



Azure Administration: Identity Management and Governance

Aligned with Microsoft Certification Exam AZ-104

ine.com

<https://t.me/learningnets>

Course Topics

Resource Management
Tenant Management
Azure AD Object Management
Role-Based Access Control
Azure Cost Management

Exam AZ-104: Microsoft Certified Azure Administrator Associate

- Manage Azure AD objects
 - + create users and groups
 - + manage user and group properties
 - + manage device settings
 - + perform bulk user updates
 - + manage guest accounts
 - + configure Azure AD Join
 - + configure self-service password reset
- Manage role-based access control (RBAC)
 - + create a custom role
 - + provide access to Azure resources by assigning roles
 - + interpret access assignments
 - + manage multiple directories
- Manage subscriptions and governance
 - + configure Azure policies
 - + configure resource locks
 - + apply tags
 - + create and manage resource groups
 - + manage subscriptions
 - + configure Cost Management
 - + configure management groups

Pre-requisites

- **Azure Fundamentals**



<https://t.me/learningnets>



Basic Resource Management

Basic Resource Management

- ❑ Resource Hierarchy
- ❑ Resource Groups
- ❑ Provision Resources
- ❑ De-provision Resources
- ❑ Demo: Manage Resources

Azure Resource Hierarchy

<https://t.me/learningnets>

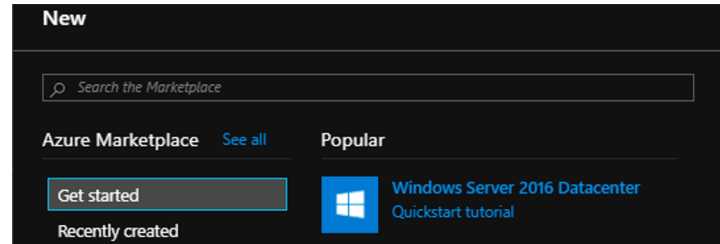


Resource Groups

- + Primary Organization Unit in Azure
- + Use cases
 - + Authorization
 - + Life cycle
 - + Resource management
 - + Billing
- + Resource management
 - + Resources can move between resource groups
 - + Related resources DO NOT need to be in the same resource group
 - + Some resource groups maintained by Azure – Kubernetes Service

Provision Resources

De-provision Resources

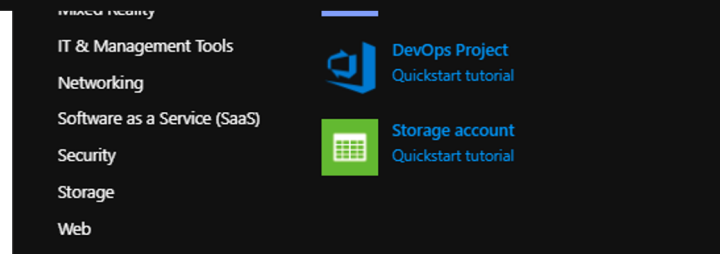


Create a virtual machine

```
1 New-AzVm -ResourceGroupName 01Tasks -Location eastus -Zone 1 -Name myVM -Credential $cred `
2 Stop-AzVM -Name myVM -ResourceGroupName 01Tasks -Force
```

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)



