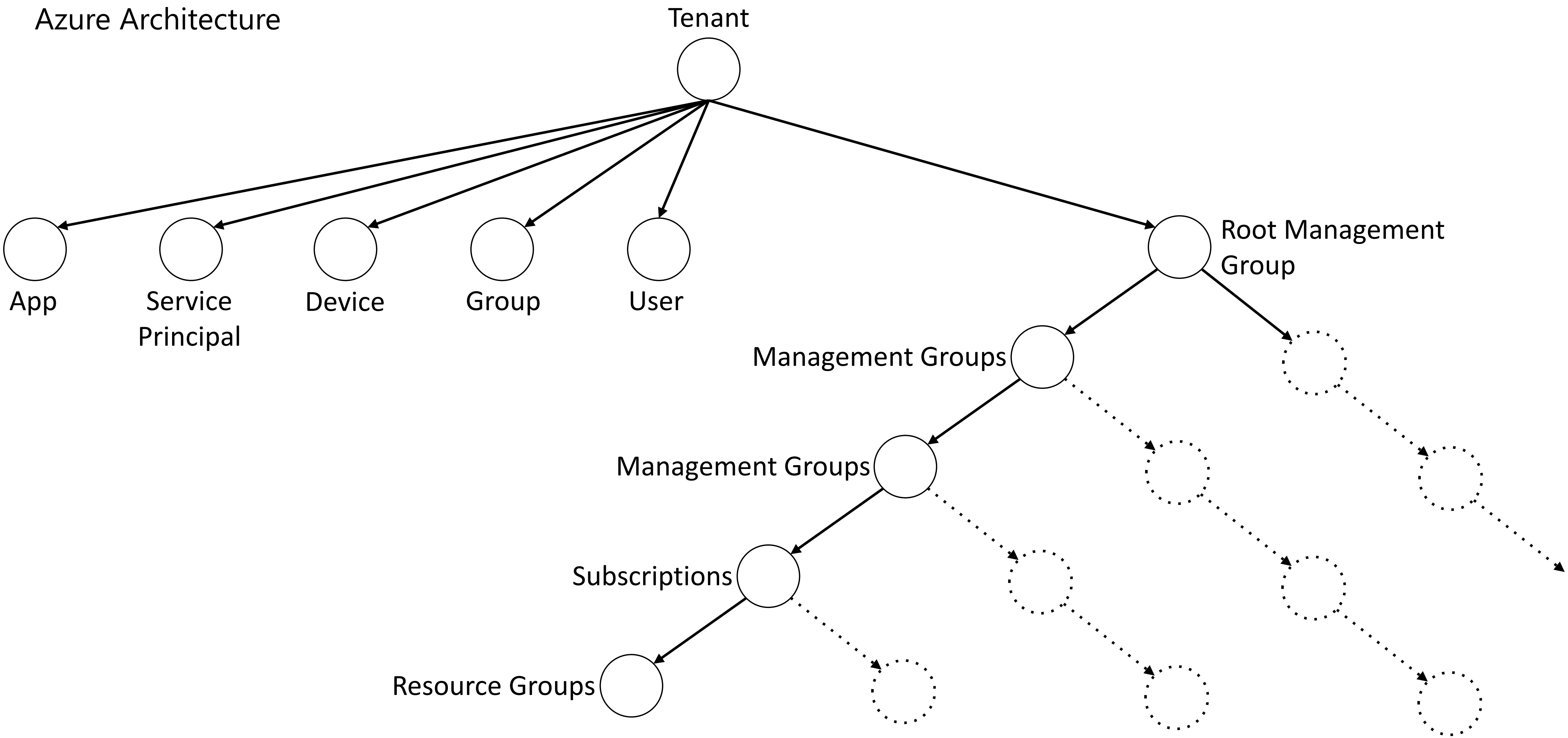
Azure Architecture



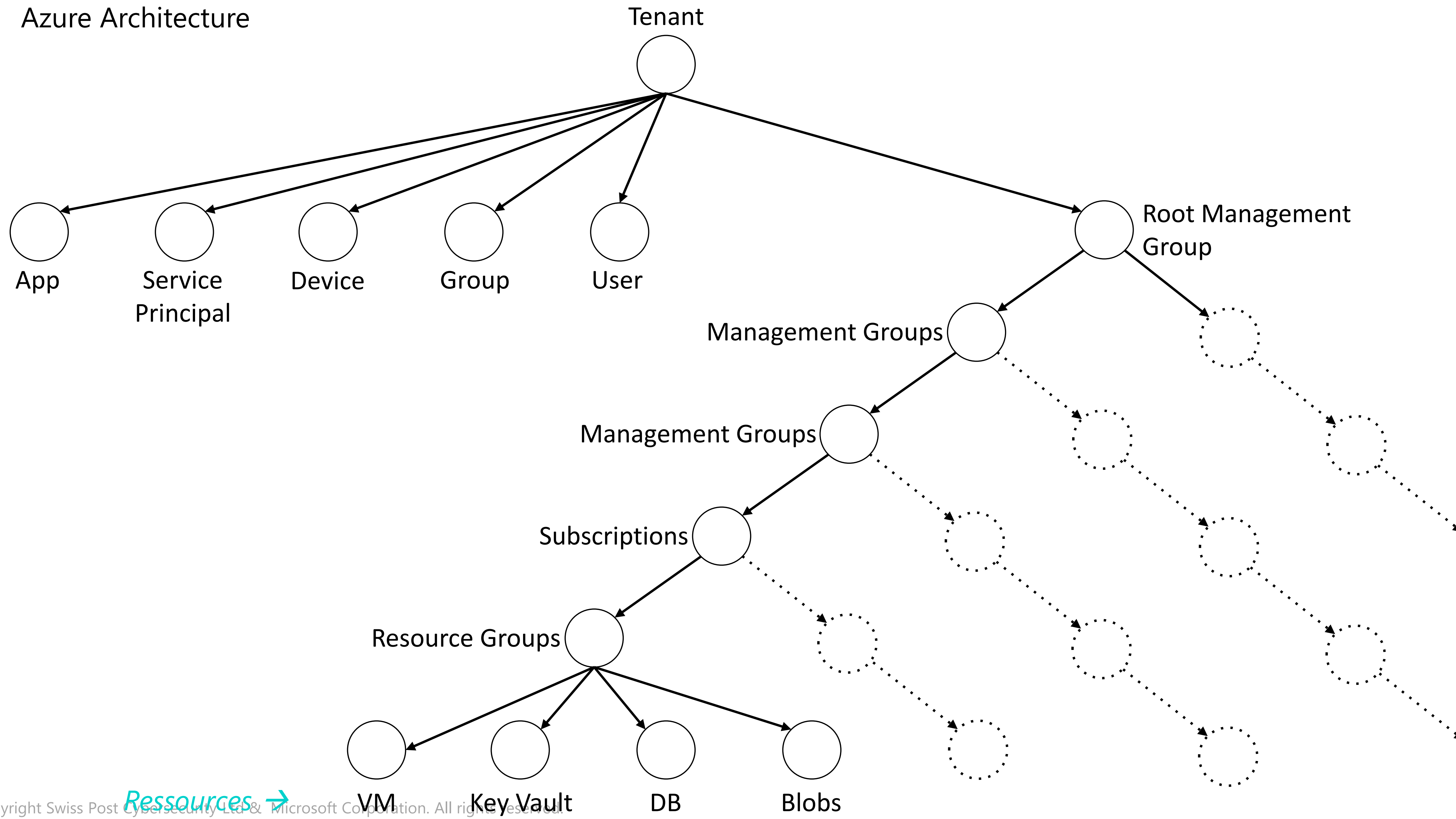
Azure Architecture



Azure Architecture

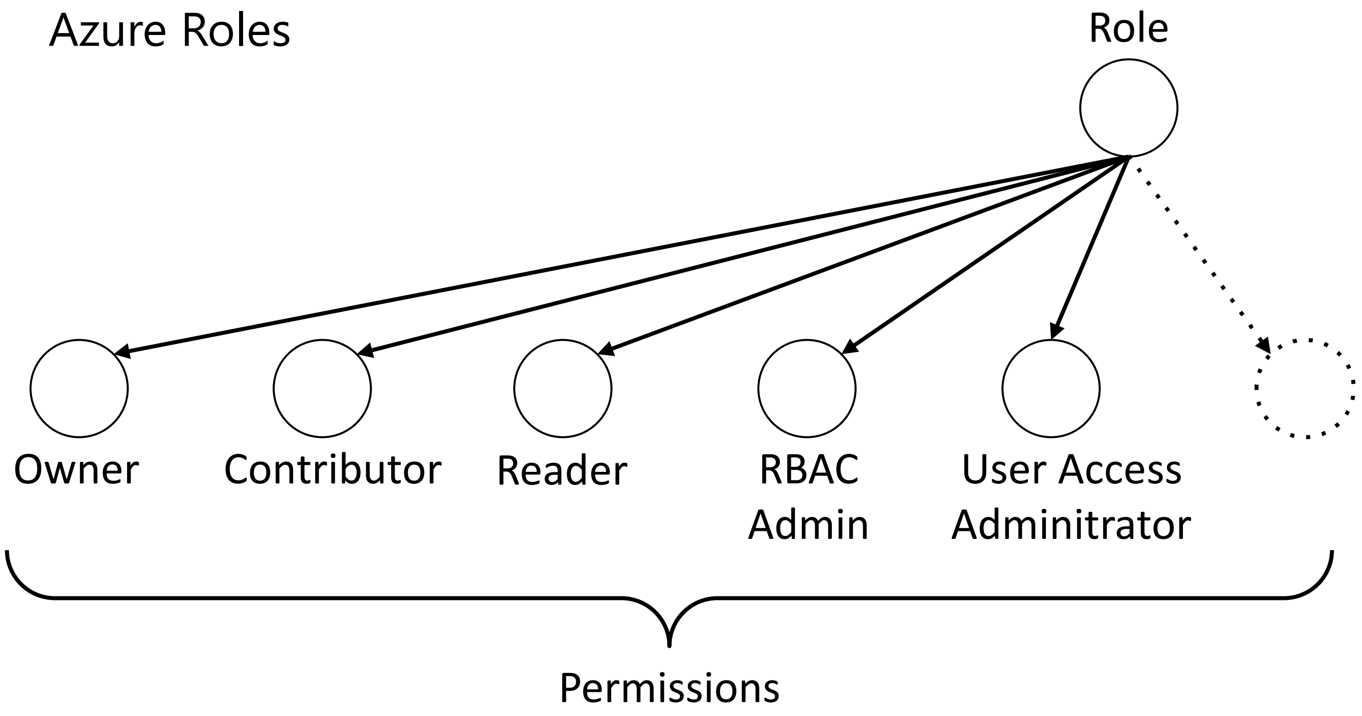


Azure Architecture



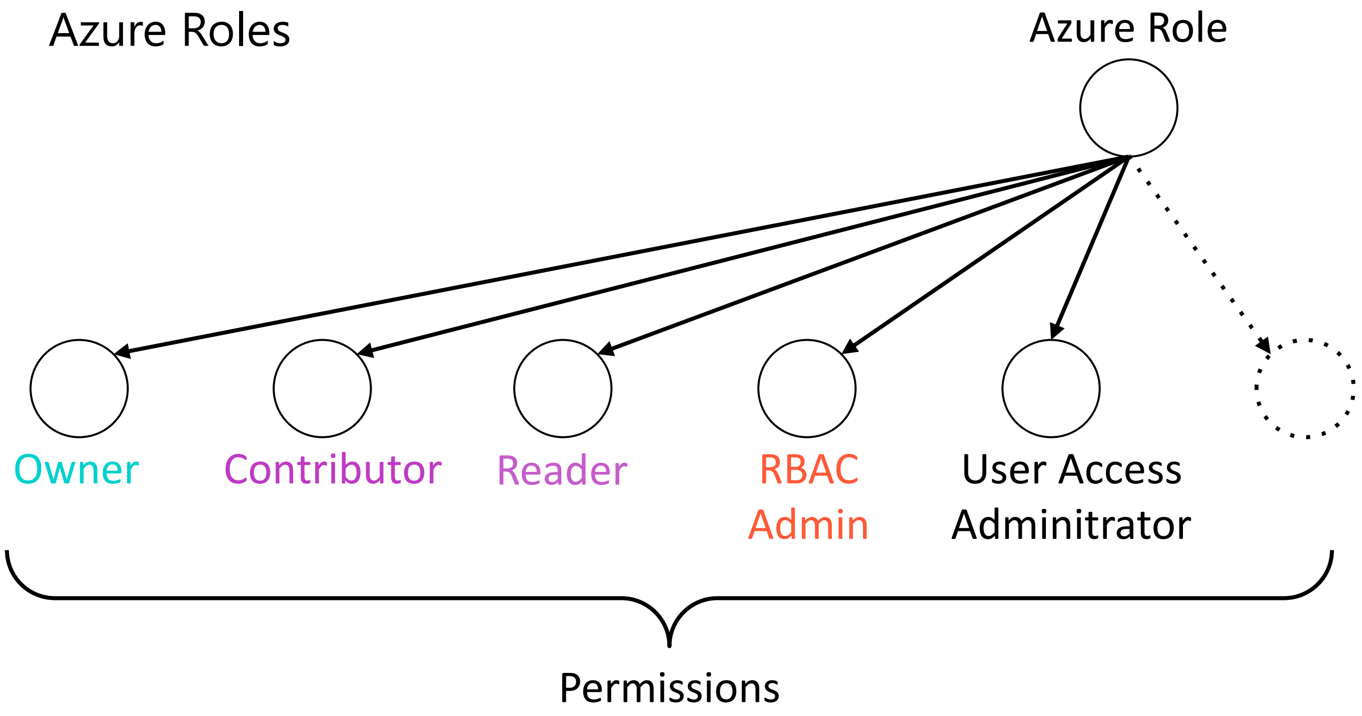
Ressources →

Azure Roles



- *Full access to all Ressources*
- *Can manage access for other users*
- *View all resources*
- *Can manage access for other users*
- *Can’t manage access using Azure Policy*
- *View all resources*
- *Can Manage access for other users*

