

# Migrate an AD DS Infrastructure to Windows Server 2022 AD DS

---



**Tim Warner**

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



# Overview



## Migrate AD DS objects with Active Directory Migration Tool (ADMT)

Users

Groups

Group Policies

Upgrade an existing forest



# Windows Server 2022: Migrate Servers and Workloads

**Migrate On-Premises Storage on Windows Server**

**Migrate On-Premises Servers to Azure**

**Migrate Workloads to Windows Server 2022**

**Migrate IIS Workloads to Azure**

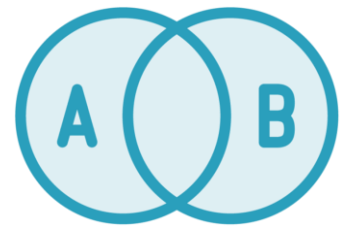
**Migrate an AD DS Infrastructure to Windows Server 2022 AD DS**



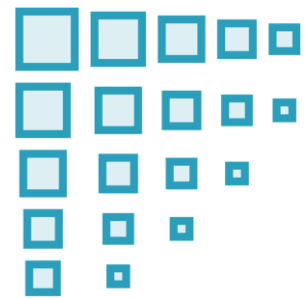
# Migrate AD Objects to Windows Server 2022



# Why Migrate to a New AD DS Forest?



**Merger or acquisition**



**Dissolution of a business unit**



**Necessity to rename a forest or domain**



**Security compromise**



# Why Consolidate Your Forest?

**Single forest, single domain**

**Fine-grained password policies**

**Forests, not domains, are the security boundary**

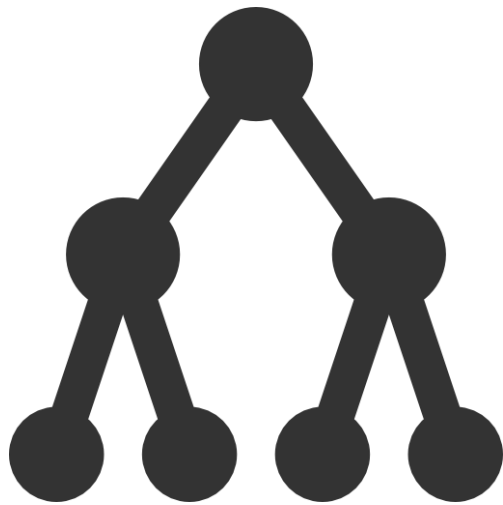
**Domain can support 100,000 objects**

**Increasing complexity can reduce security**

**Save replication bandwidth**



# Active Directory Migration Tool (ADMT)



## Toolset to move AD objects

- Interforest
- Intraforest

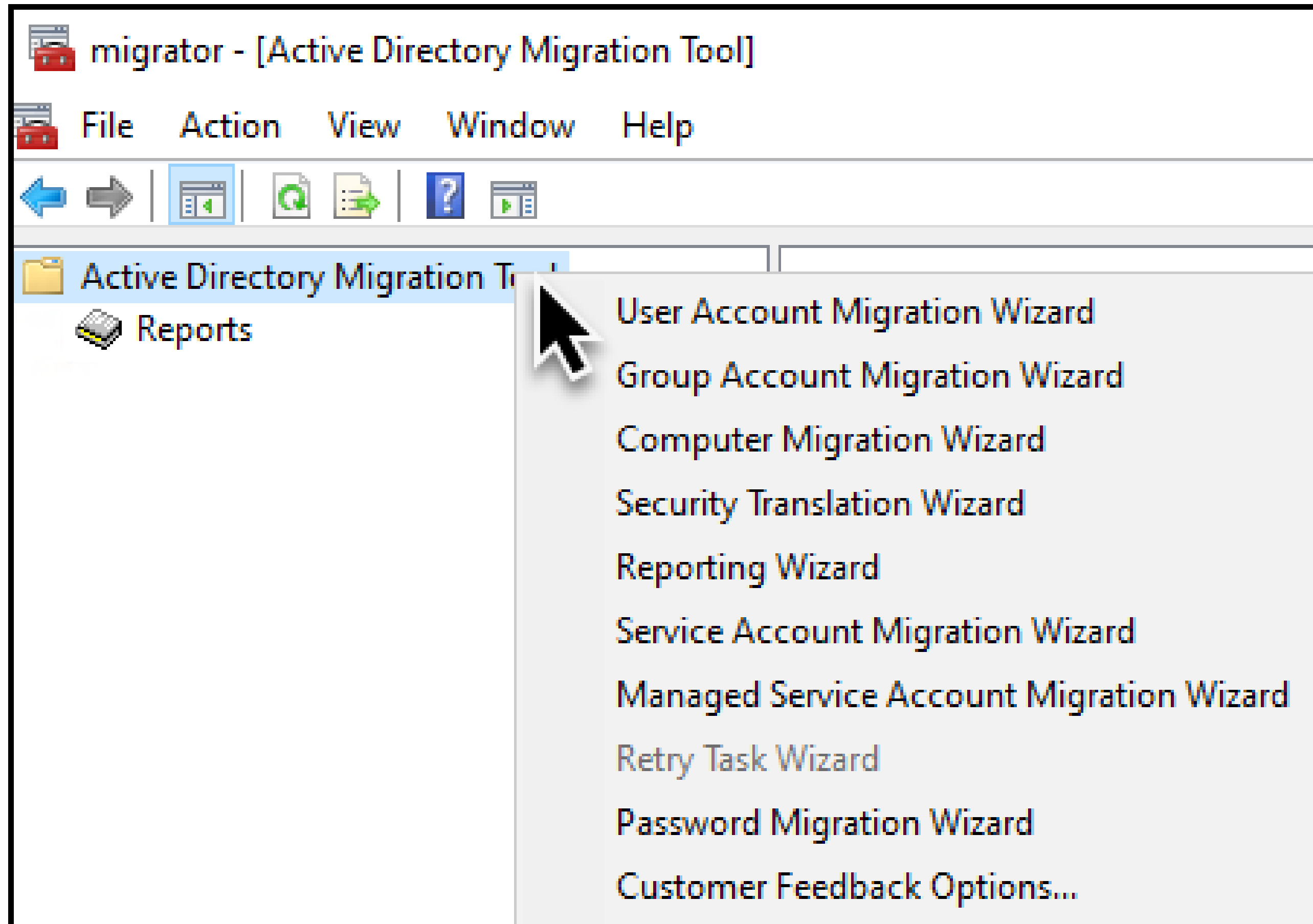
## Migrate many account types:

