# Restore von Active Directory mit einer von HP entwickelten Lösung

*(Recovering from Active Directory Disasters)*

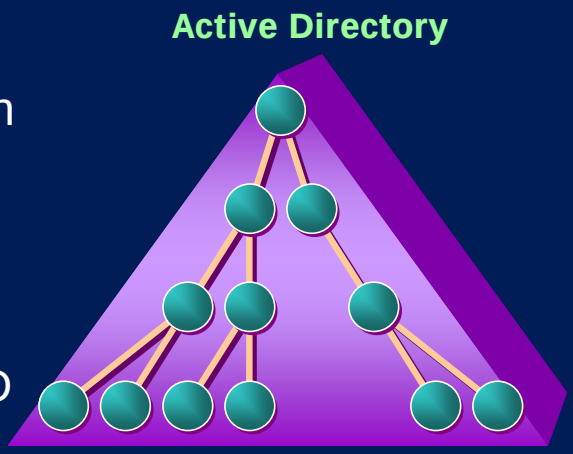
**Guido Grillenmeier**
Senior Consultant
Technology Solutions Group
Hewlett-Packard

## Agenda

- What is a Disaster?
- Authoritative Restore
- How Group-Memberships are stored
- Understanding Handling of Object-Links
- Recovering from a Disaster
- Changes in Windows Server 2003 with respect to Object-Link replication
- The HP solution: ADRAT

Active Directory is very fault-tolerant against HW failures
⇨ a dead DC is NOT a disaster !

**Disaster Scenarios:**




- Accidental deletion of objects by an administrator **(most likely cause!)**
- Malicious deletion of objects by an intruder
- Virus-Attack, deleting objects in AD
- Corruptions of objects/attributes
- Corrupt schema – could require forest recovery!

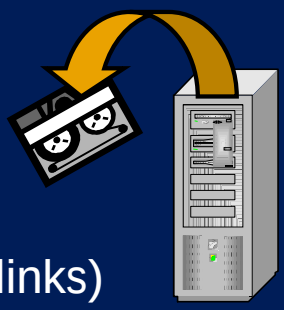


# Corrupt Schema – AD Forest Recovery

"**Roadmap**" for AD Forest Recovery:

1. Determine Forest Structure and available backups
2. Identify single DC for each domain with valid backup
3. Shutdown **all** DCs in the forest
4. First recover DC of **Forest Root Domain**
   ⇨ will ensure recovery of trust hierarchy and critical DNS resource records
5. Then recover **one** DC of **each child domain**
   ⇨ ensure recovery of parent domains prior to their child-domains to maintain trust-hierarchy
6. Cleanup and Re-Promote **all other** DCs in the forest

A good Active Directory backup includes:



1. System-State Backup of at least **two DCs** of each domain in an AD forest
   ⇨ don't require a backup of all DCs of a domain (may be different for Branch Offices with slow links)
2. If **SYSVOL** is not stored in default location, it may have to be backed up separately (depends on backup software used)
3. Separate backup of **GPOs** is a good idea to simplify restores of accidentally deleted GPOs
   ⇨ can leverage Windows Server 2003 **GPMC** to do so, but *this will NOT store the Site/Domain/OU **links** of the GPOs!*
   ⇨ also still need to backup any related external files of a GPO (e.g. logon scripts)
4. Ensure **physical security** of backup tapes!

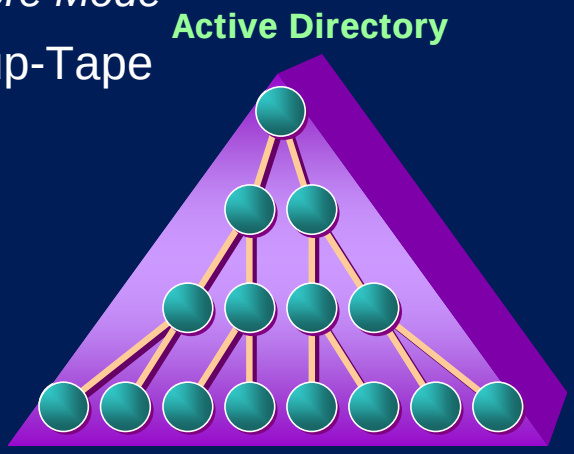


# Agenda

- What is a Disaster?
- Authoritative Restore
- How Group-Memberships are stored
- Understanding Handling of Object-Links
- Recovering from a Disaster
- Changes in Windows Server 2003 with respect to Object-Link replication
- The HP Solution: ADRAT

Deleted objects can be restored by performing an authoritative restore of the AD database

1. Boot DC to *Directory Services Restore Mode*
2. Restore System-State from Backup-Tape
3. Run **`NTDSUTIL`**
   - ⇨ `authoritative restore`
   - ⇨ `restore subtree`
     `OU=myOU,DC=mycorp,DC=com`
   - ⇨ **will update *version nr.* by 100,000 per day since time of backup**
4. Reboot DC ⇨ **restored objects will replicate to other DCs**

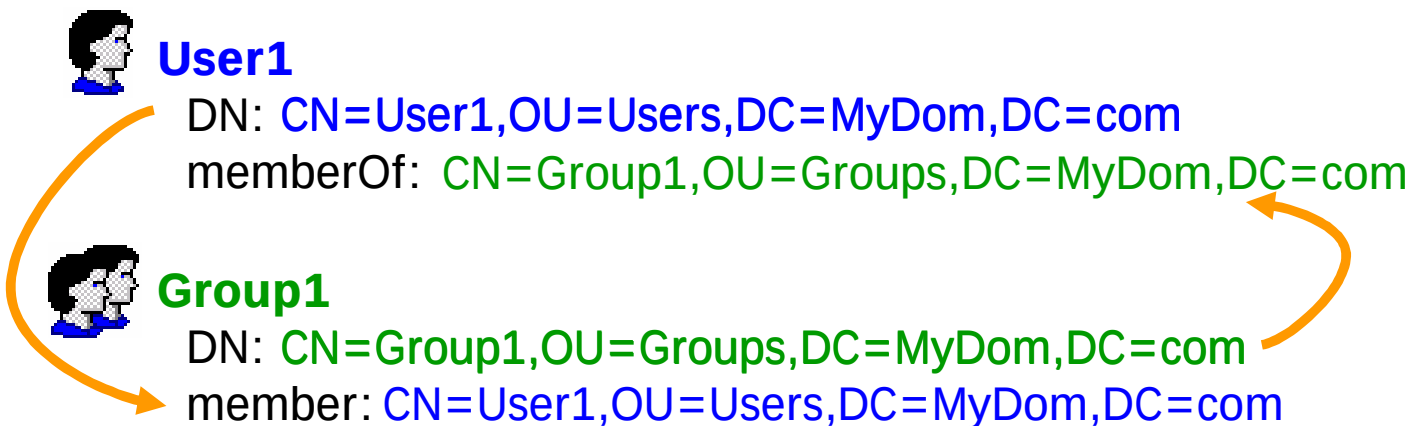



But there are some additional challenges to recover **everything** correctly...



## How Group-Memberships are stored in AD

The member-objects (e.g. Users) are stored as the DN in the **`member`** attribute of a Group. The Groups that a User belongs to are stored as the DN in the **`memberOf`** attribute of a User.



Active Directory stores group-memberships as Object-Links.


