

Active Directory Disaster Recovery



Premier/Alliance Customer Workshop
Johan Ohlén



Introduction

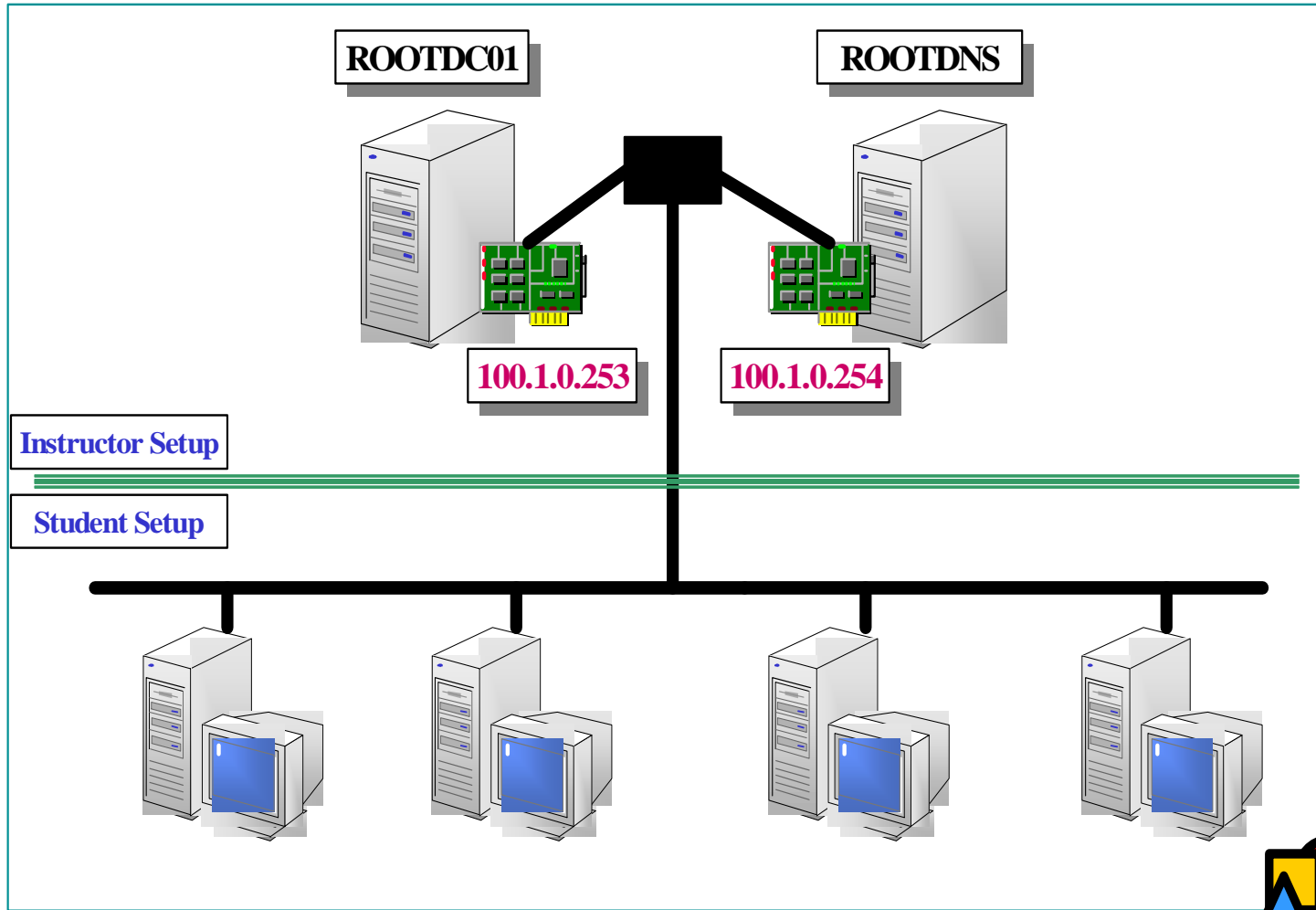
- Name
- Company
- Title/Function
- Job Responsibility
- AD Disaster Experience
- Expectations of this Workshop



Agenda

- Deploying a Backup Strategy
- Windows 2003 Backup and Restore Utility
- ERD(ASR) and Recovery Console
- AD Database Architecture
- Active Directory – Best practises Backup
- Active Directory – Type of Disaster
- Recovering Active Directory Scenarios
- Recovering Sysvol and Group Policies
- Typical PSS issues
- Forest Recovery

Room Layout





Resources

- Active Directory Product Operation Guide
 - <http://www.microsoft.com/downloads/details.aspx?FamilyId=84DFE61E-FB7B-4673-89B8-55BCC801B431&displaylang=en>
- Windows Server 2003 Active Directory Diagnostics, Troubleshooting, and Recovery
 - <http://www.microsoft.com/technet/community/events/windows2003srv/tnt1-80.mspix>
- Chapter 10 - Disaster Recovery for Branch Office Environments (AD Planning and Deployment Guides)
 - <http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/adguide/addeploy/addch10.mspix>



Developing a Strategy

- For each OS and application you introduce, you should answer the following questions:
 - What are the possible **failure scenarios**?
 - Plan for the Worst scenario:
 - HW, Power, Software failures. Deletion of objects and Files.
 - What is **critical data**?
 - **How often** should backup be performed?
 - How can we ensure that the backups are **useable**?
 - Assume failure and consequences
- A good documented plan ensures that you quickly recover your data if it's lost.



Developing a Strategy

- Guidelines for an effective strategy
 - Develop backup and restore strategies
 - Appropriate **resources** and **personnel**
 - Test your Backup's
 - Assign backup **responsibilities**
 - Back up **entire** volume (Disk Failures)
 - Keep **three** copies of the backup media
 - Keep one copy "offsite"
 - Perform trial restoration periodically
 - Verify that your files were properly backed up.
 - **Secure** storage of device and Backup media
 - Prevent an un-authorized restore to your server.



Deploying a Strategy

- New Enhanced AD, FRS and Sysvol Features
 - These features require the use of backup products that are aware of the new capabilities built into Windows 2000 and 2003.
 - Running third-party backup products designed for Windows NT 4.0 could cause loss of data.



Deploying a Strategy

- Who can perform backups and restores?
 - Backups: Domain Administrators, and Backup Operators
 - Restores: Domain Administrators
 - Custom Group:
 - **“Back up files and directories”** right assigned to a security principal



Deploying a Strategy

- Collect information before the disaster
 - Disk configuration
 - Computer name
 - IP addresses
 - Video mode settings
 - Domain information
 - Local Admin password



Backup and Restore Utility

- Ntbackup -New graphical utility
- Offers three wizards:
 - Backup
 - Restore
 - **Emergency Repair Disk – Automated System Recovery**
- Backup Media
 - Tape drive, a logical drive, a removable disk



Ntbackup What can I do

- Backup “System state” and Windows system files while DC is **online**
- Backup and Restore to hard disk or any other disk that the system can access
- Schedule regular back ups
- Create an Emergency Repair disk (ERD)



Backup and Restore tools

- NTBACKUP
- NTDSUTIL
- LDP
- ADSIEDIT
- REPADMIN , REPLMON
- EVENT VIEWER



Ntbackup Limitations

- Support only "**Normal**" backup of AD (Not incremental)
- You cannot back up AD by **itself** (Entire System state)
- "System State" cannot be backed up from **remote** PC.
- "System state" Restore can only be done when AD is **offline**
- Can "only" be restored to the **same** DC
- The Backup tool does not encrypt the unencrypted backup contents during the backup process.



The Age of your Backup

- It is not possible to restore a backup image into a replicated enterprise that is older than the tombstone lifetime value for the enterprise.
- The tombstone lifetime value represents the number of days that the deleted object (or tombstone) must be retained before it can be permanently removed from the directory

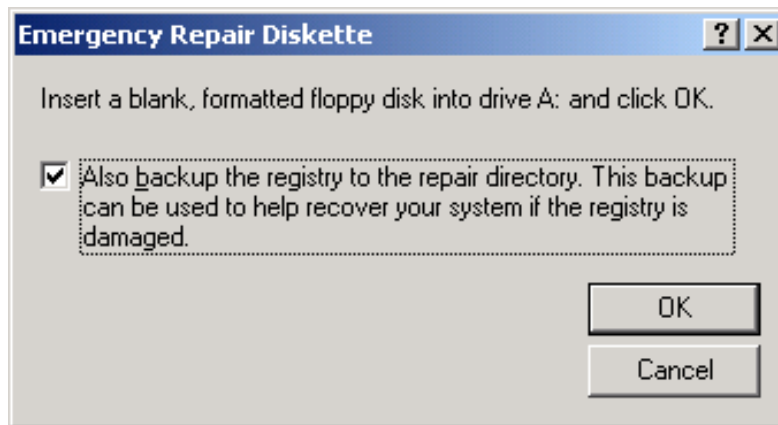


Backup Limitations

- Backup life = tombstonelifetime value
 - Default = 60 days old
 - Password Machine account change interval = 30 days
 - Password history = 2 maximum
 - **Backup useful life** = 60 days or 2 default password changes
 - Group Policy - Domain member: Maximum machine account password age 30 days
 - Group Policy - Domain member: Disable machine account password changes
 - Why?
 - Old backups can re-introduce tombstoned objects
- Schema Rollback
 - Not supported in W2K or W2K3

Creating an ERD or ASR

- Setup places backup registry files in %systemroot%\repair folder



Backup of the registry files are stored in %systemroot%\repair\regback



Using an ERD Q238359

- Two repair options in Windows 2000
 - **Manual** Repair: R= repair + M=manual
 - [] Inspect the startup environment
 - [] Verify Windows 2000 system files and replace missing or damaged files
 - [] Inspect and repair the boot sector
 - **Fast** Repair - Performs all repairs options
 - Uses files in winnt\repair to replace corrupted or missing files in winnt\system32\config
 - **ERD** contain: Autoexec.nt Config.nt Setup.log
- ASR - Automated System Recovery Q325375 W2K3
 - Safe mode, Recovery Console, and an Emergency Repair disk.



Recovery Console

- Allows administration of files on **NTFS** drives without completely loading OS
- Requires local Administrator **password**
- Can be run from the cd-rom or installed locally `Winnt32 /cmdcons`
- Q229716 Description of the Windows 2000 Recovery Console and commands



Active Directory Database

- Database Files includes:
 - Ntds.dit. The AD database
 - Edb.chk. The checkpoint file. recovery
 - Edbxxx.log. The transaction logs; circular logging only
 - Edb.log The current log file (10 MB)
 - Res1.log & Res2.log. Reserved logs. shutdown
- Located in %systemroot%\ntds by default