Demo: Manage Resources

<https://t.me/learningnets>





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

<https://t.me/learningnets>



Subscription Types

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

Subscription Access

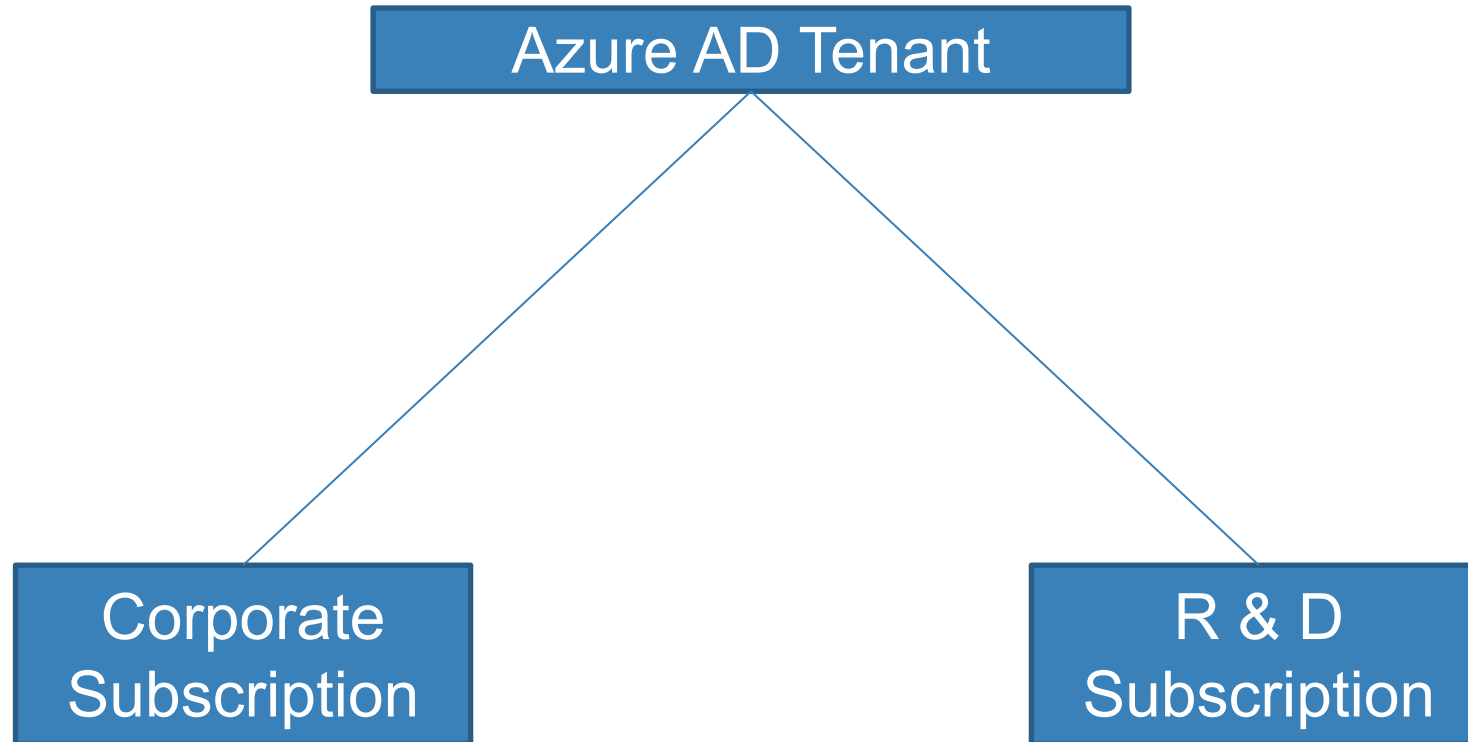
<https://t.me/learningnets>



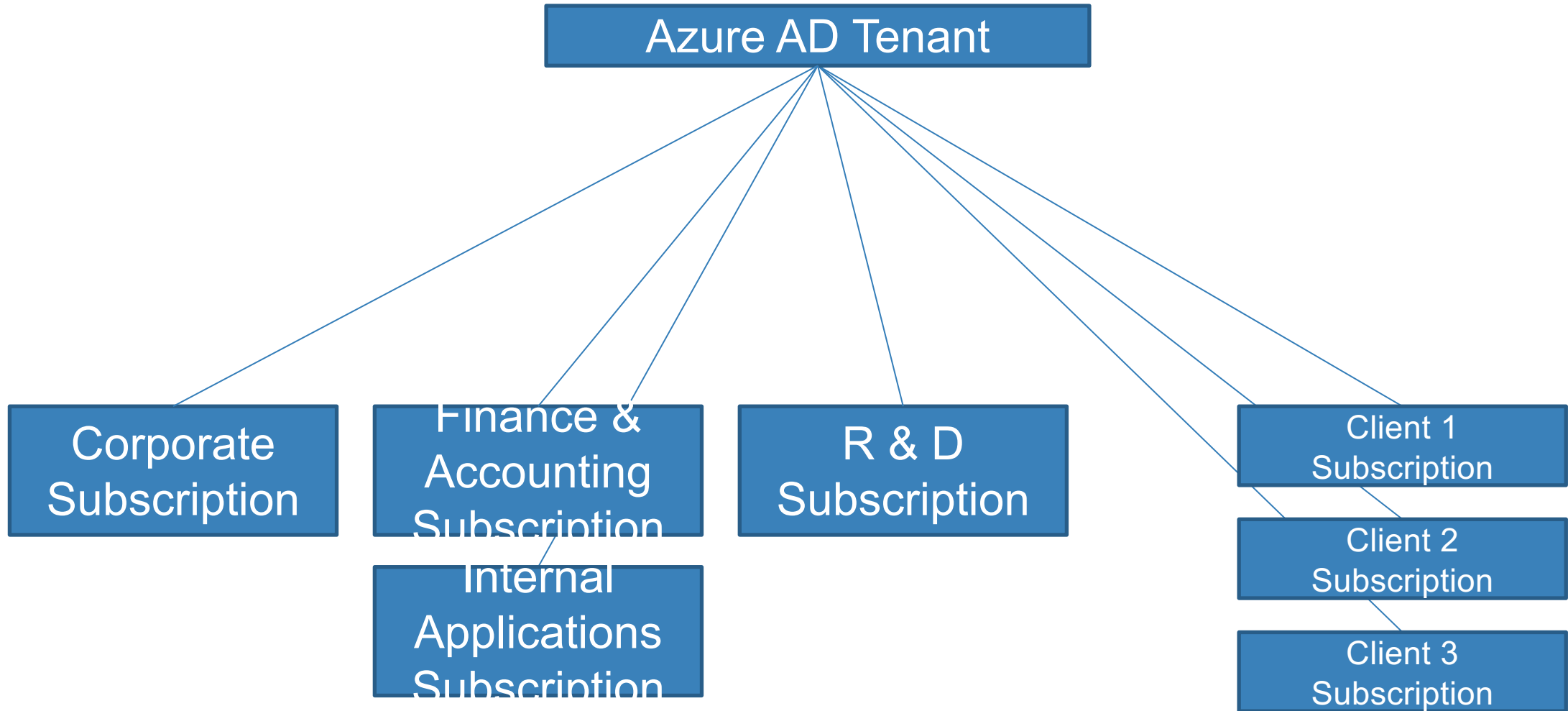
Demo: Subscription Access



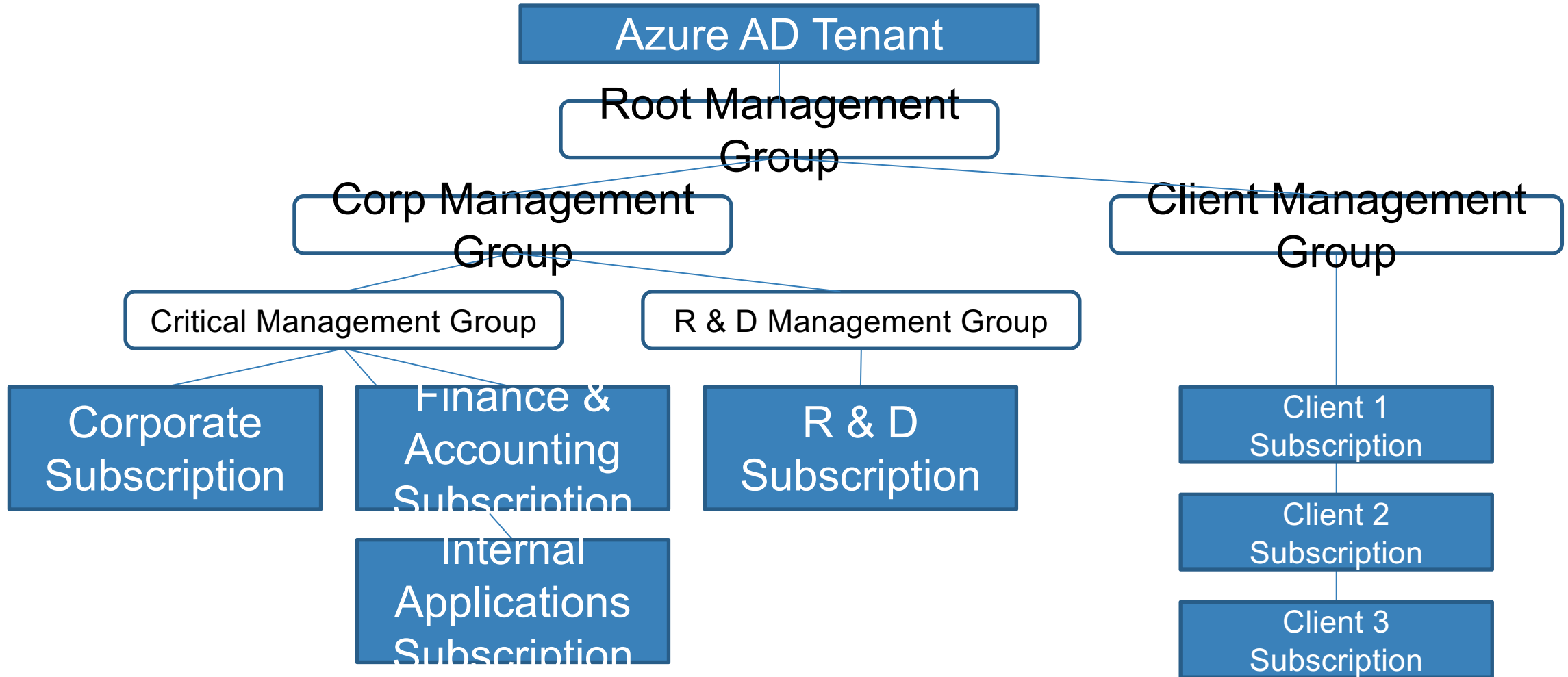
Management Groups



Management Groups



Management Groups



Demo: Management Groups





Resource Locks

Resource Locks

- ❓ Resource Locks
- ❓ Demo: Resource Locks

Resource Locks

- + Protect resources
- + Delete or Read-only
