Azure Architect: Design Identity and Security

Aligned with Microsoft Certification Exam AZ-304

ine.com

Course Topics

Design Authentication
Design Authorization
Governance
Application Security

AZ-304 Objective Domains

- Design monitoring (10-15%)
- **Design identity and security (25-30%)**
- Design data storage (15-20%)
- Design business continuity (10-15%)
- Design infrastructure (25-30%)

Exam AZ-304: Microsoft Azure Architect Design

- Design authentication
  - recommend a solution for single-sign on
  - recommend a solution for authentication
  - recommend a solution for Conditional Access, including multi-factor authentication
  - recommend a solution for network access authentication
  - recommend a solution for a hybrid identity including Azure AD Connect and Azure AD
- Connect Health
  - recommend a solution for user self-service
  - recommend and implement a solution for B2B integration
- Design authorization
  - choose an authorization approach
  - recommend a hierarchical structure that includes management groups, subscriptions and resource groups
  - recommend an access management solution including RBAC policies, access reviews, role assignments, physical access, Privileged Identity Management (PIM), Azure AD Identity Protection, Just In Time (JIT) access

Exam AZ-304: Microsoft Azure Architect Design

- Design governance
  - + recommend a strategy for tagging
  - + recommend a solution for using Azure Policy
  - + recommend a solution for using Azure Blueprint
- Design security for applications
  - + recommend a solution that includes KeyVault
  - + recommend a solution that includes Azure AD Managed Identities
  - + recommend a solution for integrating applications into Azure AD

Pre-requisites

- **Azure Administrator Associate**

Self-Service Identity Management

Self-Service Identity Management

- **Microsoft My Apps Portal**
- **Profile Management**
- **Group Management**
- **Self-Service Password Management**
- **Demo: Self Service Identity Management**

Microsoft My Apps Portal
Profile Management
Group Management
Self-Service Password Management

- Central portal for Azure AD users
- Users can
  - Launch cloud apps configured for SSO
  - Update their profile
  - Manage Groups
  - Set self-service password reset and MFA verification methods
  - Work with Access Reviews

Microsoft My Apps Portal
Profile Management
Group Management
Self-Service Password Management

- Change password
- Set up self-service password reset
- Sign out everywhere
- Manage Organizations (Azure AD tenants)

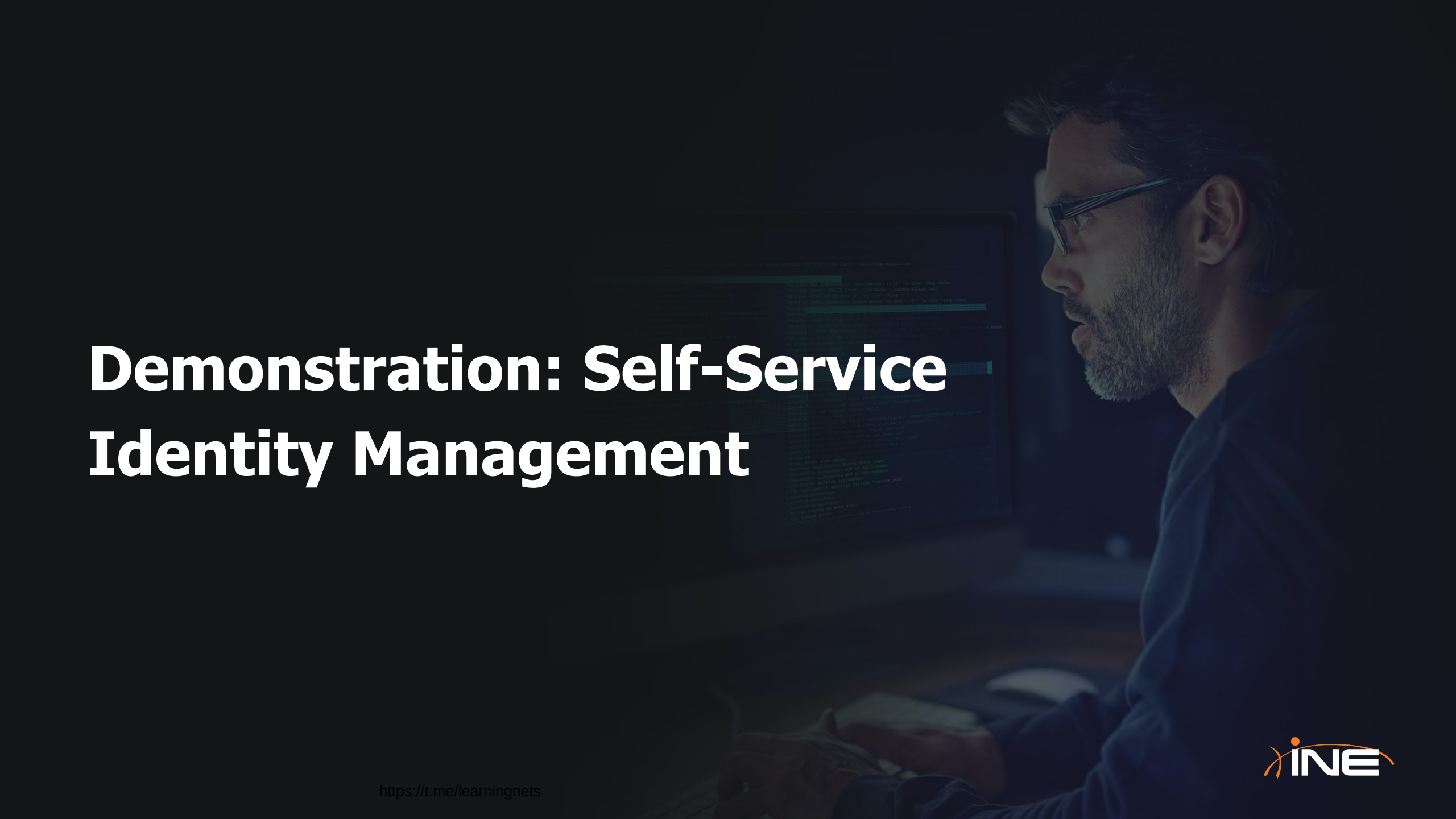
Microsoft My Apps Portal
Profile Management
Group Management
Self-Service Password Management

- View Groups
- Create Groups*
- Edit Groups
- Join Groups

Microsoft My Apps Portal
Profile Management
Group Management
Self-Service Password Management

- Update password
- Reset password

Demonstration: Self-Service Identity Management



Azure AD B2B Authentication

Azure AD B2B Authentication

- Granting Access to External Users
- Azure AD Guest Accounts
- Demo: Azure AD Guest Accounts