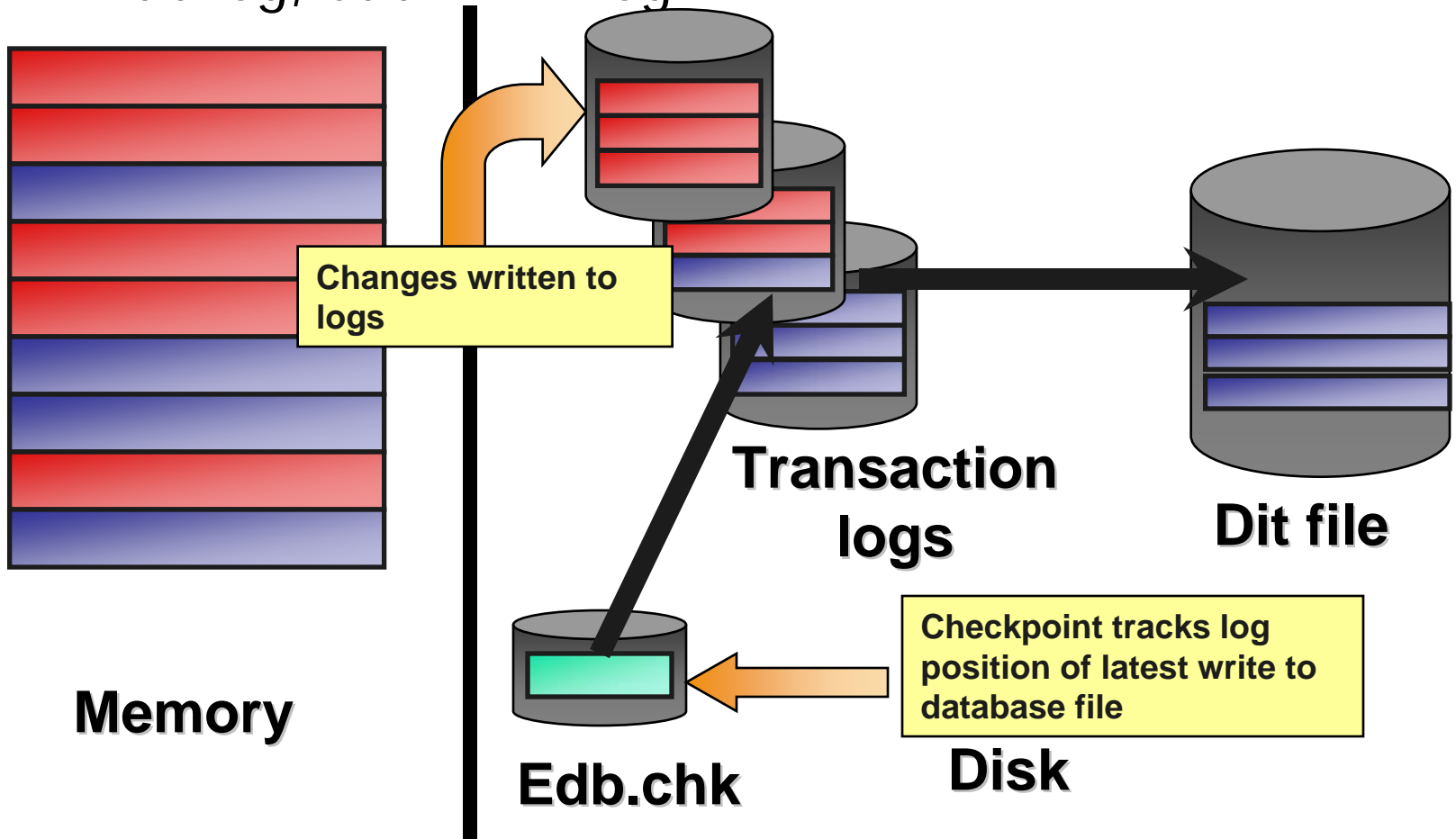


Circular Logging for AD

- Detailed info in Q247715 (LSASS.EXE)
- Database transaction written to EDB.LOG
- Shortly thereafter writes the transaction to Memory.
- When System has time or a system shutdown, transaction are written to NTDS.DIT
- When EDB.LOG is full, it rename and creates a new file EDB0001.LOG.
- Circular logging purges/removes the oldest file when the transaction have been committed to the Database
- EDB.CHK is a pointer to the last transaction within the log have been committed to the Database.

Active Directory Database

Edb.log, edbnnnnn.log





Active Directory Backup

- **System State Backup**

- System Startup Files – System files to boot
- System registry
- Class registration database of COM+
- Sysvol
- Active Directory database files
- Active Directory-integrated DNS
- Certificate Services database (if installed)
- Cluster Service (if installed)



Active Directory Backup

- What is a good backup?
 - Content
 - At least System State and system disk
 - Age
 - Never older than **tombstone** age.
 - Recommendation: Minimum two backups or more within tombstone lifetime.
 - You cannot use a backup of one DC to restore another DC
- Only type of backup supported by AD is *normal backup*.



BACKUP STRATEGY

- What to backup (minimum)
 - Backup all Operation masters role holders in your Forest. At least 1 GC in each Domain.
 - All DC's in your **root domain** (critical)
 - All DC's also working as **application** servers
 - At least 2 backups within the **tomstone** life
- Recommended
 - All DC's in your Forest
 - Quick recovery in the event of Active Directory failure or a domain controller hardware failure
 - Every week (Trust Relationship password)



Tombstoning 60 days

- **Deleting an object from AD**
 - 1. Object gets converted into a tombstone state "IsDeleted property" (not fully removed)
 - 2. Inform all other DC's for deletion
 - 3. Object is deleted when tombstone lifetime is reached. (Garbage Collection Process)
 - Tombstone lifetime [Article Q216993](#)
- After they are deleted by the garbage collection process, they no longer exist in the directory database



Garbage Collection

- Process running on every DC at regular intervals every 12 hours.
 - Deletes Tombstone objects.
 - Delete any unnecessary Log files.
 - Defrag the Database file.
- ADSI Edit is used to change the interval of Tombstone Lifetime and Garbage Collection Interval.



More Garbage Collection

- Windows 2000:
 - Each pass removes 5000 objects every 12 hours.
 - Removes max 10,000 objects a **day**.
- Windows Server 2003
 - Default still runs every 12 hours.
 - Each pass removes 5000 objects
- Difference in 2003: Garbage collection will reschedule itself to run immediately until all of the objects are removed



Restore of AD if older than the tombstone lifetime setting

- Recovery Options:
 - Reinstall the server after confirming there is at least one surviving domain controller.
 - If **every server** in the domain is destroyed, restore one server from an arbitrarily outdated backup, and replicate all other servers from the restored one.



Deleted Objects in AD on a DC

- Deleted "Objects container"
 - Use LDP.exe , Search dc=msft,dc=com
 - Filter = (isdeleted=*)
 - Scope options = Subtree
 - Search Call Type = Extended
 - Object Identifier = 1.2.840.113556.1.4.417
 - Control Type = Server
- Q258310



Reanimation of Tombstones

- Recover Deleted Objects – Described in **Q840001**
 - Limited attributes preserved - SID, Object GUID and last know parent
 - Best Suited for small scale recoveries
 - Backup and authoritative restore preferred for most scenarios
- Process
 - Search for Deleted Objects
 - Replace IsDeleted attribute and RDN
 - Manually recreate group memberships and other attributes
- Required Permissions
 - Reanimate Tombstones ACE on root of domain

Restoring Deleted Objects in W2K3



- An object can still **not** be restored when the tombstone lifetime for the object has expired
- Code example that shows how to restore a deleted object in W2K3 at MSDN:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/restoring_deleted_objects.aspBoth SID and GUID are retained
- Some **system attributes** get stripped, and there's no way of putting them back into the reanimated object

Reanimation

Modify [X]

Dn: CN=Sammich2\0ADEL:edd9d218-17bc-4e9a-

Edit Entry

Atttribute: distinguishedName

Values: CN=sam,CN=Users,DC=rc2,DC=local

Operation

Add Delete Replace

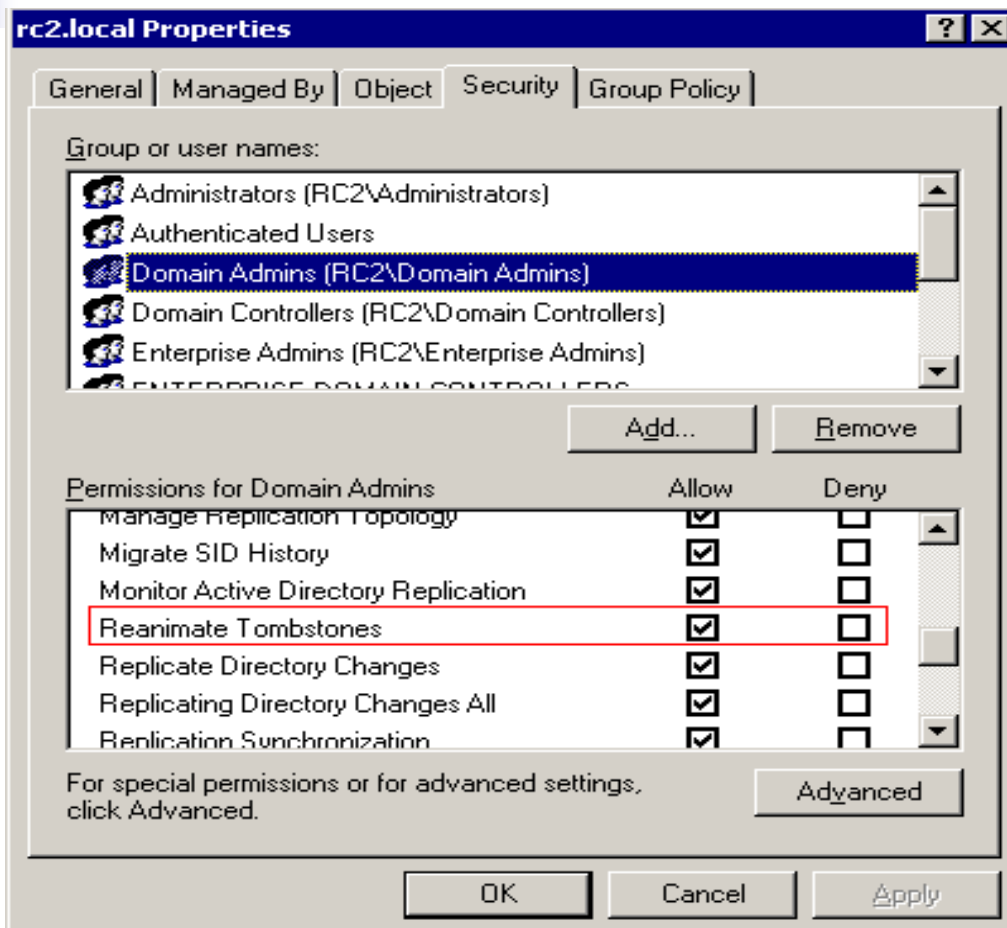
Enter List

[Delete]isDeleted:
[Replace]distinguishedName: CN=sam,CN=Users,DC=rc

Synchronous

Extended

Reanimation



Best Practices for a Good Backup



- To ensure a successful restore of Active Directory from a “Good” backup
 - **Contents**
 - **Age**
- For full disaster recovery, back up all of the drives and the System State data.
- **“Traveling” DC’s** – Offline max Tombstone age or (2x computer password change)
 - Q314282 – W2k-SP3 or later support adds support for removing **lingering objects**
 - Use LDP to search for duplicate user, group, or distribution list. (**Standard** = Loose Replication Consistency)
 - **“Strict Replication Consistency”** was created to prevent unwanted replication of lingering objects (not implemented when upgrading from W2K to W2K3)



Lingering Objects

- One or more objects never considered for replication
 - HighestCommitted USN lower than DCs Highwater mark
- Problems with Lingering Objects
 - Difficult to remove from Global Catalogs
 - Causes Name conflict
 - Halt Replication

Lingering Objects- Strict replication consistency

Event 1864, 2042, 1988

- 1. Demote or reinstall the machine(s) that were disconnected, or.....
- 2. Use the "repadmin /removelingerobjects" tool to remove inconsistent deleted objects
- 3. Resume replication. You can continue replication by using the following registry key:
 - HKLM\System\CurrentControlSet\Services\NTDS\Parameters\ "Allow Replication With Divergent and Corrupt Partner" to 1
- Once the systems replicate once, it is recommended that you remove the key to reinstate the protection.



Type of Disaster

- Database Corruption – Reinstall situations
 - **Disks** become corrupted –writeback cache is not saved to a power failure
 - **Hardware** failure – Replace DC or HW
 - **Software** failure - Prevents system boot
- Data Corruption – Restore from Backup
 - **Accidental** deletion of objects or files and has been replicated to other DC's
 - Corruption of Active Directory data, which has replicated to other domain controllers
- Fast Growing Database – DSASTAT –S
- Compare different DC's - DSASTAT -S



Type of Disaster

- Data Corruption – **Repair**
 - **Esentutl.exe** repair of database is a last resort
 - Use **integrity** check to see if database is damaged
 - High **Risk** this process will result in further loss of data
- Do **Not** spend time to Repair the Database on a single DC, if other DC's are working fine!!



AD Disaster Recovery

Objectives:

- To resolve problems on domain controllers that affect clients, the domain or forest operation in:
 - **Least amount of time**
 - **Least amount of pain**
 - **Best possible results**
- First determine what kind of disaster you have.

