Create and Manage AD DS Security Principals

Tim Warner

Principal Author Evangelist, Pluralsight

@TechTrainerTim TechTrainerTim.com

MVP
Microsoft®
Most Valuable
Professional

Microsoft
CERTIFIED
AZURE SOLUTIONS
ARCHITECT
EXPERT

Overview

Create and manage AD DS users and groups

Manage users and groups in multi-domain and multi-forest scenarios

Implement group managed service accounts (gMSAs)

Join Windows Servers to AD DS, Azure AD DS, and Azure AD

Deploy and Manage Active Directory Domain Services

- Deploy and Manage Domain Controllers
- Configure Active Directory Forest Environments
- Create and Manage AD DS Security Principals
- Implement and Manage Hybrid Identities
- Manage Windows Server with Group Policy

Manage AD Users and Groups

AD Domain User Account

```
New-ADUser -Name "Beth Workman" -GivenName "Beth" `
  -Surname "Workman" -SamAccountName "beth" `
  -AccountPassword "St@rt3rPa$$w0rd!" `
  -ChangePasswordAtLogon $true -Enabled $true
```

Group Types

Security: Assign permissions

Distribution: Email recipient

Group Scopes

Local: Standalone servers and workstations

Domain Local: Exist on domain controllers with domain scope

Global: Organize users; forest scope

Universal: Members and visibility is forest scope

Administrator Groups

Administrators: Non-domain servers and workstations

Administrators: Domain local group on DCs

Domain Admins: Global within each domain

Enterprise Admins: Members of Administrators group in every forest domain

Special Identities

System

Network Service

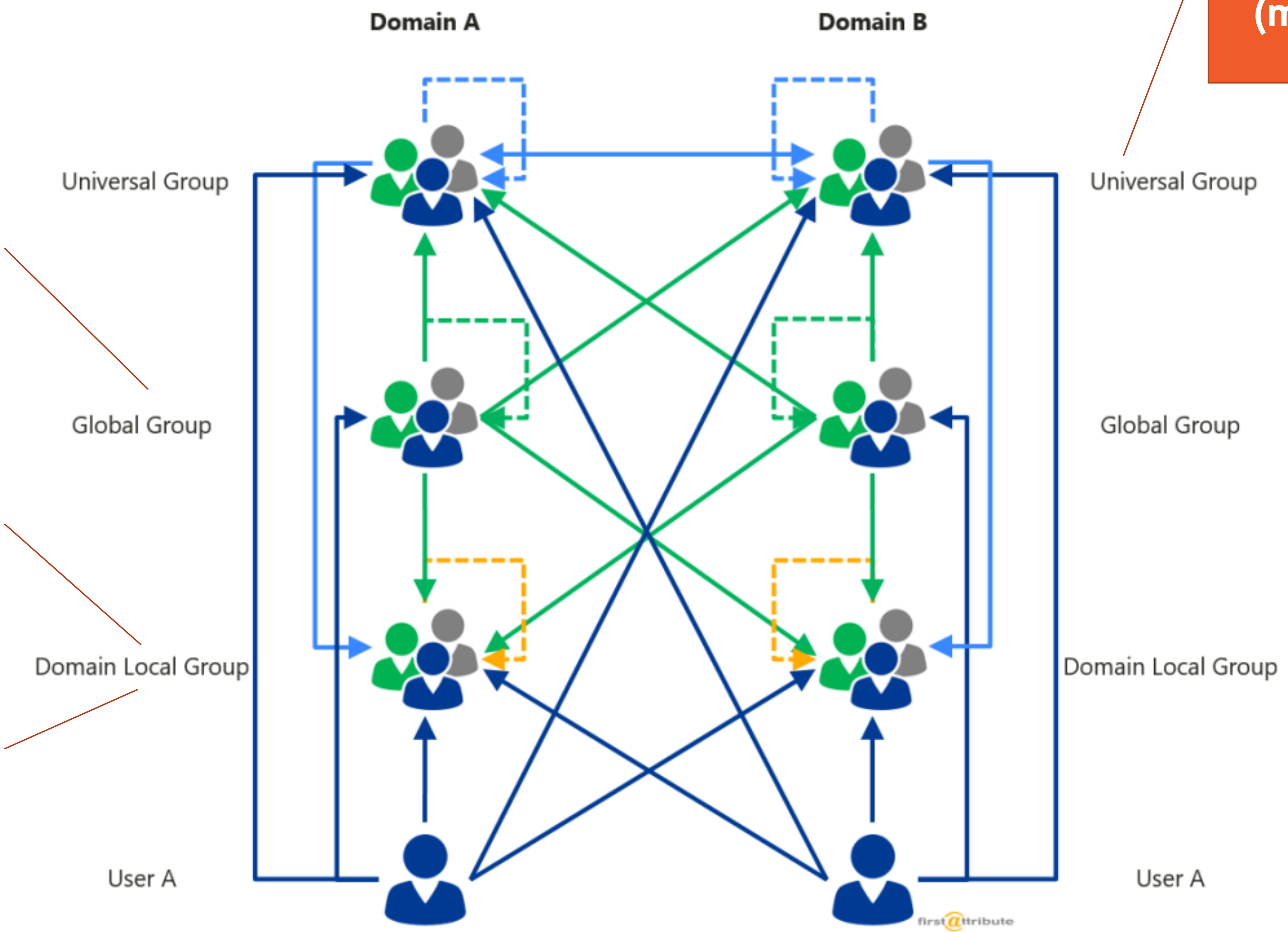
Everyone

sdf

sadf

sadf

Group Usage & Nesting



Organize domain users

Add universal/global groups

Apply permissions

Add global groups (multi-domain)

timw.info/un4

Group Managed Service Accounts

Group Managed Service Account (gMSA)

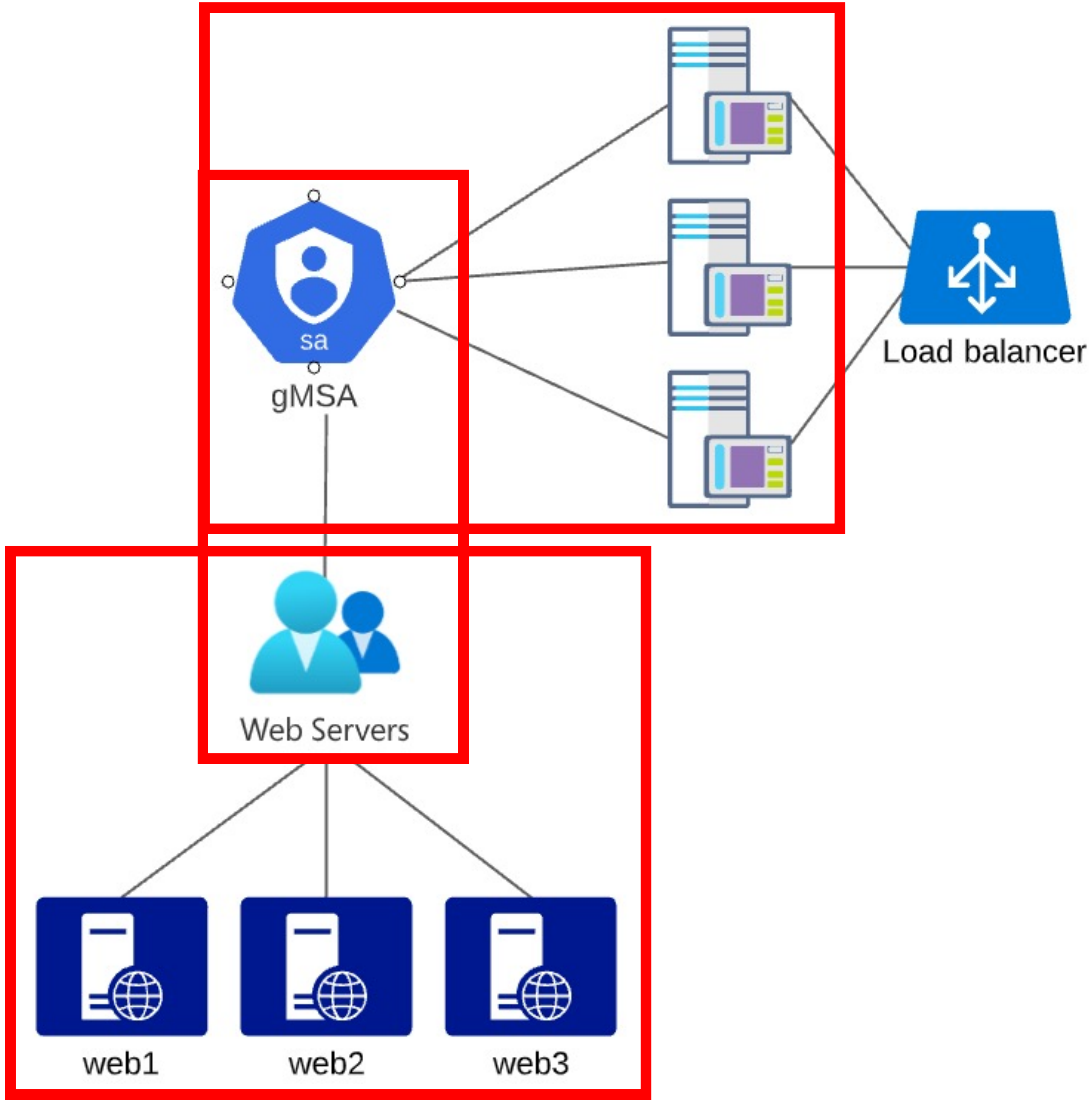
Automatic password management (240-character passwords)