Azure Roles



Azure Role

Owner

Contributor

Reader

RBAC Admin

User Access Adminitrator

Permissions

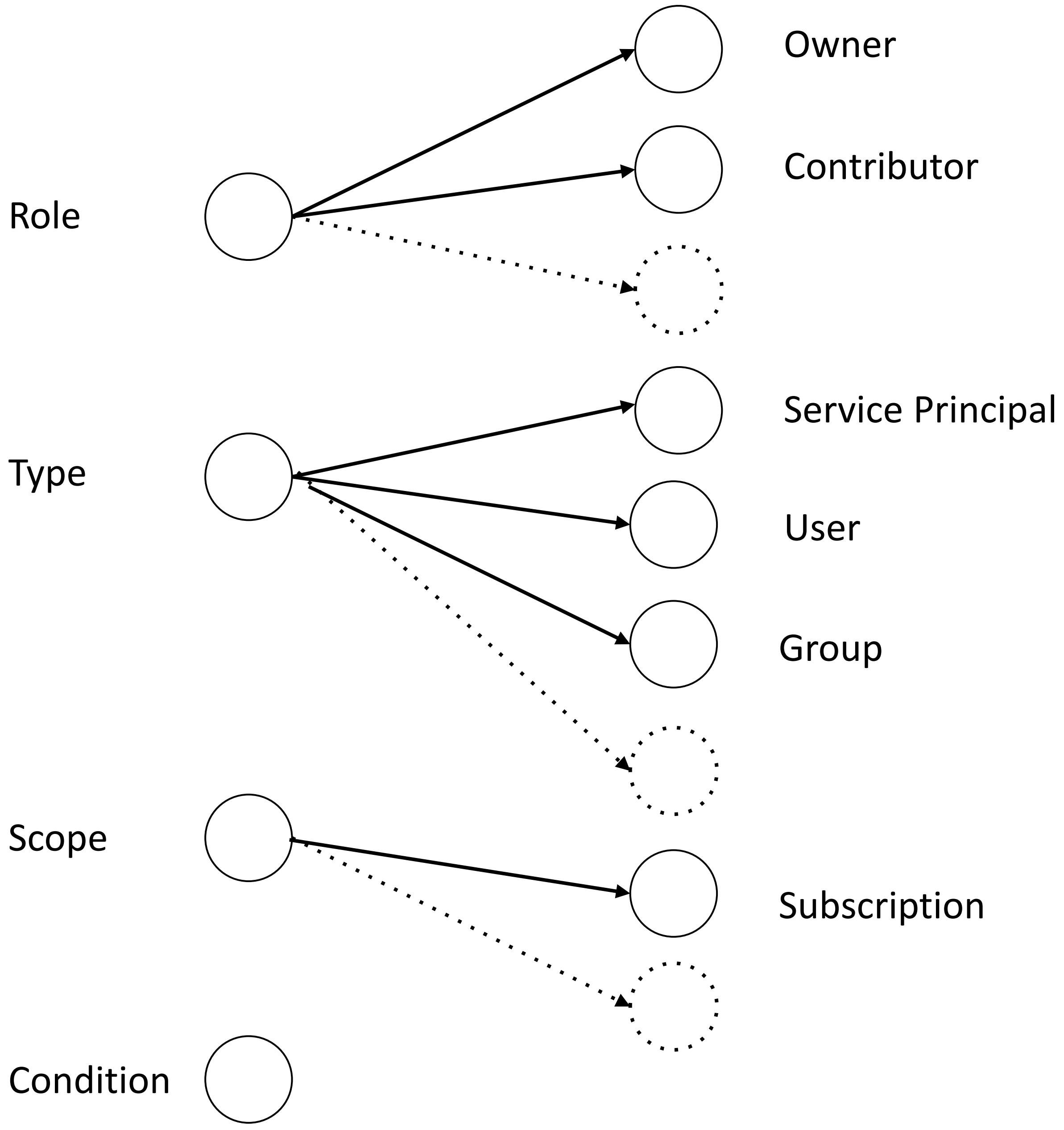
- *Full access to all ressources*
- *Can manage access for other users*
- *Full access to all ressources*
- *Cannot manage access*
- *View all resources*
- *Can manage access for other users*
- *Can’t manage access using Azure Policy*
- *View all resources*
- *Can Manage access for other users*

Applies to “All resource types

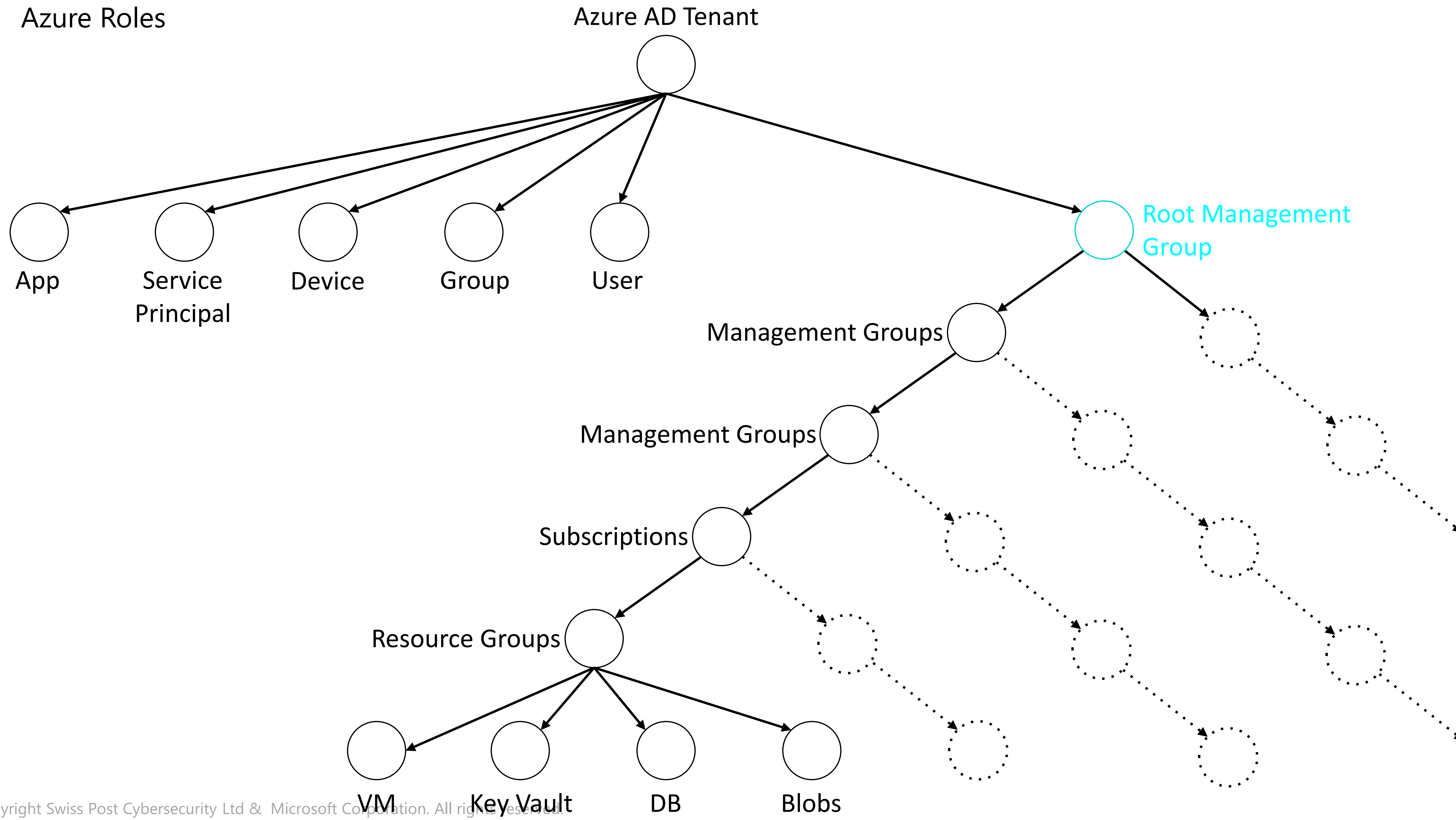
Azure RBAC has over 120 built-on roles, +400 roles on Azure services, and you can create your own custom roles

[List Azure role definitions - Azure RBAC | Microsoft Learn]

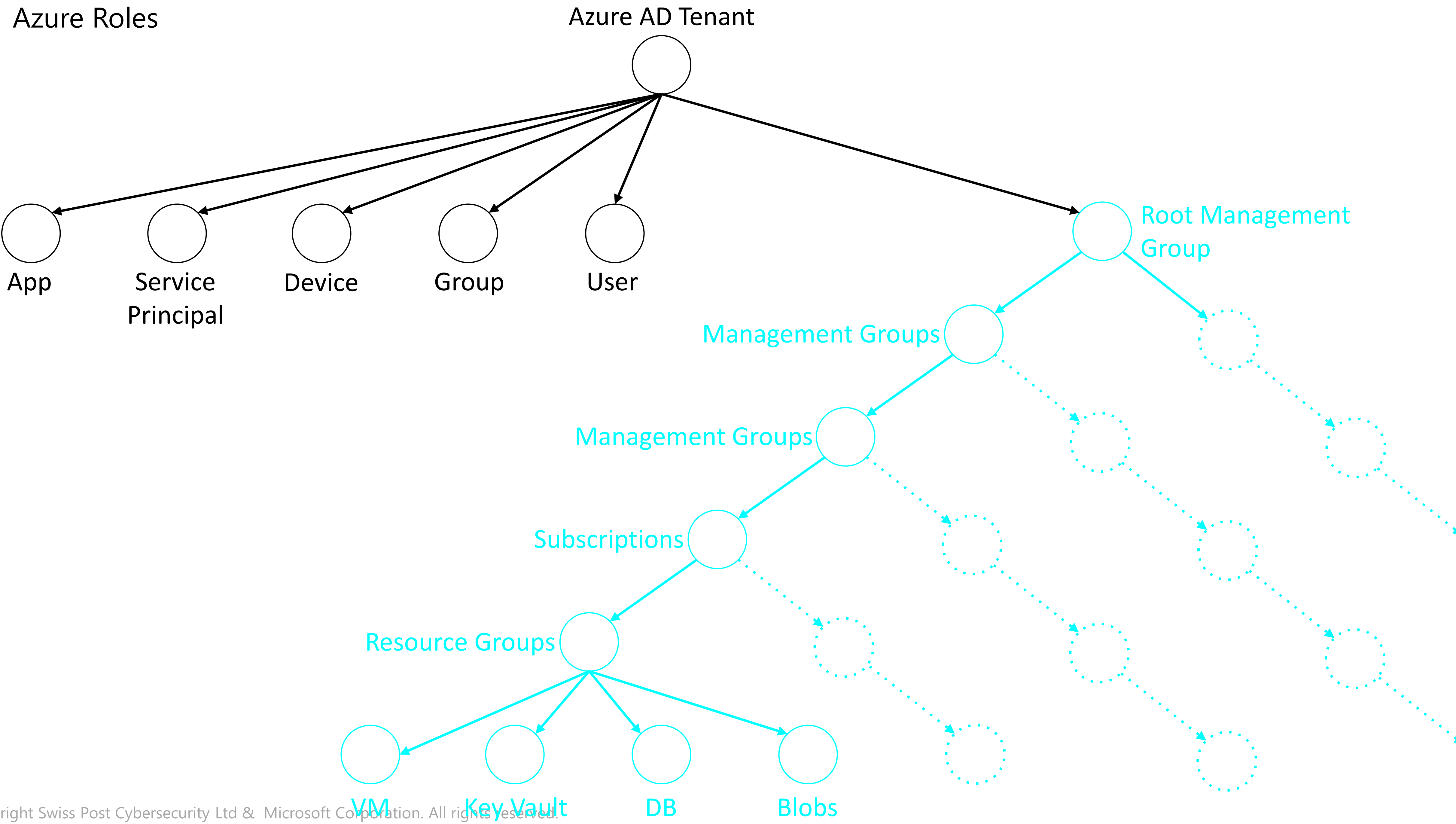
Azure Roles


Owner
Contributor
Role
Service Principal
Type
User
Group
Scope
Subscription
Condition