**Forward-Link**

- can be edited by admin
- is replicated to other DCs

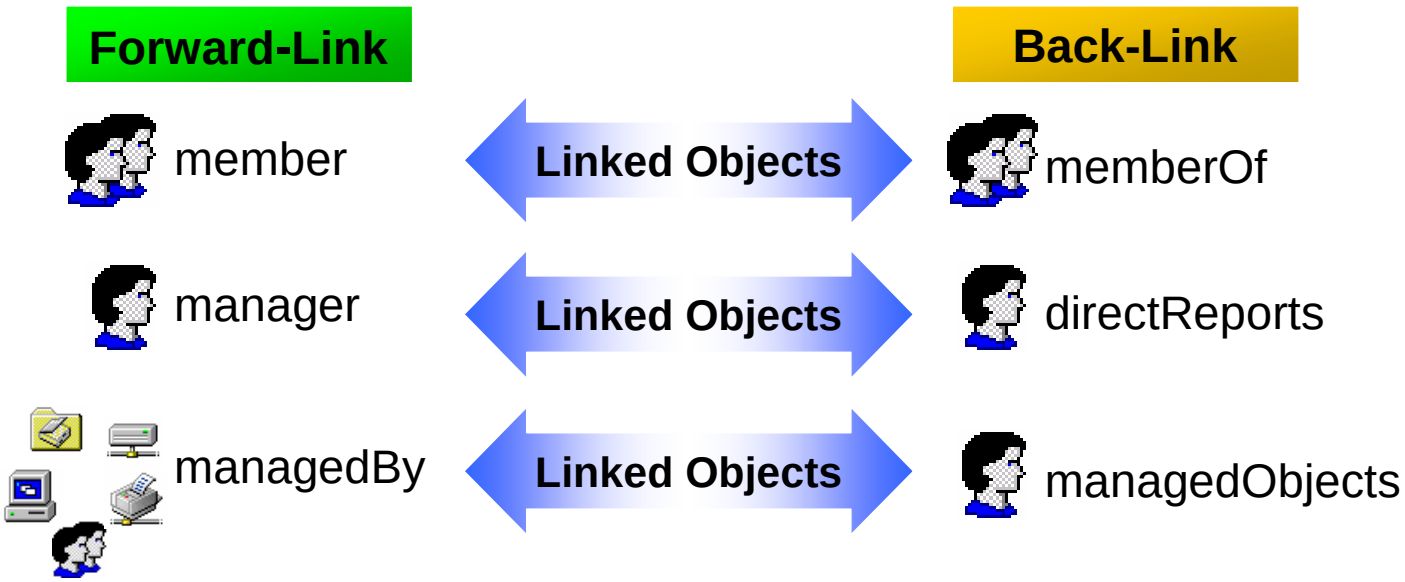
**Back-Link**

- is owned and maintained by DC
- is **not** replicated to other DCs

! *Links need special treatment during authoritative restore!*



# Other important Object-Links

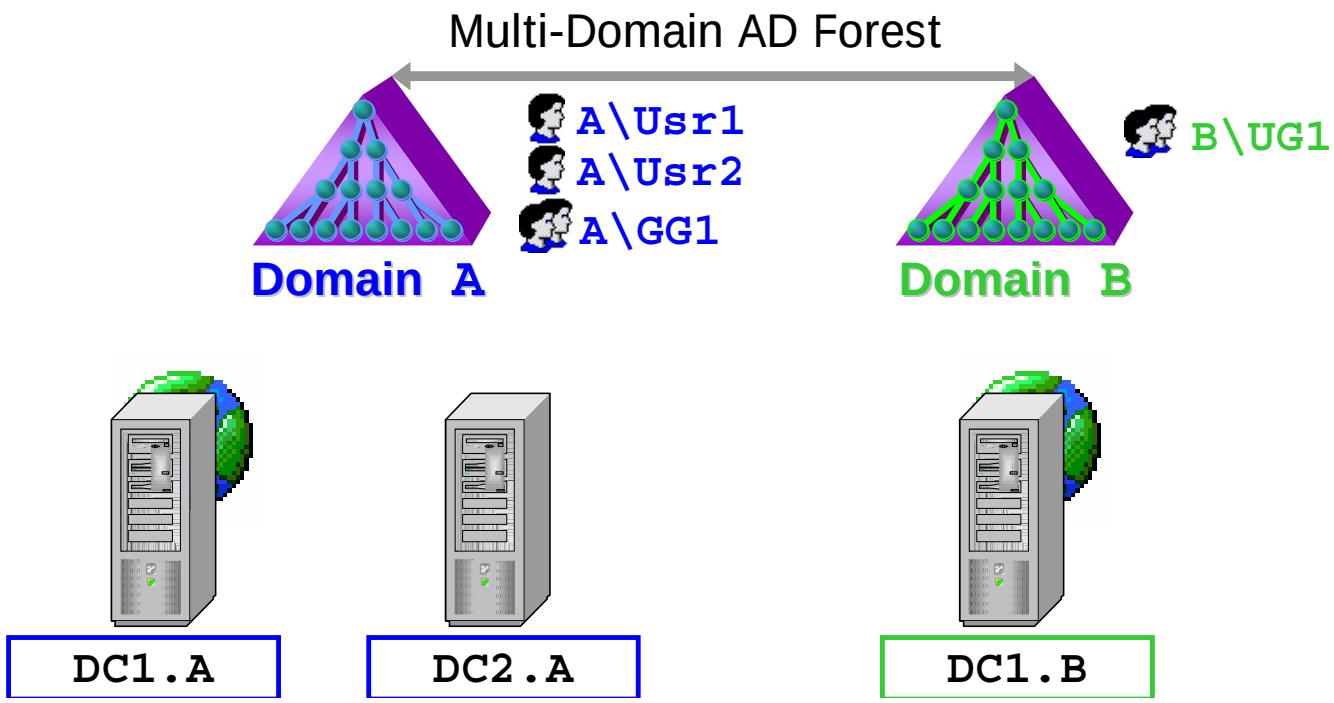


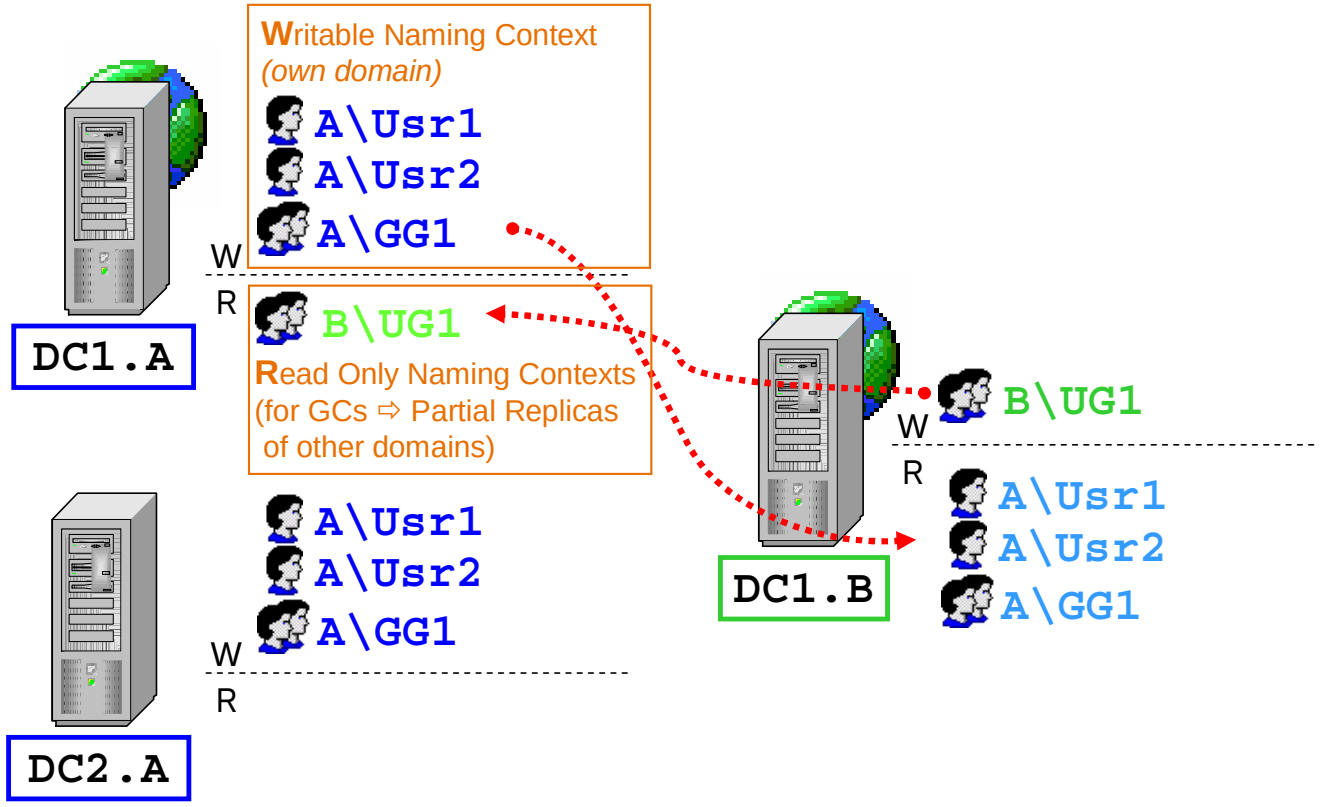