- + Apply to resource groups and resources
- + Active in the management plane

Production VM



```
Remove-AzVM -Name Production
```

Remove-AzVM : The scope './virtualMachines/Production' cannot perform delete operation because following scope(s) are locked: './resourceGroups/production'. Please remove the lock and try again.

Demo: Resource Locks

<https://t.me/learningnets>





Resource Tagging

Resource Tagging

- ❑ Tags
- ❑ Demo: Create Tags
- ❑ Demo: Enforce Tags
- ❑ Demo: Use Tags

Tags

- + Resource metadata
 - + Applied to resources and resource groups
 - + Simple name/value pairs
- + Enforce by policy
- + Using
 - + Management tools
 - + Billing
 - + API

Demo: Create Tags
Demo: Enforce Tags
Demo: Use Tags



Resource Policies and Initiatives

Resource Policies and Initiatives

- ❑ RBAC Policies
- ❑ Define Policies
- ❑ Assign Policies
- ❑ Policy Initiatives
- ❑ Policy and RBAC

RBAC Policies

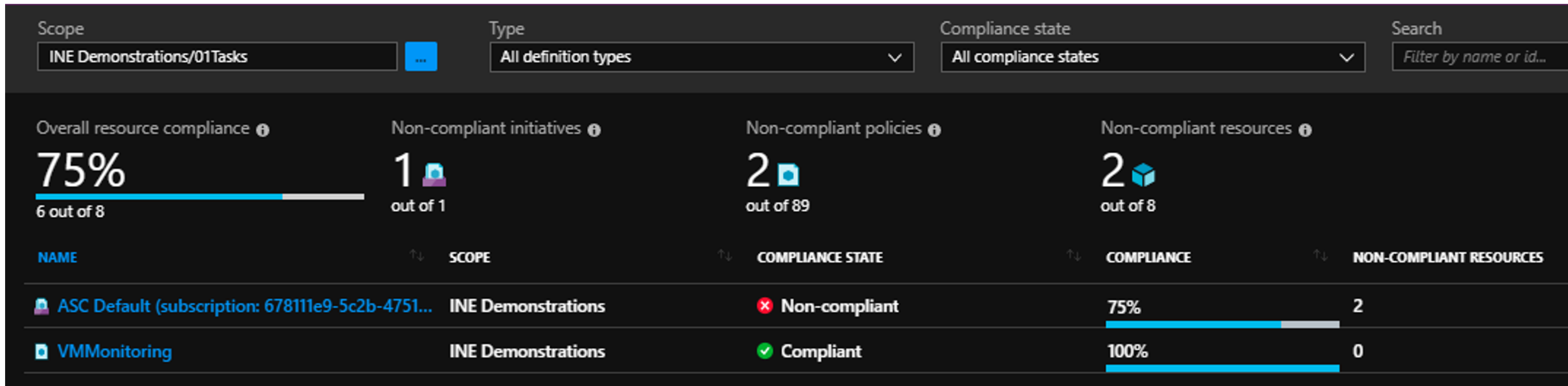
- + Use Cases
 - + Deny
 - + Monitor
 - + Audit
 - + Correct
- + Components
 - + Filter
 - + Action
 - + Parameters

Define Policy

```
"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}"  
  }  
},
```

Assign Policy

New-AzPolicyAssignment -Name Demo -Scope \$rg.id -DisplayName "Demo Assignment" -Description "... " -PolicyDefinition \$pol