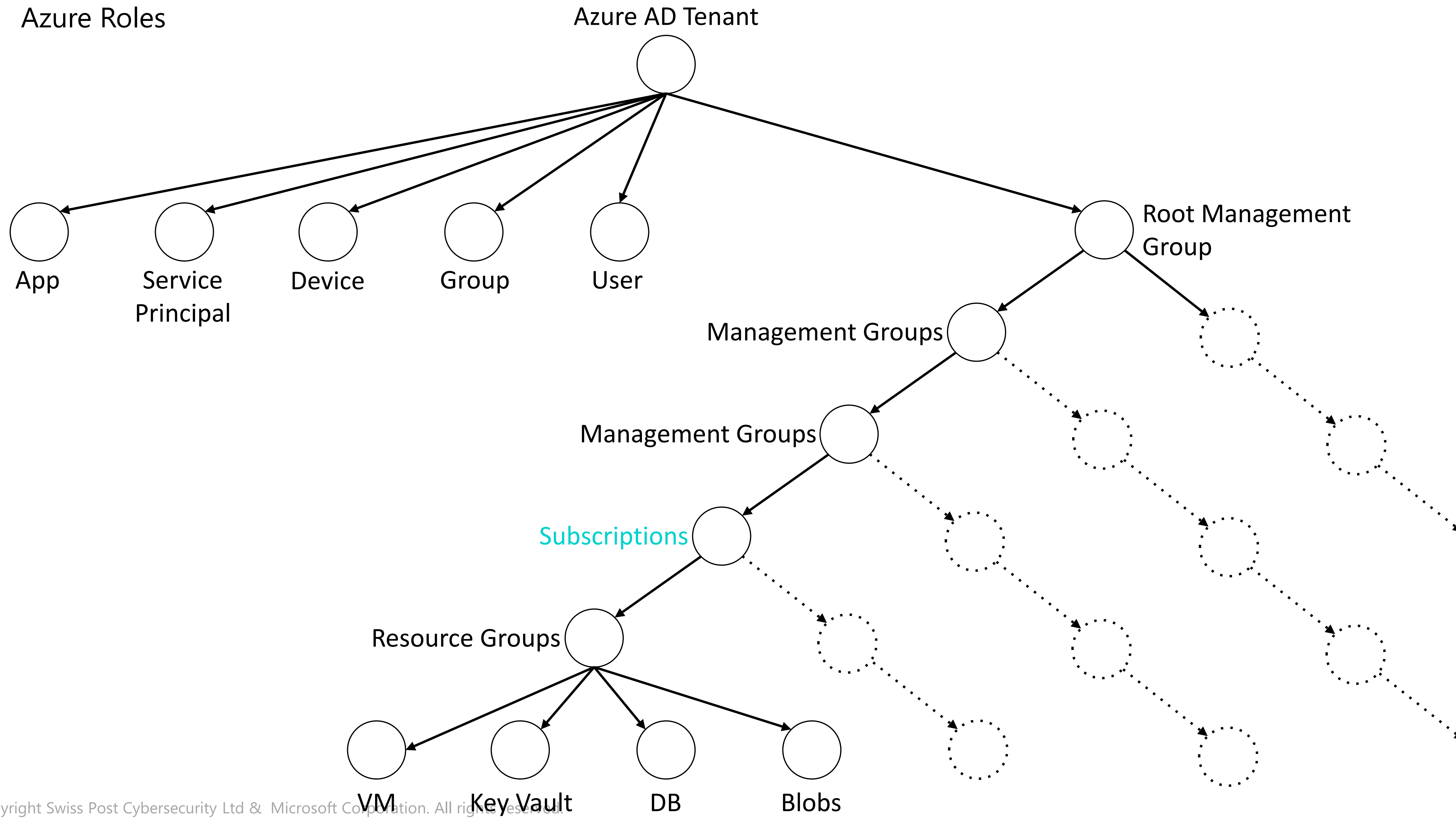
Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Blobs

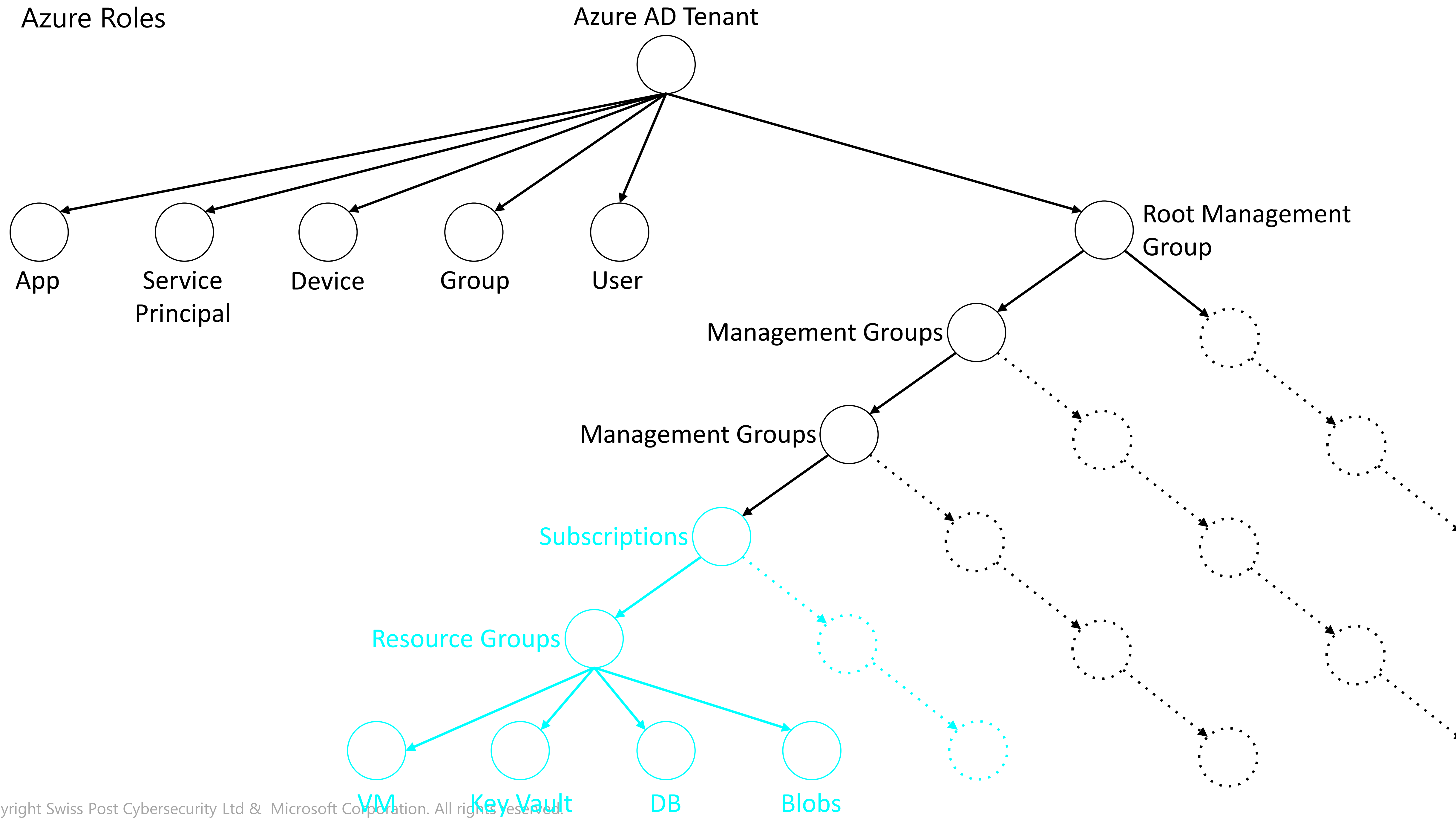
Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Blobs

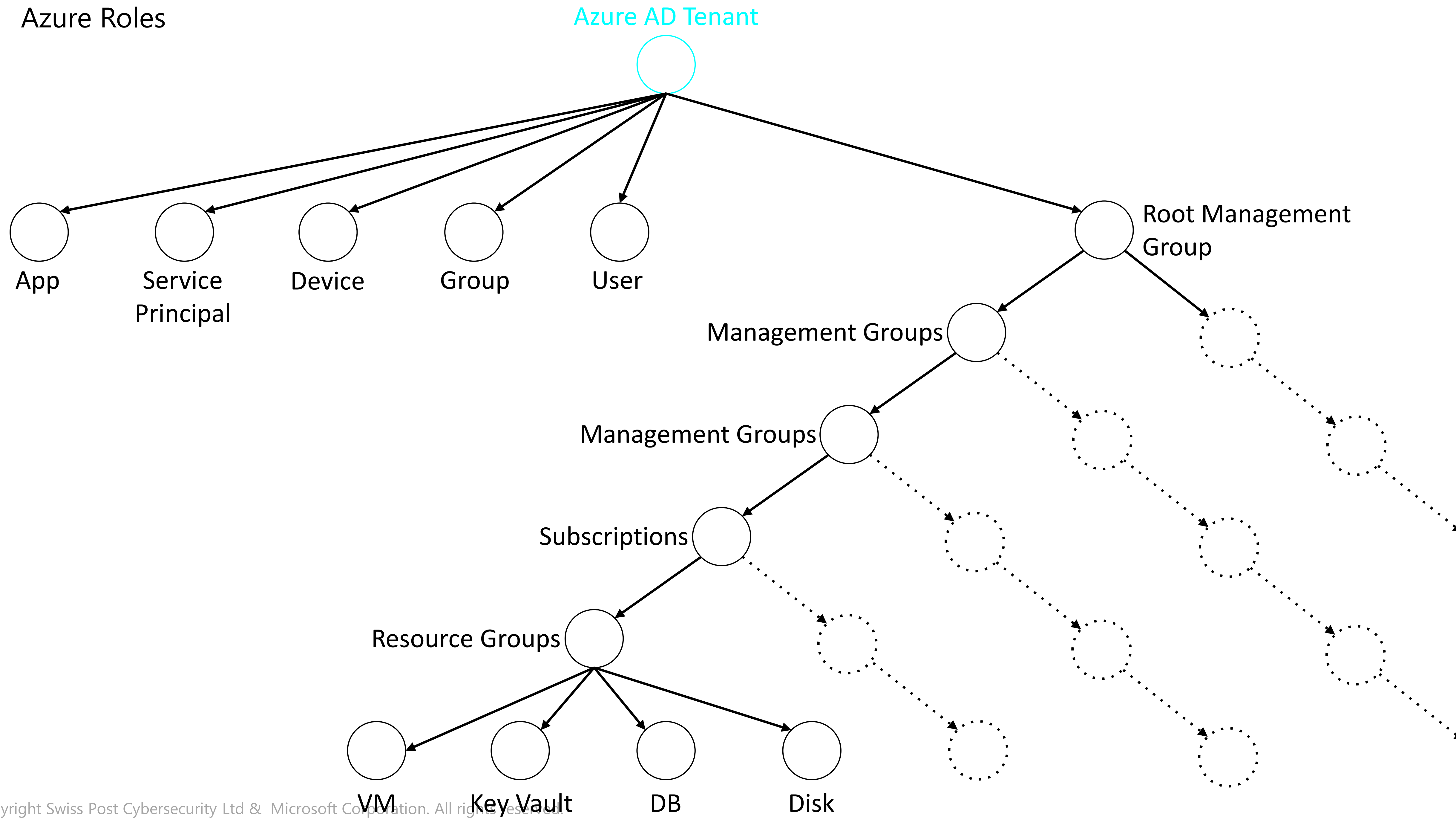
Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Blobs

