

# Troubleshoot Active Directory

---



**Tim Warner**

Microsoft Azure Solutions Architect

@TechTrainerTim   TechTrainerTim.com



# Overview



**Restore objects from Active Directory Recycle Bin**

**Recover Active Directory database using Directory Services Restore Mode**

**Troubleshoot Active Directory replication**



# Windows Server 2022: Monitor and Troubleshoot Server Environments

**Monitor Windows Server Using Local Tools**

**Monitor Windows Server Using Azure Services**

**Troubleshoot Windows Server Hybrid Networking**

**Troubleshoot Windows Server VM Deployment Failures**

**Troubleshoot Windows Server VM Connection Issues**

**Troubleshoot Active Directory**



# Active Directory Recycle Bin



# Active Directory Recycle Bin



## Recover deleted AD user and group accounts

### Retention attributes

- msDS-deletedObjectLifetime
- tombstoneLifetime (180 days from Windows Server 2003 forward)

### One-way operation

### Manage with:

- Active Directory Administrative Center
- ADSI Edit MMC console
- Windows PowerShell

```
Enable-ADOptionalFeature -Identity  
"CN=Recycle Bin Feature,CN=Optional  
Features,CN=Directory  
Service,CN=WindowsNT,CN=Services,CN=Conf  
iguration,DC=domain" -Scope  
ForestOrConfigurationSet -Target  
"company.com"
```

```
Get-ADObject -Filter {displayName -eq  
"Marc Brown"} -IncludeDeletedObjects |  
Restore-ADObject
```

```
# Default tombstone lifetime is 180 days
```

```
$RootDomain = (Get-ADForest).RootDomain
```

```
$DomainDN = (Get-ADDomain -Identity  
$RootDomain).DistinguishedName
```

```
Set-ADObject "CN=Directory  
Service,CN=WindowsNT,CN=Services,CN=Conf  
iguration,$DomainDN" -Replace  
@{tombstoneLifetime=360}
```

◀ **Enable AD Recycle Bin (one-way operation)**

◀ **Restore a deleted AD user**

◀ **Set a new default tombstone lifetime**

# Directory Services Restore Mode



# Directory Services Restore Mode



**Password-protected offline "safe mode" environment for AD recovery on domain controllers**



**Perform authoritative AD object restore and AD database maintenance**



**Accessible with NTDSUtil.exe**



**Restartable AD DS minimizes need for DSRM nowadays**





# Restartable AD DS

**net stop/start ntds**

**Also stops FRS,  
KDC, DNS**

**Object restore**

**System State  
backup**

**Offline  
defragmentation**

**Keep System State  
<180 days**



# Troubleshoot AD Replication



## Repadmin.exe

# Get syntax help

```
repadmin /?
```

# Show overall replication health

```
repadmin /replsummary
```

# Show replication partner and status

```
repadmin /showrepl
```

# Show only replication errors

```
repadmin /showrepl /errorsonly
```

# Show replication queue

```
repadmin /queue
```

# Force a pull replication

```
repadmin /syncall <out-of-sync-dc> /AeD
```

# Demo



# 1

**<make mem1 a dc>**

**AD Recycle Bin with Admin Center**

**Restartable AD DS / offline defrag**

**Reboot DSRM**



## Summary



**AD DS really hasn't changed in many, many years**

**I hope your Windows Server skills are refreshed and you're confident to pass Exam AZ-801**

**Thanks!**

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

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

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