Attributes with Object-Links are determined by their **`linkID`**

- What is a Disaster?
- Authoritative Restore
- How Group-Memberships are stored
- Understanding Handling of Object-Links
- Recovering from a Disaster
- Changes in Windows Server 2003 with respect to Object-Link replication
- The HP Solution: ADRAT



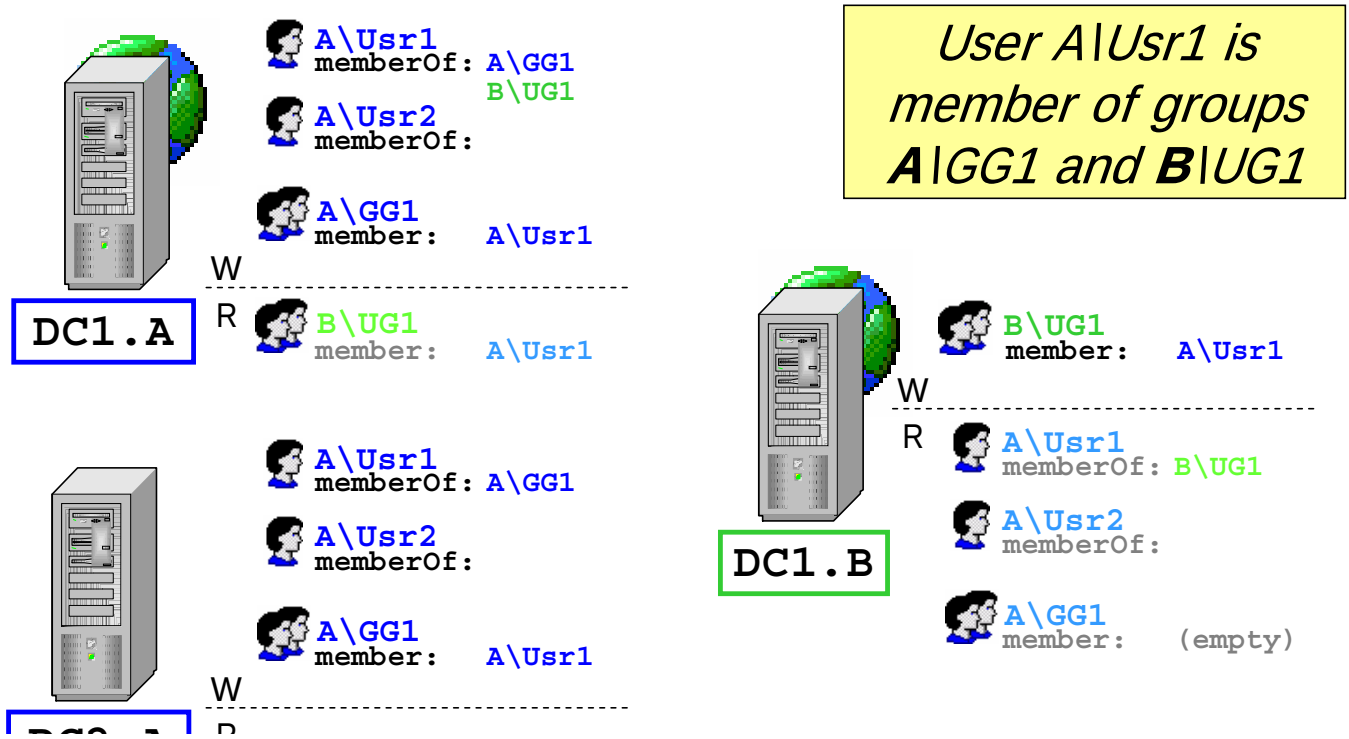
# Sample Setup (Domain View)

