



Security Implementation at Resource Group level

Mahendra Shinde

Microsoft
Partner

Silver Learning
Gold Cloud Platform



Educate

Advise

Implement

Manage

Agenda

- Quick refresher on Azure AD
- Security & Roles in Azure AD
- Role based access control
- Azure AD Groups
- Azure AD Application registration
- Role Assignment (At Resource and Resource group level)



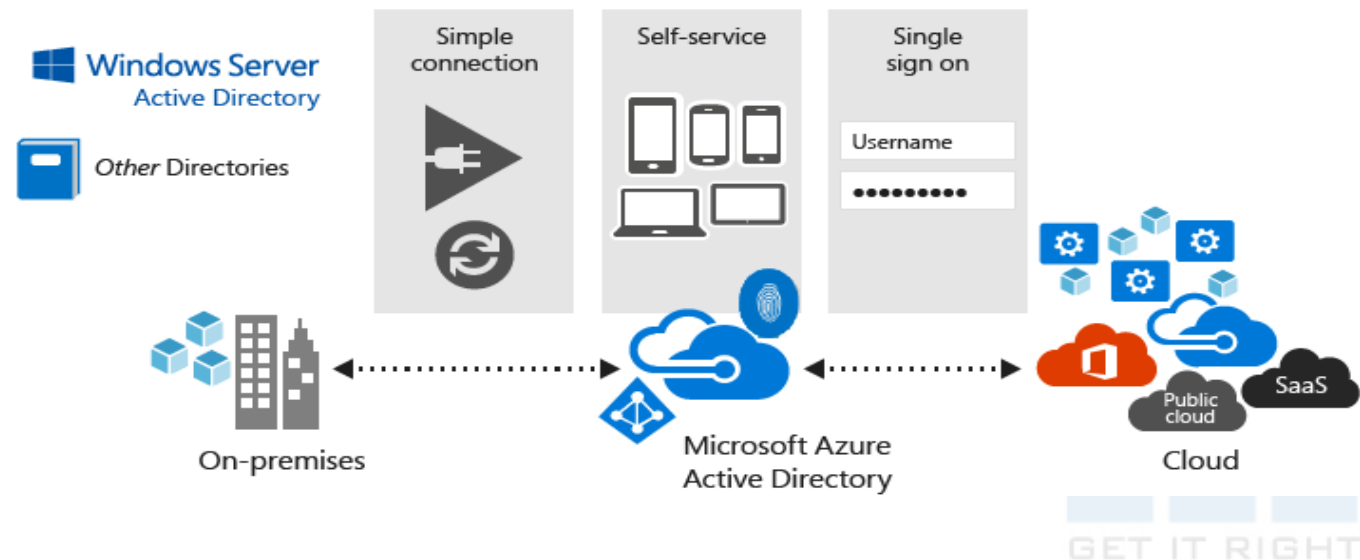
Security 101

- Authentication
 - Identifying an User
- Authorization
 - Verifying User's role and privileges.
- Encryption / Decryption
 - Making your data difficult to read!
- Cloud Based Security Solution:
 - Identify As A Service
 - Example: Azure Active Directory!



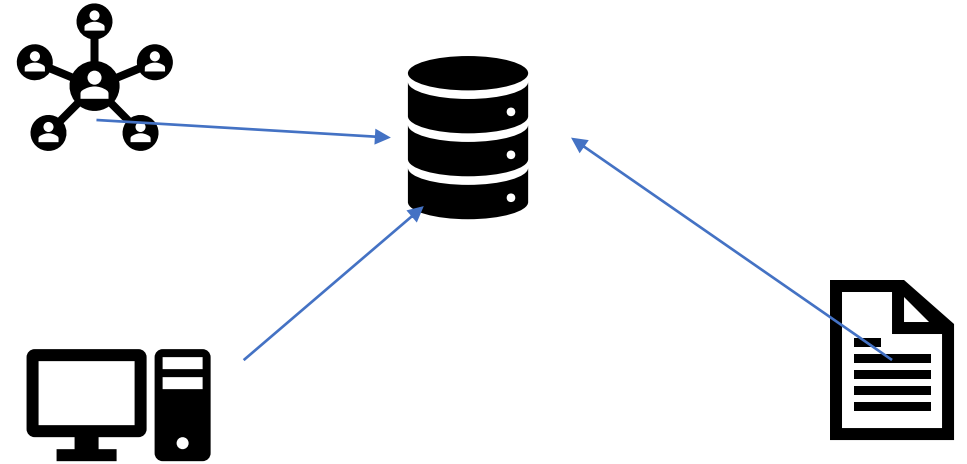
Azure Active Directory

- Microsoft's multi-tenant cloud-based directory and identity management service
- Provides SSO access
- Identity management capabilities and integration
- Integrates with Windows Server Active Directory



Active Directory Records:

- User Identities
- Device Identities
- Application Identities



Azure Active Directory Benefits

- Single sign-on to any cloud or on-premises web app
- Compatible with iOS, Mac OS X, Android, and Windows devices
- Protect on-premises web applications with secure remote access
- Extend Active Directory to the cloud
- Help protect sensitive data and applications