Initiatives

- + Grouping of policies
- + Applied as a unit
- + Policy parameter options
 - + Set value in policy
 - + Surface as policy parameter
- + Used by Azure
 - + Security Center

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



Resource Policies and Initiatives in Action

Resource Policies and Initiatives in Action

- ❑ Demo: Define Policy
- ❑ Demo: Assign Policy
- ❑ Demo: Define Initiative
- ❑ Demo: Assign Initiative

Demo: Define Policy
Demo: Assign Policy
Demo: Define Initiative
Demo: Assign Initiative



Add Custom Domains

Add Custom Domains

- Azure AD Domains
- Demo: Registering a Custom Domain

Azure AD Domains

- Default Domain - .onmicrosoft.com
- Custom domains
 - + Login as [user@company.com](#) rather than [user@tenant.onmicrosoft.com](#)
- Required for federated authentication
- Requires proof of domain ownership

Demo: Registering a Custom Domain

<https://t.me/learningnets>





Manage Multiple Directories

Manage Multiple Directories

- Multiple Directory Architecture
- Demo: Multiple Directories

Multiple Directory Architecture

- Tenants and directories are the same thing
- Each subscription is associated with one “primary” tenant
- A single tenant can be the primary tenant for multiple subscriptions
- Directory tiers and licensing
- Business-to-Business

Demo: Multiple Directories

<https://t.me/learningnets>





Create and Manage Users

Create and Manage Users

- User Types
- Create Users
- Add Guest Users
- Manage Users
- Perform Bulk-Updates
- Demo: Create and Manage Users

User Types

<https://t.me/learningnets>



Create Users

Create user
Create a new user in your organization. This user will have a user name like alice@inetasks.onmicrosoft.com.

Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

[Help me decide](#)

Identity

User name ⓘ @
The domain name I need isn't shown here

Name * ⓘ

First name

Last name

User name

Groups

Roles

User

Settings

Block sign in

Usage location

Job info

Job title

Department

```
$password = ConvertTo-SecureString "B@dPa44w0rd" -
az ad user create --display-name "demo" --password "B@dPa55word" --user-
principal-name "\"demo@tenant.onmicrosoft.com"
New-AZADUser -DisplayName "Demo user"
-UserPrincipalName "demo@tenant.onmicrosoft.com"
-Password $password
```

<https://t.me/learningnets>



Add Guest Users

- Create user**
Create a new user in your organization. This user will have a user name like alice@inetasks.onmicrosoft.com.
- Invite user**
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.


Add role assignment

Role [ⓘ]
Contributor

Assign access to [ⓘ]
Azure AD user, group, or service principal

Select [ⓘ]
demo@ine-demo.com ✓

This user will be sent an email that enables them to collaborate with INE, Inc.

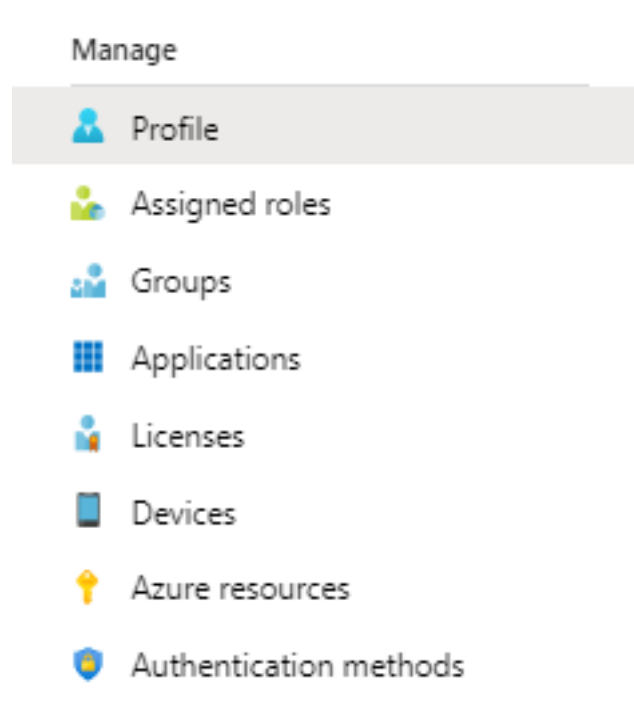
 demo@ine-demo.com (Guest)