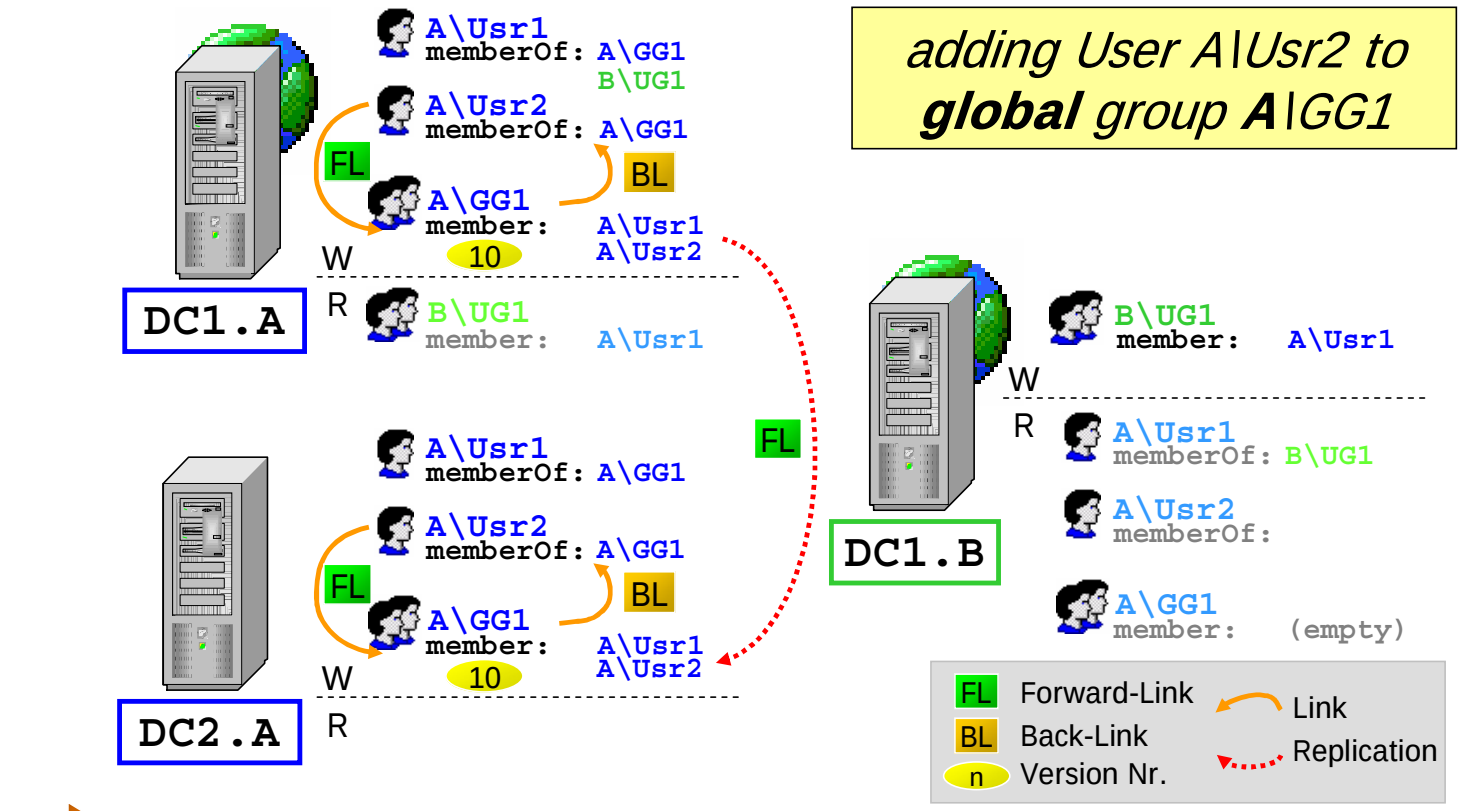







# Sample Setup (incl. attributes)

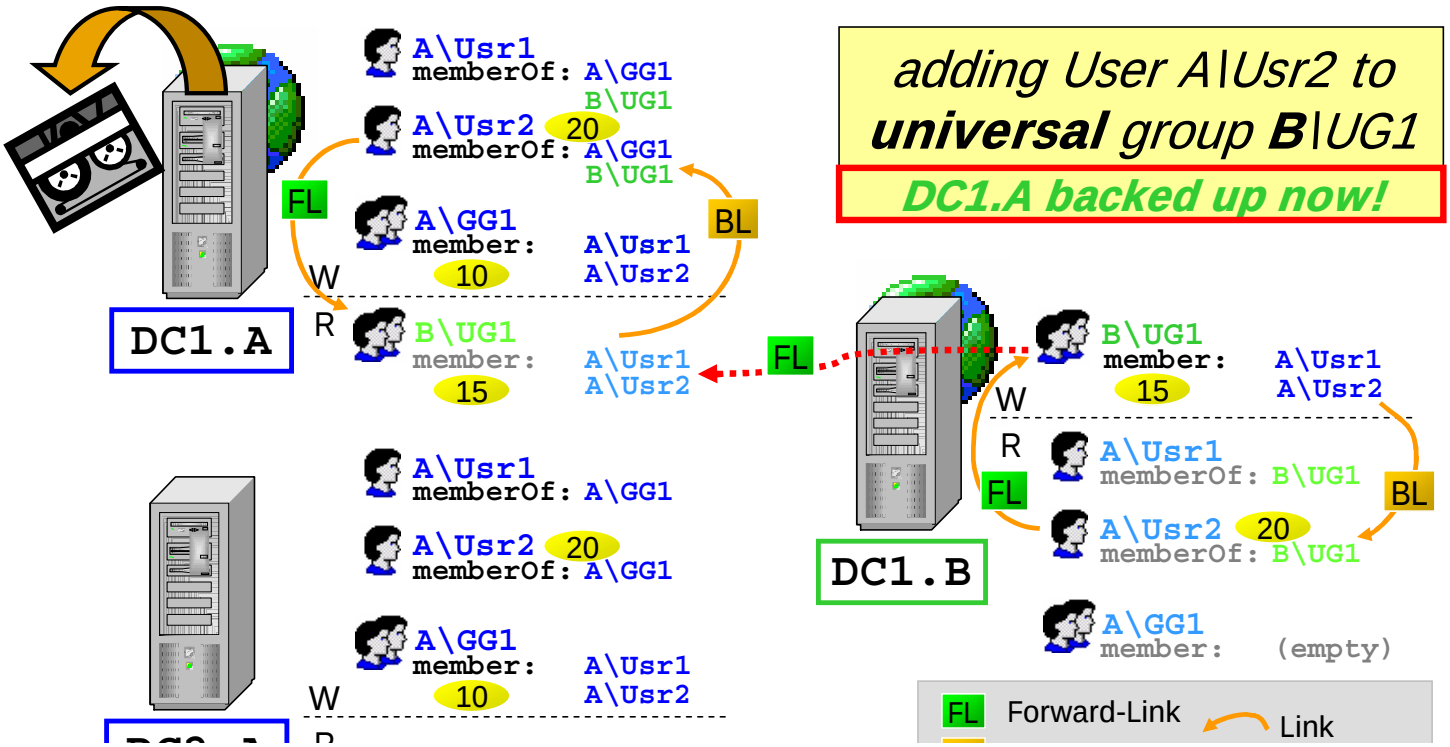


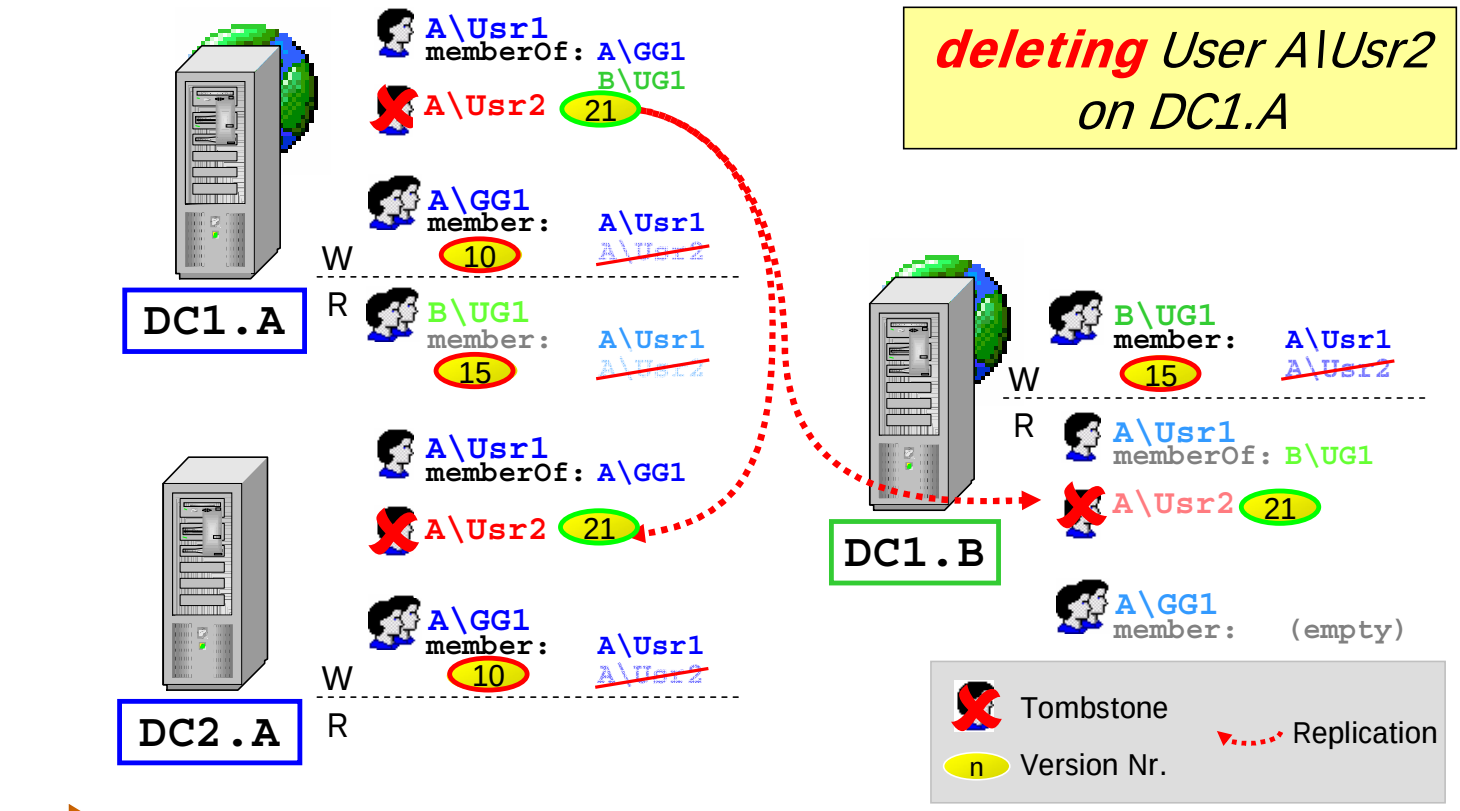



**Group updates ⇨ version-nr increases ⇨ replication takes place**



# Understanding Handling of Object-Links

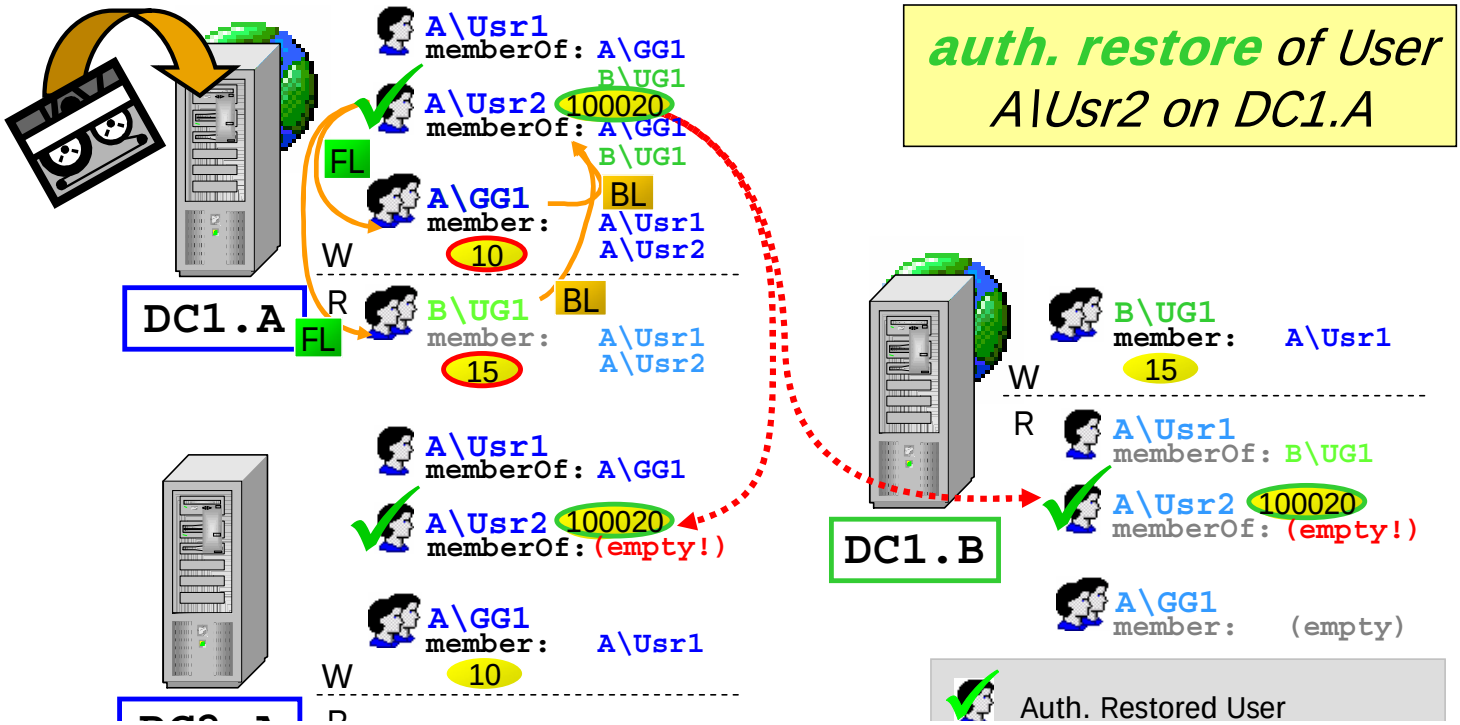





**Groups are „cleaned“, but version-nr. doesn't change...**



# Understanding Handling of Object-Links



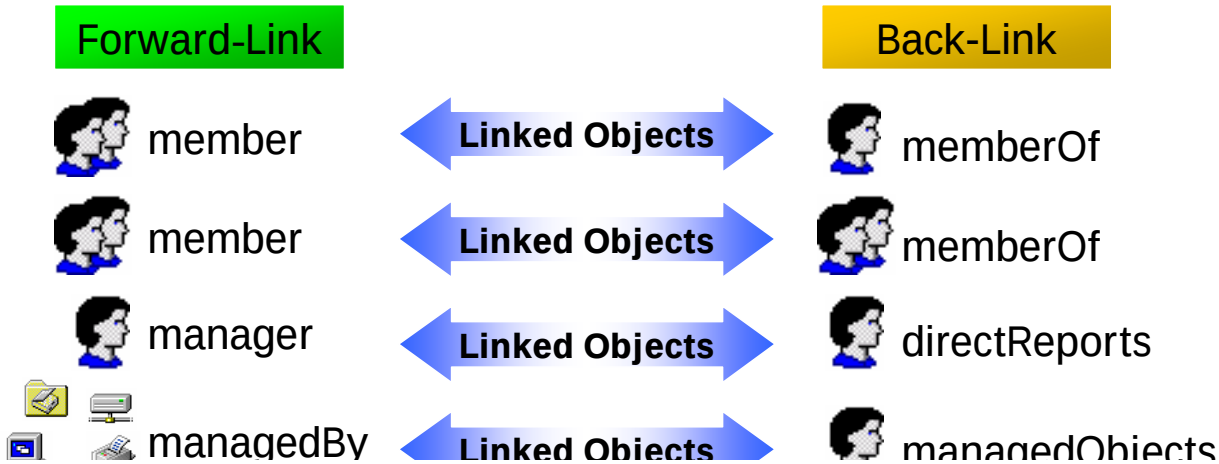
- What is a Disaster?
- Authoritative Restore
- How Group-Memberships are stored
- Understanding Handling of Object-Links
- Recovering from a Disaster
- Changes in Windows Server 2003 with respect to Object-Link replication
- The HP Solution: ADRAT



# Recovering from a Disaster

## What did we learn?

**If objects with Back-Links are deleted, their Forward-Links are cleaned up automatically. During an Authoritative Restore, the Forward-Links are NOT recovered automatically.**



## What do we have to do?

Part I

**Leverage the Back-Link information restored on DC/GC, to recover the Forward-Links! E.g. for recovery of users:**

1. Reboot DC1 to Directory Restore Mode
2. Restore AD database from backup to DC1 (should be a GC)
3. Perform Authoritative Restore of deleted objects via NTDSUTIL
4. Disable the NIC on DC1 (will **disable replication** of restored DC with other DCs in the AD forest – *not required for 2003 with Link Value Replication*)
5. Reboot DC1 to normal AD mode

***Always perform authoritative restores on a GC!***



# Recovering from a Disaster

Part II

6. Dump membership Back-Link information from object's **`memberOf`** attribute into reference-files
7. Re-activate replication on DC by enabling the NIC on DC1
8. Compare the Back-Links from DC1 to another DC of the same domain (DC2) via the reference-files
9. Leveraging the information in the reference-files, **re-add** objects to the correct groups on DC2, thus increasing the version number of the member-attribute and causing replication of the group
10. Perform the above also for UGs from other domains (will need **Enterprise Admin** privileges)

## *Another Challenge*

**Memberships of Domain Local Groups in foreign domains of the same AD forest are not stored on the DC/GC! As such, they are not contained in the Back-Links ...**

**Options:**

1. As part of your backup-plan, periodically "dump" members of Domain Local Groups from every domain in the AD forest to a separate store (e.g. reference-files). Leverage these files in case of a disaster recovery.
2. In the event of a disaster, perfom a restore of a DC/GC of every domain in the AD forest to analyse the memberships of the remote Domain Local Groups.