- Users
- Groups
- Service accounts
- Computer accounts

## Requires SQL Server



# Active Directory Migration Tool





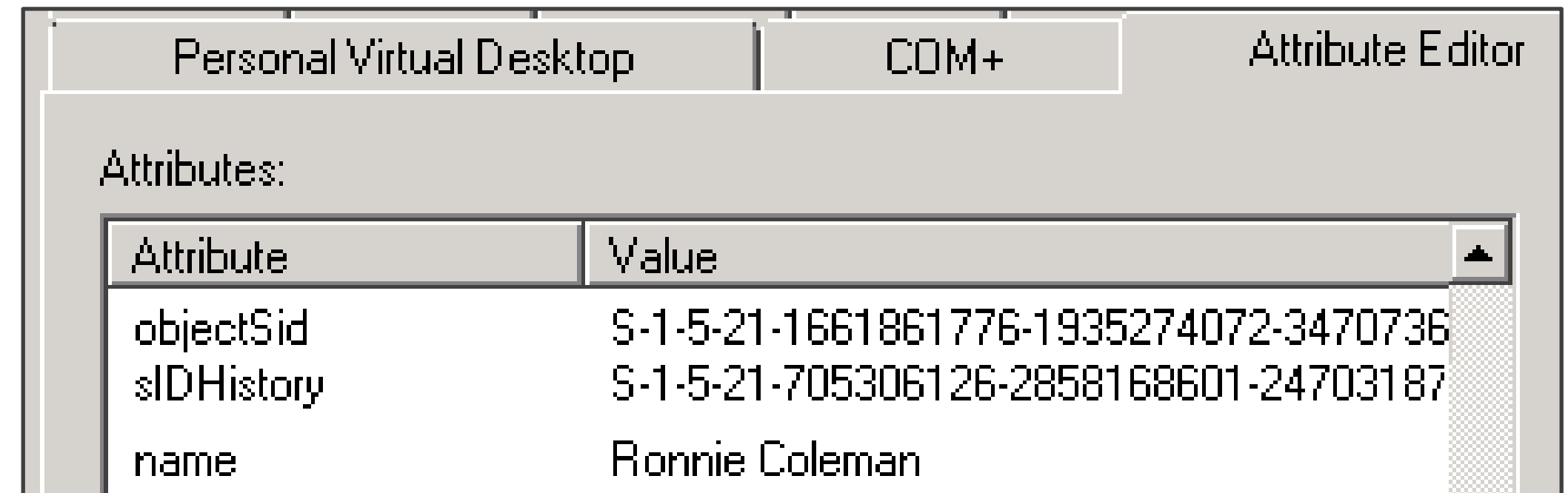
# SID Filtering

We don't want a migrated user to forge their user SID into high-privilege groups in the new domain

**SID quarantine**

**Enabled by default**

**Configure with netdom or PowerShell**



Attribute	Value
objectSid	S-1-5-21-1661861776-1935274072-3470736
sIDHistory	S-1-5-21-705306126-2858168601-24703187
name	Ronnie Coleman

# Demo



# 1

## ADMT



# Upgrade an Existing AD DS Forest to Windows Server 2022



# Upgrade Domain to Windows Server 2022

**adprep /forestprep**

**Add new  
member  
servers to  
each  
domain**

**Prepare  
the forest  
and  
domains  
with  
adprep**

**Promote  
new  
member  
servers to  
domain  
controllers**

**Transfer  
FSMO  
roles to  
new DCs**

**Demote  
legacy  
DCs to  
member  
servers**

**Set  
functional  
levels to  
Windows  
Server  
2016**

**adprep /domainprep**



# Transfer FSMO Roles

Get-ADDomain | Select-Object InfrastructureMaster, RIDMaster, PDCEmulator

Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster

Move-ADDirectoryServerOperationMasterRole -Identity forestRootDC -OperationMasterRole SchemaMaster, DomainNamingMaster

Move-ADDirectoryServerOperationMasterRole -Identity secondDC -OperationMasterRole PDCEmulator, RIDMaster, InfrastructureMaster



# Set Forest and Domain Functional Levels

# No new functional levels defined in Windows Server 2019 or Windows Server 2022

```
Set-ADDomainMode -identity timw.info  
-DomainMode Windows2016Domain
```

```
Set-ADForestMode -Identity timw.info  
-ForestMode Windows2016Forest
```



## Summary



You now have a solid grasp of not only local AD DS but how to integrate your Active Directory environment with Microsoft Azure

Thanks a lot!

Pluralsight courses: [timw.info/ps](https://timw.info/ps)

Website: [timw.info](https://timw.info)

Email: [tim@timw.info](mailto:tim@timw.info)