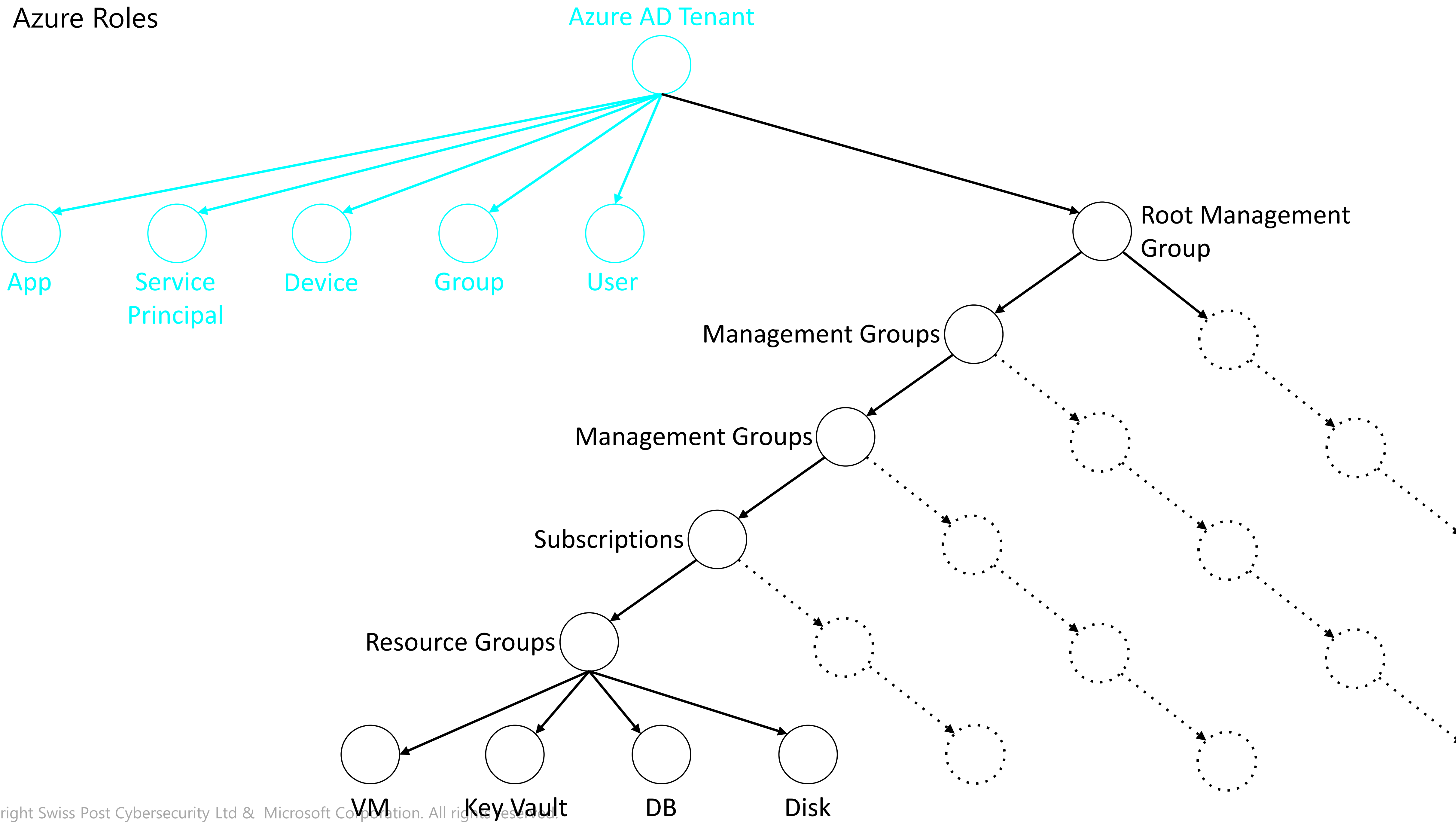
Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Blobs

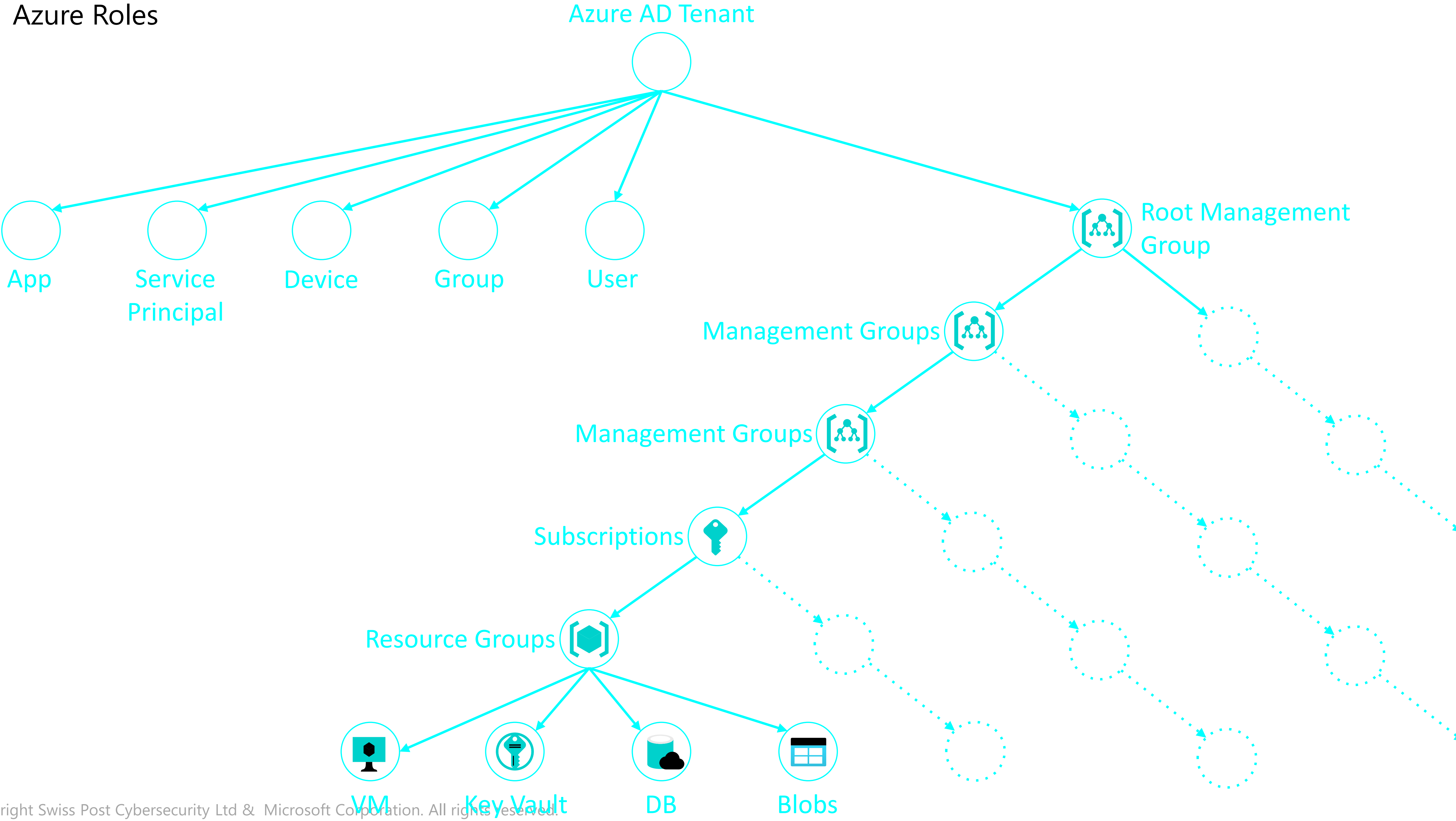
Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Disk

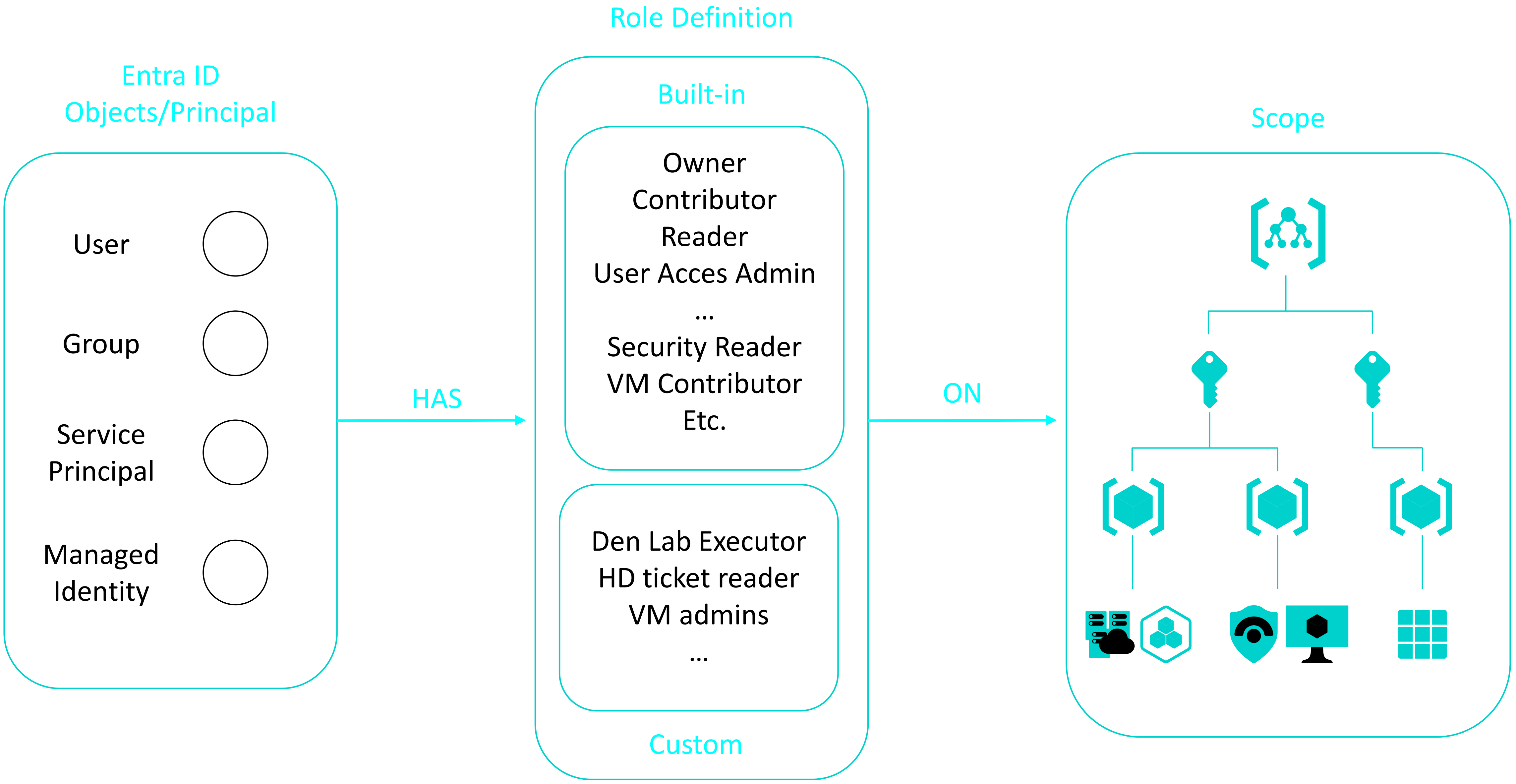
Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Disk

Azure Roles


Azure AD Tenant
App
Service Principal
Device
Group
User
Root Management Group
Management Groups
Management Groups
Subscriptions
Resource Groups
VM
Key Vault
DB
Blobs

Azure Roles



Entra ID Objects/Principal

User

Group

Service Principal

Managed Identity

HAS

Role Definition

Built-in

Owner
Contributor
Reader
User Acces Admin
…
Security Reader
VM Contributor
Etc.

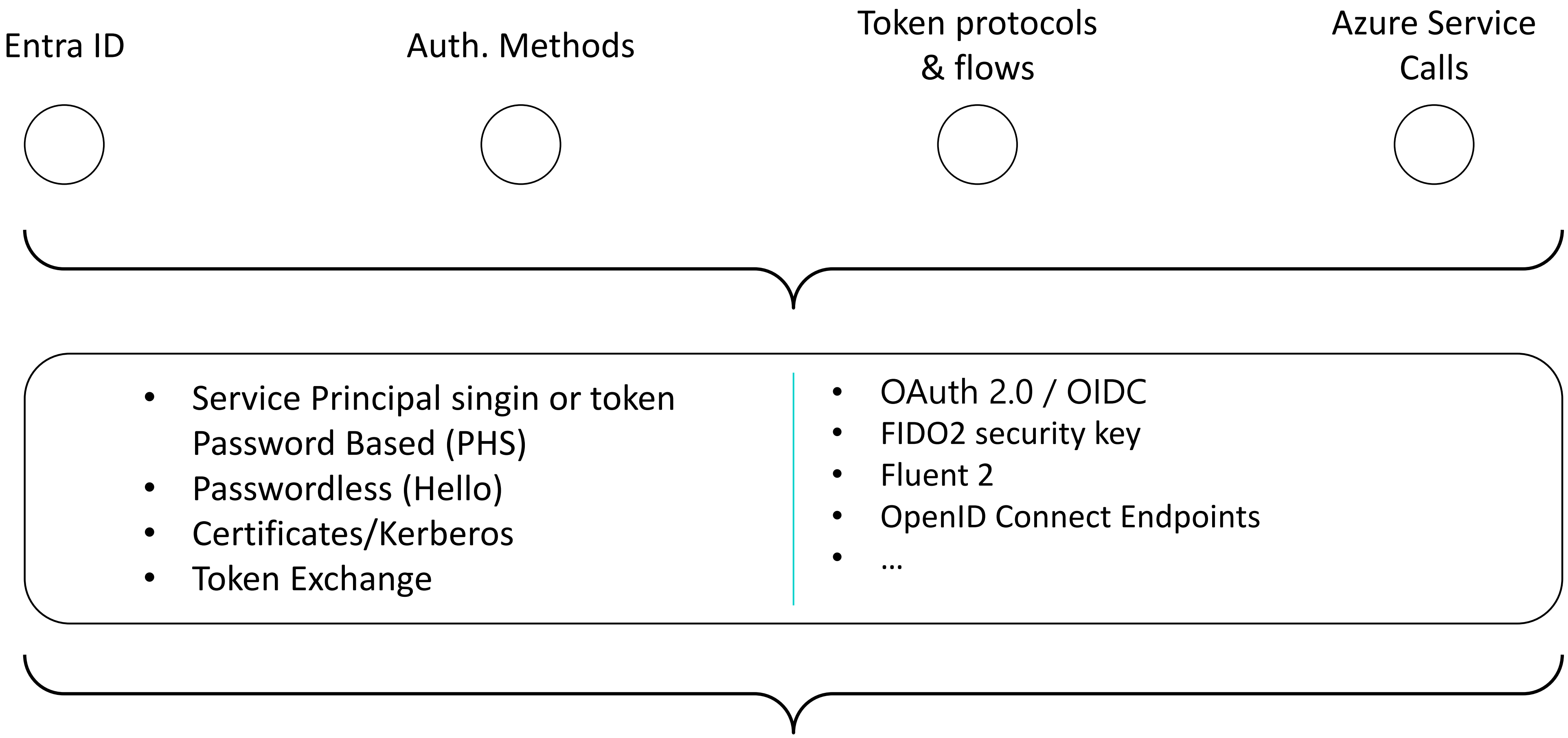
Den Lab Executor
HD ticket reader
VM admins
…