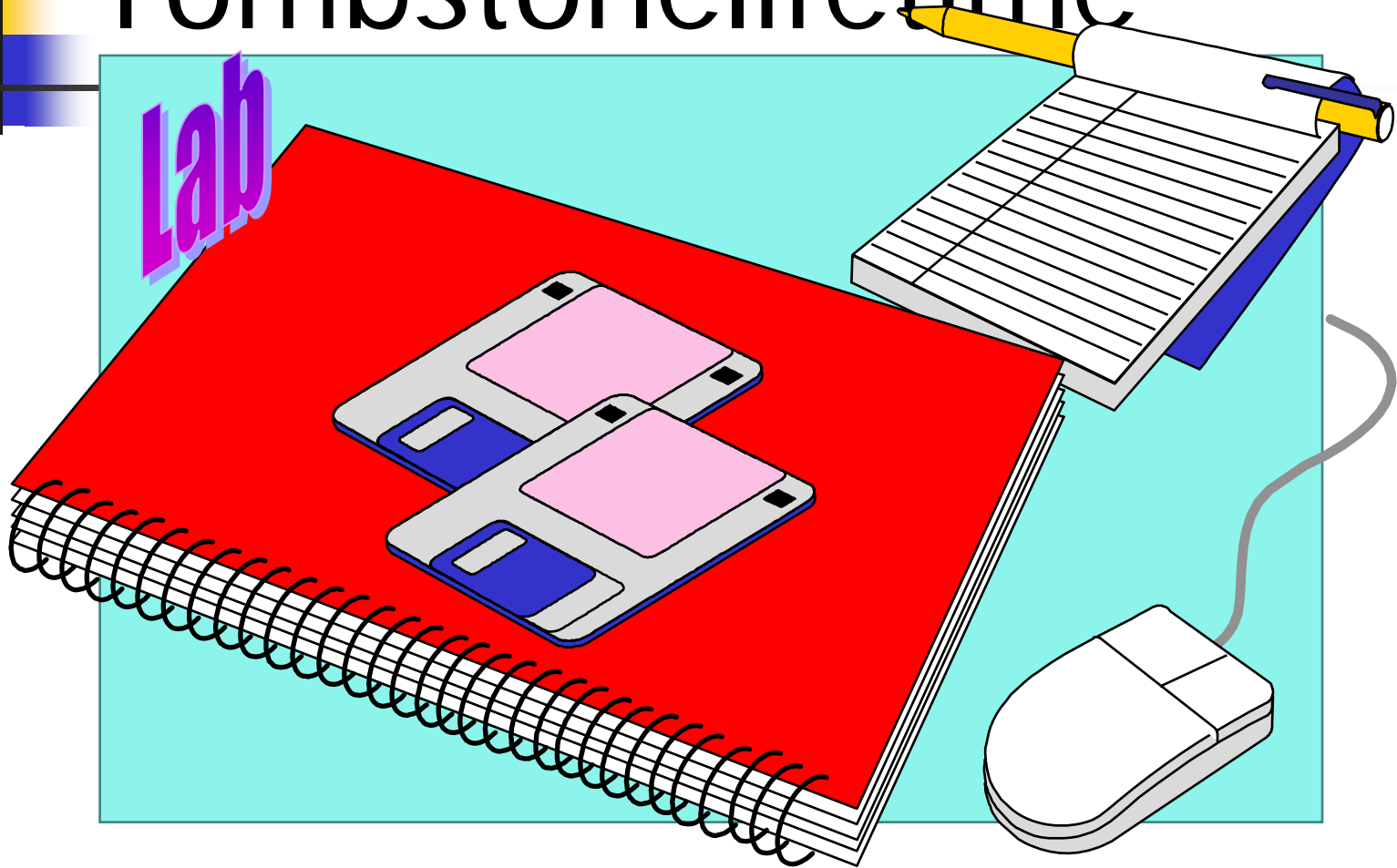


Reality

- Administrators often NOT do:
 - **Backup** – Typical PSS case
 - Test backups prior to disaster – Is my backup **ok**?
 - Test your **recovery** plan
 - Create **labs mirroring** production environment
 - Monitor failure symptoms and events – JET errors
- Administrator with **ONLY** few problems
 - Follow the steps above

Tombstonelifetime

Lab





Preferred Recovery Options

- **Reinstallation:**

- Winnt32 + DCPROMO + Re-replicate
- Winnt32 + DCPROMO → IFM (Install from media)
- ForcedRemoval + Metadata Cleanup + DCPROMO + Re-
replicate
- ForcedRemoval + Metadata Cleanup + DCPROMO → IFM

- **Restore**

- NTBACKUP restore to last known good state
- Re-Replicate changes made from other DC's

- **Repair**

- Not an recovery option for AD
- Use Integrity Check to see if database is corrupt
- Removed from Windows 2003



Core Recovery Tools

- NTBACKUP
 - Snap shots of system as state changes made
- NTDSUTIL & ESENTUTIL
 - Database validation
 - Metadata cleanup for DC / Domain removal
 - Esentutl – Database Validation and Repair
- WINNT32 & DCPROMO + (IFM)
 - Rebuild a DC faster and gives better results



Dcpromo from Media

- Benefits

- Reduced network utilization when additional DC's are promoted into an existing domain
- Faster sourcing of Active Directory and Global Catalog data to the new domain controller
- Improved recovery of domain controllers in the event of failure !!!!!!!!!!!!!!!!!!!!!!!!!!!!!



Dcpromo from Media

- When can you use it
 - Can only be used on W2k3 servers
 - Can only be used for additional Domain Controllers in the same domain.
 - Cannot be used for the first DC in a domain.



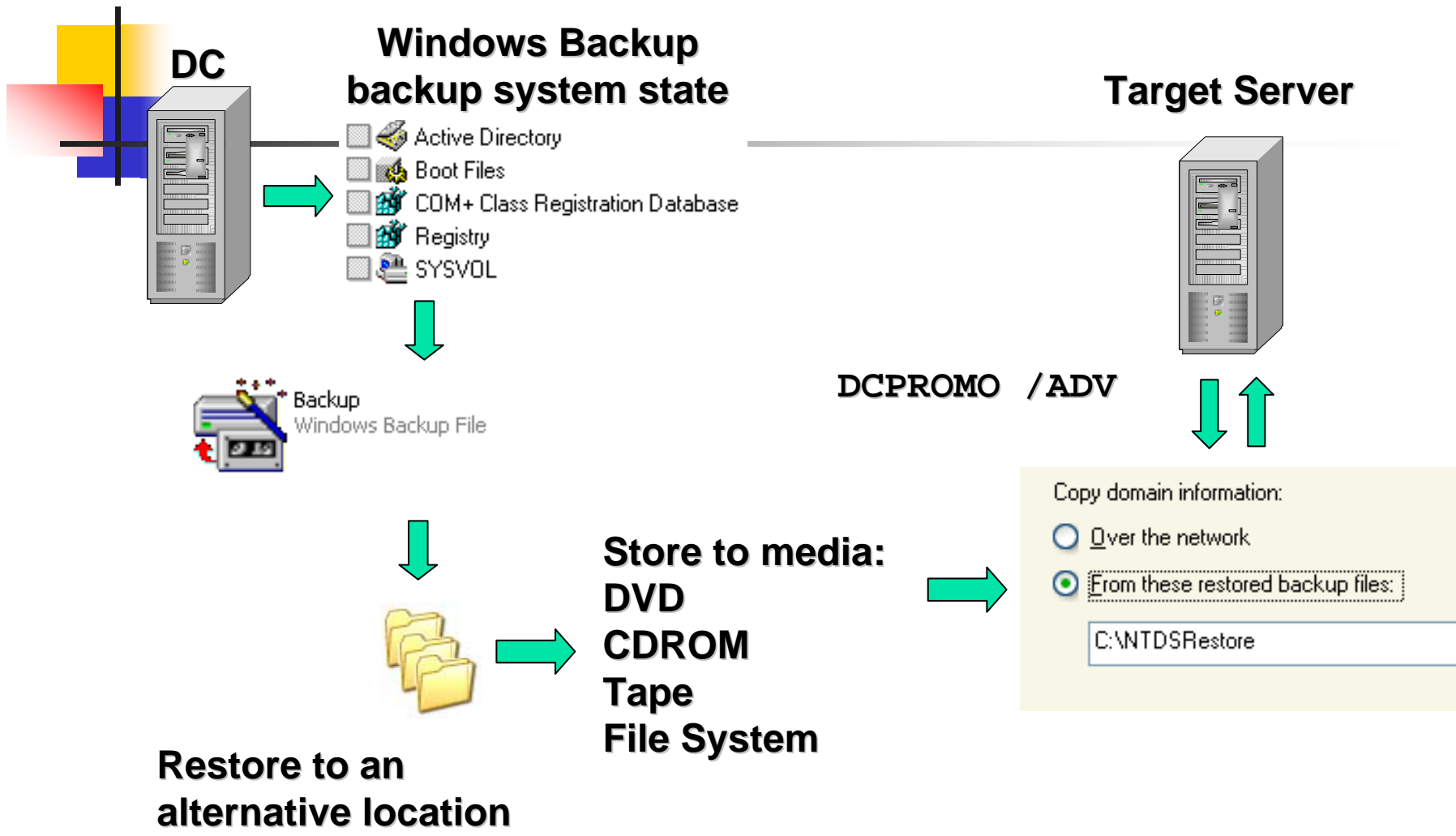
Dcpromo from Media

- When can you use it.
 - The system state backup must be no more than 60 days old. (results in reintroduction of tombstoned objects)
 - The system state backup must be taken from a Windows 2003 DC in the same domain. (GC can also be included)
 - The server you want to promote from media must be on the network and must be able to communicate with other healthy DCs.



Using "Install from Media"

- IFM promotions consist of 3 steps:
 - Performing a system state backup from a Windows Server 2003 DC to a Media(DVD)
 - Restoring the System State Backup .bkf to an "Alternate Location" on target machine
 - IFM Promotion of a Replica domain controller with DCPROMO /ADV
- <http://support.microsoft.com/?id=311078>



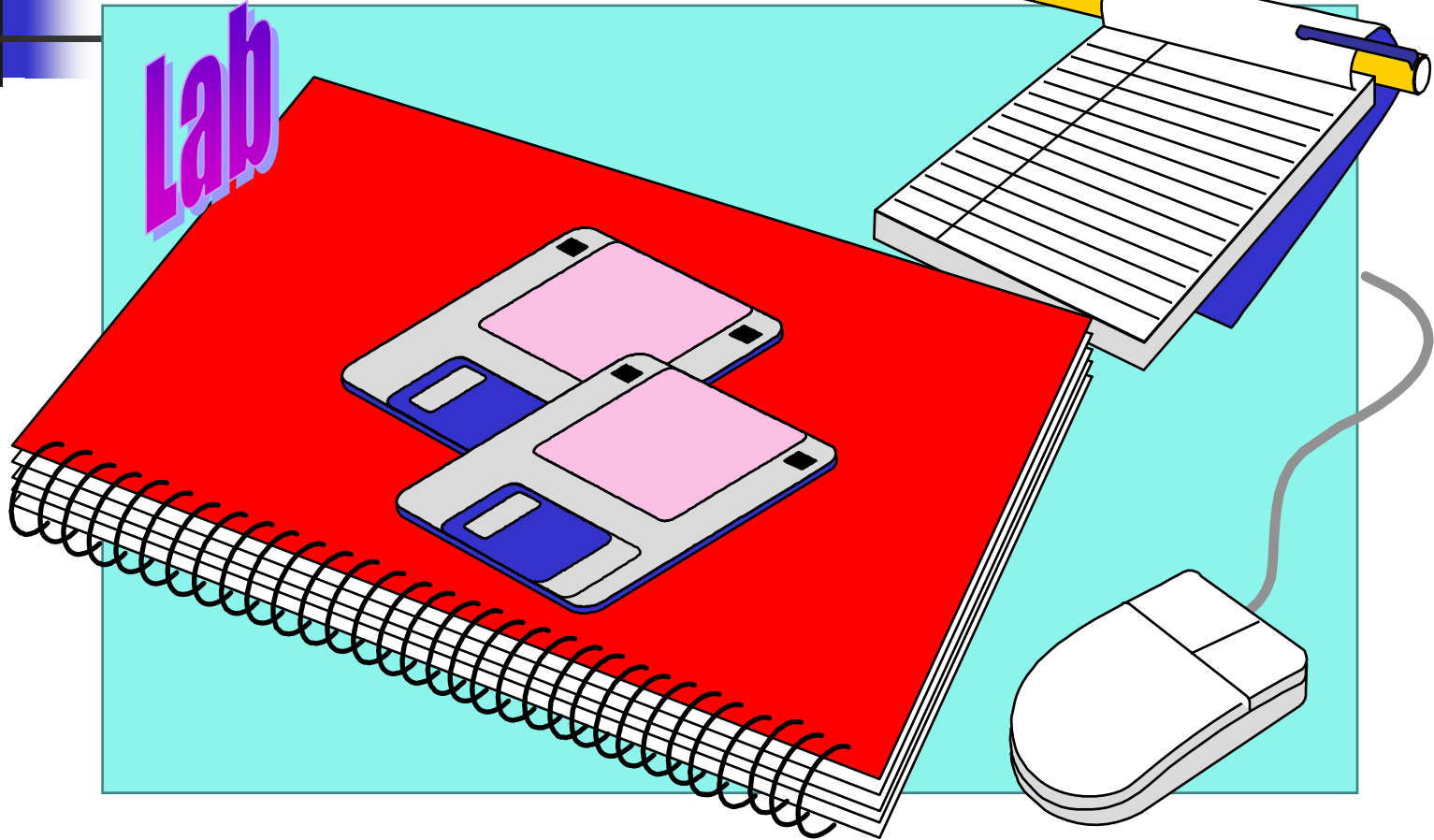


Create Replica From Media in Windows Server 2003

- Source initial replication while promoting DC from backed up files instead of the network
 - Backup DS using regular backup s/w
 - Restore/copy files to candidate DC
 - DCPROMO: source replication from restored files
 - Also works for GCs
- Network connectivity still required
- Not a general replication mechanism

INSTALL FROM MEDIA

Lab





NTDSUTIL

- Metadata cleanup
 - Remove orphaned dc's or child domains
- Integrity Check + Repair
 - Wrapper around ESENTUTL
 - Tells you if database is good or bad – Jet Error 1018. Power failure, Faulty Hardware
- Authoritative Restore
 - Mark selected objects on DC as authoritative



More NTDSUTIL

- Move the Database, Log files to another Disk.
- Offline Defragmentation.
 - To release space back to the file system.
 - Must be done on Per DC.