Granting Access to External Users

Azure AD Guest Accounts

- Add users from any Azure AD tenant
- Guest users must confirm
- Works with Microsoft and Google social accounts
- Theoretically works with other SAML providers
- Conditional access policy for MFA enforcement

Demo: Azure AD Guest Accounts

Dynamic Access Control

Dynamic Access Control

- **Dynamic Security Groups**
- **Conditional Access Policy**
- **Demo: Dynamic Access Control**

Dynamic Security Groups

Requires Azure AD Premium P1

User and device

Define membership rules – simple or advanced

Processed – initial and on-going

Add to other groups

Conditional Access Policy

- Assignments
  - User and groups
    - None/All/Select
    - All guest and external, Directory roles, Users and groups
    - Include and Exclude
  - Cloud apps or actions
    - None/All/Select
    - Include/Exclude
    - User actions – register security information
  - Conditions
    - Sign-in risk – high, medium, low, no risk
    - Device platforms – Android, iOS, Windows Phone, Windows, macOS
    - Locations – any, trusted, selected (include/exclude)
    - Client apps – browser, mobile – modern, Exchange (supported platforms option), other
    - Device State

Conditional Access Policy

- Access controls
  - Grant
    - Require MFA
    - Require compliant device
    - Require hybrid joined device
    - Require proved app
    - Require app protection policy
  - Session
    - Use app enforced restrictions
    - Use conditional access app control
    - Sign-in frequency
    - Persistent browser session

