

**SVR302**

# **Active Directory Recovery Planning**

**Chewy Chong**

Senior Consultant

Systems Engineering Practice

**Avanade Australia**

# Key Takeaways

- Prepare - Proactive steps that can be taken to **better prepare** for different disasters
- Recover - Best practice recommendations to **recover** from different disaster scenarios
- Experience - Stories from the field

# Agenda

- **Planning for the Worst**
- **Practical Recovery Examples**
- **Summary**
- **Questions**

# Agenda

- **Planning for the Worst**
  - **Assess**
  - **Prepare**
  - **Best Practices**
- **Practical Recovery Examples**
- **Summary**
- **Questions**

# Planning for the Worst

## Assess

- How well do you really know your environment?
  - People
  - Infrastructure
  - Processes and Procedures
  - Business Expectations / SLAs

# Planning for the Worst

## Assess

- Find and document your gaps
  - Lack of skills
  - Infrastructure shortcomings
  - No processes / lack of clear procedures
- **Be honest with yourself.** This was the hand you were dealt.

# Agenda

- **Planning for the Worst**
  - Assess
  - **Prepare**
  - Best Practices
- **Practical Recovery Examples**
- **Summary**
- **Questions**

# Planning for the Worst

## Prepare

- Write down your “\*YP” events
  - Oops. I deleted the ‘Executives’ OU.
  - Hmm... what would happen if I turned this on...
- Draw boundaries
  - Know when to call for help (amputated finger example)
- Create operational run books
  - Book 1 – Accidental Deletion of AD object
  - Book 2 – ...



# Planning for the Worst

## Prepare

- **Know your tools**

- **Paranoia and Patience**

- **Microsoft Tools**

- Backup utility, DNS Manager, Active Directory Domains and Trusts Microsoft Management Console snap-in, Active Directory Installation Wizard, Active Directory Schema snap-in, Active Directory Sites and Services MMC snap-in, Active Directory Users and Computers MMC snap-in, Adsi edit MMC snap-in, Dcdiag.exe, Event Viewer, Ldp.exe, Net.exe, Netdiag.exe, Netdom.exe, Nltest.exe, Ntdsutil.exe, Registry Editor, Repadmin.exe, Secedit.exe, Services snap-in, Ultrasound, W32tm.exe

- **3<sup>rd</sup> Party Tools**

- **More details... <http://firechewy.com/blog>**

# Agenda

- **Planning for the Worst**
  - Assess
  - Prepare
  - **Best Practices**
- **Practical Recovery Examples**
- **Summary**
- **Questions**

# Planning for the Worst

## Best Practices

- **An ounce of prevention is worth a pound of cure.**

# Planning for the Worst

## Best Practices

- 28.34 grams of prevention is worth 0.453 kilograms of cure.

# Planning for the Worst

## Best Practices

- 28.34 grams of **verified** prevention is worth 0.453 kilograms of cure.

# Planning for the Worst

## Best Practices – BACKUPS!!

- What am I saying?

**BACKUPS are essential for any AD recovery process.**

- Backup DCs with GC / DNS
- **Verify backups.**  
**Do not take anything for granted.**

# Planning for the Worst Best Practices – BACKUPS!!



# Planning for the Worst

## Best Practices

- **Spare DC for everyday disaster recovery purposes**
  - A small DC that can be 'mailed' somewhere
- **Do not have a multi-purposed DC**
  - File/Print/DC combo is bad news
  - To many moving parts and typically causes problems



# Planning for the Worst

## Best Practices

- **Have some sort of emergency response procedure**
  - **Lockdown**
  - **Assess**
  - **Act**
- **Be extra careful while doing stuff that may impact AD**
  - **“Only the paranoid survives”**
  - **Take steps to protect AD such as temporarily stopping replication**

# Agenda

- **Planning for the Worst**
- **Practical Recovery Examples**
  - **Object Recovery**
  - **Single DC Recovery**
  - **Multi DC Recovery**
  - **Forest Wide Recovery**
- **Summary**
- **Questions**

# Object Recovery

## Problem statement & recovery

- Object has been accidentally deleted
  - Or modified considerably
- Object can't be re-created
  - Different object as far as AD is concerned
  - Different GUID & SID
- Recovery methods
  - Authoritative restore
  - Tombstone reanimation
  - GPMC to restore a deleted GPO