Remote Administration

- Q256588 - Administrating remote servers in DS restore mode
 - Create a new entry in the Boot.ini file with
`/SAFEBOOT:DSREPAIR /SOS`
 - Set the appropriate boot option in the arch path and reboot the system
 - `multi(0)disk(0)rdisk(0)partition(2)\WINNT="W2K DC \\your server name" /fastdetect`
`multi(0)disk(0)rdisk(0)partition(2)\WINNT="W2K DC \\your server name" /fastdetect /SAFEBOOT:DSREPAIR /SOS`



How to restore AD [Winnt32]

- **Reinstall** Windows 2000
 - Winnt32+SP3+IP-config + DCPRMO
 - Normal replication process from a healthy DC in the same domain
 - Not used to restore AD to a known state
 - Computer/Server object needs to be cleaned out of AD
 - Bandwidth considerations – Slow links

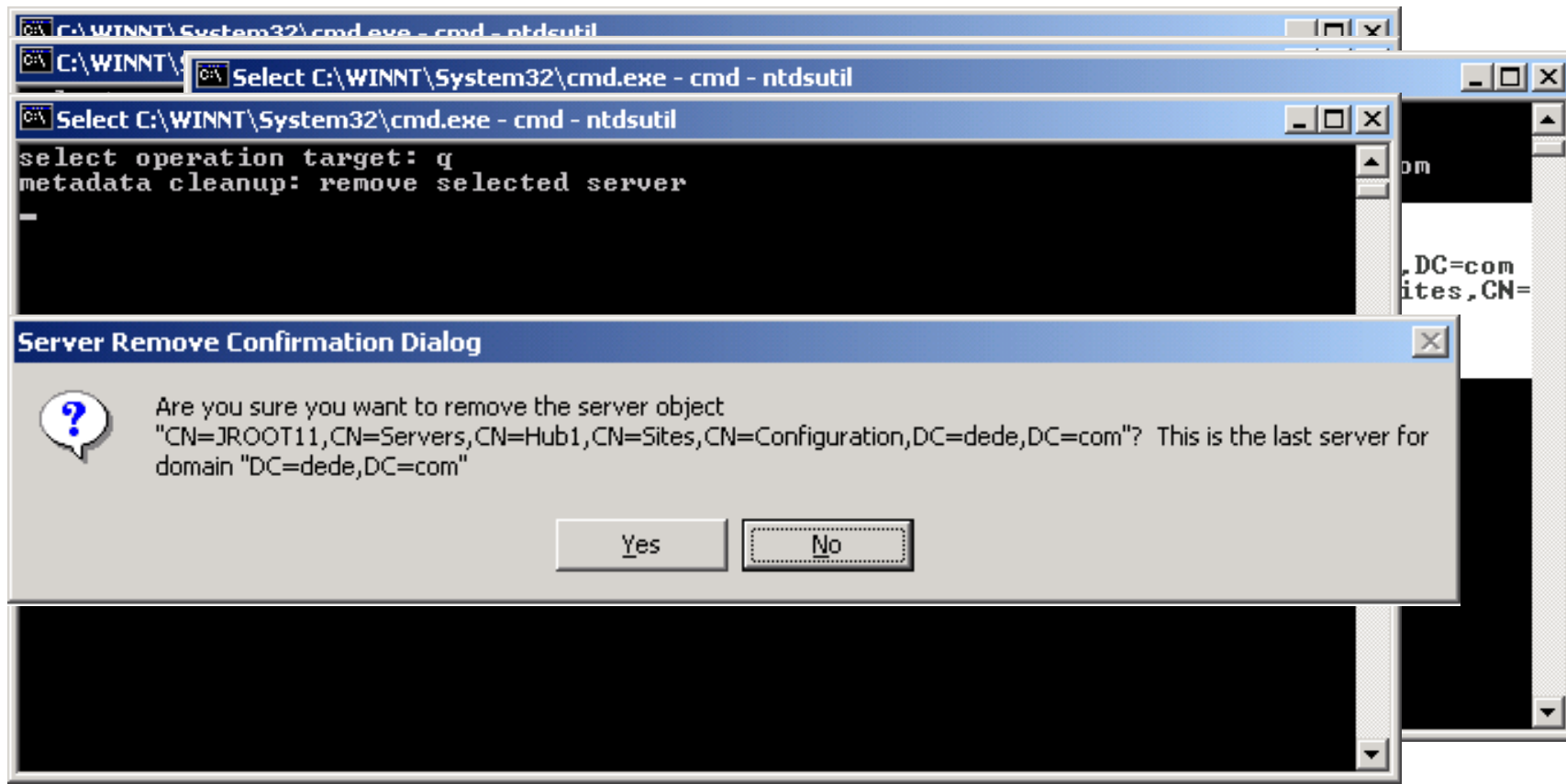


Re-installation

- Steps involved: In correct order
 1. Cleanup operation, such as removing the failed DC object from Active Directory.
 2. Installing a fresh copy of Windows 2000 Server.
 3. Running DCpromo.exe to promote this machine to the domain controller role.

NTDSUTIL

- Re-installing using the same DC name
 - Remove the failed domain controller from AD





Cleanup cont. Q216498

- Remove the cname record in the *_msdcs.root domain of forest* zone in DNS.
- If this was a DNS server, remove the reference to this DC under the **Name Servers** tab
- Delete the computer account. [Adsiedit]
 - CN=*domain controller*, OU=Domain Controllers, DC=*Your Domain Name*, DC=COM, PRI, LOCAL, NET.
- Delete the FRS member object.
 - CN=Domain System Volume (SYSVOL share), CN=File Replication Service CN=System, DC=*Your Domain*, DC=COM, PRI, LOCAL, NET
- If it was the last domain controller in a child domain and the child domain was also deleted:
 - Delete the trustDomain object for the child:
 - **Trust Domain object**, CN=System, DC=*Your Domain*, DC=COM, PRI, LOCAL, NET
- Use "Active Directory Sites and Services" to remove the Domain controller

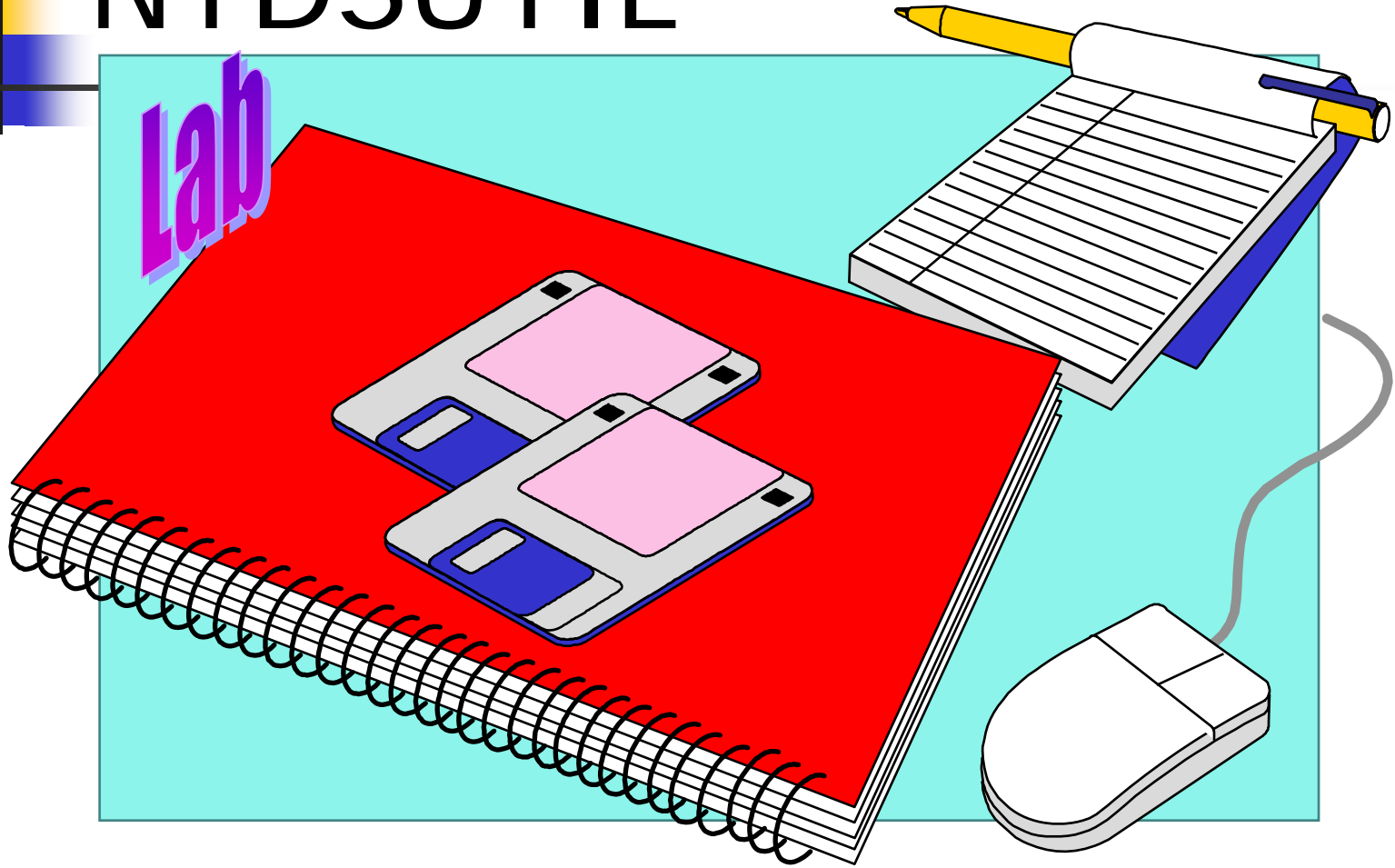


Re-installation consideration

- Allow time for the deletion of Server object to replicate throughout the forest
- Check the DCPROMO.log to verify the promotion completed successfully
- Use “Repadmin /showreps” or Replmon to verify that connection objects have been re-established
- **Disadvantage:** Other Applications needs to be reinstalled/configured

NTDSUTIL

Lab





Non-authoritative

- What is it?
 - Restore to known good point using NTBACKUP – (Maintain the version number from the backup)
 - Reboot into AD mode to apply all updates after backup
- When to use:
 - Local server problems
 - Data or application loss from reinstall too expensive
- SYSVOL
 - Will automatically be updated by a replication partner
- It is NOT possible to use the non-authoritative restore process to reinstate deleted objects from an older backup



Non-authoritative restore

- Reboot into DS Restore mode
- Restore system state and/or system disk
- Choose "Advanced restore mode" options
- Restart DC in "Normal" mode
 - AD will replicate new information
 - Non-Authoritative restore of SYSVOL
- When you restore the System State data, the location of the system root must be the same as the location when you backed up the System State data.