Demonstration: Azure Dynamic Access Control

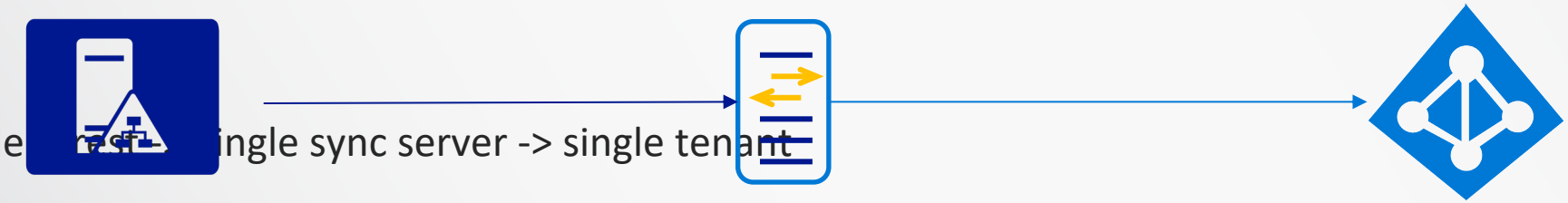
Hybrid Identity Architectures

Hybrid Identity Architectures

- Hybrid Identity
- Hybrid Identity Supported Architectures

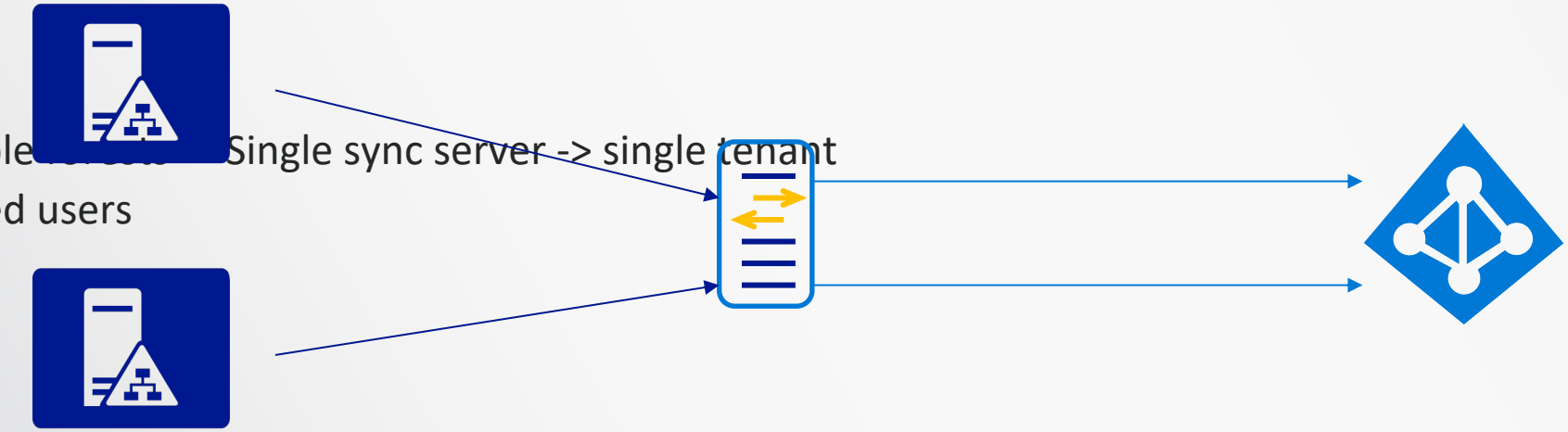
Single Forest, Single Tenant

+ Single forest -> single sync server -> single tenant

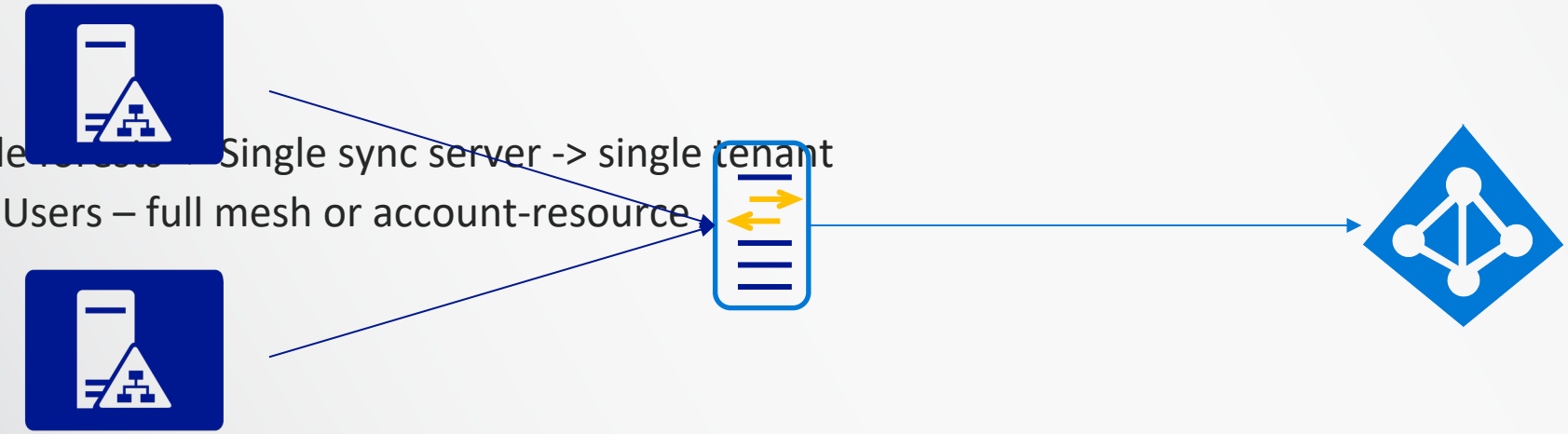


Tenant

- Multiple forests -> Single sync server -> single tenant
- Isolated users

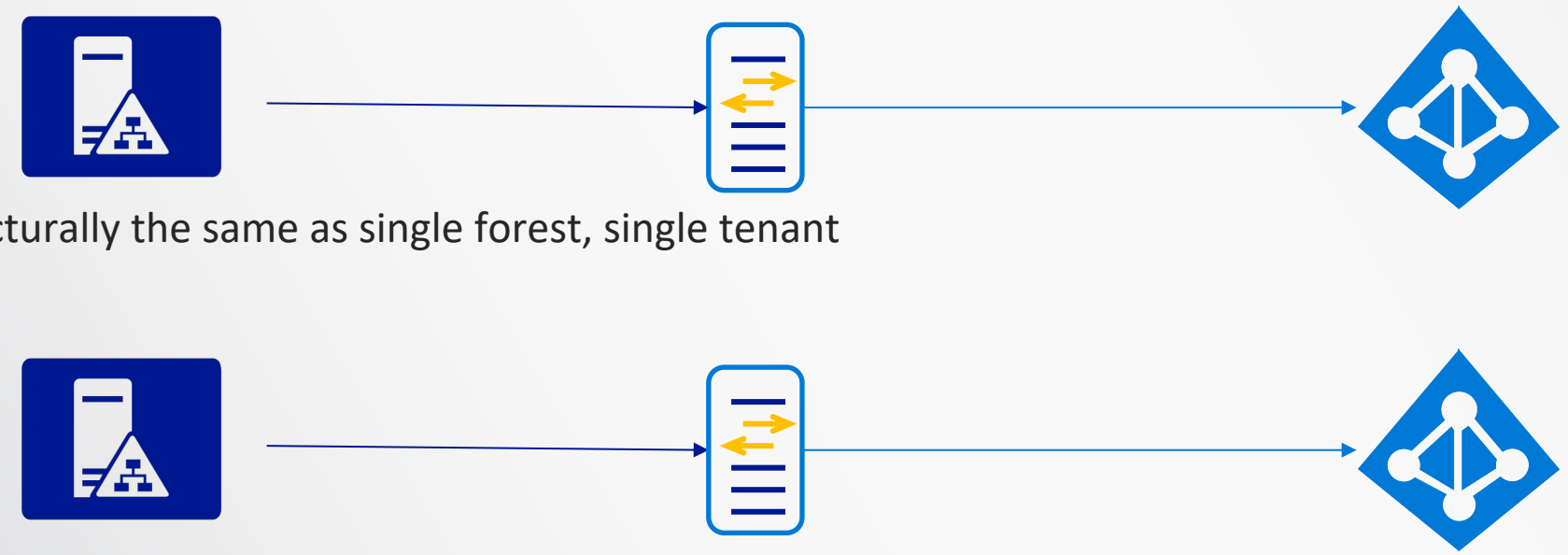


Tenant



+ Multiple forests – Single sync server -> single tenant
+ Match Users – full mesh or account-resource

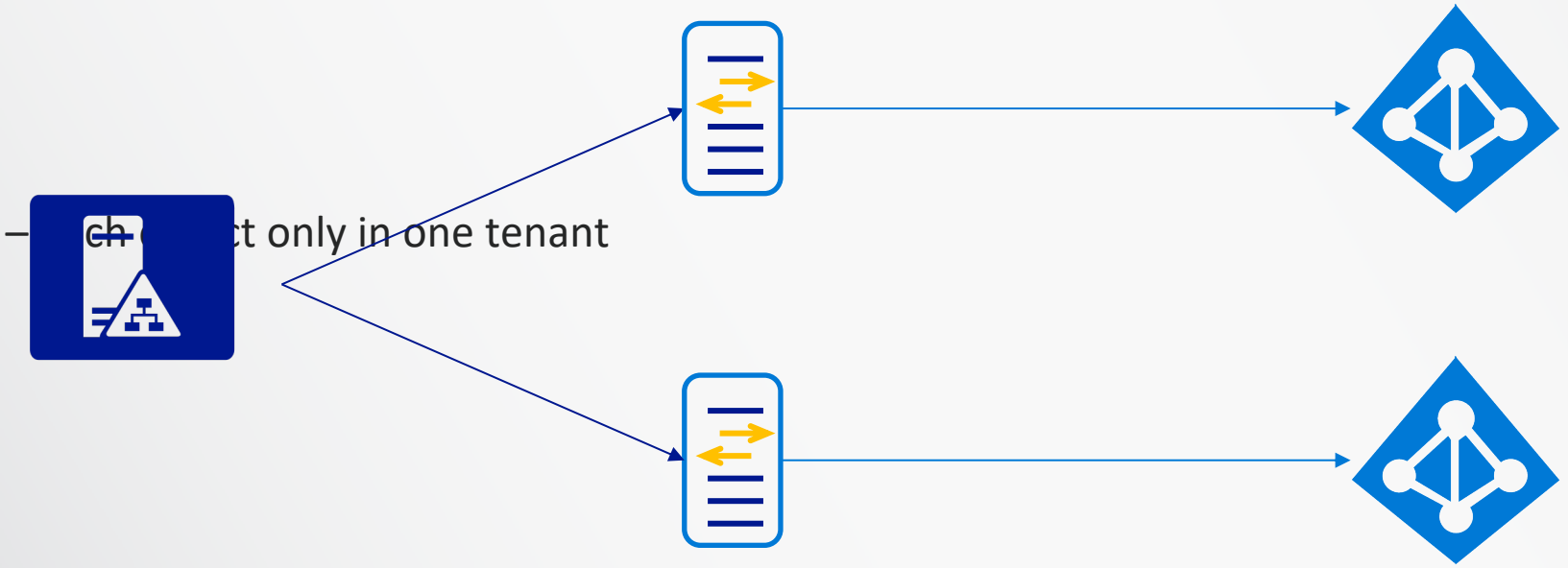
Tenant



+ Architecturally the same as single forest, single tenant

Tenant

- Filter sync – ch ct only in one tenant



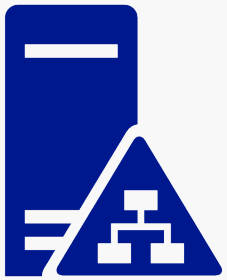
Azure AD Connect

Azure AD Connect

- Azure AD Connect Configuration
- Demonstration: Azure AD Connect

Azure AD Connect Configuration

- One active connect server
  - One or more staging servers
- SQL Server
- Pre-requisites
- Pre-requisites for ADFS
- Ports
  - Internal – DNS(53), Kerberos (88), MS-RPC (135), LDAP (389), SMB (445), LDAP SSL (636), RPC (49152-65535)
  - External – 80 (download CRL), 443 (sync)
  - ADFS – 5985 (WinRM listener)
  - ADFS WAP – 49443 (certificate authentication)