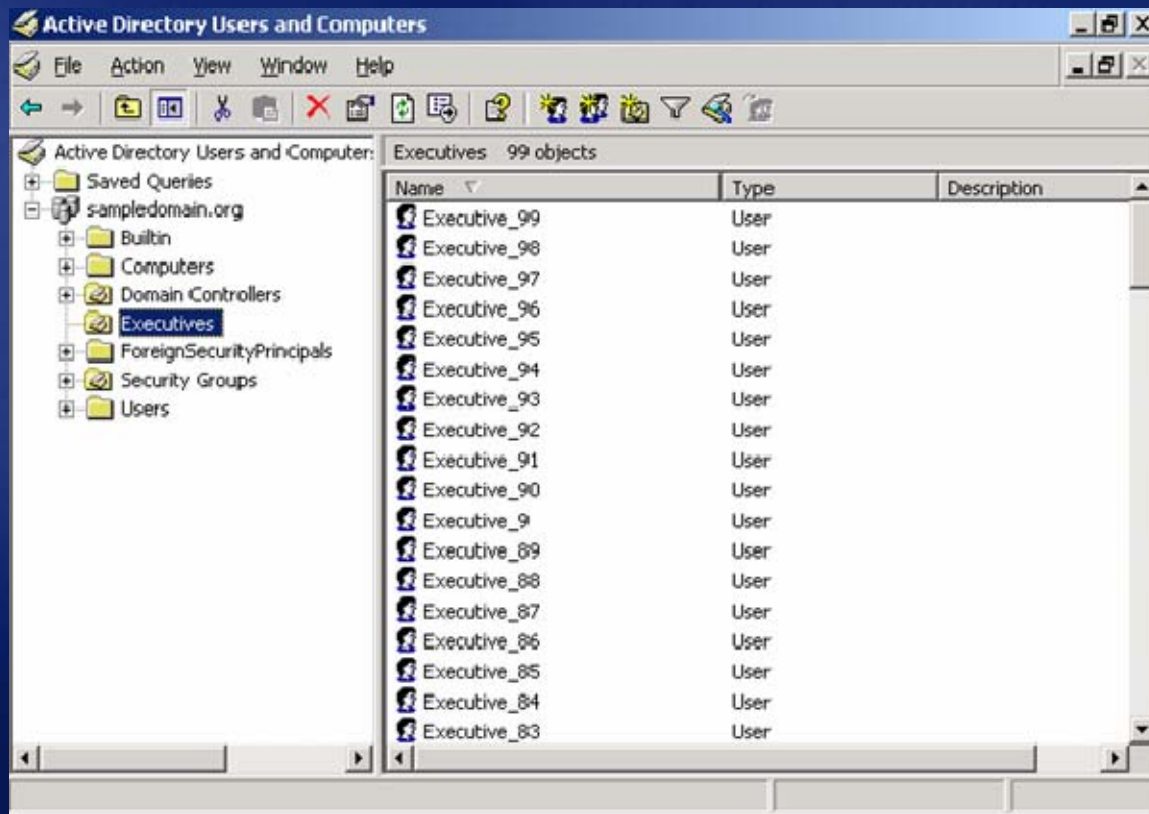
# Object Recovery

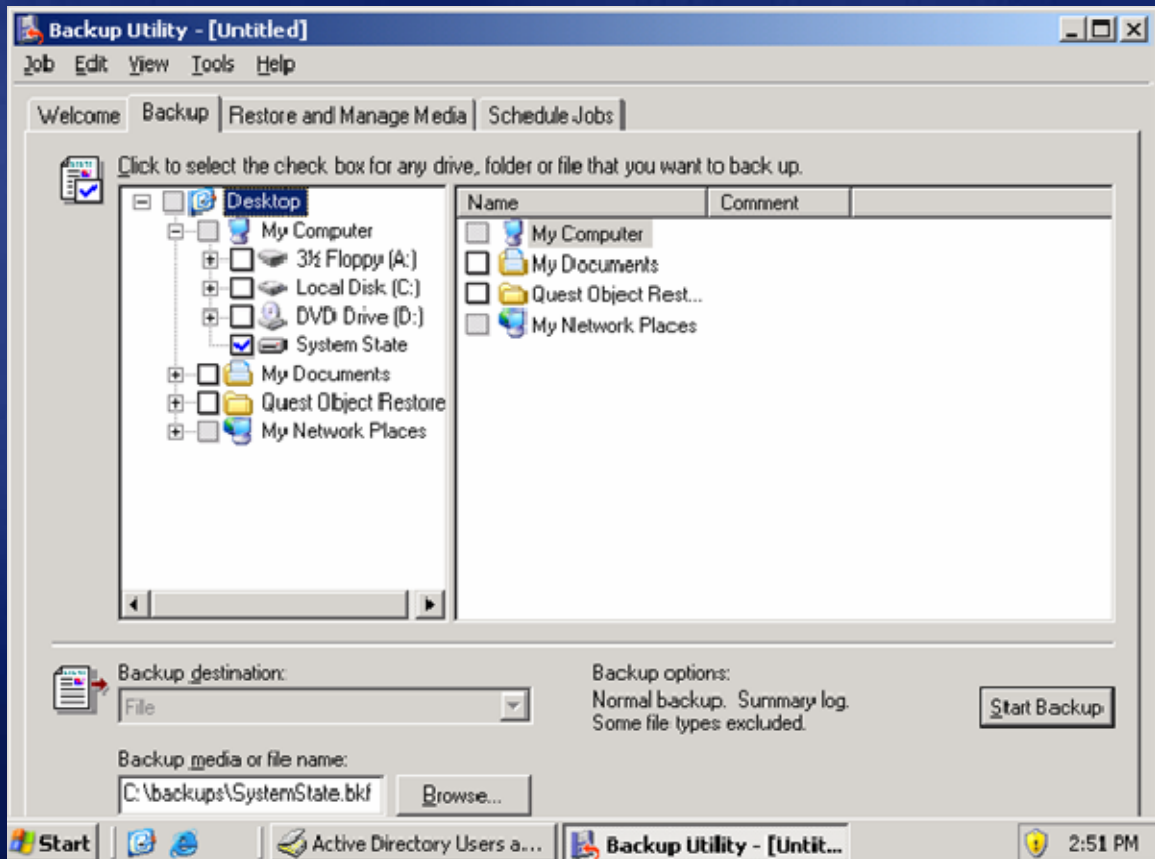
## Authoritative restore

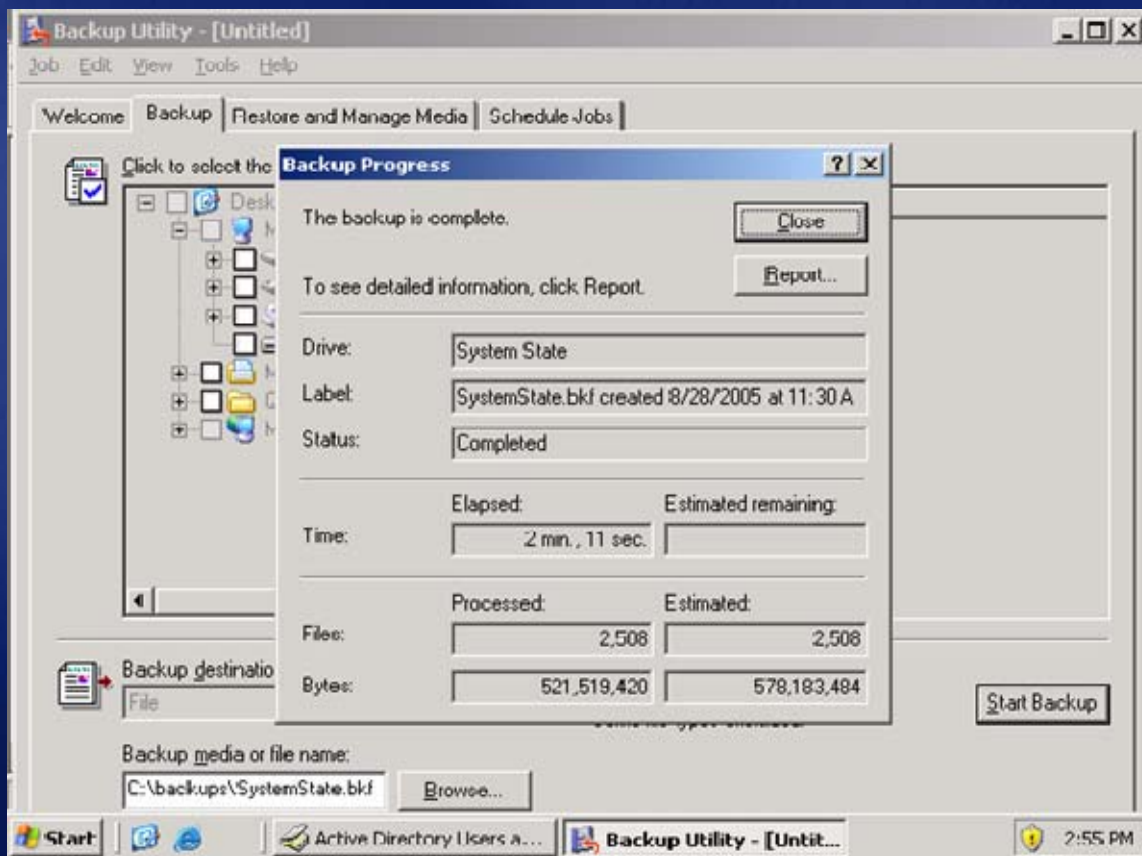
- **Boot DC in DS restore mode**
- **Restore System State but don't reboot**
- **Run Ntdsutil & mark object to be auth restored**
  - **Need to know the full DN of the object**
  - **If deleted object is an application partition, also auth restore the cross-ref object**
- **Reboot**