LAB: Non-authoritative restore

- Use NTBACKUP to backup the system state on DC2
- Unplug the network cable on DC2 (simulate a Network failure)
- Create a new OU object + a user on DC2
- Restart DC2 in DS restore mode (simulate a catastrophic event on DC2)
- Perform a **non** authoritative restore of the backup you created
- Plug in the network cable and restart the server in normal mode
- Question: What happen with your new objects created in step 3 ????



LAB RESULTS

- What did happen with your new objects?
 - The new objects that originated on the DC after the backup are lost because they were never replicated to other DC's, and therefore can't be applied to the restored DC.
- Conclusion: Always fix replication problems as soon as possible.



Authoritative Restore

- What is it?
 - Restore to known good point using NTBACKUP
 - Make objects on reference dc as “**master copy**” for DS
- When to use
 - Accidental **deletion** or **modification** of objects or containers in the domain or configuration NC
 - Ability to restore entire AD or a single object
 - Performed in DS Restore mode



Authoritative Restore

- What it isn't Q241594
 - Will not overwrite objects created after the backup
 - Only carried out on objects from the configuration and domain contexts
 - Will not overwrite objects which are tombstoned (>60 days default)



Authoritative Restore

- What it isn't
 - Auth restores of schema naming context are not supported. (Recovering AD Forest)
 - The schema cannot be authoritatively restored because it might endanger data integrity. For example, if the schema was modified and then objects of the new or modified class schema object were created, subsequent authoritative restore might replace the new or modified classes, thereby causing serious data consistency problems



Enforcing Functionality Levels

- Backup and Restore issues
 - Restore of Windows Server 2003 prior to mode increase, forest or domain
 - Restore of prior OS after version increase (upgraded DCs)
- Ntdsutil Limitations
 - Authoritative restore of msDS-Behavior-Version not allowed



Authoritative Restore

- Boot into offline restore mode
 - Press F8 during boot phase
 - Login with offline administrator account
 - Restore System state
- Mark objects in NTDSUTIL as authoritative
 - Find machine w/ objects or restore image that has them
 - Restore (entire) database (rare) or SUBTREE
 - USN, originating invocation IDs, Version Numbers on reference server are incremented to **WIN** replication



Authoritative Restore of AD

- NTDSUTIL
 - Type "Authoritative restore"
 - "Restore database" – Entire Directory
 - Restore Subtree – Specific OU
OU=market,DC=msft,DC=com
- DC Machine account Deletion
 - Restore Subtree "CN=DC3,OU=Domain Controllers,DC=msft,DC=com"
- User account Deletion
 - Restore object ([New option in W2K3](#))
CN=User1,CN=Users,DC=msft,DC=com



Authoritative Restore

- Ensure that SYSVOL and AD remain synchronized.
 - Always authoritatively restore the Sysvol folder when you authoritatively restore the entire Active Directory Database.
- Gpt.ini – Version number of the Group Policy object
- Gpoutil.exe – List all policies for your Domain. Checks version conflict with sysvol.

Auth Restore of Specific AD Objects and Corresponding GPO Objects from SYSVOL



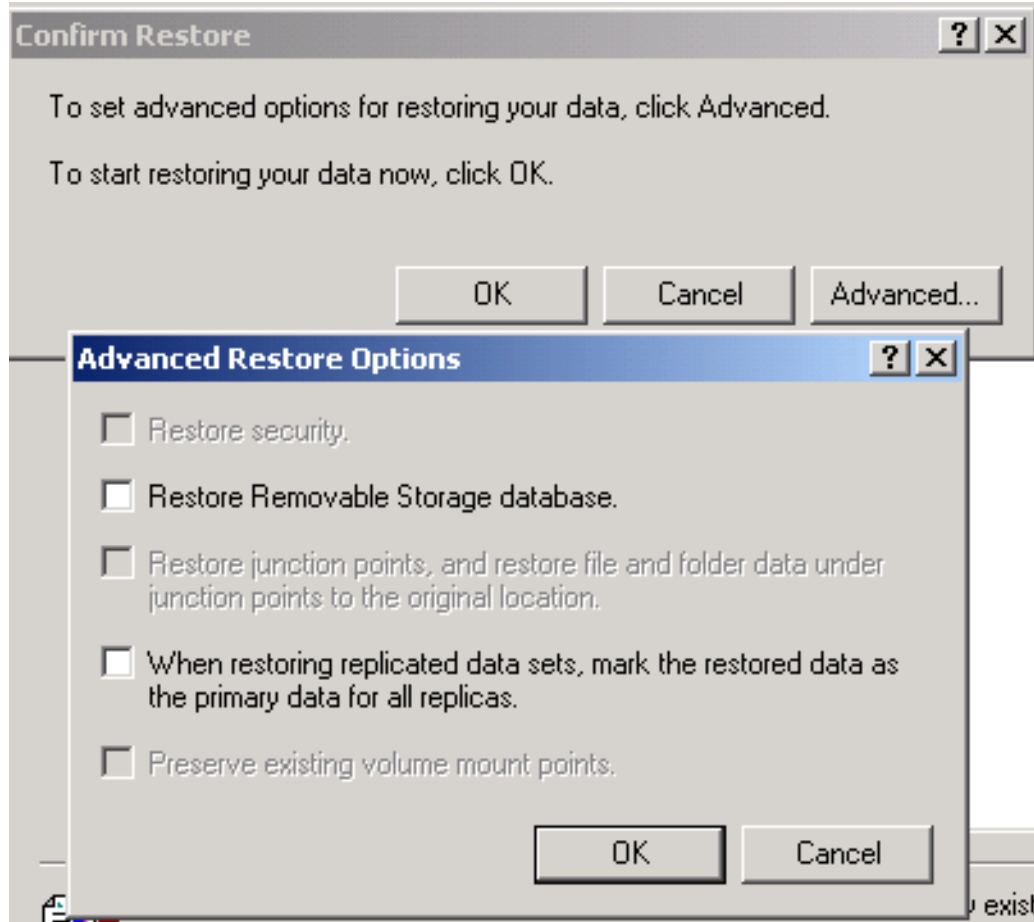
- Restart the computer in directory service restore mode
- Restore the System State data to its original location **and** to an alternate location
- By using Ntdsutil, separately mark specific Active Directory objects as authoritative
- Restart the computer in normal mode
- After the SYSVOL share is published, copy only Policy folders (identified by the globally unique identifier [GUID]) corresponding to the restored Group Policy objects from the alternate location



Authoritative Restore of Sysvol

- Advanced Restore Options:
 - “When restoring replicated data sets, mark the restored data as the primary data for all replicas”. (Only Single DC in a domain)
- System state to “Alternate location”:
 - Restore system state also to an Alt location
 - <Alternate Sysvol Location> Scripts and Policies

Advanced Options





Morphed Folders

- C:\Windows\SYSVOL\DOMAIN
 - Policies
 - Policis_NTFRS_030800fd
 - Scripts
 - Scripts_NTFRS_0004c427
- The last writer gives a non-conflicting name: Foldername_NTFRS_GUID
- The loser keeps the original name
 - The Administrator must intervene to resolve the names



Verifying Authoritative restore

- REPAIRADMIN /SHOWMETA
 - "CN=DC3,OU=Domain Controllers,DC=msft,DC=com"
- Version number incremented with 100000
- Version number replicated to other DC's
- Restore Database Verinc %d
 - Increments the version number by %d



Authoritative Restore Scenario

- **Day1**: Backup of DC3
- **Day2**: "User Two" is created and replicated to other DC's
- **Day3**: "User One" is inadvertently deleted.
- **Day4**: Authoritative Restore on DC3.
- **Result**: All users exist in domain.



Authoritative Restore

```
ntdsutil: a r
authoritative restore: restore subtree ou=ou812,dc=wizards,dc=com

Opening DIT database... Done.

The current time is 03-14-02 08:55.22.
Most recent database update occurred at 03-13-02 16:57.51.
Increasing attribute version numbers by 100000.

Counting records that need updating...
Records found: 0000000005
Done.

Found 5 records to update.

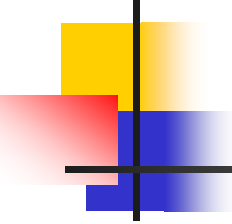
Updating records...
Records remaining: 0000000000
Done.

Successfully updated 5 records.
Authoritative Restore completed successfully.
```

Repadmin /Showmeta with Incremented Version Numbers

```
C:\WINNT\System32\cmd.exe
The directory service cannot get the attribute type for a name.
C:\Documents and Settings\Administrator>repadmin /showmeta CN=david,ou=ou812,dc=wizards,dc=com
34 entries.

Loc.USN          Originating DSA  Org.USN          Org.Time/Date    Ver Attribute
=====
110177          Default-First-Site-Name\MELF  110177  2002-03-13 16:36.09      1 objectClass
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 cn
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 description
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 givenName
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 instanceType
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 whenCreated
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 displayName
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100000 isDeleted
110275 06bd41c4-e482-489d-9a53-56aa6739a45e 110275 2002-03-14 08:55.22100001 nTSecurityDescripto
```

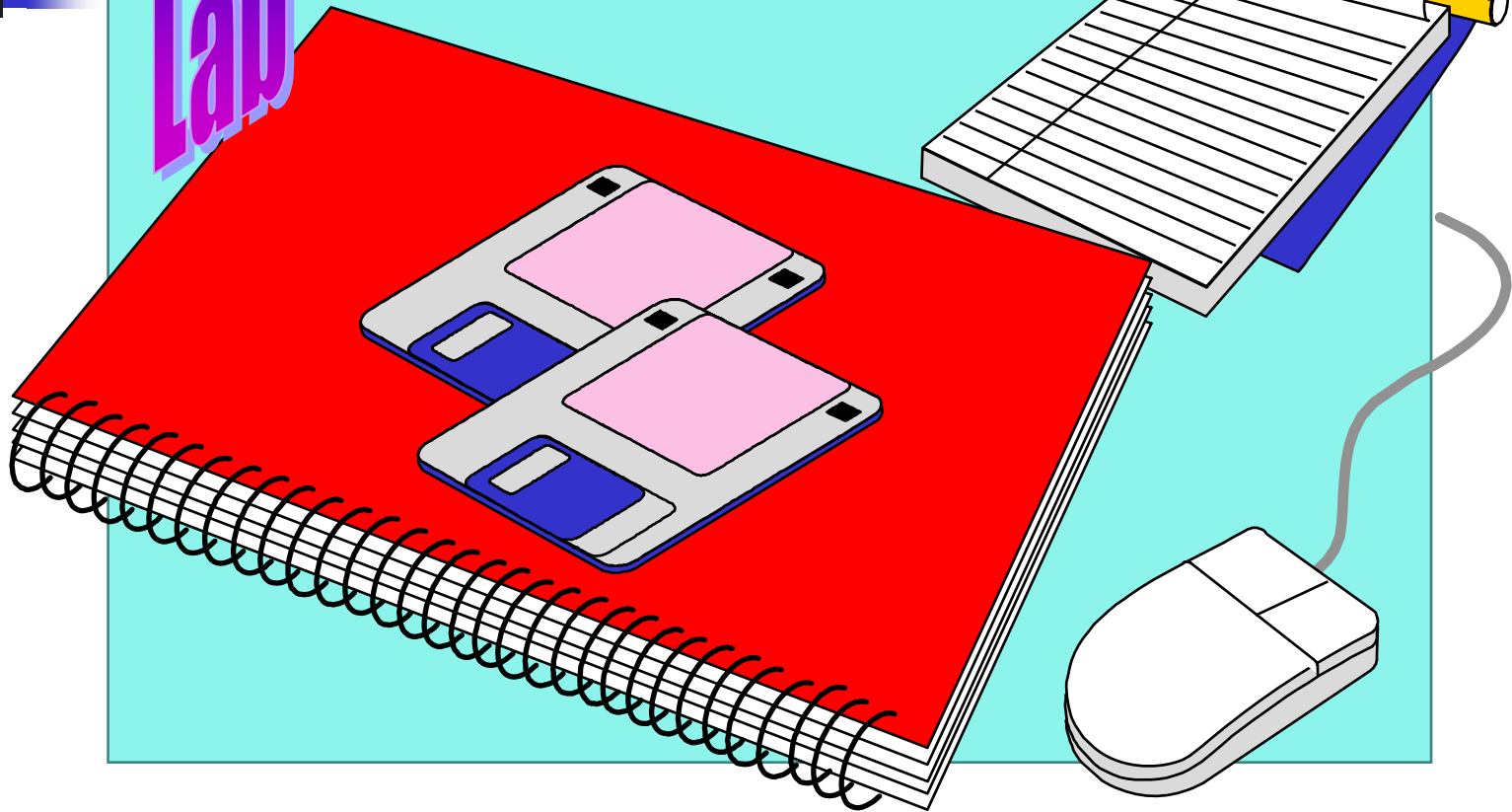


Can't remember your DS Restore Mode "Administrator Password"