Custom

ON

Scope

Azure Authentication



Entra ID

Auth. Methods

Token protocols & flows

Azure Service Calls

- Service Principal singin or token Password Based (PHS)
- Passwordless (Hello)
- Certificates/Kerberos
- Token Exchange

- OAuth 2.0 / OIDC
- FIDO2 security key
- Fluent 2
- OpenID Connect Endpoints
- …

TOKENS

ID Token/Access Token issued by Entra ID (JWS)
Primary Refresh Token (PRT)
Proof-of-Possesion Token (PoP)
Shared Access Signature token (SAS)

Module 1 introduction

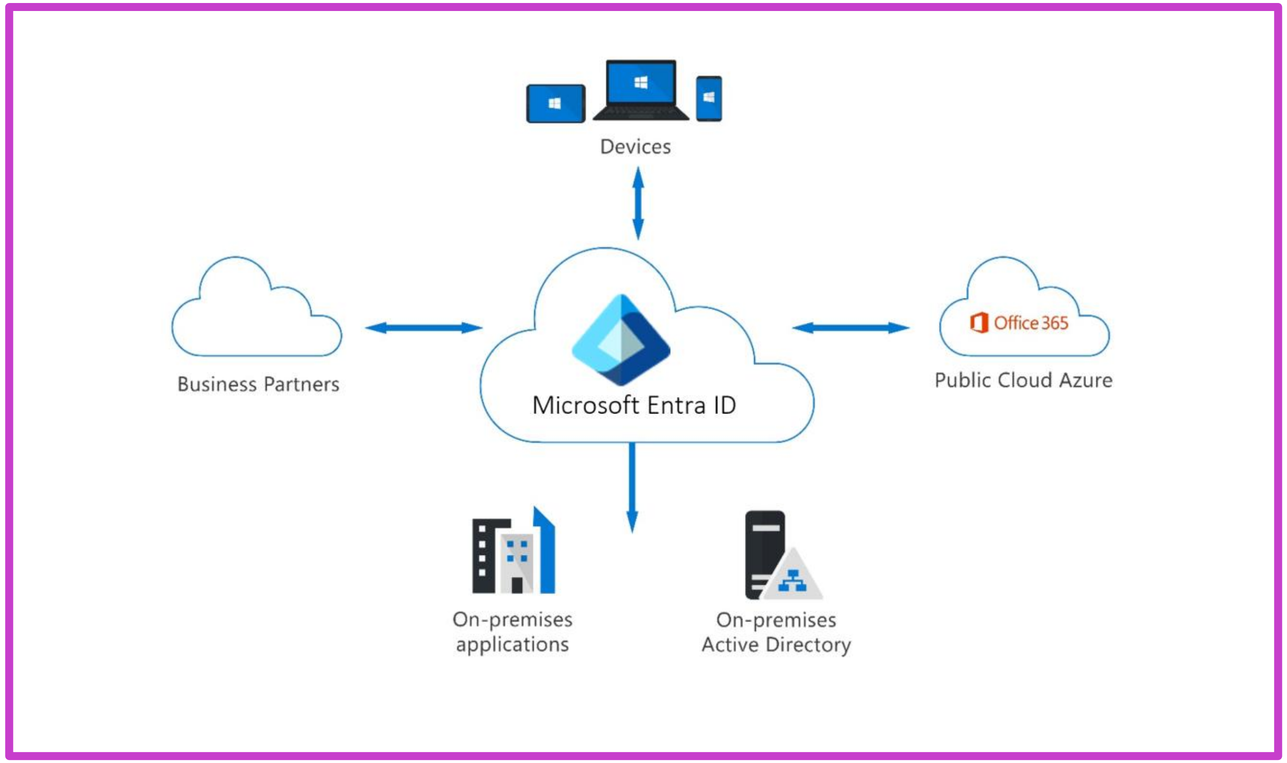
After completing this module, you'll be able to:

1. Describe the core functionality of Microsoft Entra ID.
2. Describe the types of identities supported by Microsoft Entra ID.
3. Describe the concept of hybrid identity as supported by Microsoft Entra ID.

Microsoft Entra ID

Microsoft's cloud-based identity and access management service.

- Organizations can enable their employees, guests, and others to sign in and access the resources they need.
- Provide a single identity system for their cloud and on-premises applications.
- Protect user identities and credentials to meet an organization's access governance requirements.
- Subscribers to Azure services, Microsoft 365, or Dynamics 365 automatically have access to Microsoft Entra ID.
- Identity secure score.



Identity types

Human (user) identities

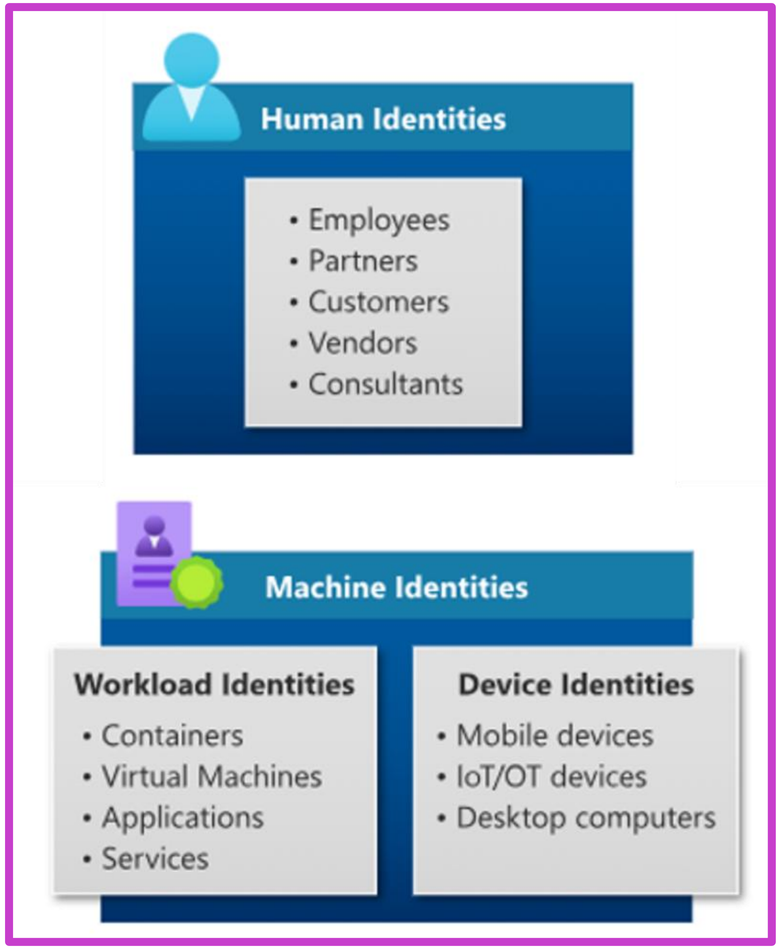
- Internal users – Employees.
- External users – Guests, partners, customers, and so on.

Workload identities (an identity assigned to an application or service)

- Service principal – Uses Microsoft Entra ID for identity and access functions; app developers manage credentials.
- Managed identities – A service principal managed in Microsoft Entra ID that eliminates the need for app developers to manage credentials.

Devices

- Microsoft Entra ID registered – Support for bring your own device.
- Microsoft Entra ID joined – Device joined via an organizational account.
- Hybrid joined – Devices are joined to your on-premises Active Directory and Microsoft Entra ID, requiring organizational account to sign in.



Human Identities

- Employees
- Partners
- Customers
- Vendors
- Consultants

Machine Identities

Workload Identities

- Containers
- Virtual Machines
- Applications
- Services

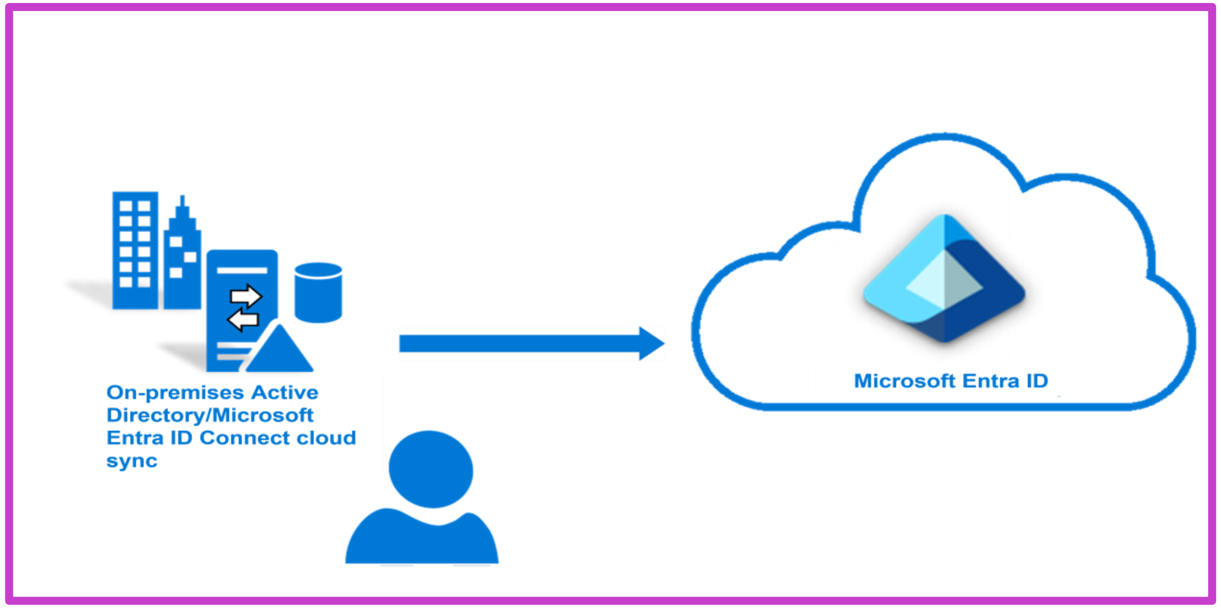
Device Identities

- Mobile devices
- IoT/OT devices
- Desktop computers

Hybrid identity

What is a hybrid identity?

- A common user identity for authentication and authorization to on-premises and cloud resources.
- Hybrid identity is accomplished through:
  - Inter-directory provisioning – A user in Active Directory is provisioned into Microsoft Entra ID.
  - Synchronization – Identity information for your on-premises users and groups matches the cloud.
- Microsoft Entra ID Connect cloud sync – A method for provisioning and synchronization.


On-premises Active Directory/Microsoft Entra ID Connect cloud sync
Microsoft Entra ID

Module 2: Explore the authentication capabilities of Microsoft Entra

Module 2 introduction

After completing this module, you’ll be able to:

1. Describe the authentication methods of Microsoft Entra ID.
2. Describe multifactor authentication in Microsoft Entra ID.
3. Describe the password protection and management capabilities of Microsoft Entra ID.