Password is unknown to any person

Password changes automatically on a regular schedule

Password change is automatically picked up by your application

Credential can be used across multiple computers



Demo

1

Show default group membership (CLI, ROOTDC1)

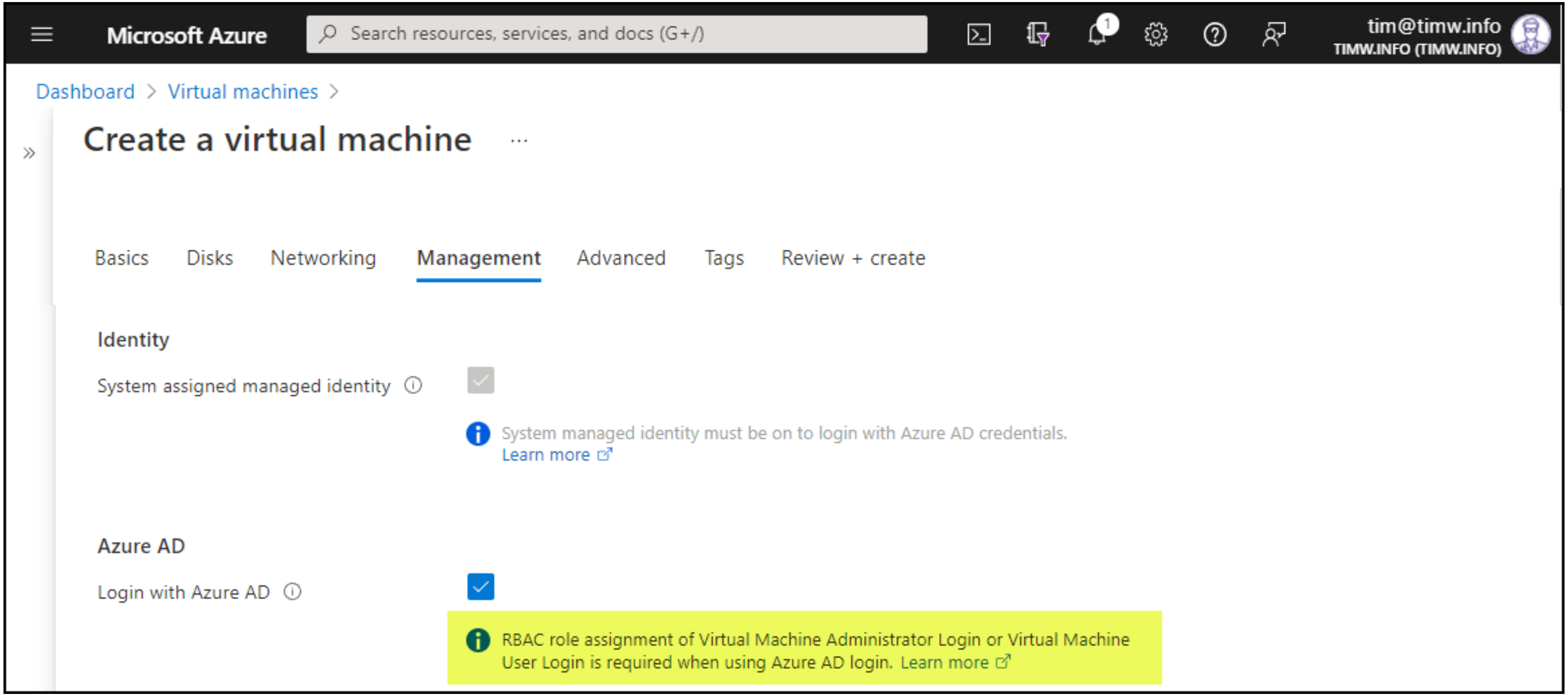
Create user, global group, universal group