Federation and Single Sign-On

Federation and Single Sign-On

- Federation Components
- Preparing for Federation

Preparing for Federation

- Custom domain name
- Certificates
- Firewall
- WinRM
- Non-domain joined – Register ADFS and WAP server with each other for WinRM

Role-Based Access Control

Role-Based Access Control

- Role-Based Access Control (RBAC) Concepts
- Role Definition

Role-Based Access Control Concepts

Role-Based Access Control Concepts

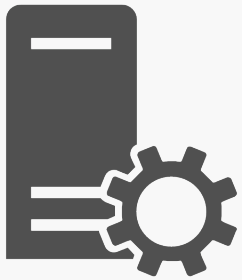
- Define role
  - Level – subscription*
  - Permission - Microsoft.Authorization/roleDefinitions/write (read)
  - Elements – Name, Description, Actions, NotActions, DataActions, NotDataActions, AssignableScopes
- Assign role
  - Level – management group, subscription, resource group, resource
  - Permission - Microsoft.Authorization/roleAssignments/*
- Effective permissions
  - Azure RBAC is additive
  - Deny assignments – blueprints and managed apps

Role Definition


```
{
        "Name": "Website Contributor",
        "Id": "de139f84-1756-47ae-9be6-808fbbe84772",
        "IsCustom": false,
        "Description": "Lets you manage websites (not web plans), but not access to them.",
        "Actions": [
                "Microsoft.Authorization/*/read",
                "Microsoft.Insights/alertRules/*",
                "Microsoft.Insights/components/*",
                …
                "Microsoft.Web/sites/*“
         ] …
```

Role Definition

```
…
        "NotActions": [],
        "DataActions": [],
        "NotDataActions": [],
        "AssignableScopes": ["/"]
}
```



RBAC In Action

RBAC in Action

- Demonstration: RBAC
- Troubleshoot RBAC

Troubleshoot RBAC

- Role definition or assignment rights
- Custom role limit - 5000 custom roles per tenant
- Migrate a subscription between tenants
- RBAC changes can take 30 minutes
- Obscure permissions
  - Web apps
  - Virtual machines

Policies and Initiatives

Policies and Initiatives

- Policies and Initiatives
- Policy Definition
- Policy and RBAC

Policies and Initiatives

- Use Cases
  - Deny
  - Monitor
  - Audit
  - Correct
- Components
  - Filter
  - Action
  - Parameters
- Initiative
  - Shared set of policies
  - Parameter control

Policy Definition

```
"Properties": {
        "displayName": "Allowed virtual machine SKUs",
        "policyType": "BuiltIn",  "mode": "Indexed",
        "description": "This policy enables you to ....",
        "metadata": {"category": "Compute"},
        "parameters": {"listOfAllowedSKUs": "@{type=Array; metadata=}"},
        "policyRule": {
                "if": "@{allOf=System.Object[]}",
                "then": "@{effect=Deny}"
        }
},
```

Policy and RBAC

- RBAC focuses on permissions
- Policy focuses on resource properties
- RBAC defaults to deny
- Policy defaults to allow
- Policy and RBAC should be used together
  - VM Contributor
  - VM Sku policy

Policies and Initiatives in Action

Policies and Initiatives in Action

- Demonstration: Apply a Custom Policy
- Demonstration: Apply a Custom Initiative

Access Review

Access Review

- Access Review Concepts
- Demonstration: Implement Access Review

Access Review Concepts

- Recertify, attest, audit
- Office groups, Azure AD groups, Apps, Azure AD roles, RBAC roles
- Approve or deny continued access - recommendation
- Choose reviewers – group owners, group members, individual accounts, self
- One-time or recurring
- Licensing
  - Enterprise Mobility + Security E5 or Azure AD Premium 2
  - Based on number of reviewers

Azure AD Identity Protection

Azure AD Identity Protection

- What is Azure AD Identity Protection?
- Demonstration: Configuring Identity Protection

What is Azure AD Identity Protection

- Machine learning system to monitor and categorize risk associated with Azure AD
  - Sign-in risk
  - User risk
- Risk events – Atypical travel, anonymous IP address, Unfamiliar sign-in properties, malware linked IP address, Leaked credentials
- Risk levels – low medium, high
- Risk policies – sign-in risk, user risk
- Azure AD Premium P2

Azure Subscription Management

Azure Subscription Management

- Azure Subscriptions
- Subscription Types
- Subscription Access
- Demo: Subscription Access
- Management Groups
- Demo: Management Groups
- Enterprise License Management
- Azure Service Lifecycle