Authentication methods of Microsoft Entra

Passwords (primary auth)

Phone-based authentication

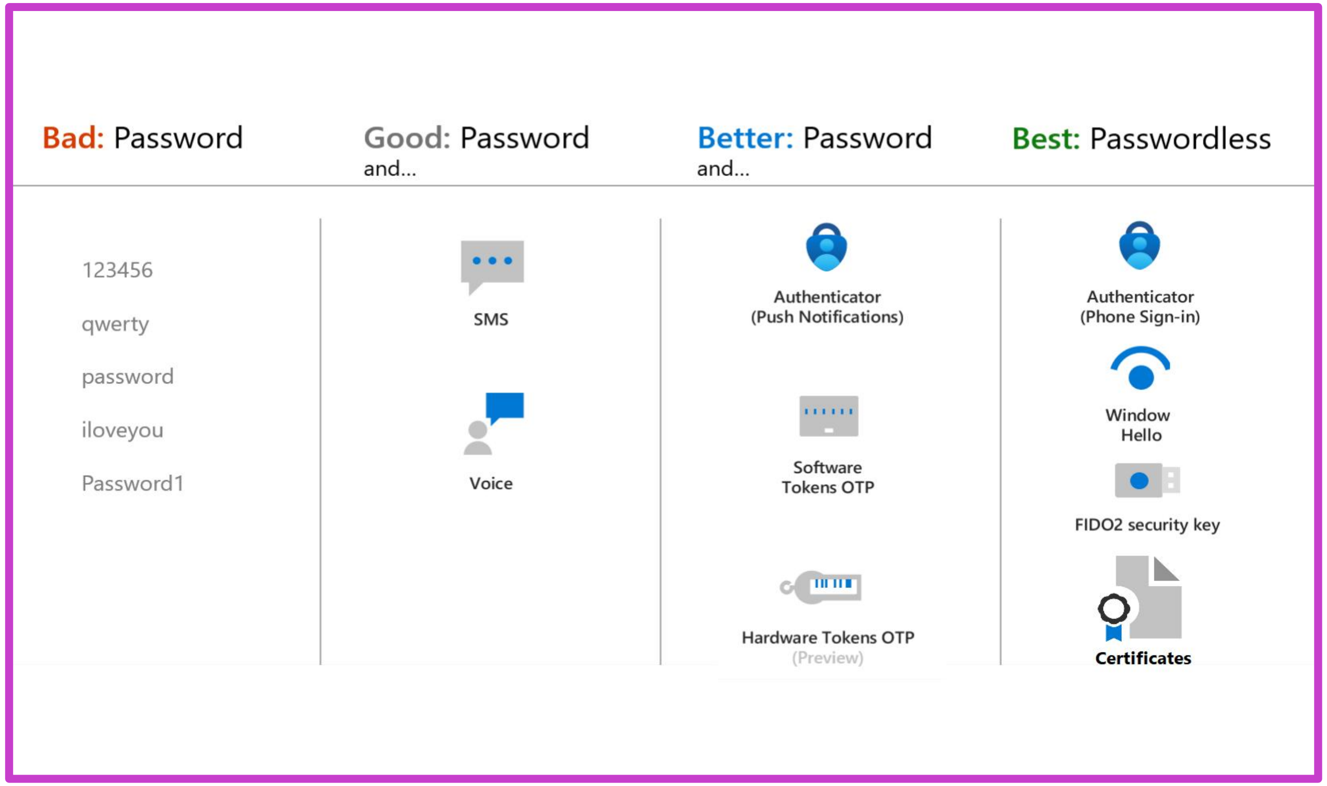
- SMS (primary and secondary auth)
- Voice (secondary auth)

OATH (secondary auth)

- Standard for how one-time password codes are generated
- SW tokens
- HW tokens

Passwordless (primary and secondary auth)

- Windows Hello
- Microsoft Authenticator
- FIDO2
- Certificates (primary auth)



Bad: Password	**Good:** Password and...	**Better:** Password and...	**Best:** Passwordless
123456 qwerty password iloveyou Password1	SMS Voice	Authenticator (Push Notifications) Software Tokens OTP Hardware Tokens OTP (Preview)	Authenticator (Phone Sign-in) Window Hello FIDO2 security key **Certificates**

Multifactor authentication (MFA)

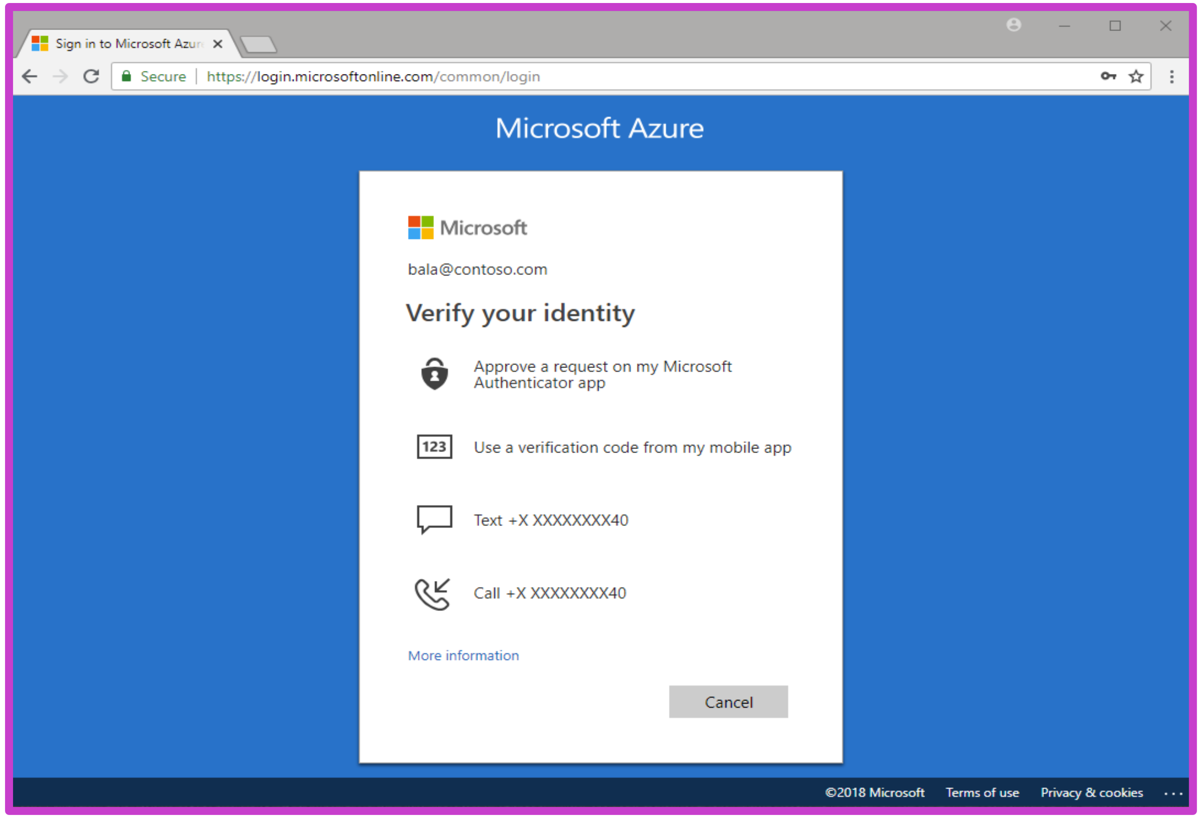
Dramatically improves the security of an identity, while still being simple for users.

MFA requires more than one form of verification

- Something you know.
- Something you have.
- Something you are.

Security defaults

- Requires all users to complete MFA as needed.
- Forces administrators to use MFA.
- Enforces MFA for all users.



Sign in to Microsoft Azur
Secure | https://login.microsoftonline.com/common/login
Microsoft Azure
Microsoft

bala@contoso.com

Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

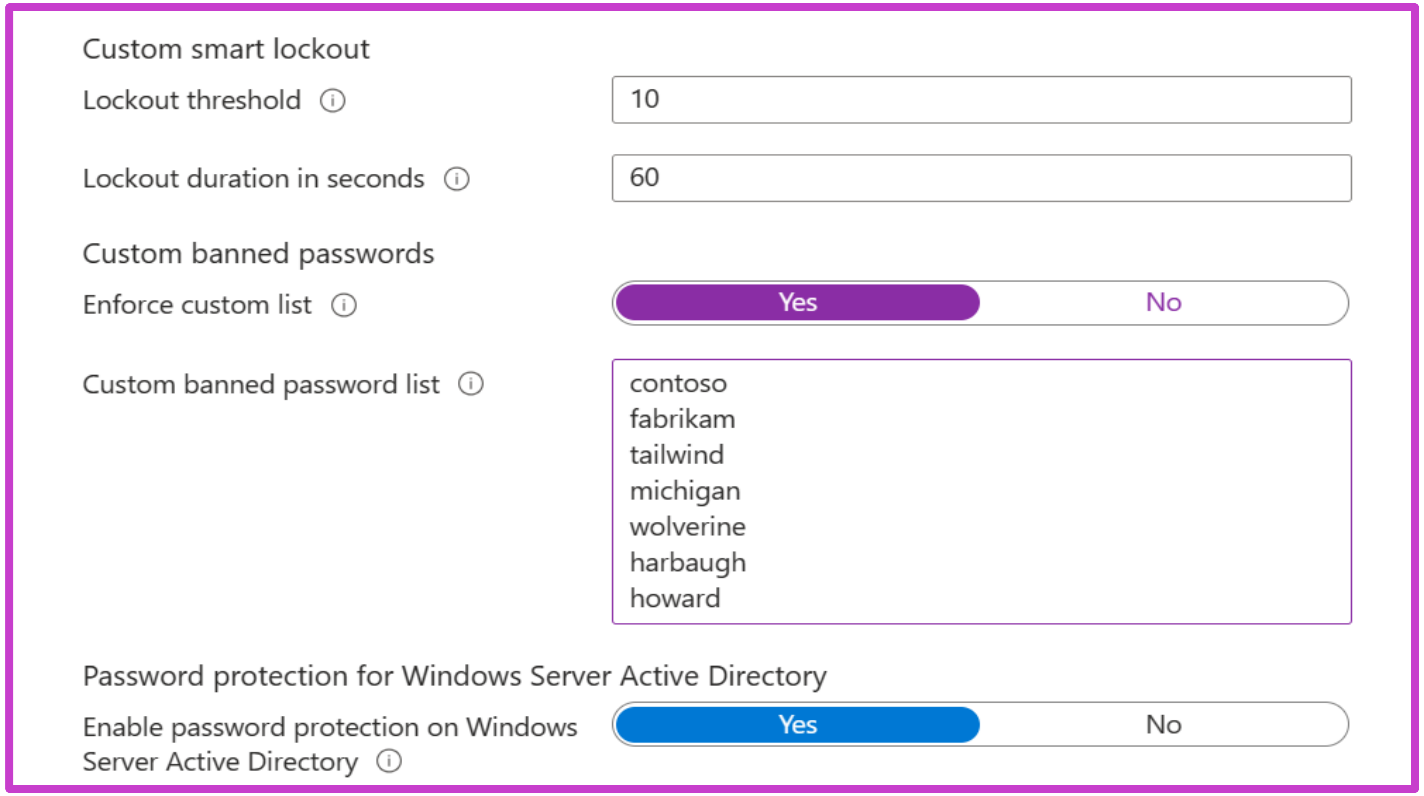
Text +X XXXXXXXX40

Call +X XXXXXXXX40

Password protection and management capabilities

Reduce the risk of users setting weak passwords:

- Global banned password list.
- Custom banned password lists.
- Protecting against password spray.
- Integrates with an on-premises Active Directory environment.



Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ [✓ Yes] No

Custom banned password list ⓘ

contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ [✓ Yes] No

Module 3: Explore the access management capabilities of Microsoft Entra

Module 3 introduction

After completing this module, you'll be able to:

1. Describe Conditional Access and its benefits.
2. Describe Global Secure Access.
3. Describe Microsoft Entra ID roles and role-based access control (RBAC).

Conditional Access

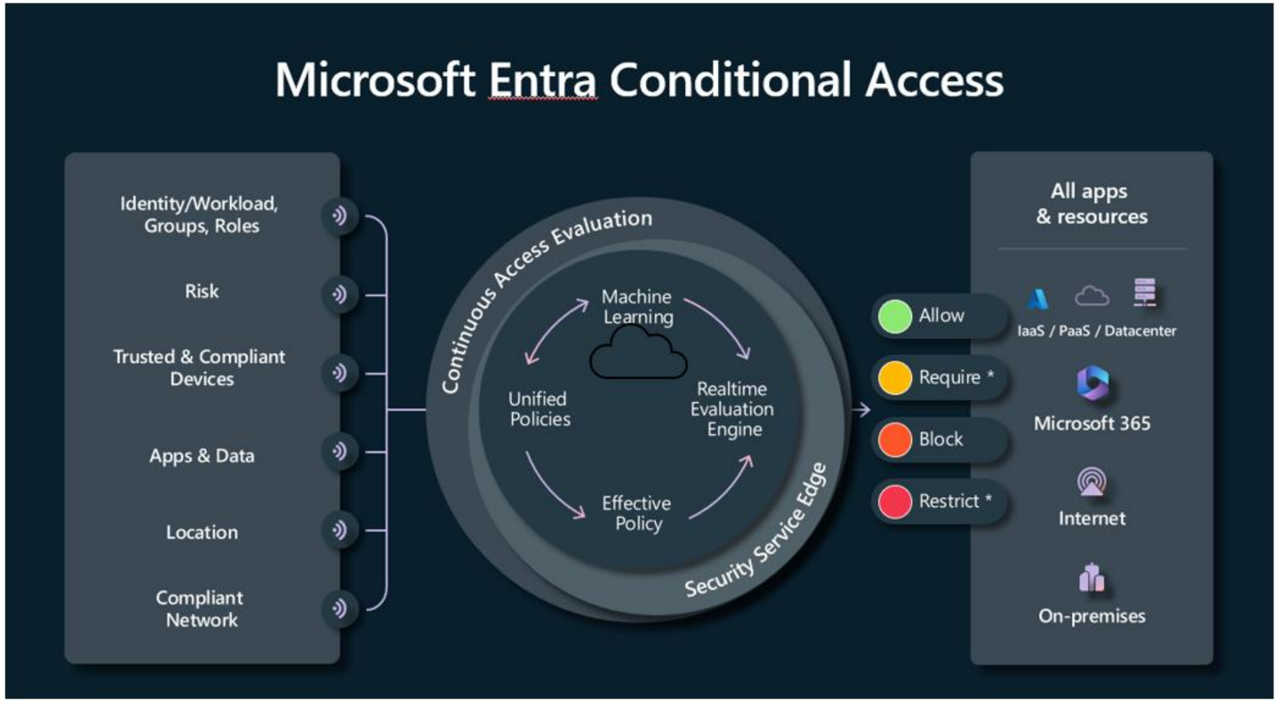
At their simplest, Conditional Access (CA) policies are if-then statements.