- Same password is also used by Recovery Console
- The SAM-based account and password are computer specific
- SP2: `c:\winnt\system32\Setpwd`
 - Specify a new password. Q239803
- Setpwd on a Remote DC
 - `Setpwd /s:<servername>`

Authoritative Restore

Lab





Scenarios

- Hardware Failures
- Event ID 1018s
- Event ID 1168
- Recovering deleted objects
- Deleted printer objects
- FSMO's
- Duplicate SIDS after restore
- Critical system objects
- Objects with passwords
- File System Policy
- Restores and FRS
- Impact on Group Membership
- Forcefully demote a DC



Hardware Failure

- Scenario:
 - DC experiences catastrophic hardware failure
- Goal:
 - Restore the DC to new hardware
- Test
 - Restoring to similar and dissimilar hardware
- Ideal Scenario:
 - Target hardware identical to source
 - NICS + Video + HAL + Kernel + # of Processors



Dissimilar Hardware W2K

- Reality
 - Not a trivial process. Complex and time consuming.
 - Use KB Q263532 to improve results
- Requirements (few examples.....)
 - Backup SYSVOL + SYSTEM STATE
 - Higher probability if %SYSTEMROOT% backed up
 - Target machine has **same number of drives & drive letters** for entities being restored. Disk Controller.....
 - Incompatible Boot.ini File. If you backup and restore the boot.ini file, you might have some incompatibility with your new hardware configuration, resulting in a failure to start.
 - Logical drives on destination **same size or larger**
 - Uninstall **NIC** and **Video card** before you restore data, if it's different. Let plug&play make necessary changes



Dissimilar Hardware

- Restoring AD to dissimilar Hardware
 - Perform Clean Install as a stand-alone server
 - Restore System partition and system state
 - Select “Always replace the file on disk” in advanced restore settings
 - Reboot the server in normal mode



Dissimilar Hardware in Windows 2003

- Backup the System State from the Source DC
- Use DCPROMO /ADV with "Install from Media" option on target computer.
- Choose "Additional domain controller for an existing domain"



Jet Error 1018 Event 404 (1)

- Problem

- Jet error 1018: possible data corruption from faulty hardware.

- Symptoms

- Successful write is reported, though write fails
- Events may not be logged
- All classes and price points of hardware affected

- Causes

- Can vary from faulty RAID & SCSI Firmware, Termination Bad Hard Drives



Jet Error 1018 (critical)

- Impact:
 - Corrupts AD, and FRS jet databases
 - Backups may also be corrupt
- Resolution:
 - Check with HW vendors for known issues
 - Replace/test Physical drives
 - Restore the database
 - Defragment the database with NTDSUTIL
 - Hard repair the database with NTDSUTIL – Can result in loss of data (if you not have an **ok** backup)



Event ID 1168s

- Problem
 - Active Directory fails to boot with Event ID 1168s
 - 1168s generic events: contact Premier Support
 - Unable to start the Active Directory
- Cause
 - Permissions too restrictive on NTDS.DIT & LOGS or the NTDS folder
 - Unscheduled loss of power that can cause the Ntds.dit file or log files to become un-readable
- Resolution: Q265089
 - Define Default permissions
 - Delete/rename EDB.CHK file – Soft Recovery
 - non-auth restore to recover
 - Reinstall the operating system on the failed computer



Recovering deleted objects

- Problem
 - Accidental deletion of OU or other objects
- Resolution
 - Restore + Authoritative Restore in NTDSUTIL
 - Restore recent backup
 - Mark deleted objects as authoritative
 - Authoritative Restore in NTDSUTIL
 - **Find replica dc that hasn't received deletions**
 - Mark deleted DN as authoritative (no restore required)



Recovering AD objects

- No Good System state Backup – Q237677
 - **LDIFDE** - Export and Import Directory Objects
 - Export OUs, users, and groups from an entire forest
 - Run LDIFDE export commands against each domain in the forest, or alternatively, run the query once against the global catalog (GC).
 - No SID history



Recovering deleted DNS zone

- Deleted a DNS Zone called: Test.sample.com and want to restore it back:
- Restore System state from backup in "DS restore mode"
- Start NTDSUTIL
- Restore Subtree
DC=test.sample.com,cn=MicrosoftDNS,cn=system,DC=MS,DC=COM
- Reboot DC in normal mode



Deleted Printer objects

- Printer Pruning on DC's (for it's own site)
 - A process which keeps printer information in Active Directory current.
 - Controlled by GPO's. Q234270
 - "Allow pruning of published printers"
 - "Directory pruning interval" - Default 8hours
 - Stop the Spooler service on the offline DC
- If a DC does not see the printers for a period of time, it may consider the printers orphaned when the DC come back online

Deleted Objects in Active Directory



■ Protection

- Set replication schedule once every >four days on “backup domain controller”
- Mark objects as authoritative when deletion detected



FSMO

- **Rules**
 - **Transfer** if role needed before current owner goes offline
 - **Seize** if current role owner offline & *never* coming back
- **Roles and Dependencies**
 - PDC: Down level clients, Policy updates, DFS updates,
 - RID: Inability to add any new security objects as users, groups, computers **beyond local rid pools** on each DC
 - Domain Naming Master: Domains cannot be added/removed
- **Seizure Rules**
 - Install of OS that held seized role can never come back online
 - Reinstall with same names is ok. Do Not use old Backup's.



RID Master

- Considerations for performing a Seizure on a RID Master.
 - Risk of Duplicate RIDs.
 - Original Master should NEVER come back online again if a Seizure is performed.
 - Instead, the original role holder must be reinstalled before introduced in the Domain again.



Duplicate SIDS after restore

- Problem after Backup and Restore of a DC.
 - RID pool is set to a range that has already been used to allocate SIDs
 - Duplicate SIDS are created as the customer creates new users & groups on restored DC
 - May not be immediately detected
- NTDSUTIL: "check duplicate sid"
"cleanup duplicate sid" Q315062
- Resolution: Finally SP4 Q316201 or W2K3



Restoring Operations Masters

- Seize the role if you not intend to restore the original role holder from a backup.
- Seize a fsmo role ONLY as last resort.
- Active Directory continues to function when the operations master roles are not available.



Schema operations master

- Isolate Schema additions made by adprep.
- **Prevent a full Forest Recovery:**
 - Temporarily disable outbound replication
 - repadmin /options
+DISABLE_OUTBOUND_REPL
 - X:\I386\>adprep /forestprep
 - view the Adprep.log file in the
%systemroot%\System32\Debug\Adprep\Logs\
<Latest_log> folder
 - Enable replication again on the Schema Master



Recommendations for Returning to service after Seizure

- Schema Master
 - **Not** recommended. Can lead to a corrupt Forest and require a Forest Recovery
- Domain Naming Master
 - **Not** recommended. Can require rebuilding Domains.
- PDC Emulator
 - Allowed. No Permanent damage occurs.
- Infrastructure Master
 - Allowed. No damage occurs to the Directory
- RID Master
 - **Not** recommended. Duplicate RID pools can be allocated to DC's, leading to data corruption in the Directory.



Backup / Restore FSMO Rules

- Backup
 - Document the machine names of FSMO role holders when you do the backup
 - Include %windir%?
- Restore
 - DC's that have not replicated for TSL # of days should not get fixed. They should get removed and rebuilt.
 - Do not reduce TSL unless verifying end to end replication of forest.
 - As a general rule, do not reduce TSL to low # of days to accelerate deletion of a tombstone
 - Never restore FSMO's except as last restart - implies awareness of where FSMO was when backup made.
 - Rules: Don't transfer or seize FSMO role of current owner offline unless you are performing dependent operation



Procedures for seizing fsmo's

- 1. First replicate all AD changes to all DC's in your forest.
- 2. Verify successfull replication for your DC which seize the role.
- 3. Seize the FSMO role.
- 4. View the current FSMO role holders.
- "Netdom query fsmo". Replmon



Critical Objects

- Machine Accounts for DC's
 - Machine account password and Trust relationship password is reset every 30 days
 - Q257288: Recover from a **Deleted** DC Machine Account
 - Dcdiag /s:localhost /repairmachineaccount
 - Demote and then re-promote the server. (Services)
 - Or, Dcpromo /forceremoval + clean up metadata + re-promote
- NTLM Trust Relationships
 - Password is reset every 7 days
 - Authoritative Restore - NOT older than 14 days
 - To **reset** NTLM trust relationships to Windows 2000 or downlevel domains, the trust must be removed and re-created.



DC Computer Accounts

- Problem:
 - AD replication uses locally held password for Kerberos authentication
- Defaults
 - Password **default** change interval = 30 days (N)
 - Backup useful life = 60 days
 - Password history = N + N-1
- Symptoms of mismatch?
 - AD Replication fails with "access denied"



Recovering File System Policy

- Scenario:

- File system portion of policy has been deleted

- Cause

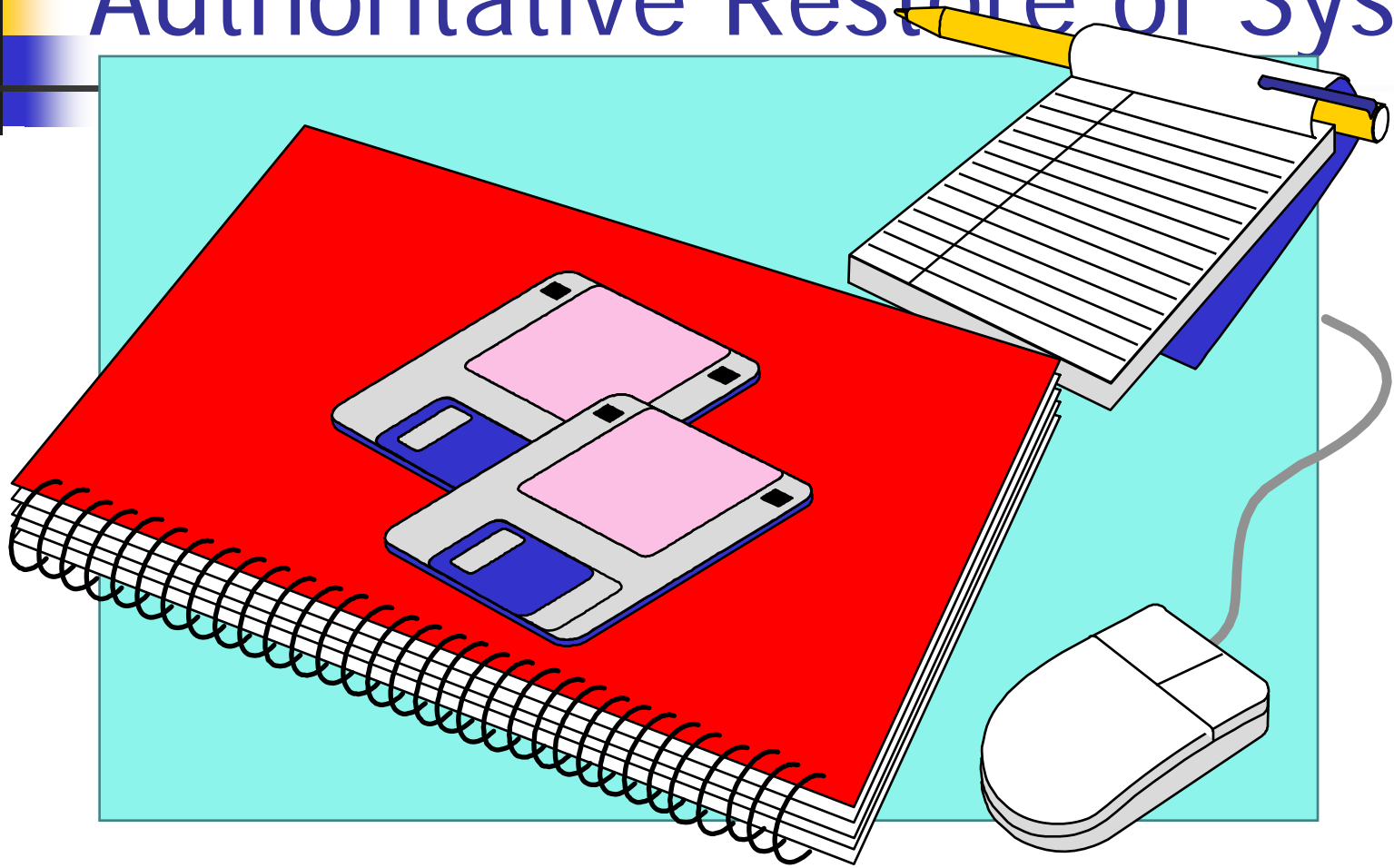
- Administrators deleted policy to rebuild from scratch
- Deleting a File/Directory from Sysvol on one DC, results in FRS replicated deletion to all members of set.
- If C:\Winnt\sysvol is copied to alternate location D:\sysvol = The junction points in sysvol are also transferred to the alternate location. Junction points still points to original location C:\Winnt\sysvol



Recovering File System Policy

- Recovery:
 - Locate policy files
 - Restore backup image of SYSVOL to alternate location
 - Turn off “Mark restored data as primary for all replicas”
 - Locate files on member with delayed schedule
 - Locate files in pre-existing directory
 - Copy files to member and let replication take place

Authoritative Restore of Sysvol





Rebuild Sysvol with Burflags

- BURFLAGS = (backup / restore flags)
 - NET STOP NTFRS
 - HKLM\System\CCS\Services\NtFrs\Parameters\Backup/Restore\Process at Startup\D2
 - D2: Will perform a full synch of the replica set from it's Upstream partner
 - BURFLAGS registry key to D4 (authoritative mode)
- Also used as last resort to fix FRS replication related problems.