***Domain Local Groups need extra special care!***



# Preventing the Disaster

**The following are a couple of options to help prevent the big disaster:**

1. Get your Security in AD setup correctly! Do not delegate high level permissions to too many people.
2. Ensure, that you have recent backups of the System-State of at least one DC of every domain in the AD forest.
3. Take special precautions to manage the memberships of Domain Local Groups, as these are most difficult do recover.
4. Document your disaster recovery plans!
5. Check-out **Online** AD-Recovery Tools from 3rd-party vendors *(must read MS Q296257 !)*

- What is a Disaster?
- Authoritative Restore
- How Group-Memberships are stored
- Understanding Handling of Object-Links
- Recovering from a Disaster
- Changes in Windows Server 2003 with respect to Object-Link replication
- The HP Solution: ADRAT



# Changes in Windows Server 2003 with respect to Object-Link replication

Windows Server 2003 Active Directory introduces Linked Value Replication (LVR). This improves recovery of forward-links in the same domain:

- Upon restoring objects with Back-Links, the Forward-Links are **revived** and will be replicated to the other objects **within the domain** (own NC)
  - namely, the membership of a global or local group is automatically re-replicated to other DCs in the same domain, where it was previously "cleaned" due to the deletion of the user object

...but does **not** help for the recovery of forward-links in remote domains:

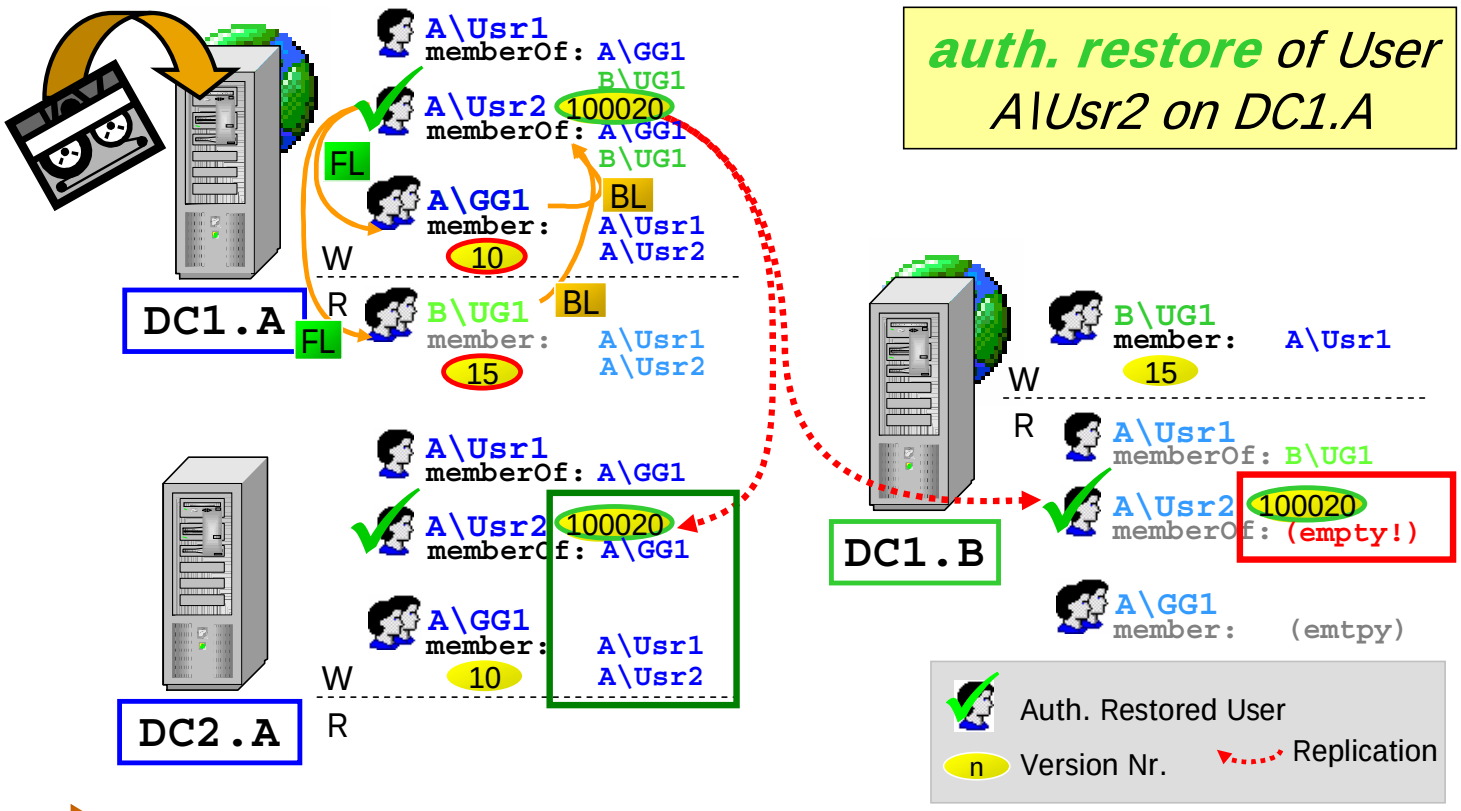
- Forward-links to objects in **other NCs** are **NOT** correctly recovered by an authoritative restore in Windows 2003 AD
  - even though the memberships in universal groups are also **revived** in the GC of a foreign domain, this GC will never replicate changes of the UG back to the originating domain, as it only has a "read only" copy of this NC.



## Changes in Windows Server 2003 with respect to Object-Link replication

Is the **Domain Local Group** issue fixed in Windows Server 2003?

- **No**, the problem with recovering lost memberships in DLGs remains exactly the same, as objects in remote domains will not contain any back-links to a foreign DLG ⇨ this means, that memberships in **DLGs will need the same special care as in Windows 2000**
- Have placed bug-report with MS – a tool to support the recovery may become available as a post-release to Windows 2003, but as the problem is an integral part of how replication works in the OS, it cannot be fixed with a