demo

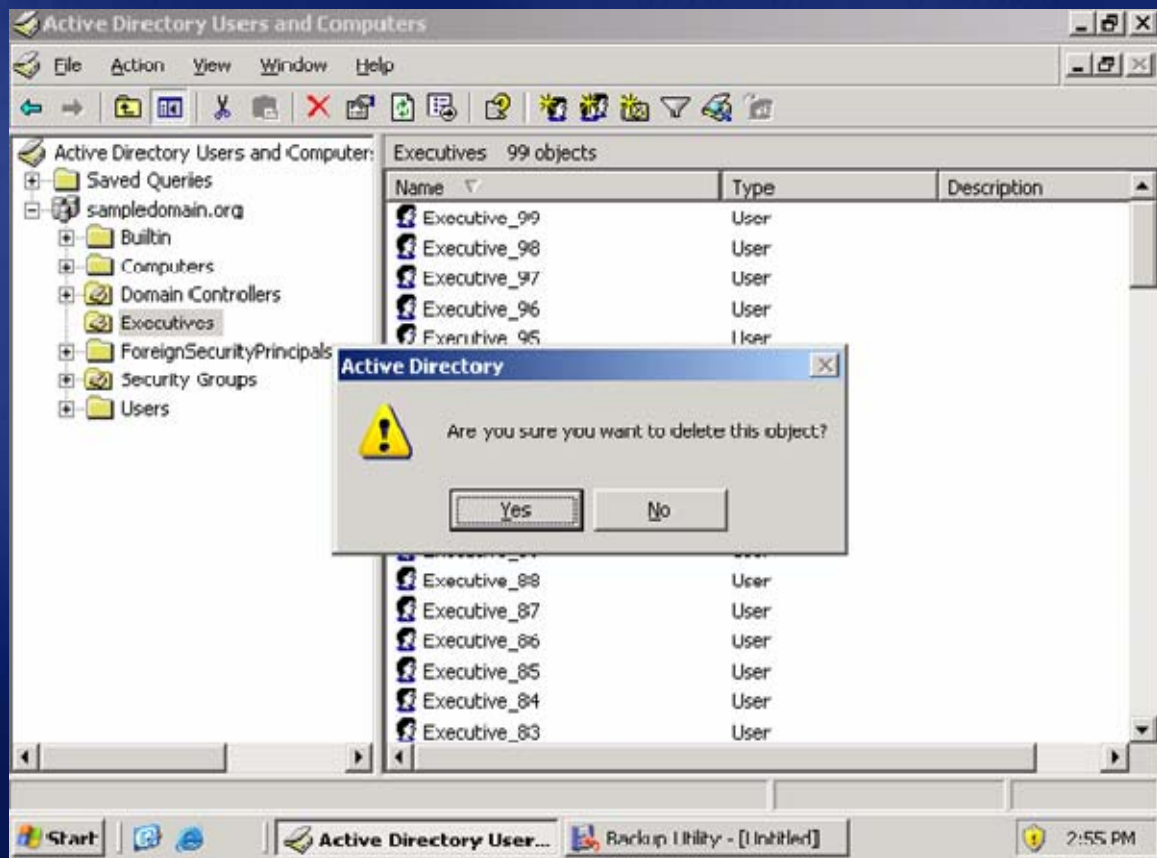
**Object Restore Using an  
Authoritative Restore**