Assignments determine which signals to use

- Users, groups, workload identities, directory roles.
- Cloud apps or actions.
- Sign-in and user risk detection.
- Device or device platform.
- IP location.
- More…

Access controls determine how a policy is enforced

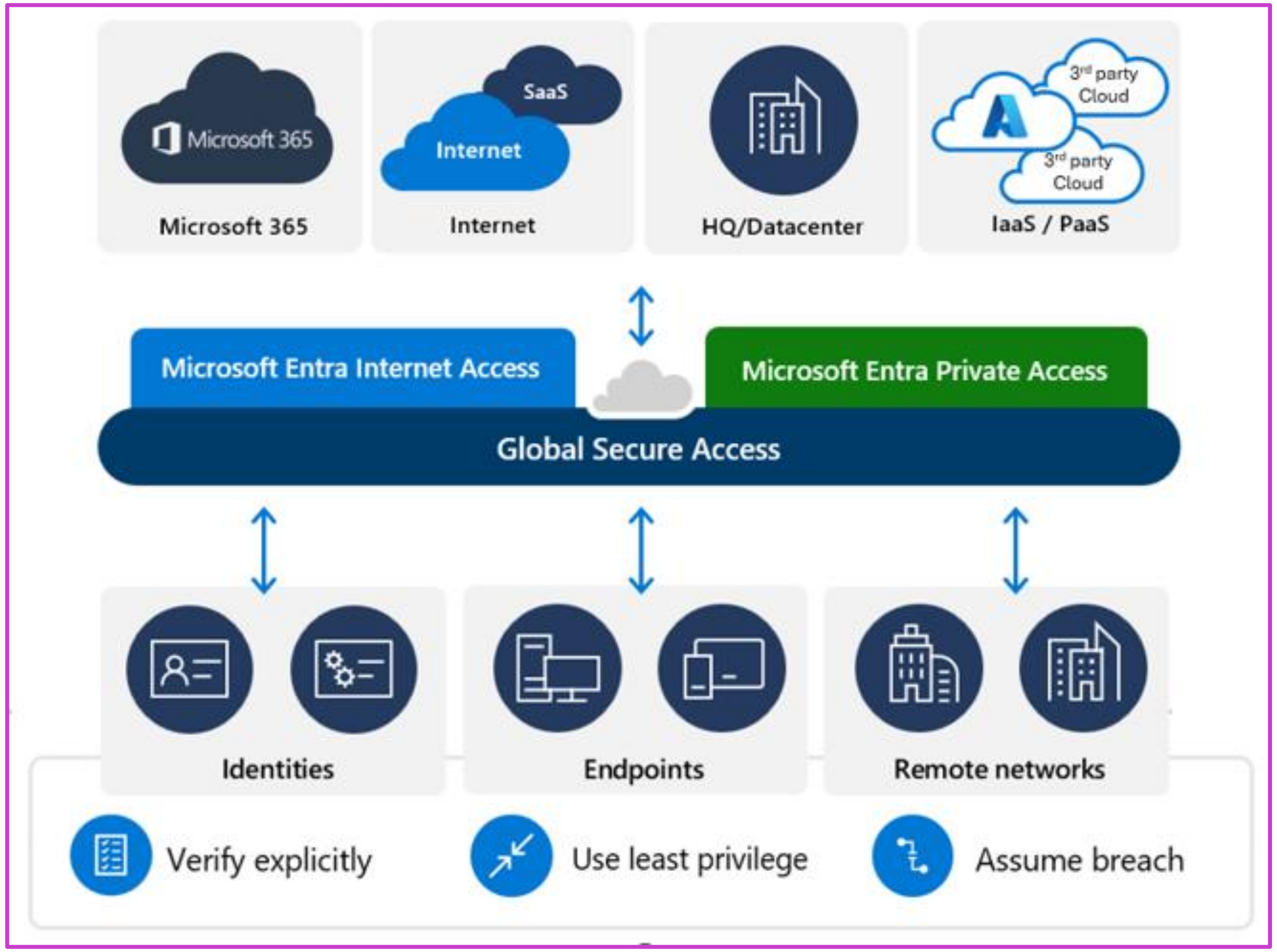
- Block access.
- Grant access – Require one or more conditions to be met before granting access.
- Session control – Enable a limited experience.



Microsoft Entra Global Secure Access

GSA converges **Zero Trust network, identity, and endpoint access controls** to secure access to any app or resource, from any location, device, or identity.

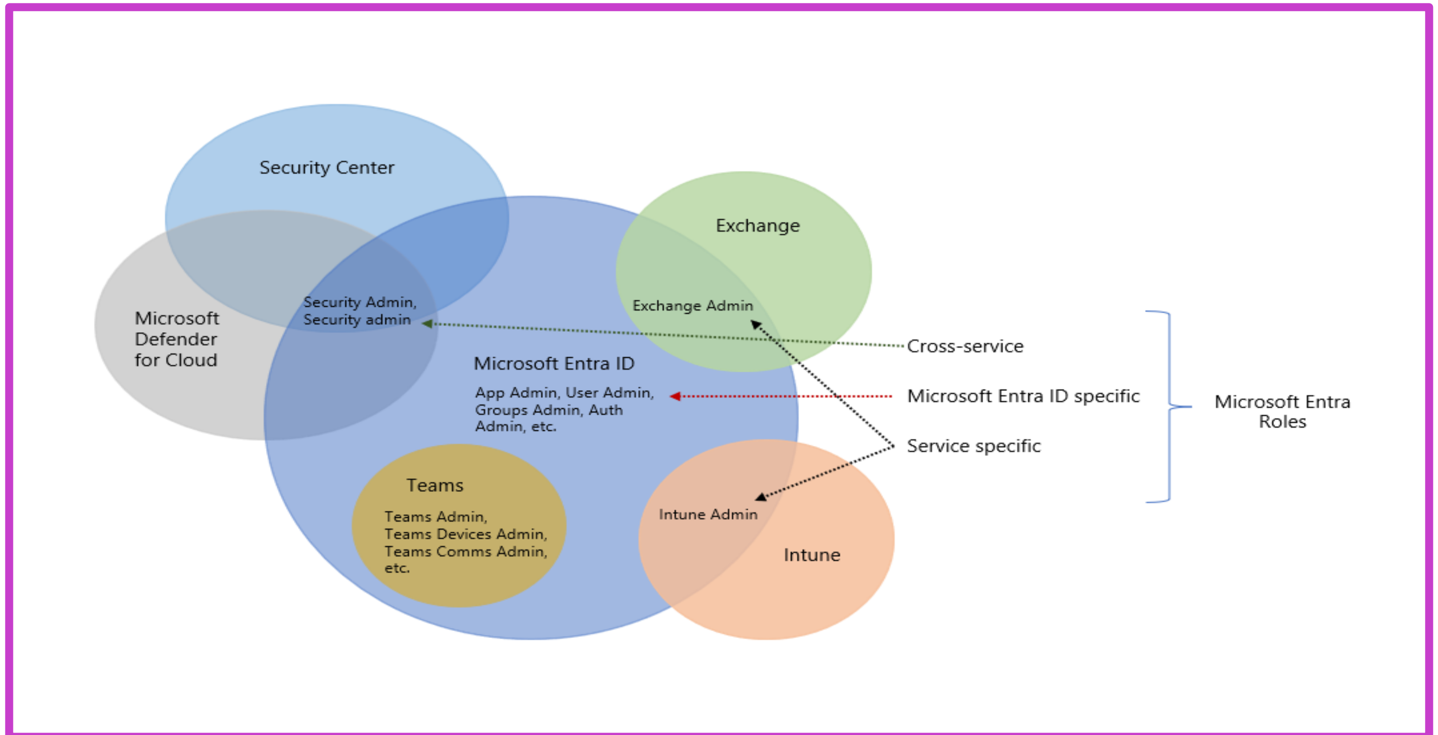
- **Microsoft Entra Internet Access** secures access to SaaS applications, including Microsoft Services, and public internet apps.
- **Microsoft Entra Private Access** provides your users secure access to your private, corporate resources.



Microsoft Entra roles and role-based access control (RBAC)

Microsoft Entra ID roles control permissions to manage Microsoft Entra resources.

- Built-in roles.
- Custom roles.
- Categories of Microsoft Entra roles:
  - Microsoft Entra specific
  - Service-specific
  - Cross service
- Only grant the access users need.


Security Center
Exchange
Security Admin, Security admin
Exchange Admin
Microsoft Defender for Cloud
Cross-service
Microsoft Entra ID
App Admin, User Admin, Groups Admin, Auth Admin, etc.
Microsoft Entra ID specific
Microsoft Entra Roles
Service specific
Teams
Teams Admin, Teams Devices Admin, Teams Comms Admin, etc.
Intune Admin
Intune

Module 4: Describe the identity protection and governance capabilities of Microsoft Entra

Module 4 introduction

After completing this module, you'll be able to:

1. Describe the identity governance capabilities of Microsoft Entra.
2. Describe Privileged Identity Management (PIM).
3. Describe the capabilities of Microsoft Entra Identity Protection.
4. Describe Microsoft Entra integration with Microsoft Security Copilot.

Identity governance in Microsoft Entra

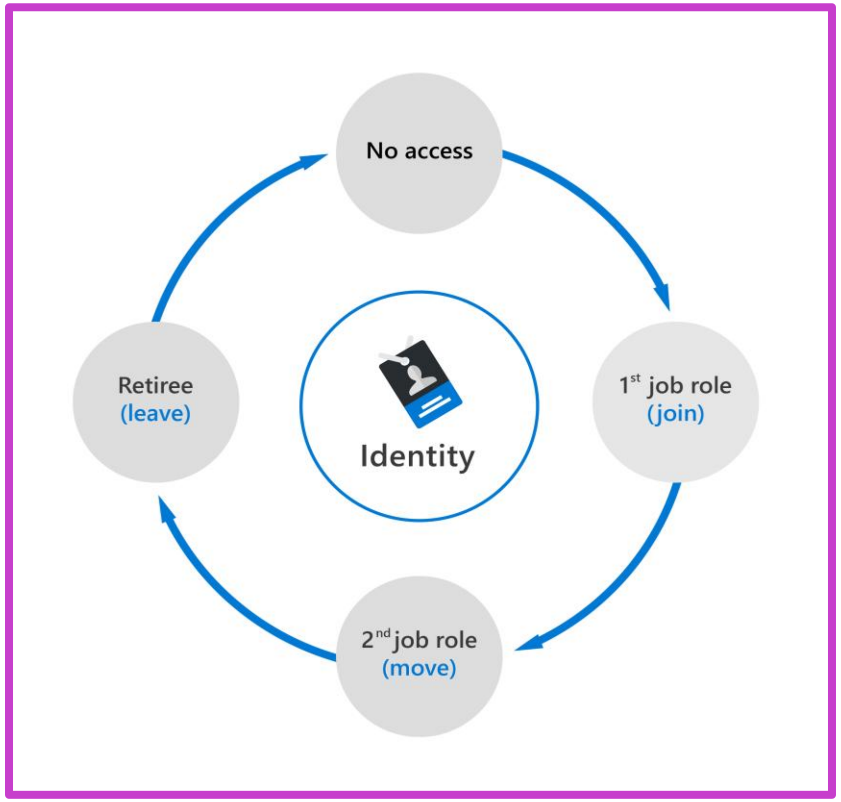
The right people have the right access to the right resources.

The tasks of Microsoft Entra identity governance

- Govern the identity life cycle.
- Govern access life cycle.
- Secure privileged access for administration.

Identity life cycle

- Join: A new digital identity is created.
- Move: Update access authorizations.
- Leave: Access may need to be removed.