Put in domain local groups in child and remote forest

gMSA

Join Windows Server to AD DS, Azure AD DS, and Azure AD

Azure AD Sign-in for Azure VMs



Create a virtual machine

Identity

System assigned managed identity ☑

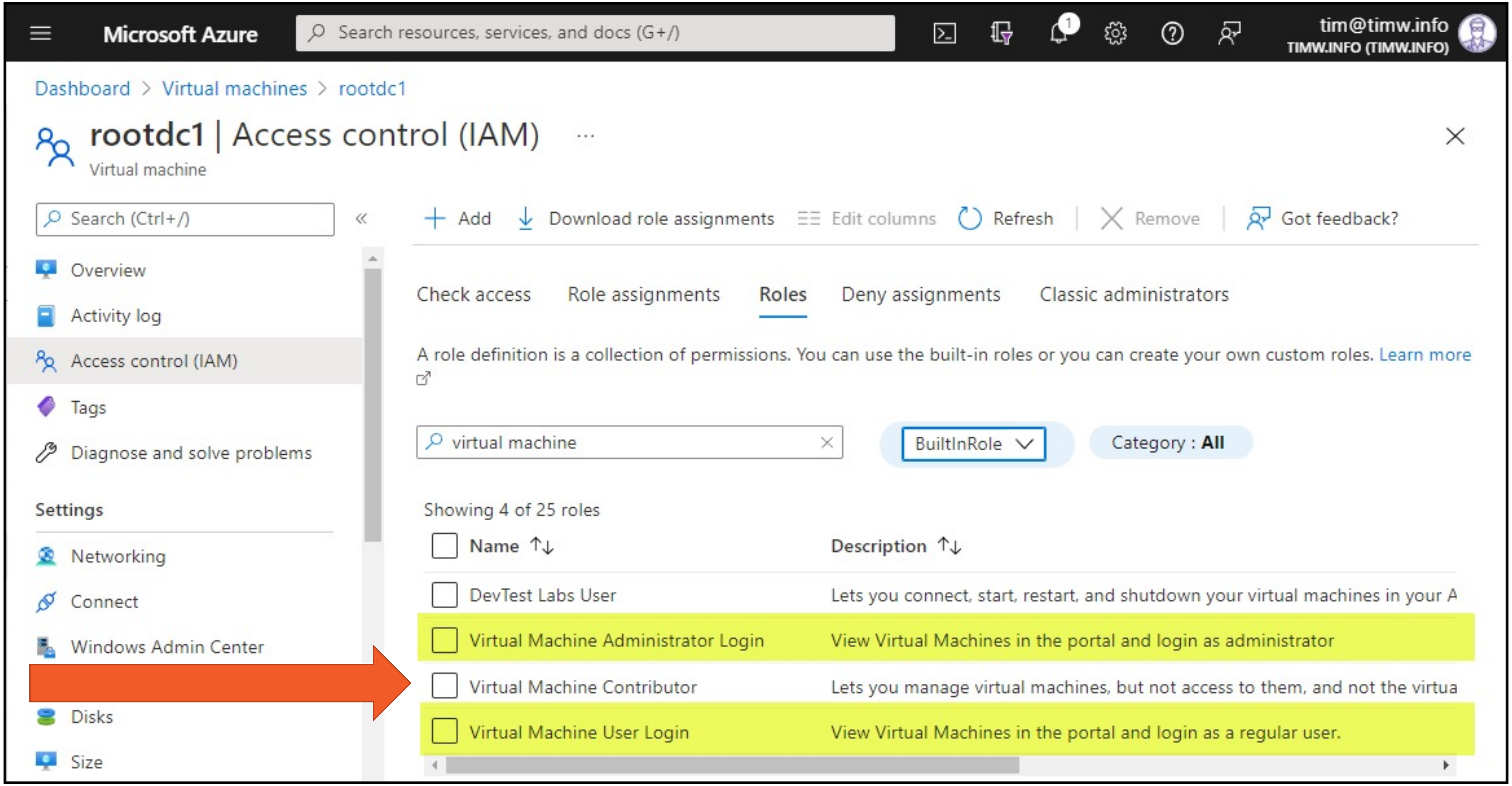
System managed identity must be on to login with Azure AD credentials. Learn more

Azure AD

Login with Azure AD ☑

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. Learn more

Azure AD Sign-in for Azure VMs



rootdc1 | Access control (IAM)

