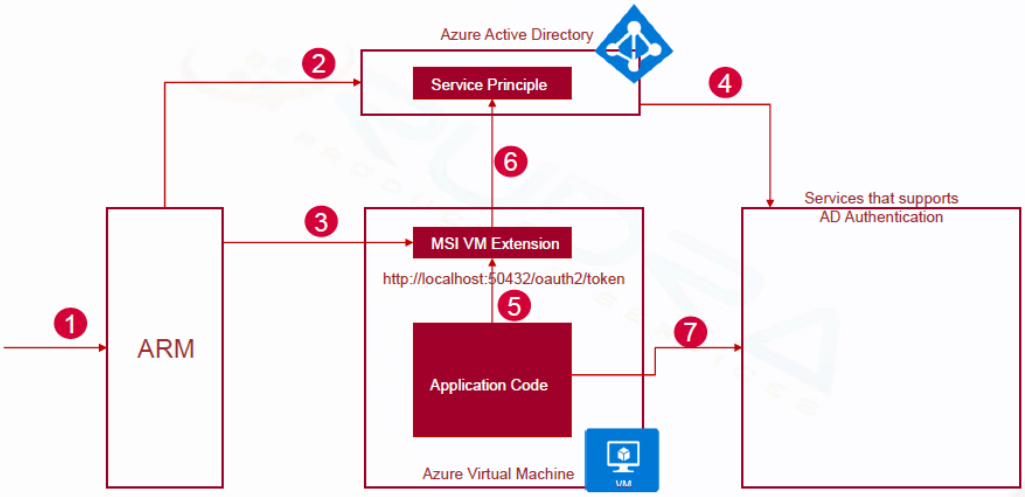
Azure active directory

- Each Azure subscription is associated with one Azure Active Directory (AD) directory.
- Users, groups, and applications from that directory can manage resources in the Azure subscription.
- Grant access by assigning the appropriate RBAC role to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource.
- Azure RBAC has three basic roles that apply to all resource types:
  - **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.

Azure security center

- Security Center identifies potential virtual machine (VM) configuration issues and targeted security threats. These might include VMs that are missing network security groups, unencrypted disks, and brute-force Remote Desktop Protocol (RDP) attacks.
- Set up data collection
- Set up security policies
- View VM configuration health
- Remediate configuration issues
- View detected threats

Managed service identity



Other security features

- Network security group
- Microsoft Antimalware for Azure
- Encryption
- Key Vault and SSH Keys
- Policies