Job info
Job title
Department

<https://t.me/learningnets>



Manage Users



Perform Bulk-Updates

- No intrinsic tool for bulk updates
- 3rd party tools
- Build custom API app – Microsoft Graph
- Implement PowerShell (CLI) script
 - + Updates in a CSV file
 - + Import-Csv
 - + Foreach loop
 - + Set-AzureADUser
 - + Set-AzureADUserExtension
 - + Set-AzureADUserLicense
 - + Set-AzureADUserManager
 - + Set-AzureADUserPassword
 - + Set-AzureADUserThumbnailPhoto

Perform Bulk-Updates

```
$UpdateUsers = import-csv -Path "d:\updates\deptChange.csv"
```

```
Foreach ($ UpdateUsers in $ UpdateUsers) {  
    Set-AzureADUser -ObjectID $updateUser.upn `  
        -Department $updateUser.department  
}
```

Demo: Create and Manage Users

<https://t.me/learningnets>





Create and Manage Groups

Create and Manage Groups

- Azure AD Groups
- Create Groups
- Manage Groups
- Demo: Create and Manage Groups

Azure AD Groups

<https://t.me/learningnets>



Create Groups

New Group

Group type *

Security



Group name * ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Membership type * ⓘ

Assigned



Assigned

Dynamic User

Dynamic Device

Members



Create Groups

New Group

Group type *

Security

Group name * ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Membership type * ⓘ

Assigned

Assigned

Dynamic User

Dynamic Device

Members

Add members

Select member or invite an external user ⓘ

demo










Demo User
demo@ine-demo.com

Create Groups

```
$group = New-AzureADGroup -Description "Demo security group"  
-DisplayName "Demo Group" -SecurityEnabled $true -  
MailEnabled $false  
Add-AzureADGroupMember -ObjectId $group.Id -RefObjectId  
$userId
```

Manage Groups

Manage

-  Properties
-  Members
-  Owners
-  Group memberships
-  Applications
-  Licenses
-  Azure resources

Demo: Create and Manage Groups

<https://t.me/learningnets>





Manage Devices

Manage Devices

- Device Integration
- Device Registration
- Device Join
- Device Management
- Demo: Device Join

Device Integration

Option	Purpose	Requirements
Azure AD Registered Devices	Cloud Application SSO Conditional Access ¹ On-prem access via Web Application Proxy ²	Windows 10, iOS, Android, MacOS
Azure AD Joined Devices	Cloud BitLocker key storage MS Passport Sign-in Phone and PIN sign-in Enterprise state roaming	Windows 10
Hybrid AD Joined	Extend on-prem device management to Azure AD for SSO, enterprise state roaming ³	Windows 7 and above ³