Azure Subscriptions

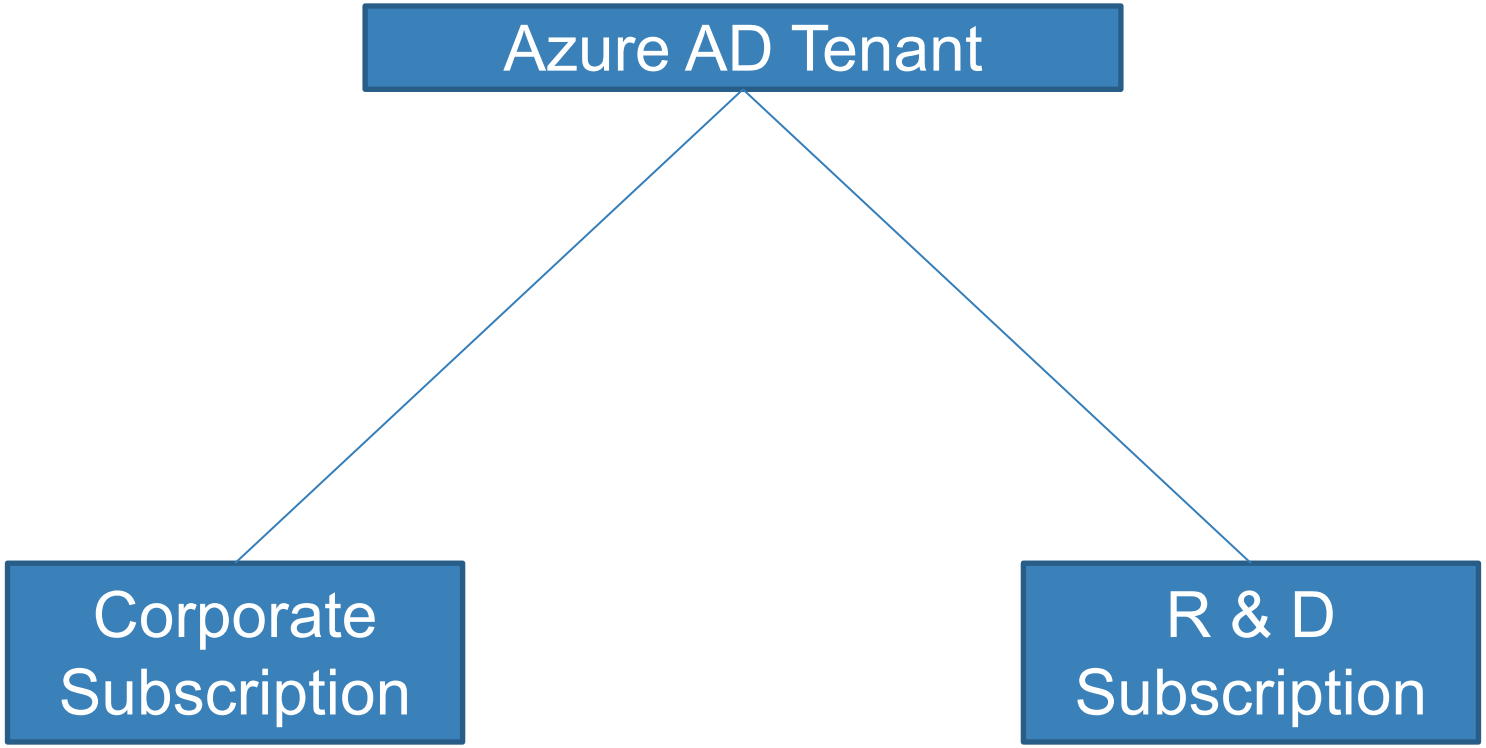
Subscription Types

- Pay as you go
- Enterprise
- 3rd party
- Free
- Credit

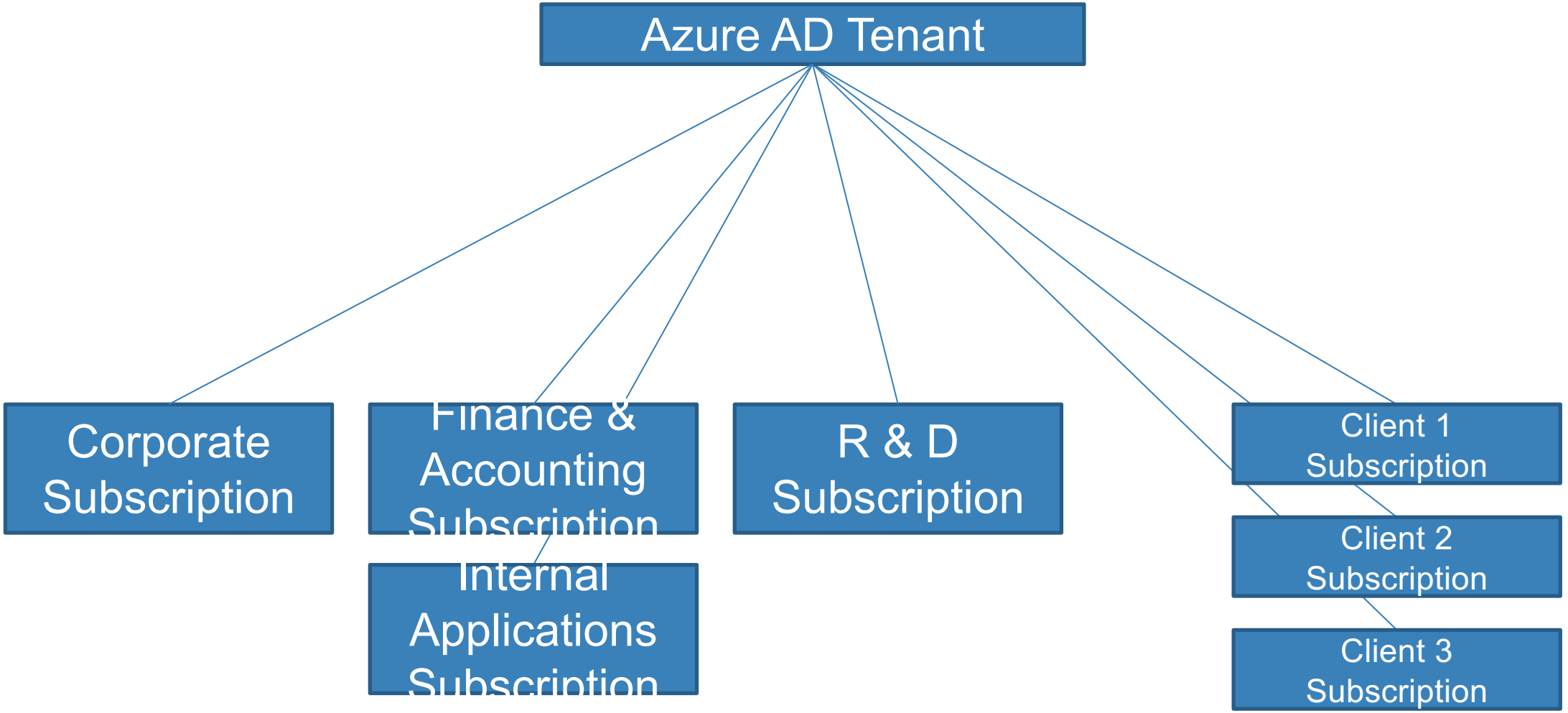
Subscription Access

Demo: Subscription Access

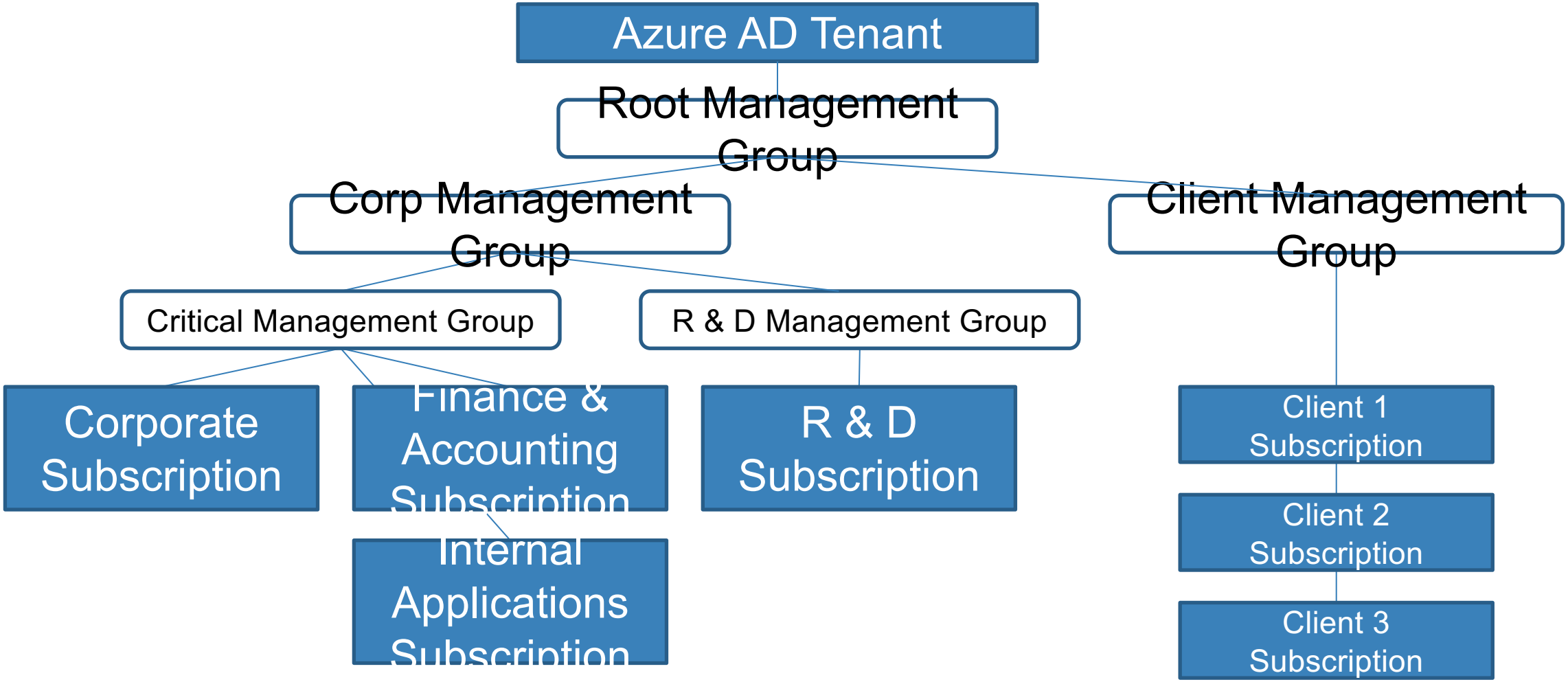
Management Groups



Management Groups



Management Groups



Demo: Management Groups

Enterprise License Agreement

- Azure stand-alone enrollment or as part of on-premises enrollment
- Azure EA portal
  - Departments, accounts, subscriptions
  - Roles – enterprise administrator, department administrator
- Cost reporting is different
  - Spending Quota – department level
- Enterprise Dev/Test Subscriptions
  - Lower cost
  - No SLA
  - Licensed for dev/test only

Azure Service Lifecycle

- General availability