Authoritative FRS Restore

- When to use: (rare) Q315457
 - SYSVOL replica set meltdown, requiring a complete rebuild from an Authoritative member to perform a full sync.
- Resolution:
 - Stop NTFRS service on all DC's
 - Set D4 on primary machine
 - Set D2 on all other members
 - Start NTFRS service on primary machine
 - Start NTFRS service on all other members



Group Policies

- GPOTool.exe
 - Verifies the health of the GPO on a DC
- DCGPOFix.exe
 - Restores the Default Domain Controller and Default Domain Group Policies to the state when the DC was installed
- GPMC – Group Policy Management Console
 - Backup/Restore, Import/Export of Group Policy objects.
 - Help full during disaster recovery scenario if a Backup of GPOs exists
- White Paper: Administering Group Policy with the GPMC
<http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.aspx>

Unable to open Group Policy Snap-In



- Sysvol and NetLogon are not shared out
 - Are all directories and files in Sysvol
 - Netlogon and frs services running
 - ACLs are correct for c:\winnt\sysvol
 - Are AD replication working ok?
 - Create a test.txt file in sysvol. Does it replicate?
 - Initialization of the system volume:
 - Value of SysvolReady to 1
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
 - W2K3 article: Q327781 - How to Troubleshoot Missing SYSVOL and NETLOGON Shares



Recommendation for GPO's

- Accept the defaults that are set within the Default Domain Policy and the Default Domain Controllers Policy.
- Create new policies instead.
- Default Domain Policy – Account Policies
 - Password Policy
 - Account Lockout Policy
 - Kerberos Policy
- Default Domain Controllers Policy
 - User Rights Assignment
- Ensure all DCs receive consistent Group Policy settings
 - Do not filter policy settings on individual DCs
 - All DCs should remain in the Domain Controllers OU



Forcefully demote a DC W2K

- If DCPROMO **fails**, how to demote....
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ProductOptions
 - Edit menu, click String, type ServerNT
 - Promote the computer to a different forest
 - demote the computer as standalone server
 - Q216498 Removing Active Directory Data After an Unsuccessful Demotion



Forcefully demote a DC

- If re-installation is NOT an option and...
 - **Parent** domain DC is NOT accessible when attempting to demote last DC in a child.
 - **Replica** DC in same domain is NOT accessible when trying to demote.
 - **Replication** failure due to failed authentication or replication error.
 - DC hasn't **replicated** in Tombstone life number of days.

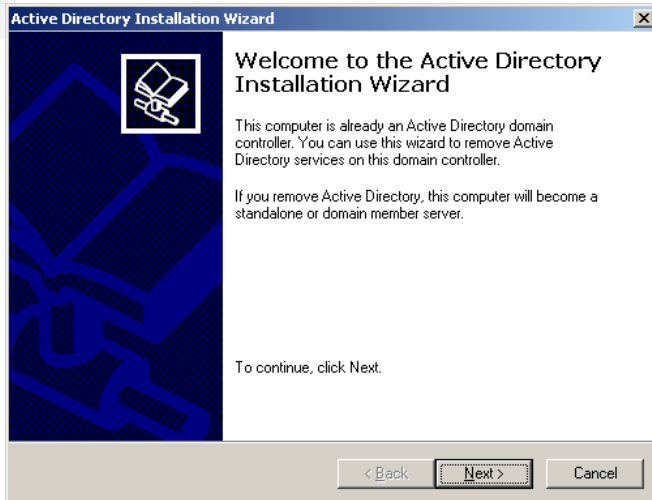


W2K3 and W2K-SP4 Forcefully

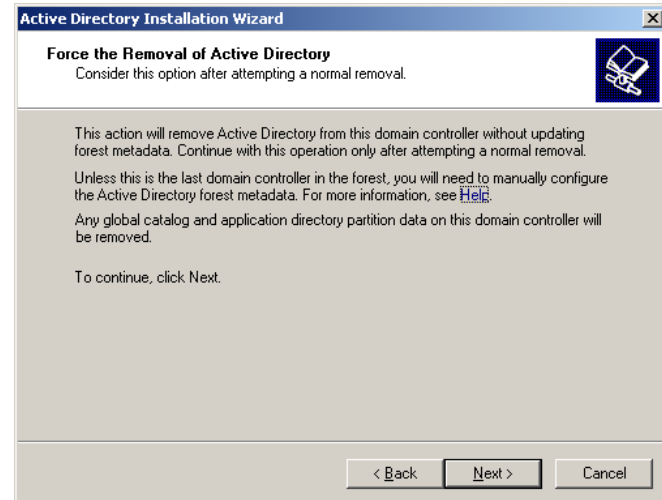
- Force demotion
 - W2K3 → DCPROMO /FORCEREMOVAL
 - W2K → DCPROMO /FORCEREMOVAL
 - Need Windows 2000 SP4
- Does not cleanup metadata from other DC's in AD
 - Use NTDSUTIL to cleanup the metadata
 - Q315148 - Remove Old Metadata from the Active Directory Database
- <http://support.microsoft.com/?id=332199>
- Currently the DCPROMO /FORCEREMOVAL command doesn't work in DSREPAIR mode

Force Demotion Wizard

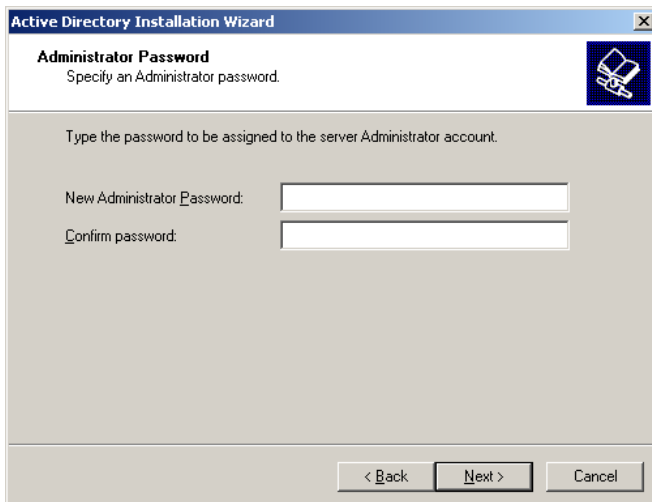
1



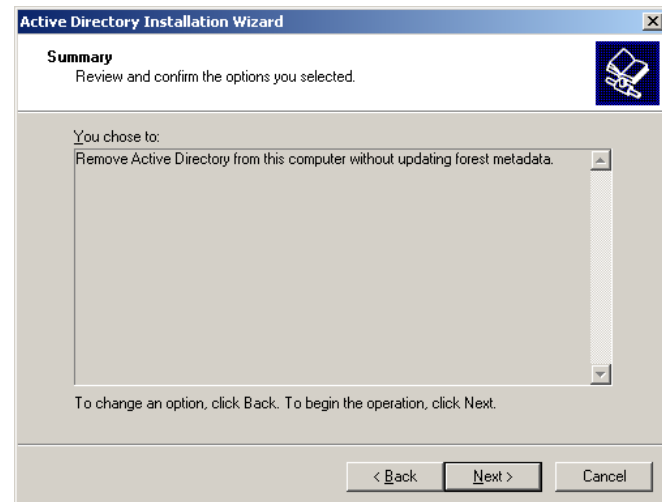
2



3



4





Remove a DC from a Domain

- Standard/recommended method of removing a DC from a domain – demotion using DCPROMO.
- If a DC decommissioned incorrectly – need to clean up Stale metadata for that DC.
- Cleanup stale Metadata from Active Directory – NTDSUTIL
- Cleanup stale metadata from DNS
 - Delete the A and CNAME Records.
- Optionally Cleanup metadata from DNS, WINS servers.



Domain Removal from a forest

- GC maintains read-only partitions for every other domain in the forest
- Read-only partitions need to be destroyed when
 - Corresponding domain removed from Forest.
 - GC is demoted to non GC
- Tear down of these partitions done by KCC
- In windows 2000
 - KCC deletes 500 objects/NC every time it runs
 - KCC runs every 15 minutes by default
 - Cause long delays in destroying large NC
- In Windows server 2003
 - KCC runs asynchronously at full throttle to rip apart the NC faster
 - Helps to Cleanup the removed the Domain faster



Restoring Groups and Users

- If Groups and Users are authoritatively on one DC
 - There is No guarantee that the users will replicate in advance of the group
- If a Group is replicated in advance of a User that is a member of the Group
 - The receiving DC has no record of the User and deletes it from the Group



Impact on Group Membership

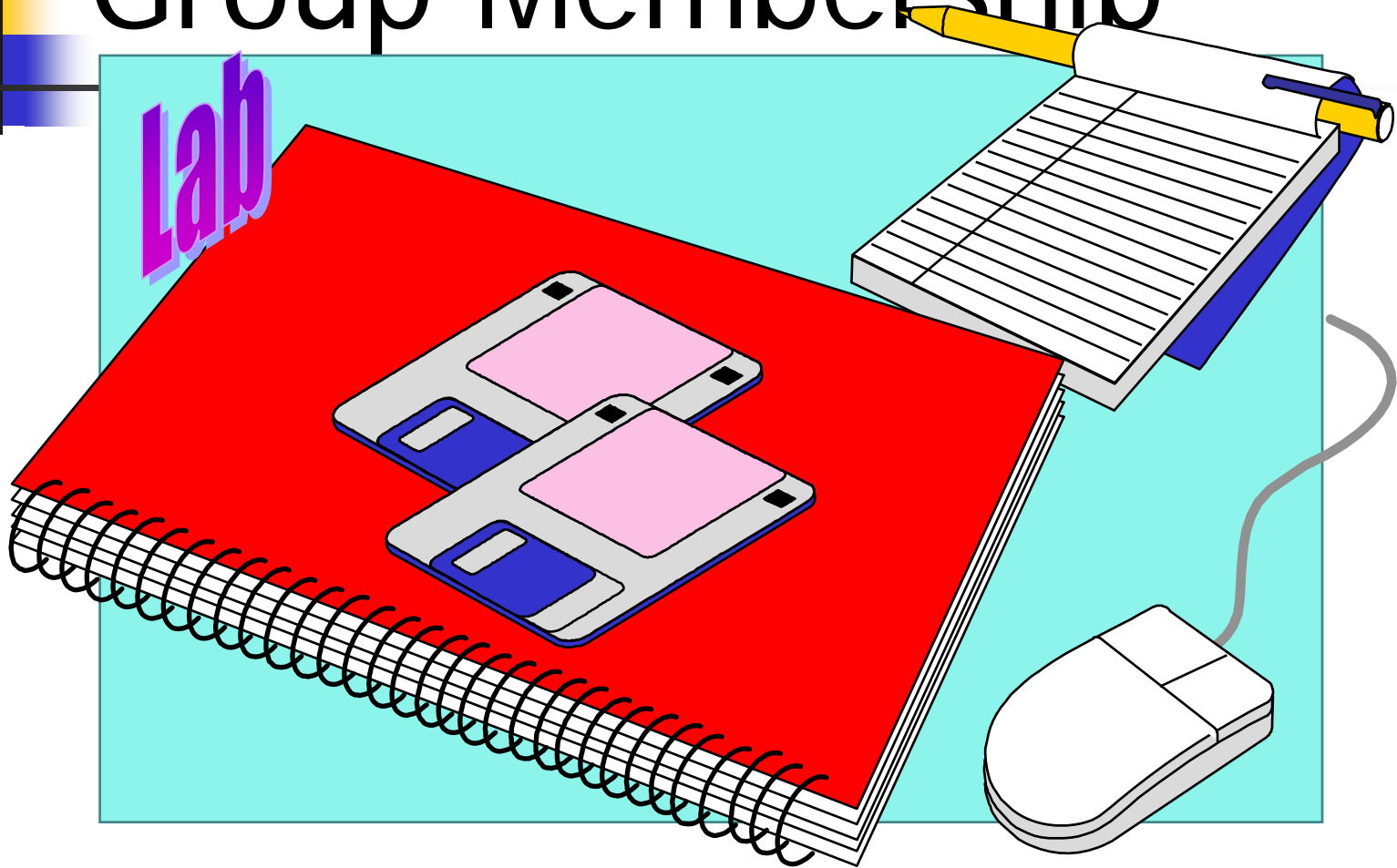
- Problem:
 - Group Membership information can be lost if groups are restored before users
- Cause:
 - Backlinks to non-existent users are removed
 - No way to define which objects replicate first after an authoritative restore
 - If the group is restored prior to the member, the membership will be removed during replication, as you can't have a live group referring to a deleted member
- Resolution: Q280079 + (840001)
 - All users and computers must be authoritatively restored and replicated out to all DC's, and then all group objects must be authoritatively restored and replicated out to all DC's again