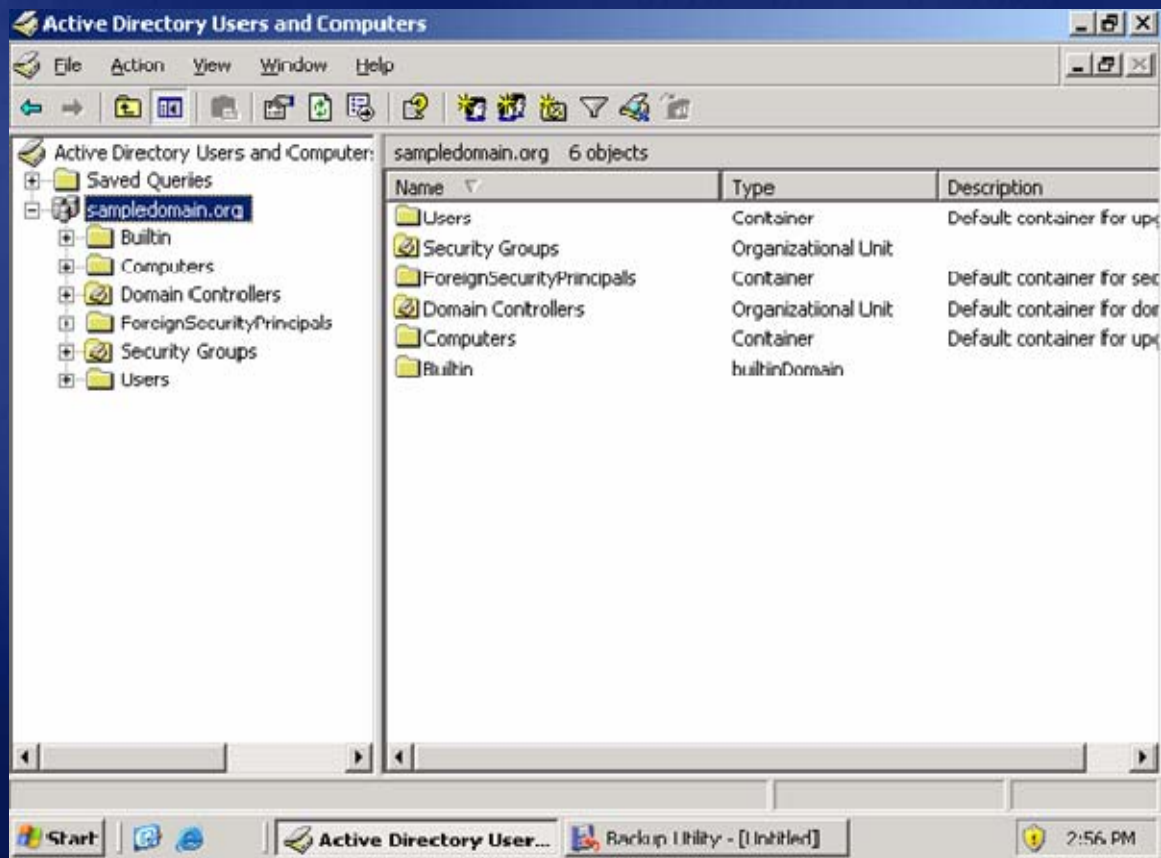












Windows Advanced Options Menu

Please select an option:

Safe Mode

Safe Mode with Networking

Safe Mode with Command Prompt

Enable Boot Logging

Enable VGA Mode

Last Known Good Configuration (your most recent settings that worked)

Directory Services Restore Mode (Windows domain controllers only)

Debugging Mode

Disable automatic restart on system failure

Start Windows Normally

Reboot

Use the up and down arrow keys to move the highlight to your choice.



Microsoft (R) Windows (R) Version 5.2 (Build 3790: Service Pack 1)  
1 system Processor [300 MB Memory]  
The system is booting in safemode - Directory Services Repair

Safe Mode

Microsoft (R) Windows (R) (Build 3790: Service Pack 1)

Safe Mode

Log On to Windows



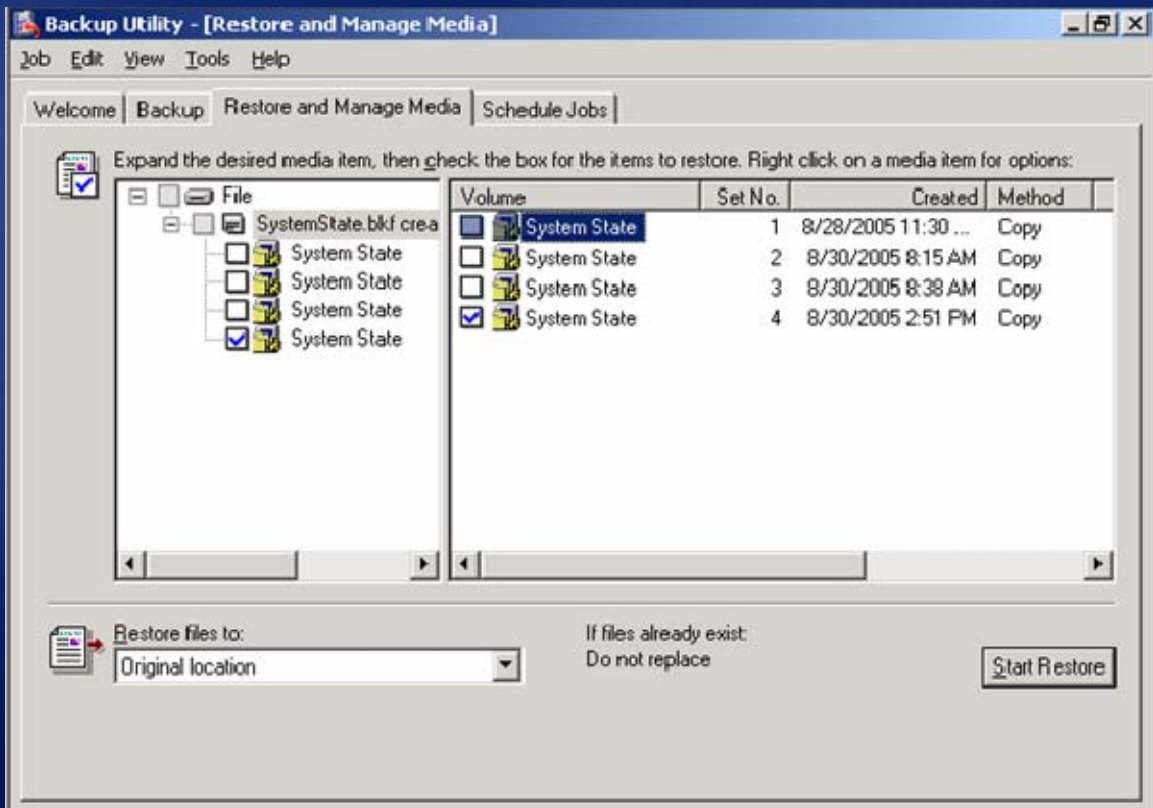
Copyright © 1985-2003 Microsoft Corporation Microsoft