1 – requires Azure AD premium

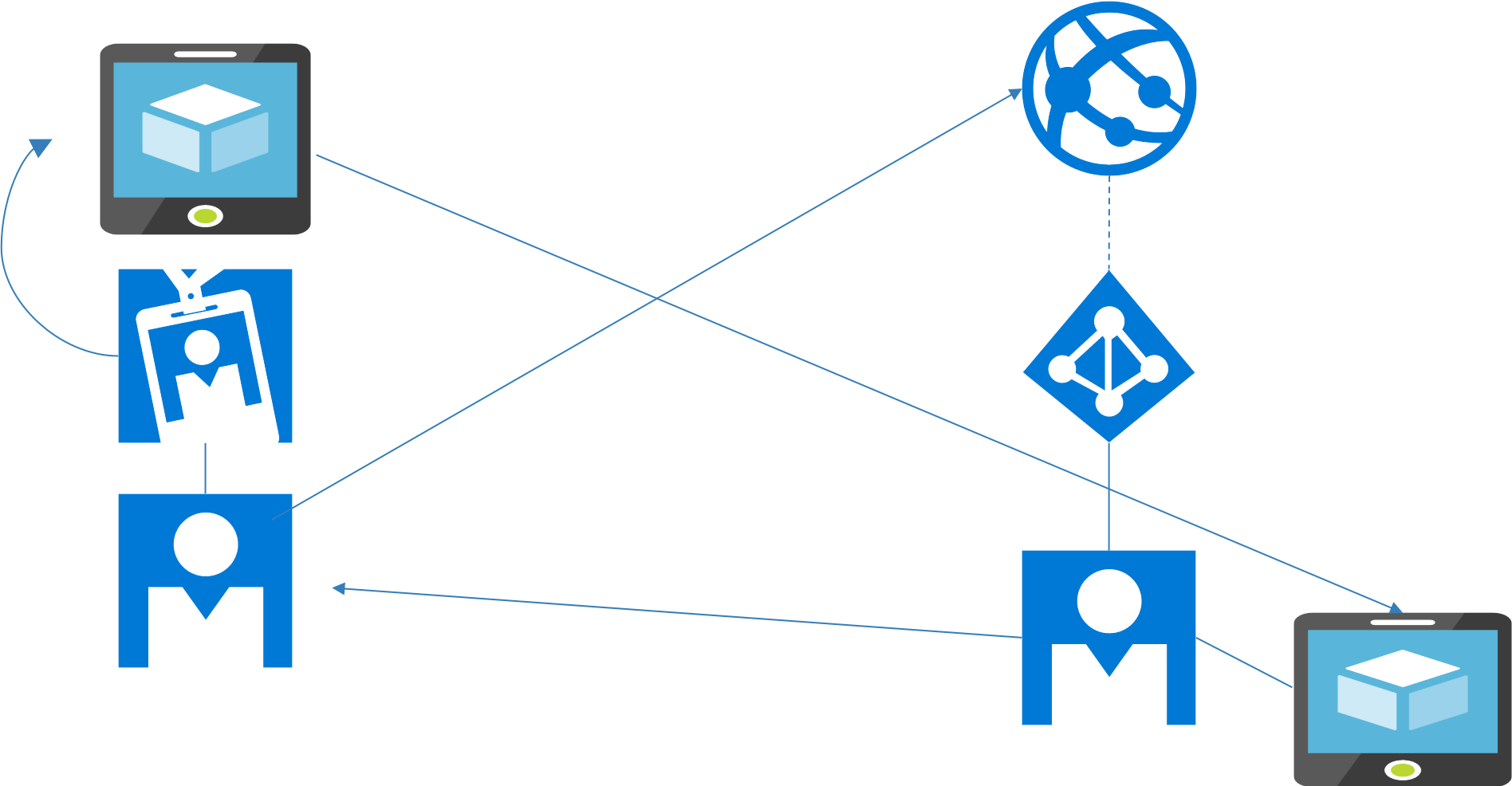
2 – requires Azure AD basic

3 – not all features are available to down-level Windows versions

<https://it.me/learningnets>



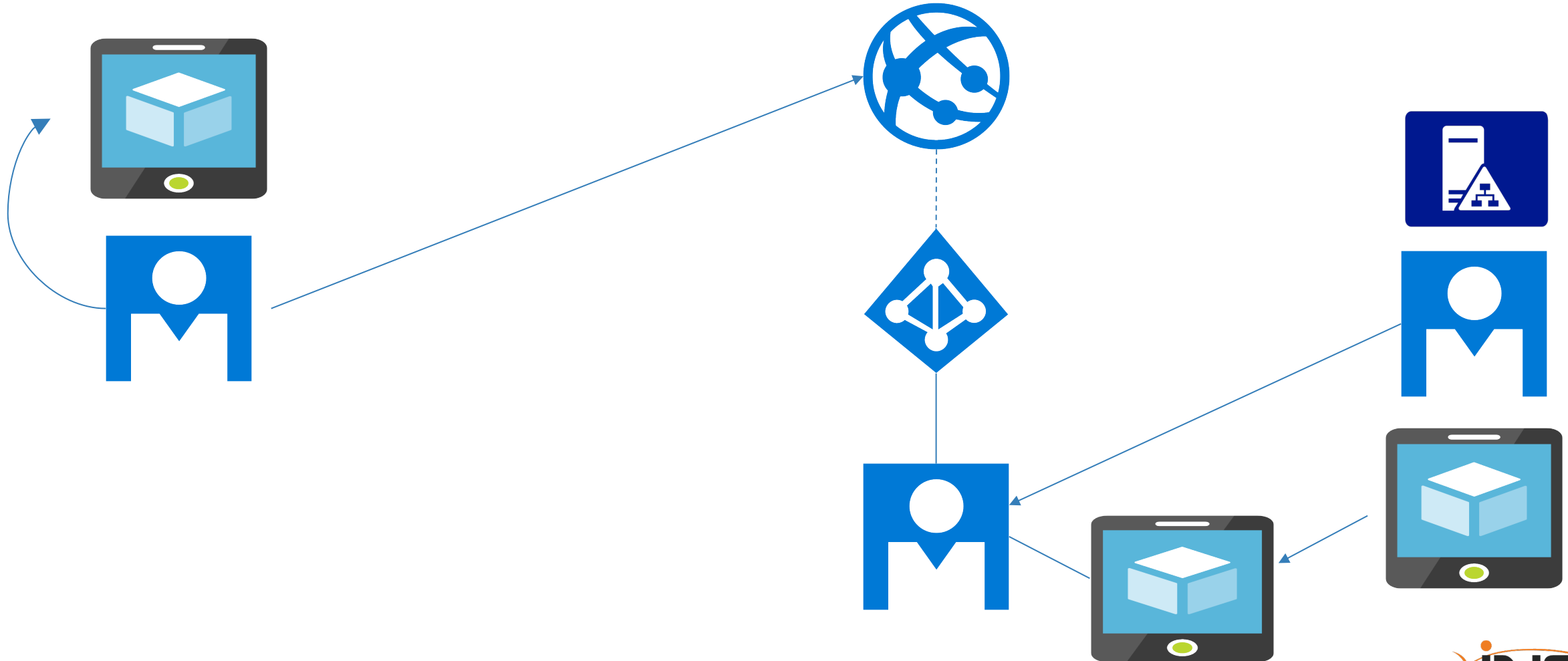
Device Registration



<https://t.me/learningnets>



Hybrid Join



<https://t.me/learningnets>



Device Management

- Azure AD options
 - + Control join access
 - + Add local admins to joined devices
 - + Allow device registration
 - + Require MFA to join devices
 - + Enterprise state roaming
- Integrate with management tools
 - + MDM - Microsoft Intune – integrated with conditional access
 - + Group Policy – hybrid joined
 - + MAM – Mobile application management tools

Demo: Device Join

<https://t.me/learningnets>





Configure Self-Service Password Reset

Configure Self-Service Password Reset

- Self-Service Password Reset Concepts
- Demo: Self-Service Password Reset

Self-Service Password Reset Concepts

- Licensing
- Options
 - + Mobile app notification (preview)
 - + Mobile app code (preview)
 - + Email
 - + Mobile phone*
 - + Office phone*
 - + Security questions
- Policy
 - + Two-gate policy for administrator roles – no phone calls
 - + Cloud user accounts – standard account options

* not available for free/trial Azure AD tenants

Demo: Self-Service Password Reset

<https://t.me/learningnets>





Role-Based Access Control



Role-Based Access Control

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

Role-Based Access Control Concepts

<https://t.me/learningnets>



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": ["/"]  
}
```



Custom Roles

Custom Roles

- ❑ Define Custom Roles
- ❑ Assign Custom Roles
- ❑ Demo: Custom Roles

Define Custom Roles

```
{  
  "Name": "Security Admin",  