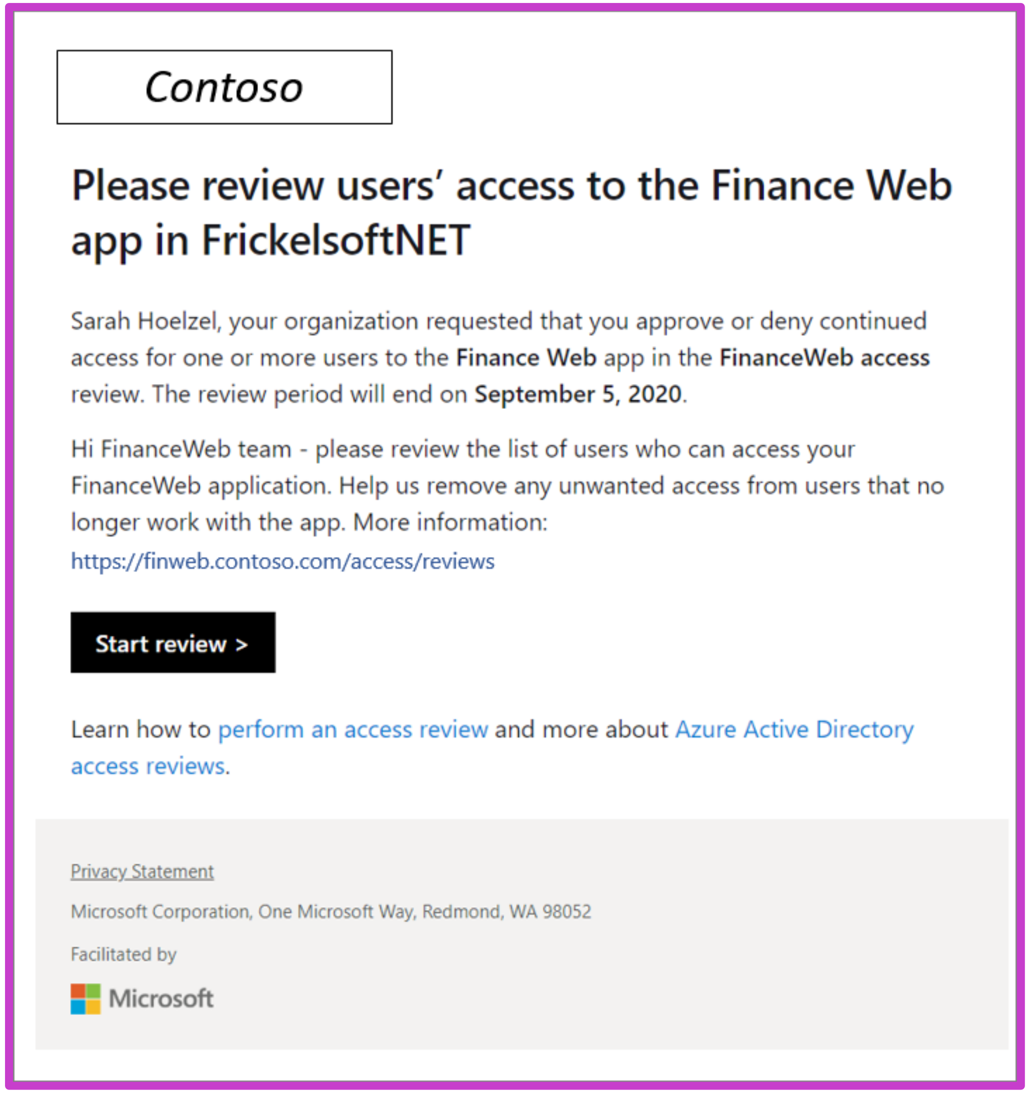
Access reviews

Access reviews

- Enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignment.
- Ensure that only the right people have access to resources.
- Used to review and manage access for both users and guests.

Multistage access reviews

- Support up to three review stages.
- Support workflows to meet recertification and audit requirements calling for multiple reviewers.
- Reduce the number of decisions each reviewer is accountable for.



Contoso

Please review users' access to the Finance Web app in FrickelsoftNET

Sarah Hoelzel, your organization requested that you approve or deny continued access for one or more users to the **Finance Web** app in the **FinanceWeb access** review. The review period will end on **September 5, 2020**.

Hi FinanceWeb team - please review the list of users who can access your FinanceWeb application. Help us remove any unwanted access from users that no longer work with the app. More information: https://finweb.contoso.com/access/reviews

Learn how to perform an access review and more about Azure Active Directory access reviews.

Privacy Statement

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitated by

Privileged Identity Management (PIM)

PIM enables you to manage, control, and monitor access to important resources in your organization.

1. Just in time, providing privileged access only when needed, and not before.
2. Time-bound, by assigning start and end dates that indicate when a user can access resources.
3. Approval-based, requiring specific approval to activate privileges.
4. Visible, sending notifications when privileged roles are activated.
5. Auditable, allowing a full access history to be downloaded.

Microsoft Entra Identity Protection

Detect

- User risk
- Sign-in risk

Investigate

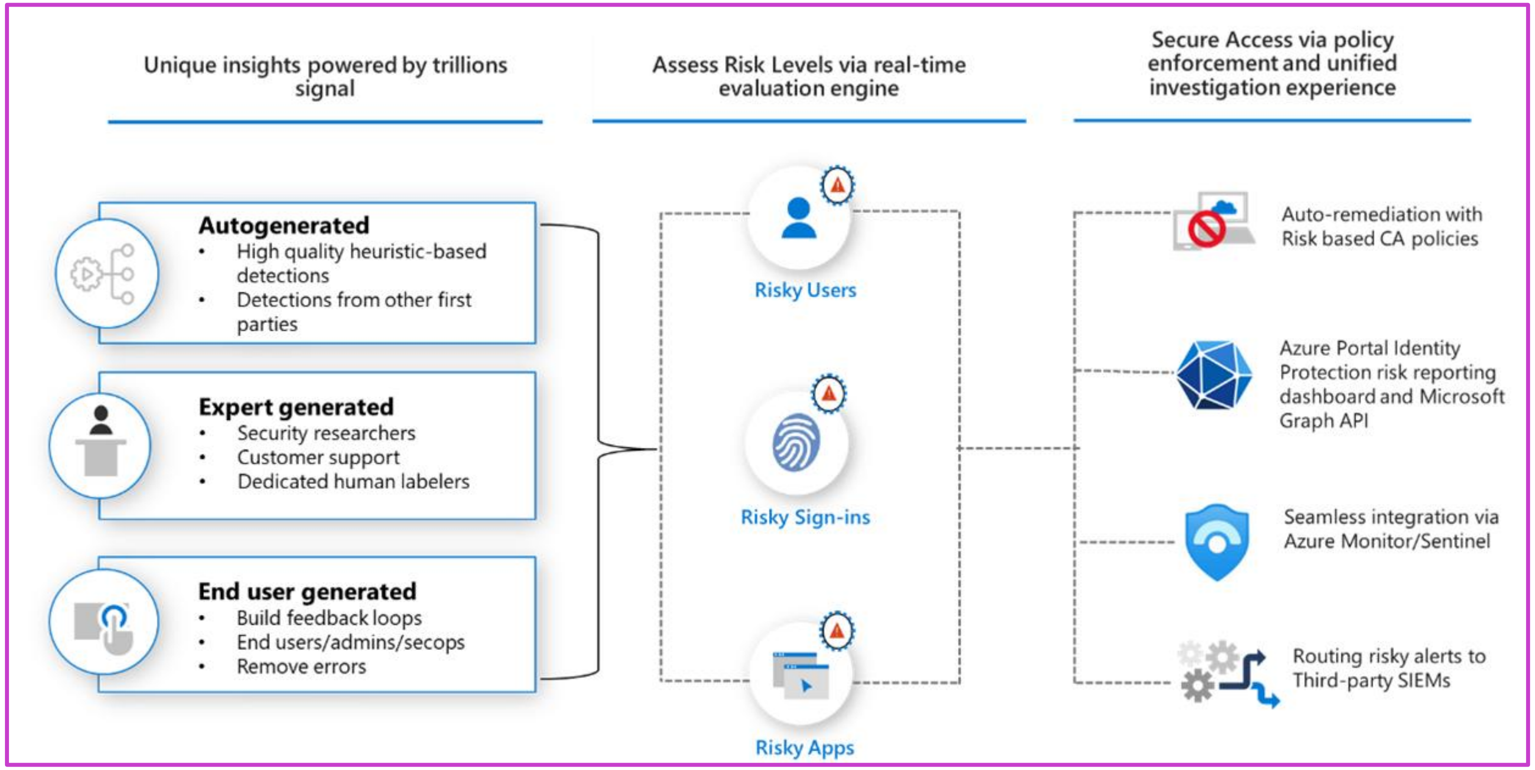
- Risk detections report
- Risky sign-ins report
- Risky users report (embeds Copilot)
- Risky workload identities report

Remediate

- Automated remediation
- Manual remediation

Export

- Export risk detection data to first and third-party utilities for further analysis.



Unique insights powered by trillions signal

Autogenerated
- High quality heuristic-based detections
- Detections from other first parties

Expert generated
- Security researchers
- Customer support
- Dedicated human labelers

End user generated
- Build feedback loops
- End users/admins/secops
- Remove errors

Assess Risk Levels via real-time evaluation engine

Risky Users

Risky Sign-ins

Risky Apps

Secure Access via policy enforcement and unified investigation experience

Auto-remediation with Risk based CA policies

Azure Portal Identity Protection risk reporting dashboard and Microsoft Graph API

Seamless integration via Azure Monitor/Sentinel

Routing risky alerts to Third-party SIEMs

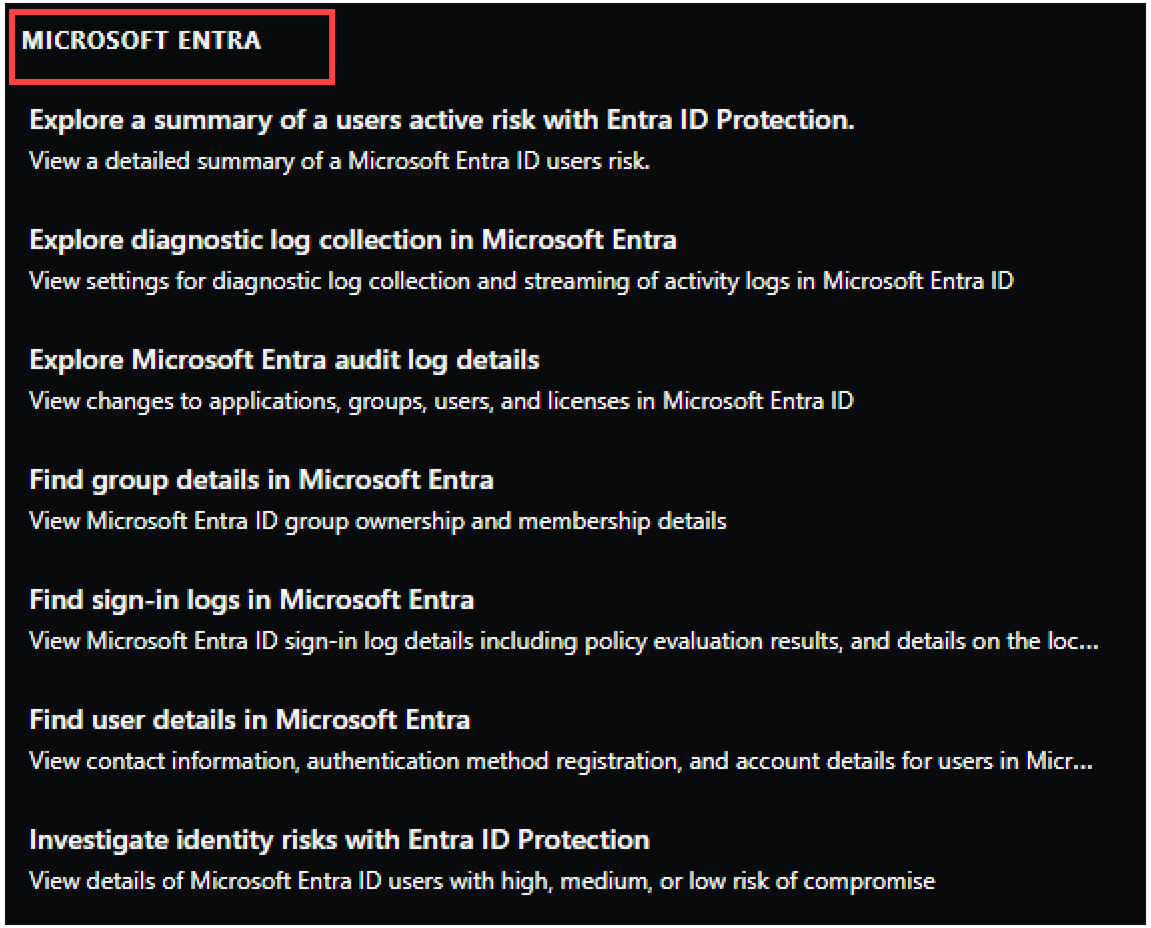
Microsoft Entra integration with Microsoft Security Copilot

Standalone experience:

- Capabilities in standalone experience are built-in prompts.
- Use natural language to create your own prompts.

Embedded experience:

- Supported in Risky users' report.
- Summarize a user's risk level, provide insights, and provide recommendations for rapid mitigation.



MICROSOFT ENTRA

Explore a summary of a users active risk with Entra ID Protection.
View a detailed summary of a Microsoft Entra ID users risk.

Explore diagnostic log collection in Microsoft Entra
View settings for diagnostic log collection and streaming of activity logs in Microsoft Entra ID

Explore Microsoft Entra audit log details
View changes to applications, groups, users, and licenses in Microsoft Entra ID

Find group details in Microsoft Entra
View Microsoft Entra ID group ownership and membership details

Find sign-in logs in Microsoft Entra
View Microsoft Entra ID sign-in log details including policy evaluation results, and details on the loc...

Find user details in Microsoft Entra
View contact information, authentication method registration, and account details for users in Micr...

Investigate identity risks with Entra ID Protection
View details of Microsoft Entra ID users with high, medium, or low risk of compromise

Swiss Post
Cybersecurity

Questions?

Microsoft
Solutions Partner
Security

Specialist
Threat Protection