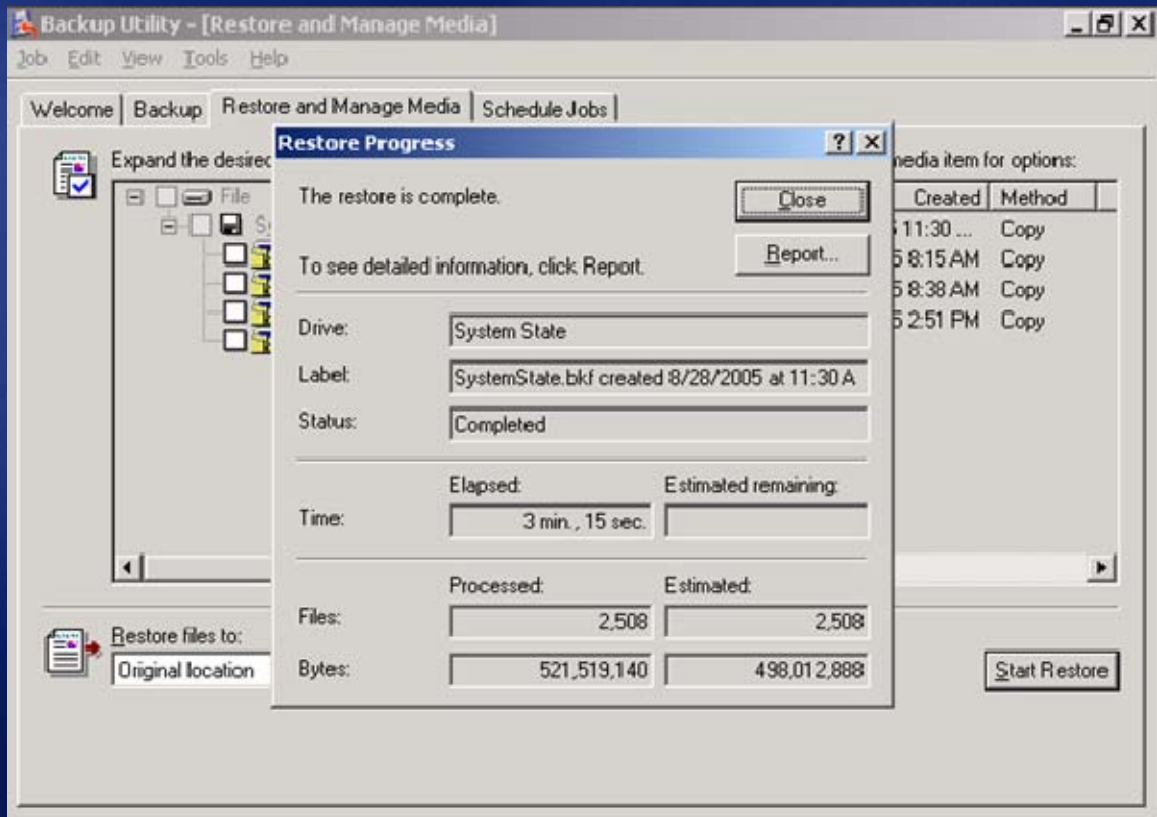
User name:

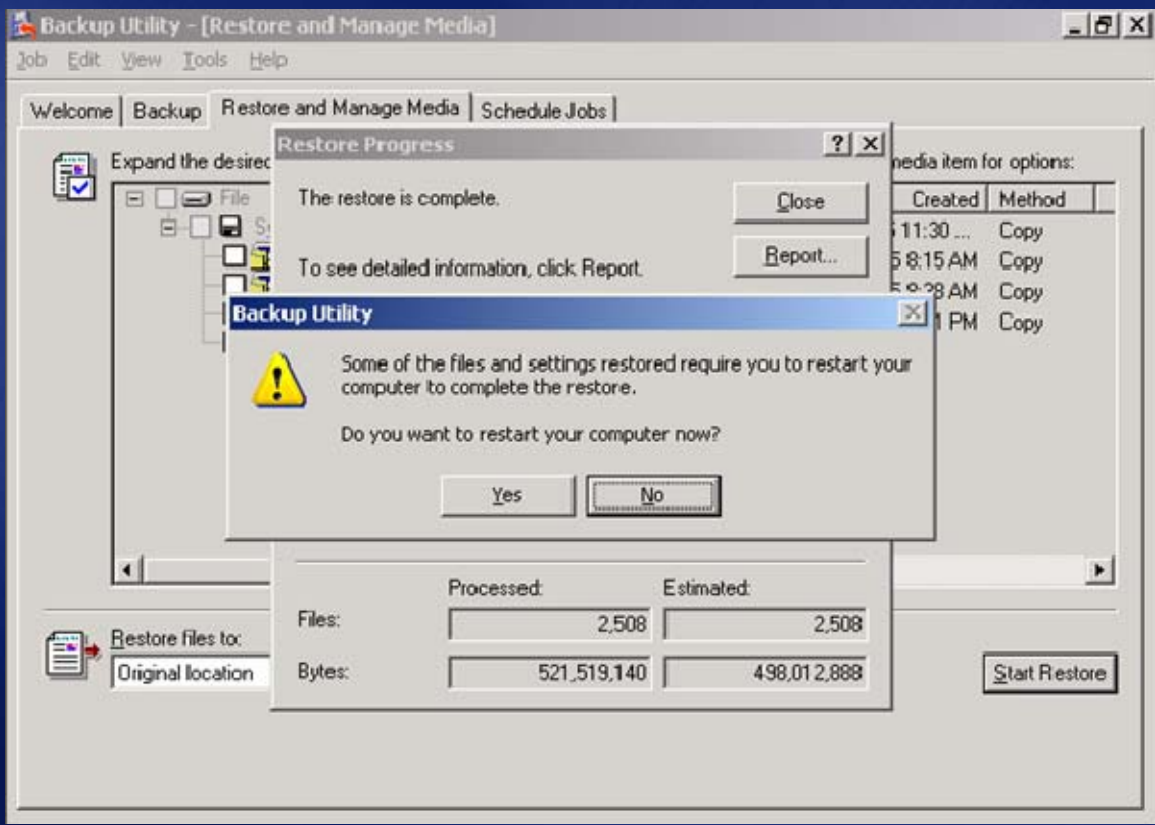
Password:

Safe Mode

Safe Mode









```
Command Prompt - ntdsutil
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ntdsutil
ntdsutil: ?

? - Show this help information
Authoritative restore - Authoritatively restore the DIT database
Configurable Settings - Manage configurable settings
Domain management - Prepare for new domain creation
Files - Manage NDS database files
Help - Show this help information
LDAP policies - Manage LDAP protocol policies
Metadata cleanup - Clean up objects of decommissioned servers
Popups %s - (en/dis)able popups with "on" or "off"
Quit - Quit the utility
Roles - Manage NDS role owner tokens
Security account management - Manage Security Account Database - Duplicate
D Cleanup
Semantic database analysis - Semantic Checker
Set DSRM Password - Reset directory service restore mode administrator account password


ntdsutil: authoritative restore
```