  "Description": "Security Admin Role",  
  "Actions": [  
    "Microsoft.Authorization/*/read",  
    "Microsoft.Authorization/policyAssignments/*",  
    "Microsoft.Authorization/policyDefinitions/*",  
  ],  
  "NotActions": [],  
  "DataActions": [],  
  "NotDataActions": [],  
  "AssignableScopes": ["/Subscriptions/<your subscription>, /Subscriptions/<another subscription>]  
}
```

New-AzRoleDefinition -InputFile C:\Temp\roleDefinition.json


Assign Custom Roles

Add role assignment ✕

Role ⓘ
DemoRole

Assign access to ⓘ
Azure AD user, group, or service principal

Select ⓘ
tr ✓

 TW Tracy Wallace
twallace@inetraining.onmicrosoft.com

Demo: Custom Roles

<https://t.me/learningnets>





Manage Costs

Manage Costs

- ❑ Azure Cost Management
- ❑ Demo: Cost Management Tools

Azure Cost Management

The screenshot displays the Azure Cost Management dashboard. On the left, a navigation menu includes 'Cost analysis', 'Cost alerts', 'Budgets', 'Advisor recommendations', and 'Clouddyn'. The main area features a cost chart at the top with 'ACTUAL COST' at \$171.18 and 'FORECAST-CHART VIEW ON' at \$235.10. Below the chart, the 'Active alerts' section shows one alert: 'Budget - cost exceeded threshold' with the name 'Actual > 50% (Demo, August 2019)' and date 'Thursday, September 26, 2019'. The 'Advisor recommendations' section shows a message: 'You are following all of our cost recommendations for the selected subscriptions and resources. See list of cost recommendations'. Red arrows point from the navigation menu items to their corresponding sections in the dashboard.

TYPE	NAME	DATE	STATUS
Budget - cost exceeded threshold	Actual > 50% (Demo, August 2019)	Thursday, September 26, 2019	Active

Demo: Cost Management Tools

<https://t.me/learningnets>

