

Configure Hybrid Active Directory Account Security



Tim Warner

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



Overview



Restrict access to domain controllers

Configure account security

Manage AD built-in administrative groups

Manage AD delegation

**Implement and manage Microsoft
Defender for Identity**



Windows Server 2022: Secure On-premises and Hybrid Infrastructure

Secure the Windows Server Operating System

Secure Hybrid Active Directory Accounts

Configure Hybrid Active Directory Account Security

Remediate Windows Server Security Issues with Azure Services

Secure Windows Server Networking

Secure Windows Server Storage



Restrict Access to Domain Controllers



Restrict Access to Domain Controllers

Authentication Policy Silos

GPO user rights assignment

**Defender Firewall Network
Access Groups (NAGs)**

Restricted Groups



Active Directory Account Security and Delegation



Built-in Active Directory Groups

Built-in container – Domain Local groups

- Administrators
- Server Operators

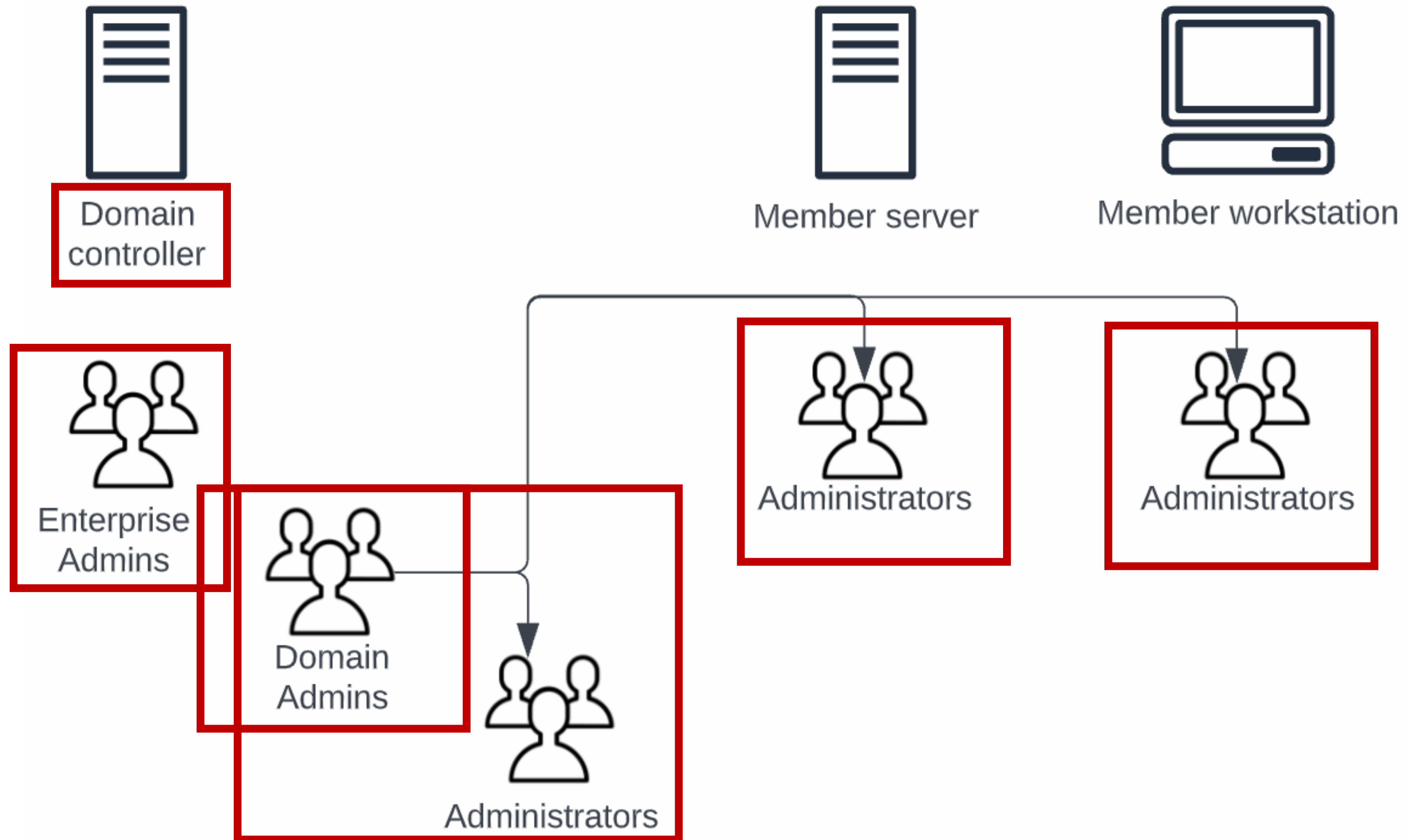
Users container – Universal and Global groups