Virtual machine

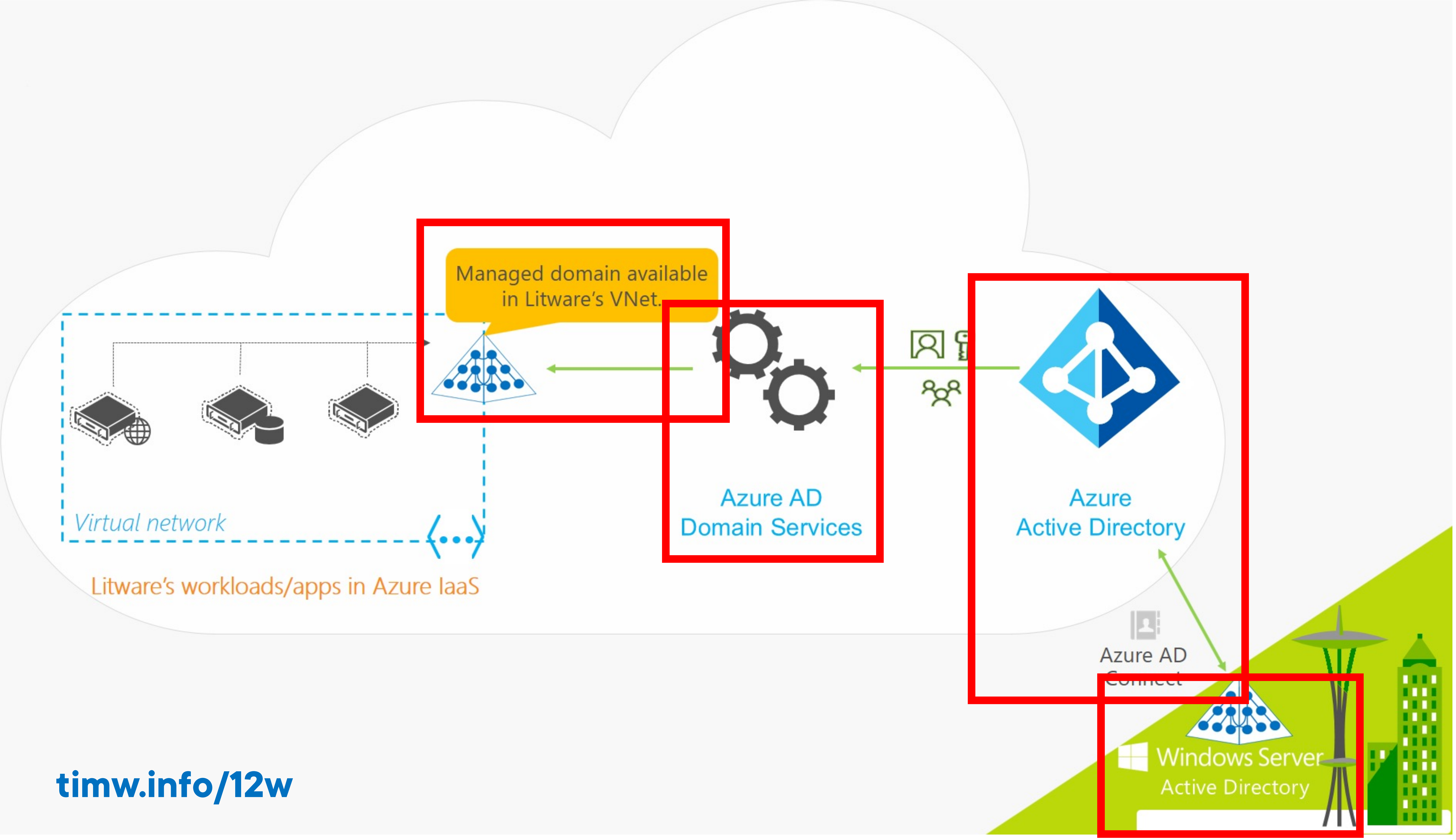
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