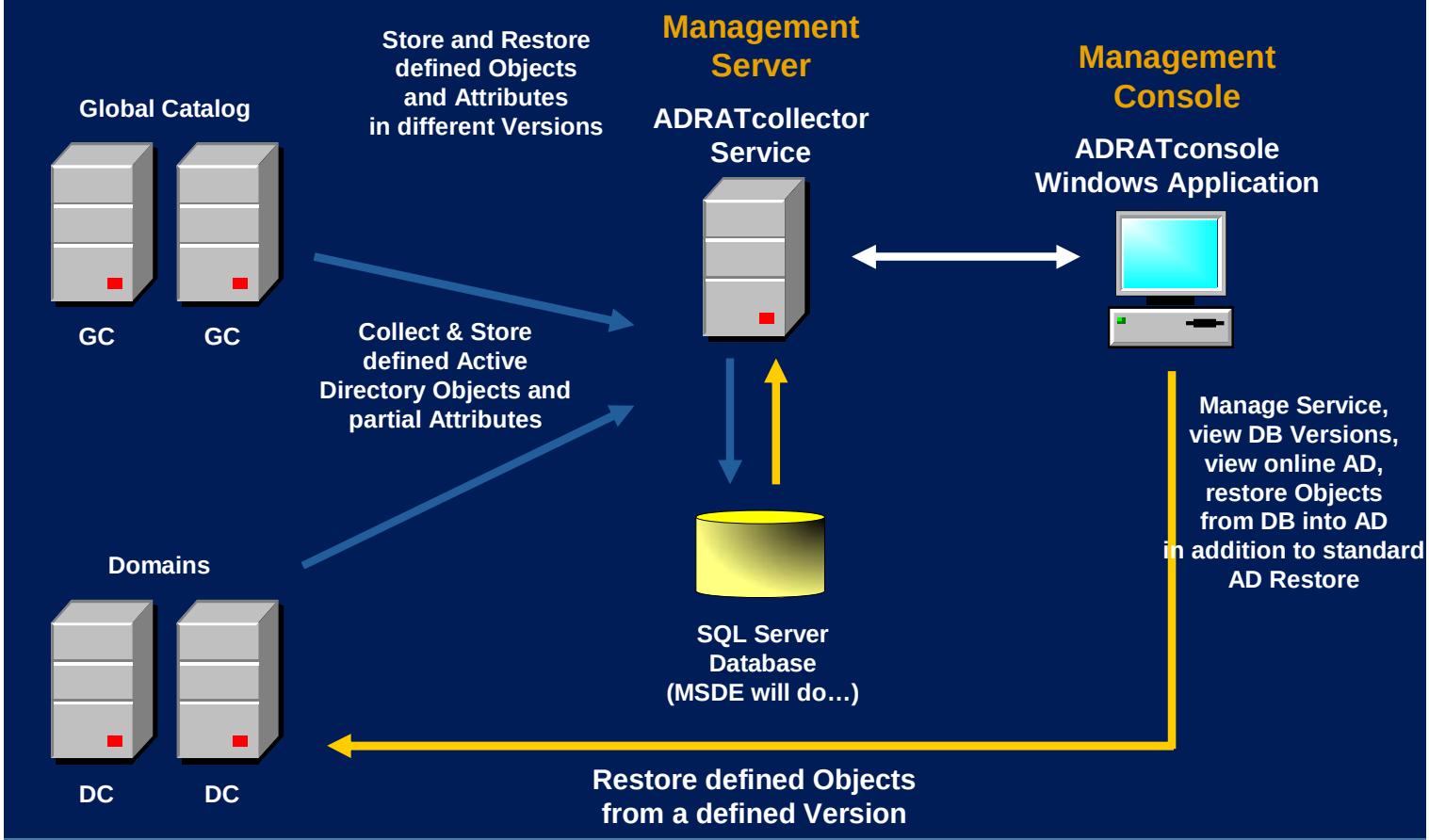



***User is restored, only membership in own domain is restored!***



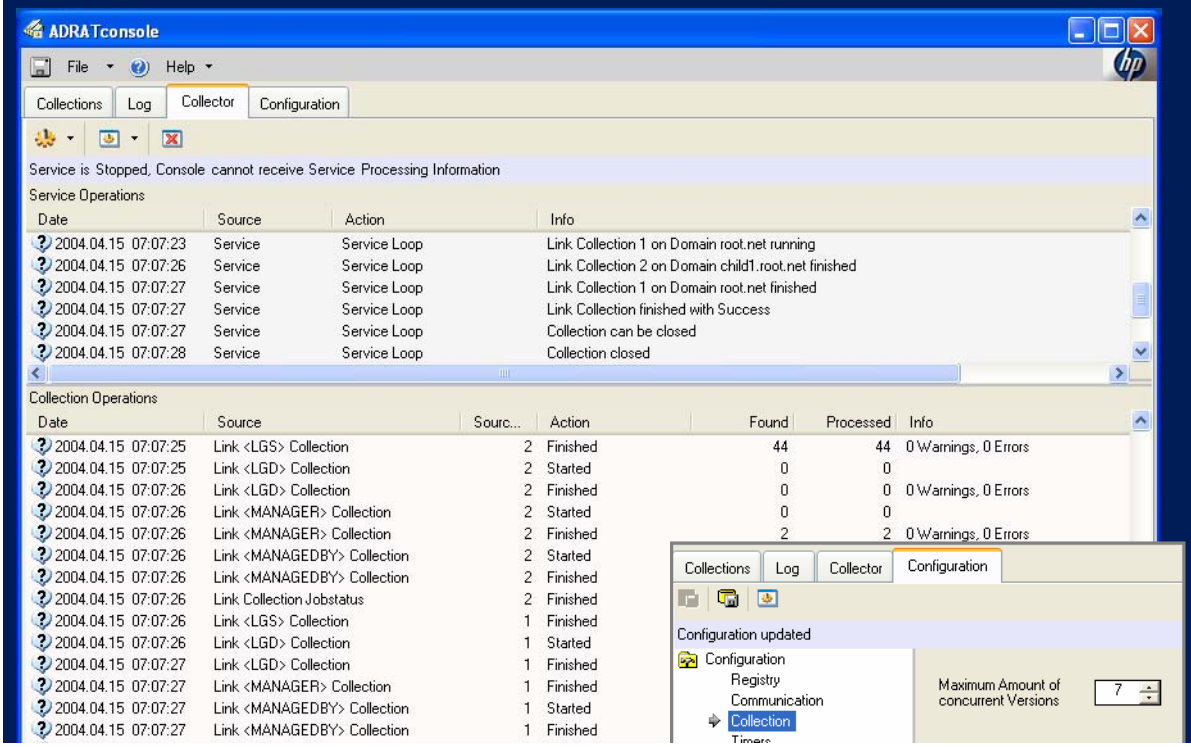
# Agenda

- What is a Disaster?
- Authoritative Restore
- How Group-Memberships are stored
- Understanding Handling of Object-Links
- Recovering from a Disaster
- Changes in Windows Server 2003 with respect to Object-Link replication
- The HP Solution: ADRAT