Command Prompt - ntdsutil

```
? - Show this help information
Create ldif file(s) from %s - Creates ldif file(s) using specified
                             authoritatively restored objects list
                             to recreate back-links of those objects.
Help - Show this help information
List NC CRs - Lists Partitions and cross-refs. You need
              the cross-ref of a Application Directory
              Partition to restore it.
Quit - Return to the prior menu
Restore database - Authoritatively restore entire database
Restore database verinc %d - ... and override version increase
Restore object %s - Authoritatively restore an object
Restore object %s verinc %d - ... and override version increase
Restore subtree %s - Authoritatively restore a subtree
Restore subtree %s verinc %d - ... and override version increase
```

authoritative restore: restore subtree ou=Executives,dc=sampldomain,dc=org

Authoritative Restore Confirmation Dialog

 Are you sure you want to perform this Authoritative Restore?

```
Command Prompt - ntdsutil
Restore subtree %s - Authoritatively restore a subtree
Restore subtree %s verinc %d - ... and override version increase

authoritative restore: restore subtree ou=Executives,dc=sampldomain,dc=org
Opening DIT database... Done.

The current time is 08-30-05 15:17.11.
Most recent database update occurred at 08-30-05 14:44.26.
Increasing attribute version numbers by 100000.

Counting records that need updating...
Records found: 0000000100
Done.

Found 100 records to update.

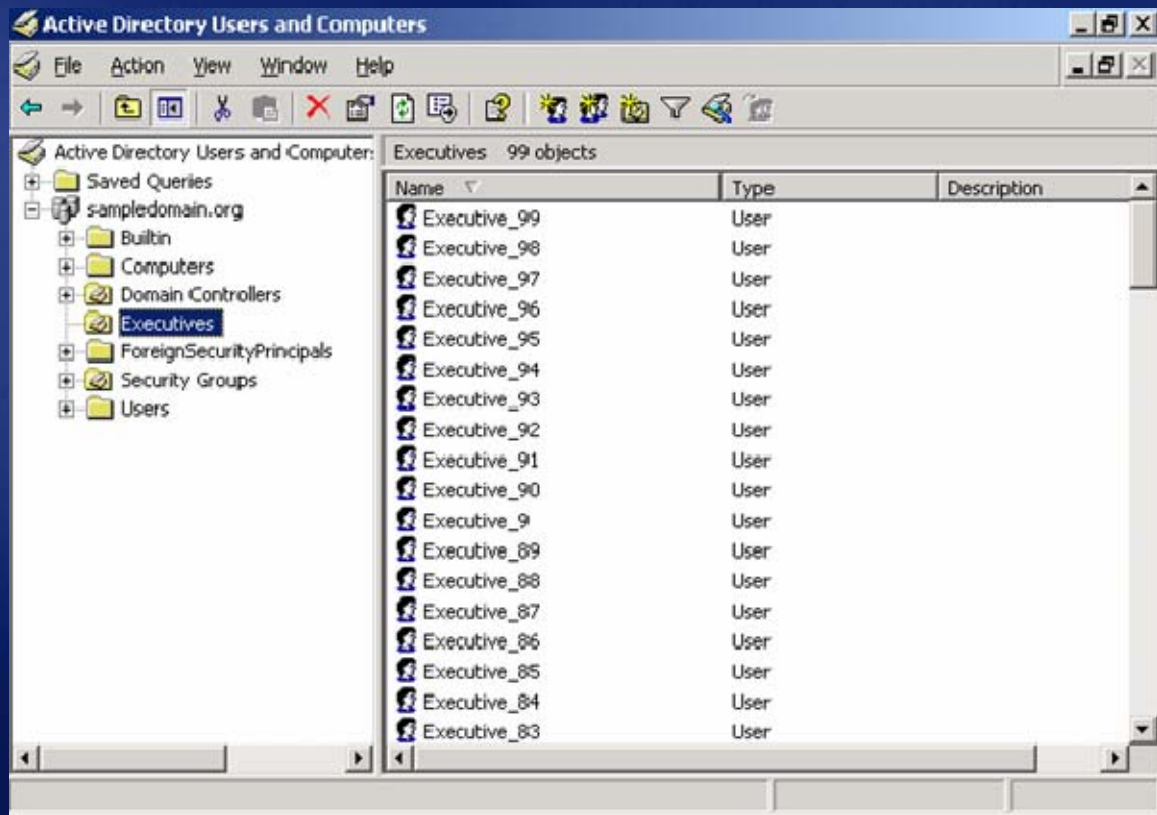
Updating records...
Records remaining: 0000000000
Done.

Successfully updated 100 records.

The following text file with a list of authoritatively restored objects has been
created in the current working directory:
ar_20050830-151711_objects.txt
None of the specified objects have back-links in this domain. No link restore
file has been created.

Authoritative Restore completed successfully.

authoritative restore: _
```