- Public preview
- Private preview

Privileged Identity Management (PIM)

Privileged Identity Management (PIM)

- What is PIM?
- Demo: PIM

What is PIM?

What is PIM?

- Just-in-time privileged access
- Time limited access
- Approval
- MFA requirements
- Notification
- Access review
- Audit

Demo: PIM

Using Tags for Organization, Managing and Monitoring

Using Tags for Organization, Managing and Monitoring

- Defining Metadata
- Enforcing Tagging
- **Demonstration**: Using Tags in Azure

Using Tags

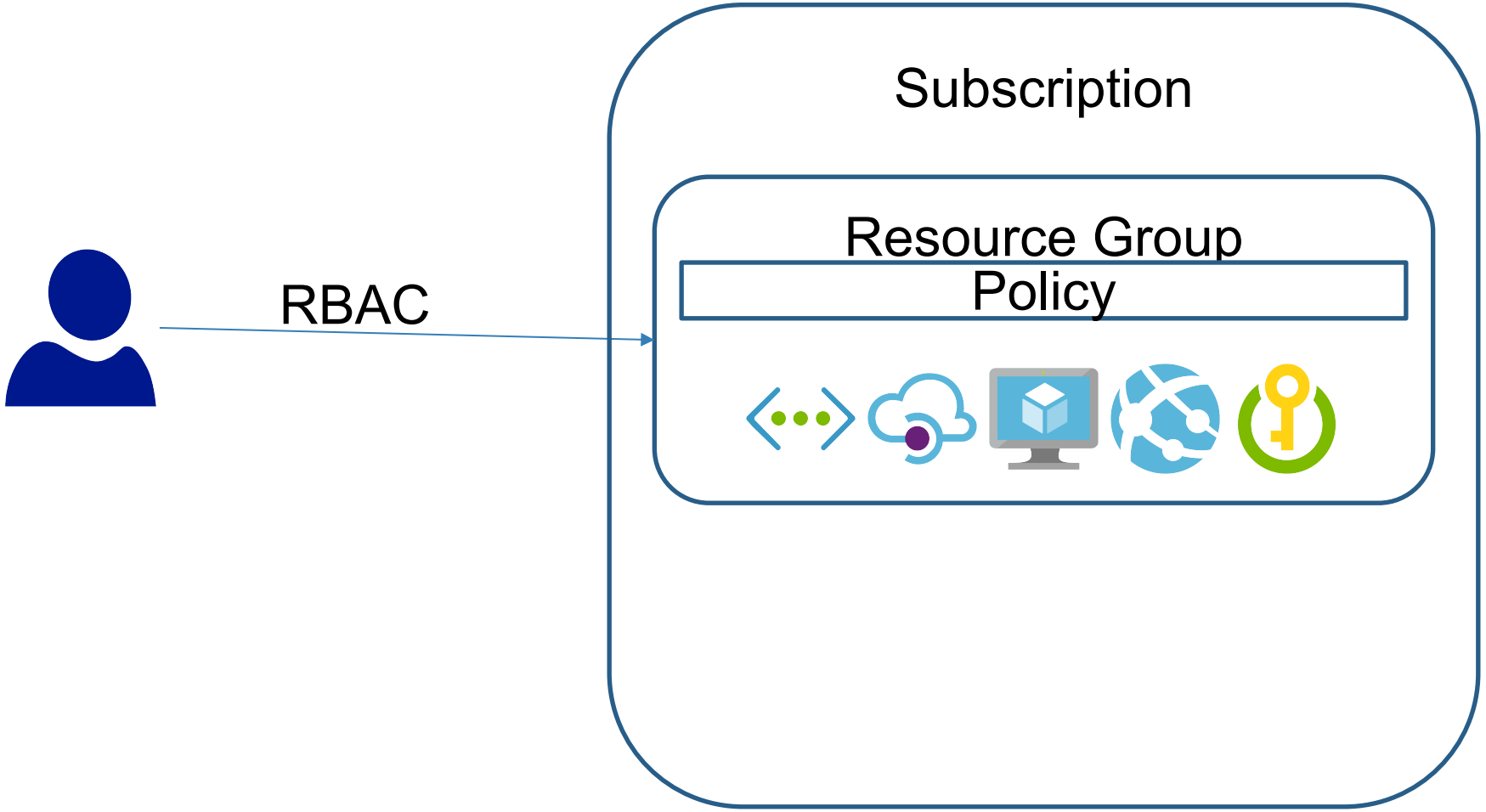
- **Tags define metadata**
  - Free form name/value pairs
  - Example - Cost Center: VOD 3451
- **Use Tags**
  - Billing
  - Search
  - Portal
- **Enforce Tagging**
  - Policy to require tags
  - Policy to assign tags