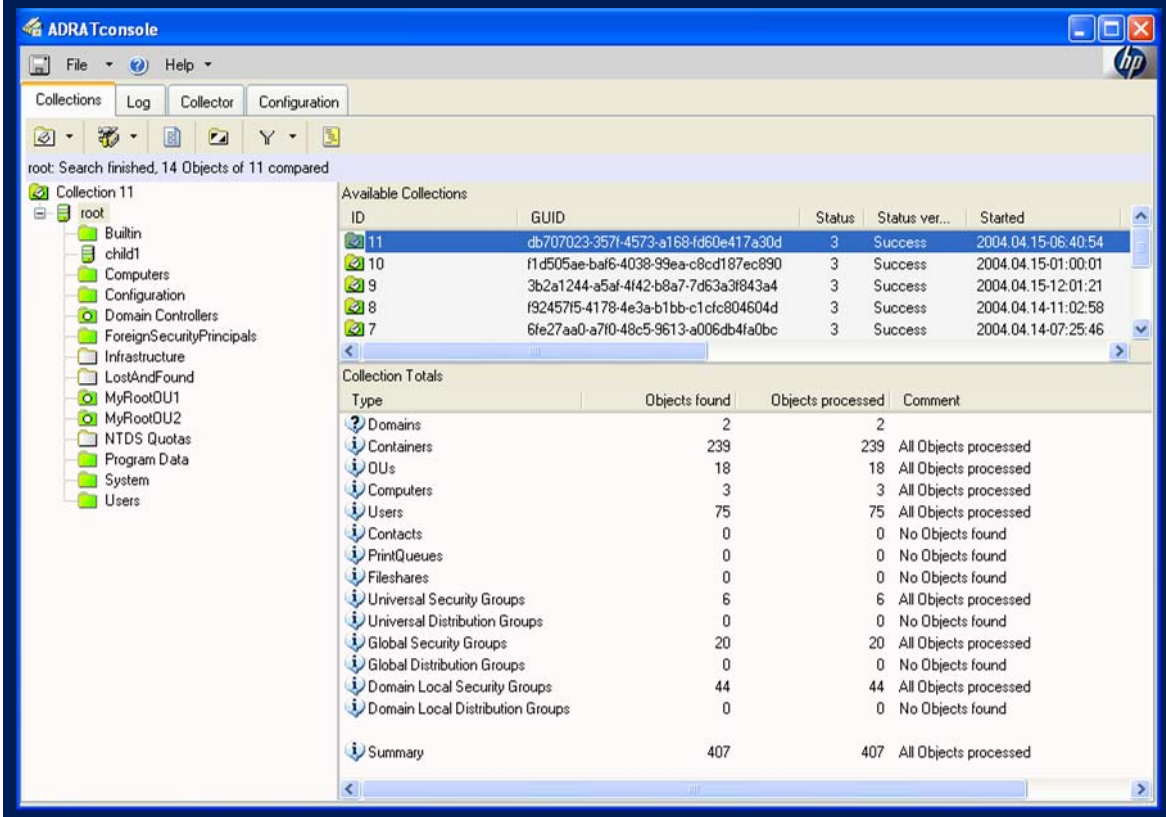





# HP AD Restore AddOn Tool (ADRAT)



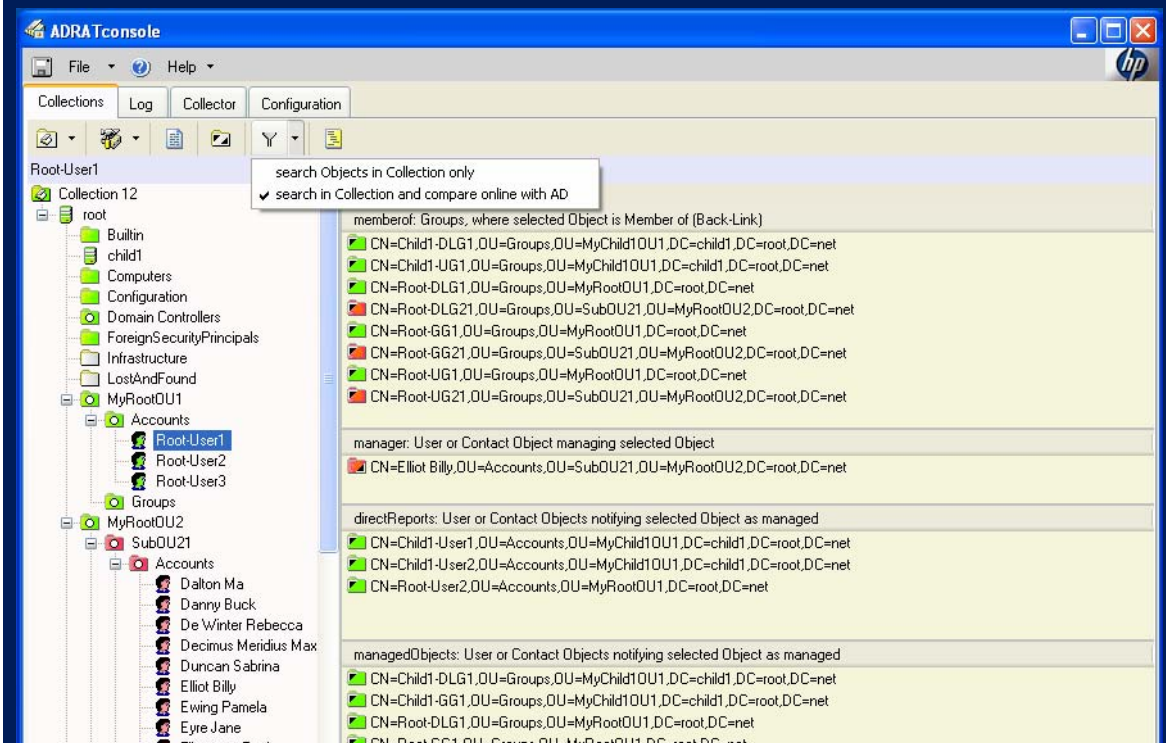

- **Collector** is implemented as a service and runs independently of the console
- processing data is **visible** in console
- writes link-information to SQL Database multi-threaded
- **Schedule**



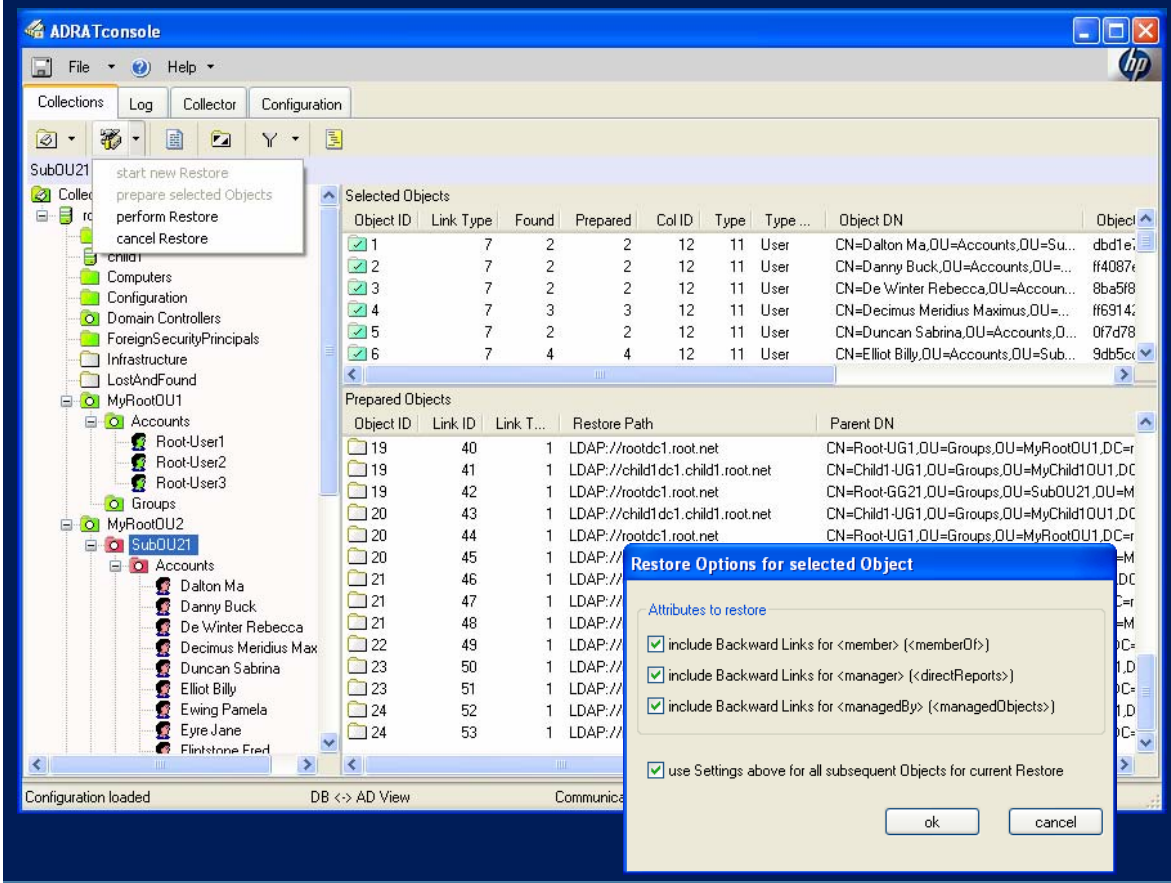

- easy to use Console Application
- reads data from SQL DB
- can handle multiple version of link-backups
- multi-console capable
- shows statistics of collected objects



# HP AD Restore AddOn Tool (ADRAT)




- will allow to browse DB and **compare** against AD (to **see** what's missing prior to performing a restore...)
- this will also aid admins to know which objects to authoritatively restore in AD




- **RESTORE** allows to select the objects for which to recover the **links** in AD
- can select single object or **whole OU**
- preparing restore shows the links that will be restored
- last step is to write links back to AD



# More information...

- **HP Active Answers - Whitepaper**
  - **Active Directory Disaster Recovery for Windows 2000** http://activeanswers.compaq.com/aa_downloads/6/100/225/1/42305.pdf
- **Microsoft Articles**
  - Q280079 Authoritative Restore of groups can result in inconsistent membership information across DCs
  - Q256588 Restore Active Directory over Terminal Services
  - **Windows 2000 Forest Recovery (Whitepaper)** http://www.microsoft.com/downloads/details.aspx?displaylang=e

guido.grillenmeier@hp.com