virtual machine

Showing 4 of 25 roles

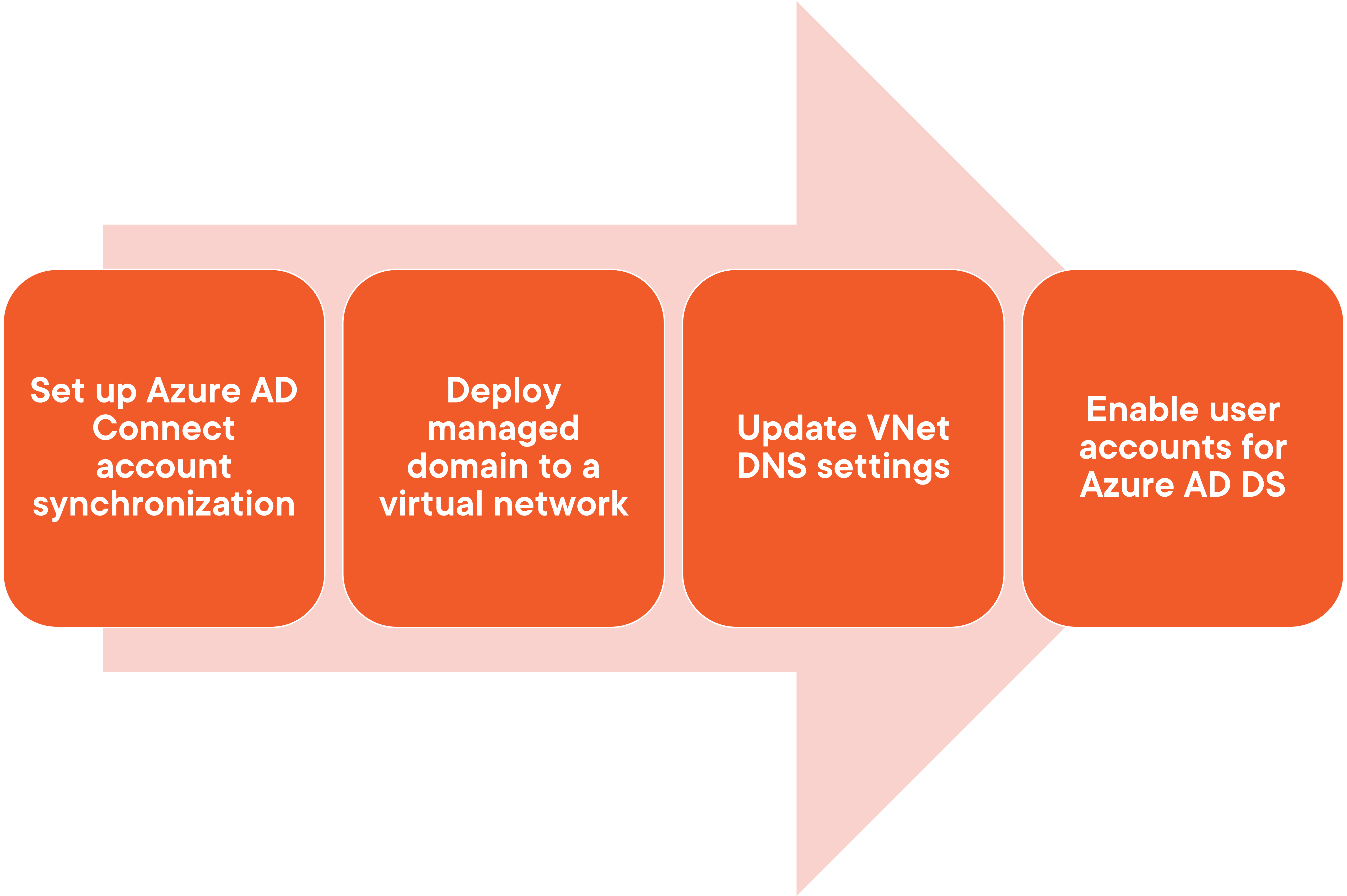
□	Name ↑↓	Description ↑↓
□	DevTest Labs User	Lets you connect, start, restart, and shutdown your virtual machines in your A
□	Virtual Machine Administrator Login	View Virtual Machines in the portal and login as administrator
□	Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtua
□	Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.

Azure AD Domain Services


Managed domain available in Litware's VNet.
Virtual network
Litware's workloads/apps in Azure IaaS
Azure AD Domain Services
Azure Active Directory
Azure AD Connect
Windows Server Active Directory

timw.info/12w

Azure AD Domain Services Deployment



Set up Azure AD Connect account synchronization

Deploy managed domain to a virtual network

Update VNet DNS settings

Enable user accounts for Azure AD DS

Demo

2

Azure AD DS deployment

Azure AD join

- Azure AD sign into Azure VM

Summary

AD user and group management hasn't changed much at all over the past 20 years

Keep in mind that Azure AD DS is a special-case product

Think about the local AD accounts you'd like synchronized to Azure AD to facilitate single sign-on (SSO) to cloud apps

Up Next:
Implement and Manage Hybrid Identities