# demo

**Object Restore Using a  
3<sup>rd</sup> Party Object Recovery Tool  
and Windows 2003**

# Recovery Manager Console

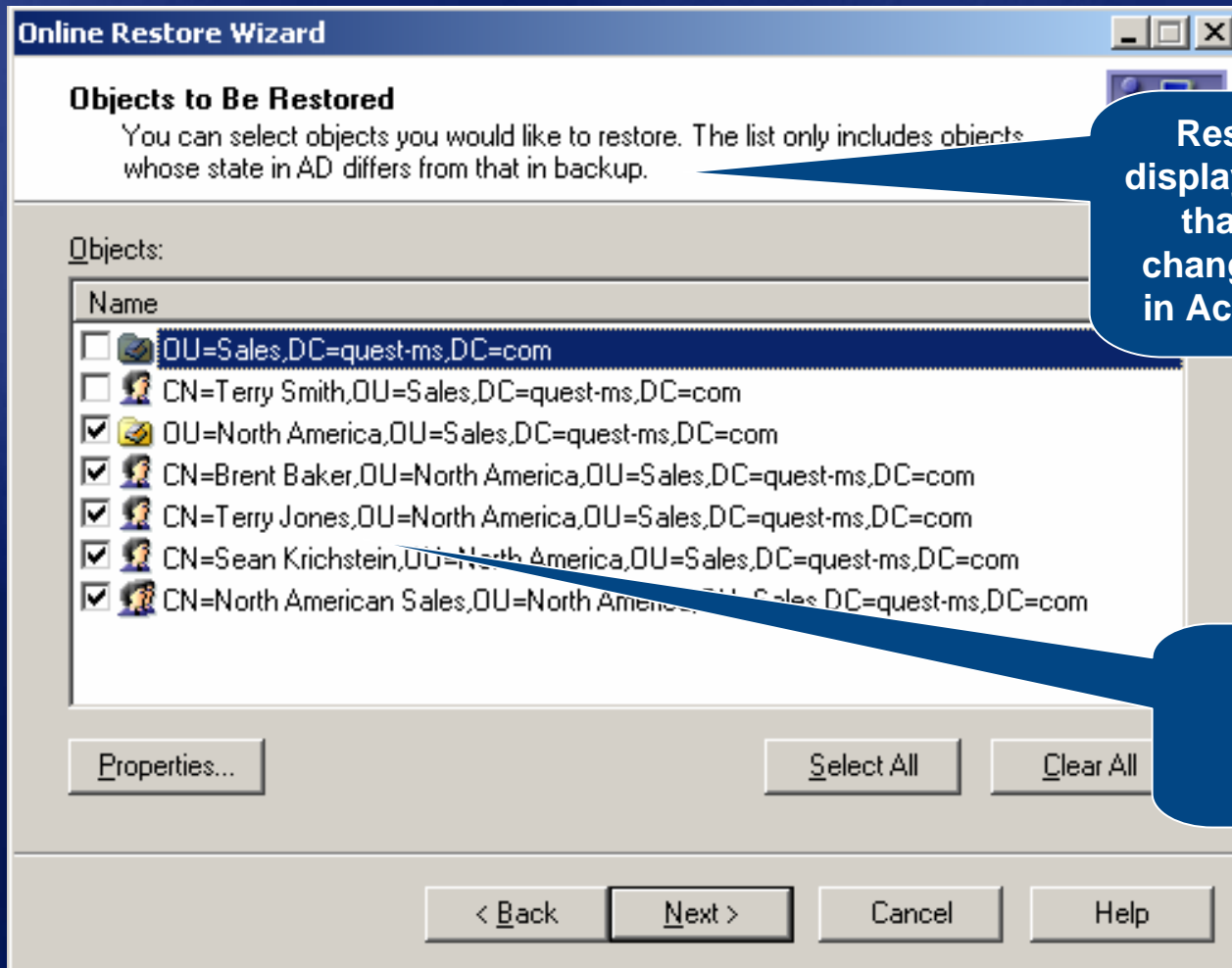
The screenshot displays the Quest Recovery Manager for Active Directory console. The interface includes a menu bar (Console, Window, Help), a toolbar with various icons, and a main workspace divided into a tree view on the left and a data table on the right.

**Tree View:**

- Recovery Manager for Active Directory
  - Computer Collections
  - Active Directory
    - Forest "wm-quest.com"
      - All Domain Controllers
      - Sites
      - Domains
    - Sessions
      - 12/29/2004 1:40:52 PM - <N/A>
      - 1/5/2005 10:34:36 AM - <N/A>
      - 1/5/2005 11:00:26 AM - <N/A>
    - Backups
      - Active Directory
      - ADAM

DC	Domain	Date	Size	Path	Site	Age
questdc2k.wm-quest.com	wm-quest.com	12/29/2004	8 MB	C:\D...	CN=Default-First-Si...	6 days
questdc2k.wm-quest.com	wm-quest.com	1/5/2005	6 MB	C:\D...	CN=Default-First-Si...	1 hour
questdc2k.wm-quest.com	wm-quest.com	1/5/2005	6 MB	C:\D...	CN=Default-First-Si...	1 hour

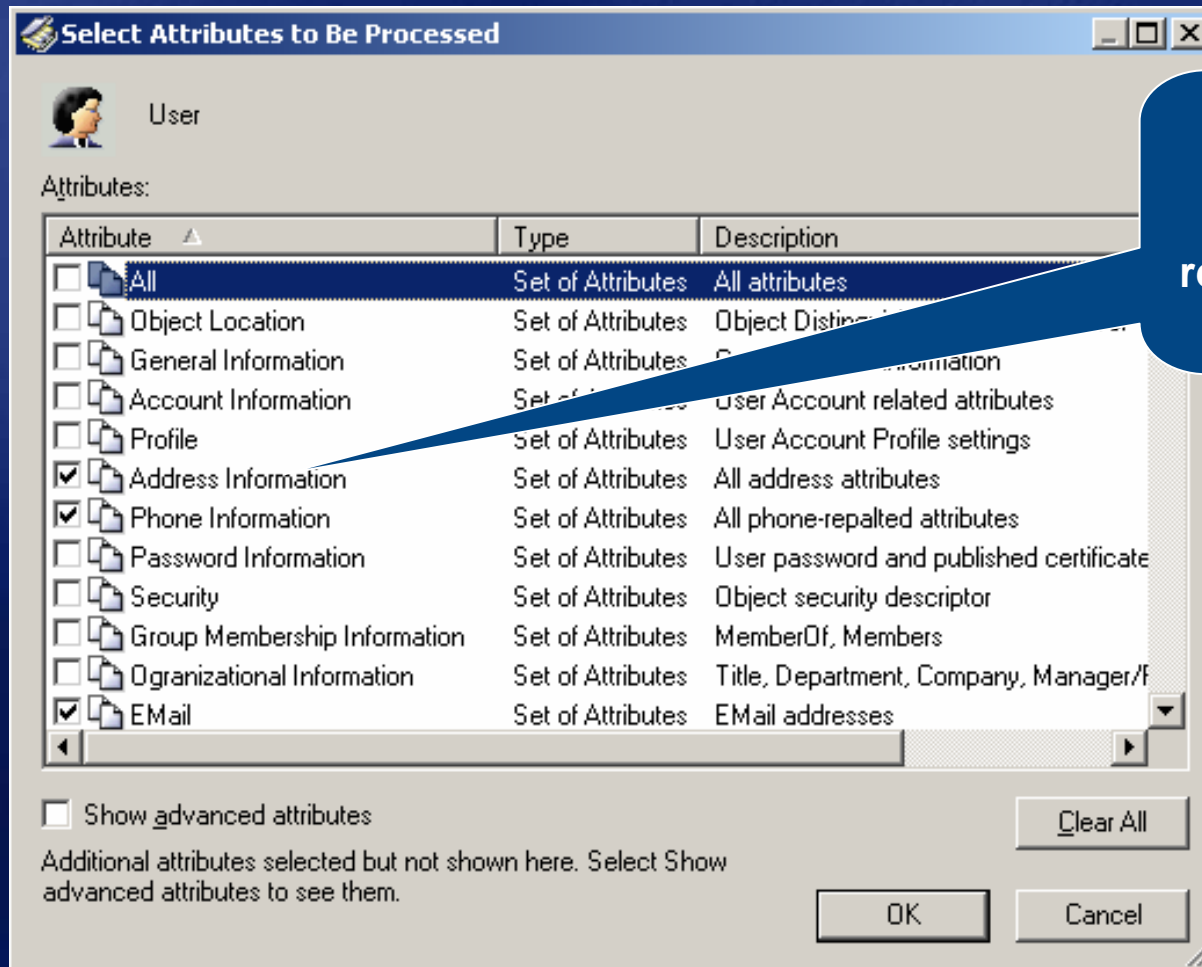
# Granular Restore



Restore Wizard displays only objects that have been changed or deleted in Active Directory.