Azure Blueprints

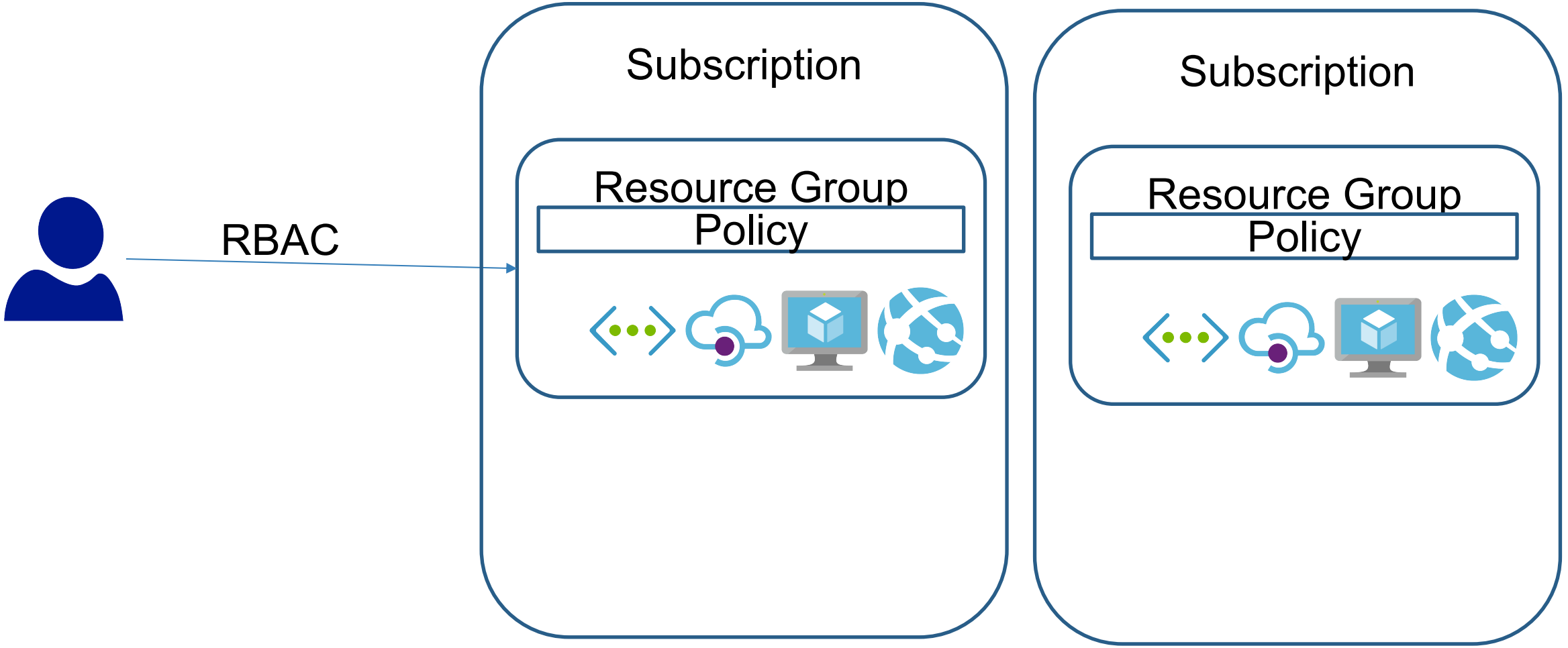
Azure Blueprints

- Managing Governance at Scale
- Azure Blueprints
- Demo: Azure Blueprints

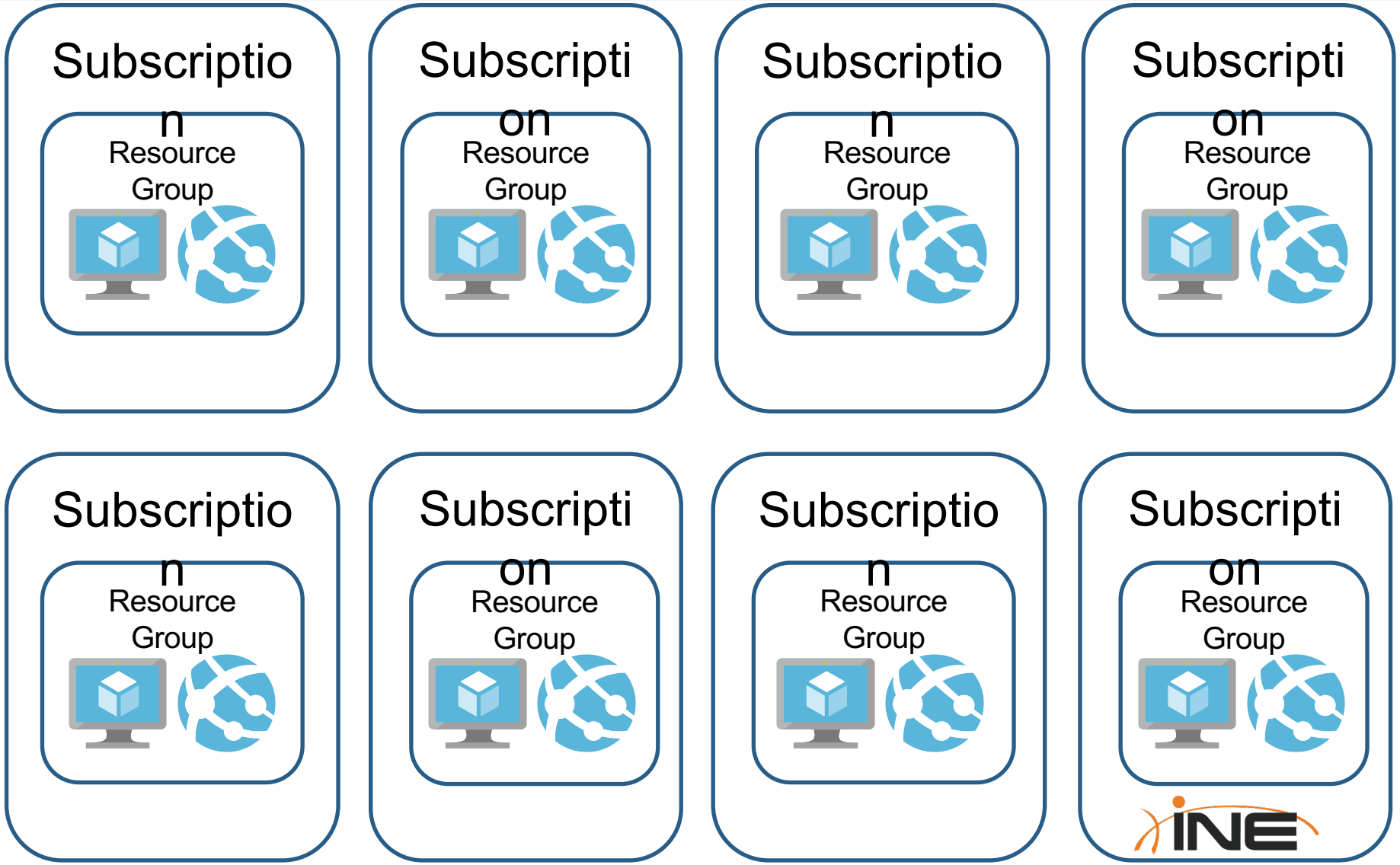
Managing Governance at Scale



Managing Governance at Scale

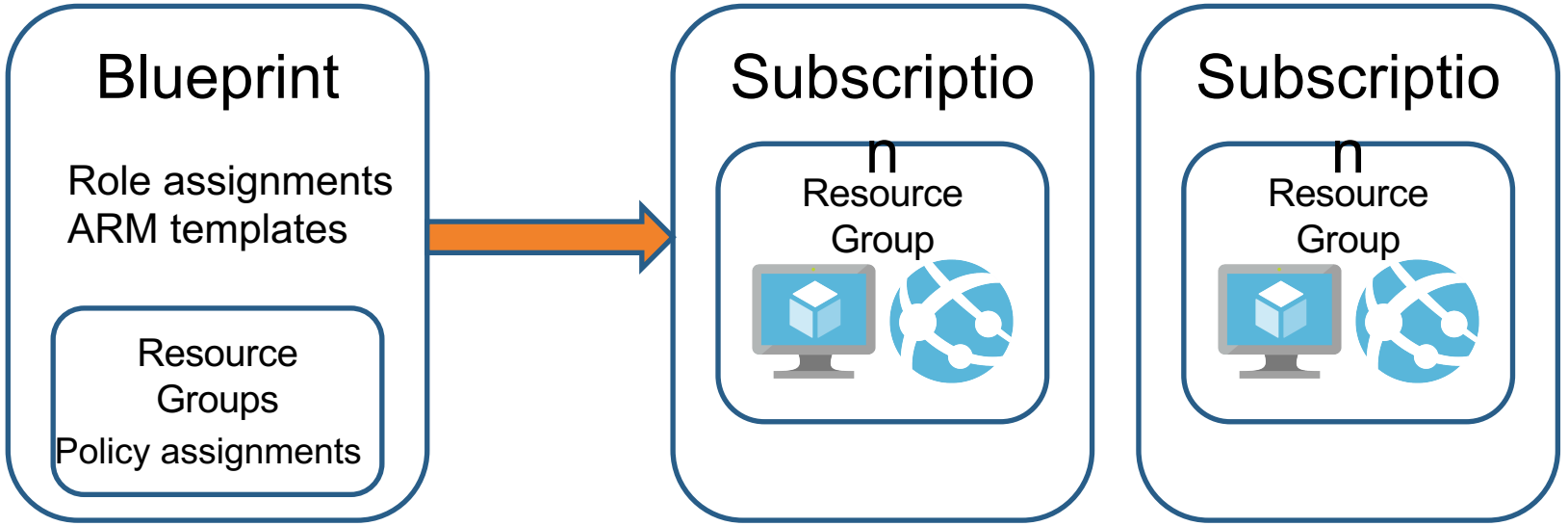


Managing Governance at Scale



Azure Blueprints

- Role Assignments
- Policy Assignments
- Azure Resource Manager Templates
- Resource Groups



Demo: Azure Blueprints

Using the KeyVault API

Using the KeyVault API

- Azure Key Vault
- Using the Azure Key Vault API to Manage Sensitive Data
- Demonstration: Using the Azure Key Vault API to Manage Sensitive Data

Implement Service Principal Authentication

Implement Service Principal Authentication

- Using Service Principals
- Demonstration: Generate and Use an Azure AD Service Principal

Azure Managed Identities

Azure Managed Identities

- Azure Managed Identities
- Demonstration: Secure Access to SQL Server From a Web App

Implement Authentication Options

Implement Authentication Options

- Integrating Azure AD Authentication
- Azure AD Authentication Options

Azure AD Authentication Options

- Certificate-based Authentication
- Token-based Authentication
- Forms-based Authentication
- Windows-based Authentication

Azure AD Certificate-Based Authentication

- Primarily used with mobile device applications
- Device app has a certificate
- CA registered as a trusted CA
- Revocation list must have public internet endpoint

Azure AD Token-Based Authentication

- Most common for Azure AD integrated applications
- User authenticates with Azure AD and generates tokens
  - Bearer – Used to request access and refresh tokens
  - Access – Verified user identity token with expiration
  - Refresh – Silent request for a new identity token
- Tokens are JWTs (JavaScript Web Tokens)
- Azure AD tokens are well documented - decomposable

Azure AD Forms-Based Authentication

- Password-based single sign-on

Azure AD Windows-Based Authentication

- On-prem – federated solution, SSO option for password-hash and passthrough
- On-prem resources – Azure AD Application proxy

Implement OAuth2 Authorization

Implement OAuth2 Authorization

- Authentication/Authorization Using OAuth2
- Demonstration: Integrating Azure AD OAuth2 Based Authentication

OAuth 2

- Technically OAuth 2.0 is an authorization protocol
- Protocol based on Token
  - Credentials (not token)
  - Authorization Code
  - Access Token and Refresh token
  - Sends access token in authorization header