- Administrator
- Domain Admins
- Enterprise Admins
- Protected Users
- Schema Admins

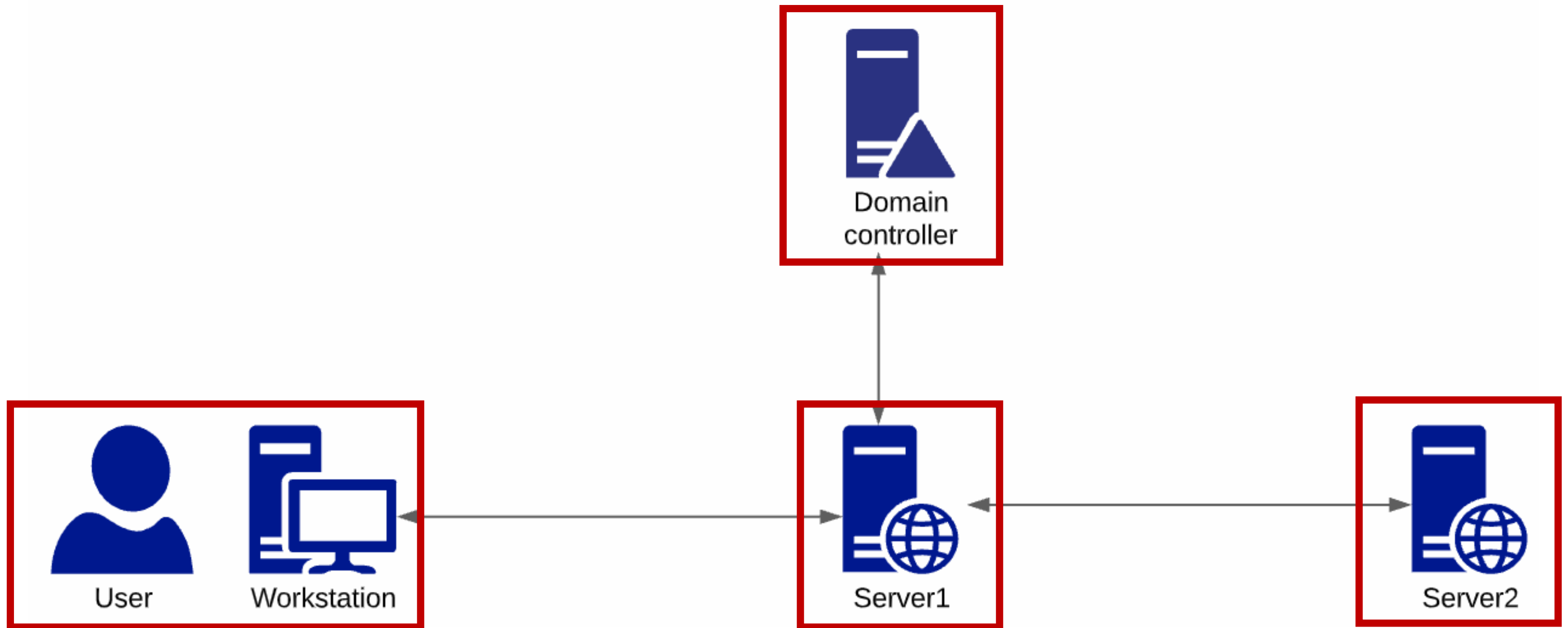
User rights assignments



Built-in Active Directory Groups



Delegation and Kerberos "Second Hop" Problem



Microsoft Defender for Identity



Formerly called Azure Advanced Threat Protection (ATP)

Cloud-based security solution that monitors your local AD DS infrastructure

- Report on user and entity behavior
- Protect AD credentials (passwords, group memberships)
- Identify, alert, and investigate anomalous behavior



Demo



1

Tour built-in admin groups

Delegation of control MMC wizard

CredSSP and Kerberos delegation

Defender for Identity setup



Summary



Keep least privilege authorization at top of mind

MDI is (yet) another example of bringing cloud-powered AI to your on-premises Active Directory environment



Up Next:

Remediate Windows Server Security Issues
with Azure Services