1000s of apps,
1 identity



Enable business
without borders



Manage access
at scale



Cloud-powered
protection

Role Definitions

- Each role has a role definition defined in a JSON file
- The **Actions** and **NotActions** properties allow or deny actions
- The **AssignableScopes** property specifies the affected subscriptions, resource groups, or resources

Name: Owner

ID: 8e3af657-a8ff-443c-a75c-2fe8c4bcb65

IsCustom: False

Description: Manage everything, including access to resources

Actions: {*}










NotActions: {}

AssignableScopes: {/}

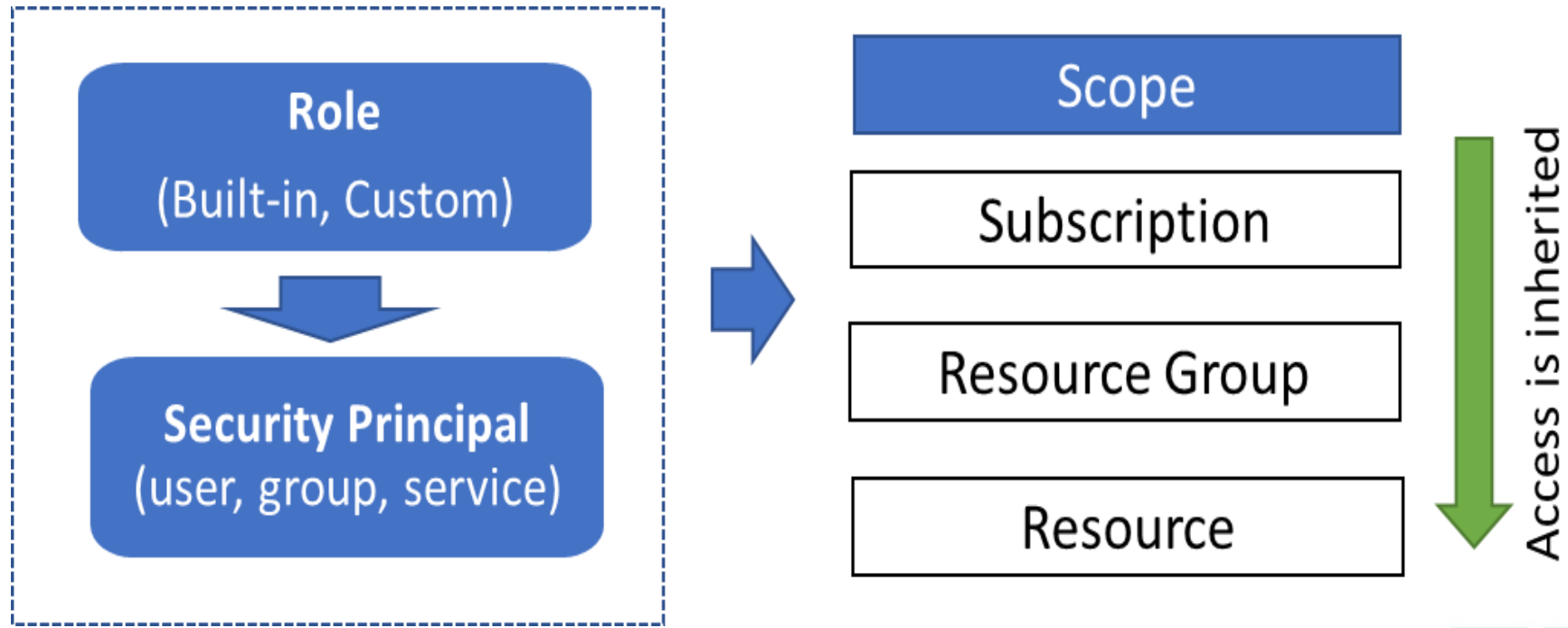


Azure AD Security & Roles

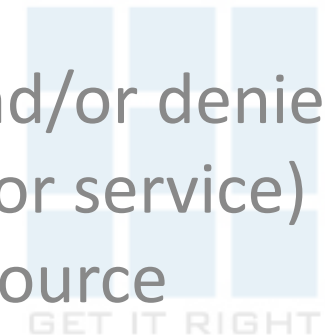
- Azure AD has many [built-in roles](#)
- Owner has full access to all resources including the right to delegate access to others.
- Contributor can create and manage all types of Azure resources but can't grant access to others
- Reader can view existing Azure resources

Roles		
ASH		
NAME	USERS	GROUPS
 Owner ⓘ	0	1
 Contributor ⓘ	4	0
 Reader ⓘ	1	0
 AcrImageSigner ⓘ	0	0
 AcrQuarantineReader ⓘ	0	0
 AcrQuarantineWriter ⓘ	0	0
 API Management Service Contributor ⓘ	0	0
 API Management Service Operator Role ⓘ	0	0
 API Management Service Reader Role ⓘ	0	0

Role based access control



1. Select a role (the definition of what actions are allowed and/or denied)
2. Associating the role with a security principal (user, group, or service)
3. Scope to a subscription, a resource group, or a specific resource



Security Demo

- Create User & Groups
- Grant Access for Resource & Resource groups



Custom Roles



GET IT RIGHT