Best Practices OU Structure - Auth Restore



Group Membership

Lab





Restore of Schema failures

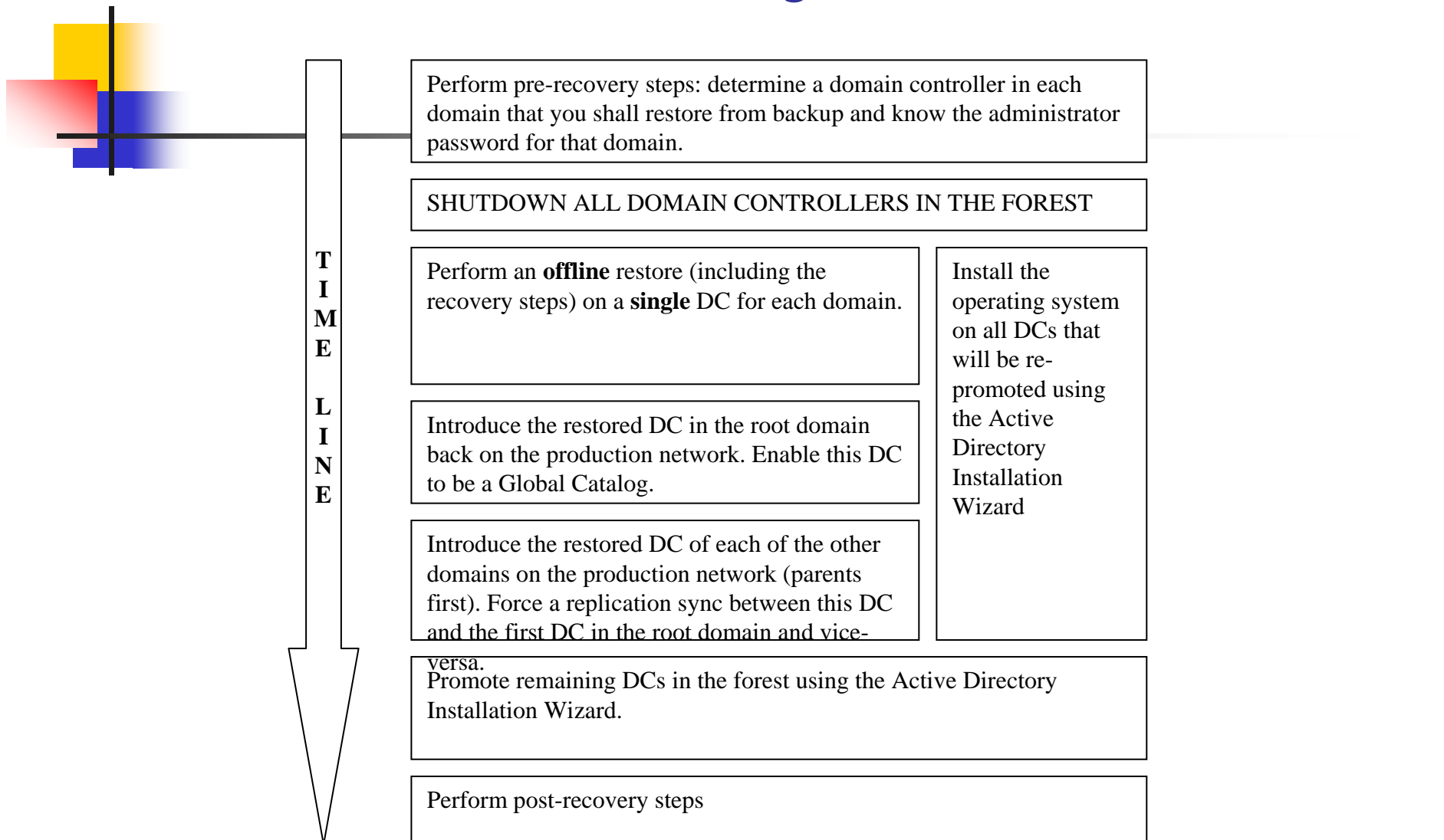
- Examples Scenarios
 - Schema corruption due to bug or user mistake replicated to all DC's.
 - Schema objects required by one application modified by other application.
- You need to restore the whole Forest to a point in time before corruption occurred.
 - Use as a Last option, after determining the cause and possible remedies
 - Applies only if, "All" DC's in the Forest are affected



Forest Recovery Roadmap

- Recover Forest Root Domain first
- Proceed to recover the remaining Domain's.
 - Rule of thumb, Restore the Parent Domain before Child Domain
- For each Domain
 - Restore only one DC from a Good Backup!!!
 - Promote remaining DC's using DCPROMO
 - For Windows 2003 DC's use "Install from media"

Forest Recovery Timeline



Recovering the Root Domain



- Step 1: Restore AD marking SYSVOL primary
- Step 2: Verify Data on the restored DC
- Step 3: Configuring/Modifying DNS Server
 - Step 3A: DNS server present prior to Failure OR
 - Step 3B: DNS server absent prior to Failure
- Step 4: Disabling GC Flag if restored DC is a GC prior to failure
- Step 5: Seize FSMO roles
- Step 6: Clean up metadata of all other DC's in the Domain
- Step 7: Delete Server and Computer objects for all other DC's in the Domain
- Step 8: Raising the current RID pool
- Step 9: Reset Computer account password of the restored DC and LSA secret
- Step 10: Reset krbtgt password
- Step 11: Reset trust password
- Step 12: Introduce restored DC in Production Network
- Step 13: Enable the restored DC to be a GC



Recovering the Forest

- Detailed description in the following White Paper:
- Best Practices: Active Directory Forest Recovery
 - <http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3EDA5A79-C99B-4DF9-823C-933FEBA08CFE>



Best Practices

- The tombstone Lifetime Interval should not be reduced in a large environment
- A DC can not be off longer than the tombstone lifetime for the forest
- Separate the Database and Log files
- Backup "System state" of DC's frequently
- Perform Offline Defragmentation Only if you can recover a Significant amount of Hard Disk space
- DHCP and WINS databases requires special procedures to handle open files

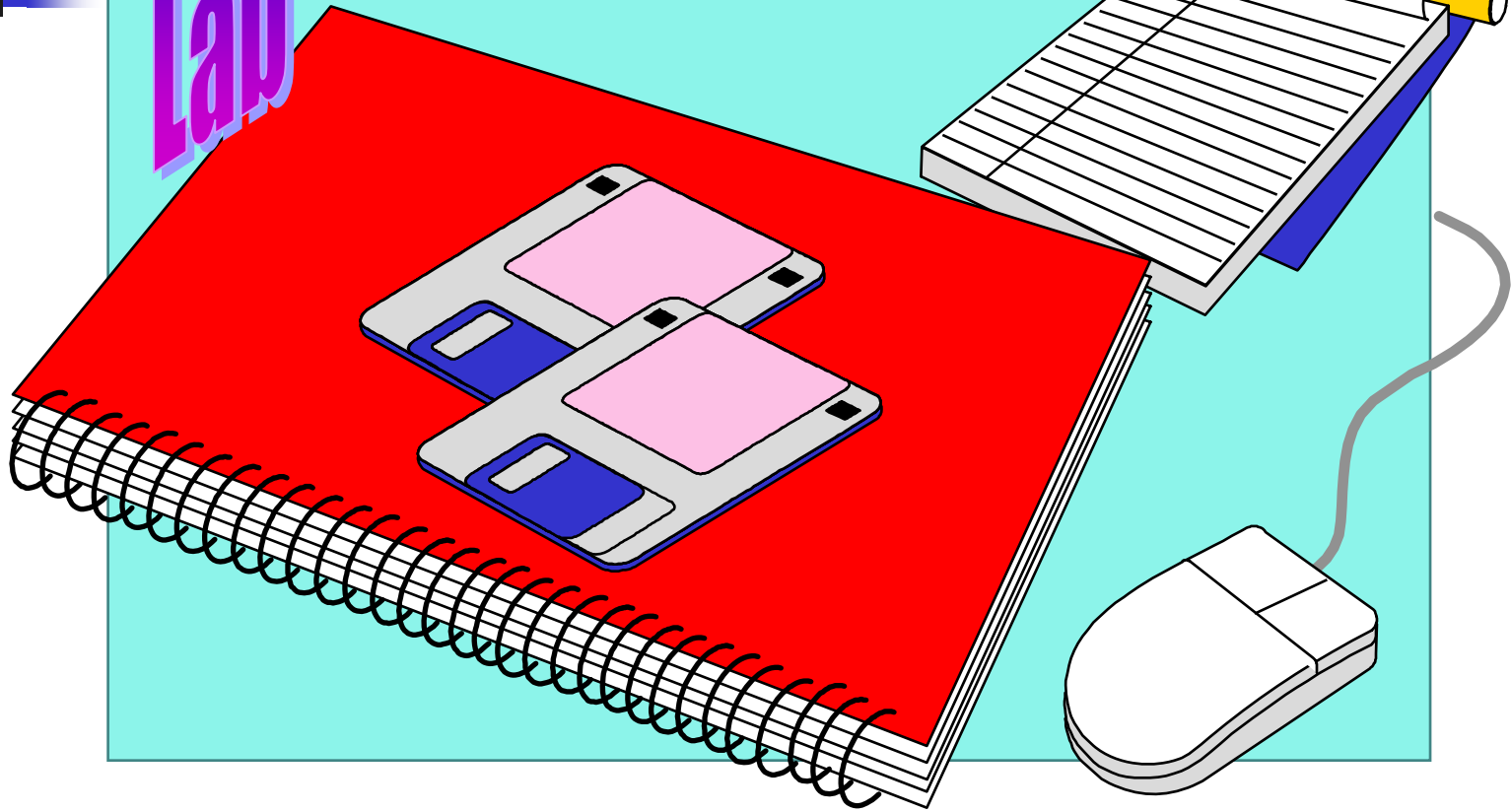


Summary

- Common sense
 - Take the least extreme method
 - Affect least number of objects possible
 - Most deterministic results
 - Least amount of time
 - Determine Root Cause: Understand how you got here
 - Learn from your mistakes
 - Take steps to avoid repeat performances
 - Make backups before you do anything so you can get back to where you started

Recover Root Domain

Lab



The Microsoft logo graphic, consisting of four overlapping squares in yellow, red, green, and blue, with a black crosshair.

Microsoft®

Where do you want to go today?



Microsoft®