Granular selection of objects to restore

# Granular Attribute Restore



**Granular selection of attributes to restore/rollback for the object**



# Comparison Reporting

Reports provide a list of all objects that have been changed or deleted in Active Directory.

Name	State	Type
CN=Brent Baker,OU=North America,DC=quest-ms,DC=com	Deleted	User
CN=North American Sales,OU=North America,DC=quest-ms,DC=com	Deleted	Group
CN=Sean Krichstein,OU=North America,DC=quest-ms,DC=com	Deleted	User
CN=Terry Jones,OU=North America,OU=Sales,DC=quest-ms,DC=com	Deleted	User
CN=Terry Smith,OU=Sales,DC=quest-ms,DC=com	Changed	User
OU=North America,OU=Sales,DC=quest-ms,DC=com	Deleted	Organizational Unit
OU=Sales,DC=quest-ms,DC=com	Changed	Organizational Unit

# Comparison Reporting

Reports provide a list of all objects that have been changed or deleted in Active Directory.

Name	State	Type
CN=Brent Baker,OU=North America,DC=quest-ms,DC=com	Deleted	User
CN=North American Sales,OU=Sales,DC=quest-ms,DC=com	Deleted	Group
CN=Sean Krichstein,OU=North America,DC=quest-ms,DC=com	Deleted	User
CN=Terry Jones,OU=North America,OU=Sales,DC=quest-ms,DC=com	Deleted	User
CN=Terry Smith,OU=Sales,DC=quest-ms,DC=com	Changed	User
OU=North America,OU=Sales,DC=quest-ms,DC=com	Deleted	Organizational Unit
OU=Sales,DC=quest-ms,DC=com	Changed	Organizational Unit

## Object Details - Microsoft Internet Explorer

**CN=Terry Smith,OU=Sales,DC=quest-ms,DC=com**

Type: User

State: Changed

Attribute

State

Value

Office Location

Added

Ottawa

Drill down in the report to determine exactly what data was modified.

# Object Recovery

## Best Practices

- That 'spare DC' would come in handy
- **Never** auth restore whole database
- Remember DSRM admin password
  - Every DC's is potentially different
- Auth restore is not the end of it
  - You have other tasks such as restoring group memberships
- Expedite restore by backing to disk
- Backup Group Policy using GPMC

# Agenda

- Planning for the Worst
- **Practical Recovery Examples**
  - Object Recovery
  - **Single DC Recovery**
  - Multi DC Recovery
  - Forest Wide Recovery
- Summary
- Questions

# Single DC Recovery

## Problem statement

- **Lost single DC to AD failure or hardware failure**
- **Originating changes that haven't replicated to other DCs are lost**
- **Temporary loss of FSMO/GC/DNS Role**
- **Increased workload on other DCs**

# Single DC Recovery

## Recovery method

- **Method I: Restore DC from its own backup**
  - Boot into DSRM or reinstall OS
  - Restore from backup
  - Reboot
- **Method II: Promote DC**
  - Force demote DC or reinstall OS
  - Clean metadata of old DC
  - Install AD:
    - Via replication
    - From backup media (Windows Server 2003 only)
  - Seize FSMO role (if required)

# Single DC Recovery

## Pros and Cons

- **Method I**

- **Restore is faster than replication**
- **Fewer moving parts**
  - **No dcpromo; No metadata cleanup**
  - **No FSMO role seizure required (unless machine is unavailable for long time)**

- **Method II**

- **Good backup of failed DC not available**
- **Upgrading to different hardware**

# Single DC Recovery

## Best Practices

- **Have sufficient DCs to handle client workload in absence of one DC**
- **Have quick access to backup media**
  - **Store a recent backup on disk**
- **Have a well defined procedure and personnel who have rehearsed the process**
- **Have DSRM password handy (or OS CD)**
- **Know which FSMO roles the machine has**
- **Know which applications/services are installed**



# Agenda

- Planning for the Worst
- **Practical Recovery Examples**
  - Object Recovery
  - Single DC Recovery
  - **Multi DC Recovery**
  - Forest Wide Recovery
- Summary
- Questions

# Multi-DC Recovery

## Problem statement

- Lost more than 1 DC in the domain (potentially the whole domain)
- Physical location housing site is partially or completely destroyed by catastrophic event (fire)
- Temporary loss (or slowness) of operations in that site
  - Clients will find other DCs (potentially in other sites)

# Multi-DC Recovery

## Problem statement

- **Story: Louisiana High Water**

# Multi-DC Recovery

## Recovery method

- Same as single DC recovery done multiple times
- If whole domain is destroyed, then following additional steps need to be performed
  - During restore operation, mark SYSVOL of exactly 1 DC as “primary”
    - So that SYSVOL data is pushed to other DCs
  - Raise RID Available Pool by a large value
    - So that new Security Principals get fresh SIDs

# Multi-DC Recovery

## Best Practices

- Provide redundancy by not having entire domain in a single physical location
- Backup multiple DCs (GCs) per domain, in different physical locations
- Store backups securely offsite
- Have similar hardware available
- Have a well defined procedure and copy of your AD infrastructure

# Agenda

- Planning for the Worst
- **Practical Recovery Examples**
  - Object Recovery
  - Single DC Recovery
  - Multi DC Recovery
  - **Forest Wide Recovery**
- Summary
- Questions

# Forest Recovery

## Problem statement

- **Every** DC in the forest is “**affected**” by some replicated “**corruption**”
- Affected DCs might provide some level of service or none at all

# Forest Recovery

## Problem statement

- **Story: DC's "USE BY:xx-xx-xx" Date**

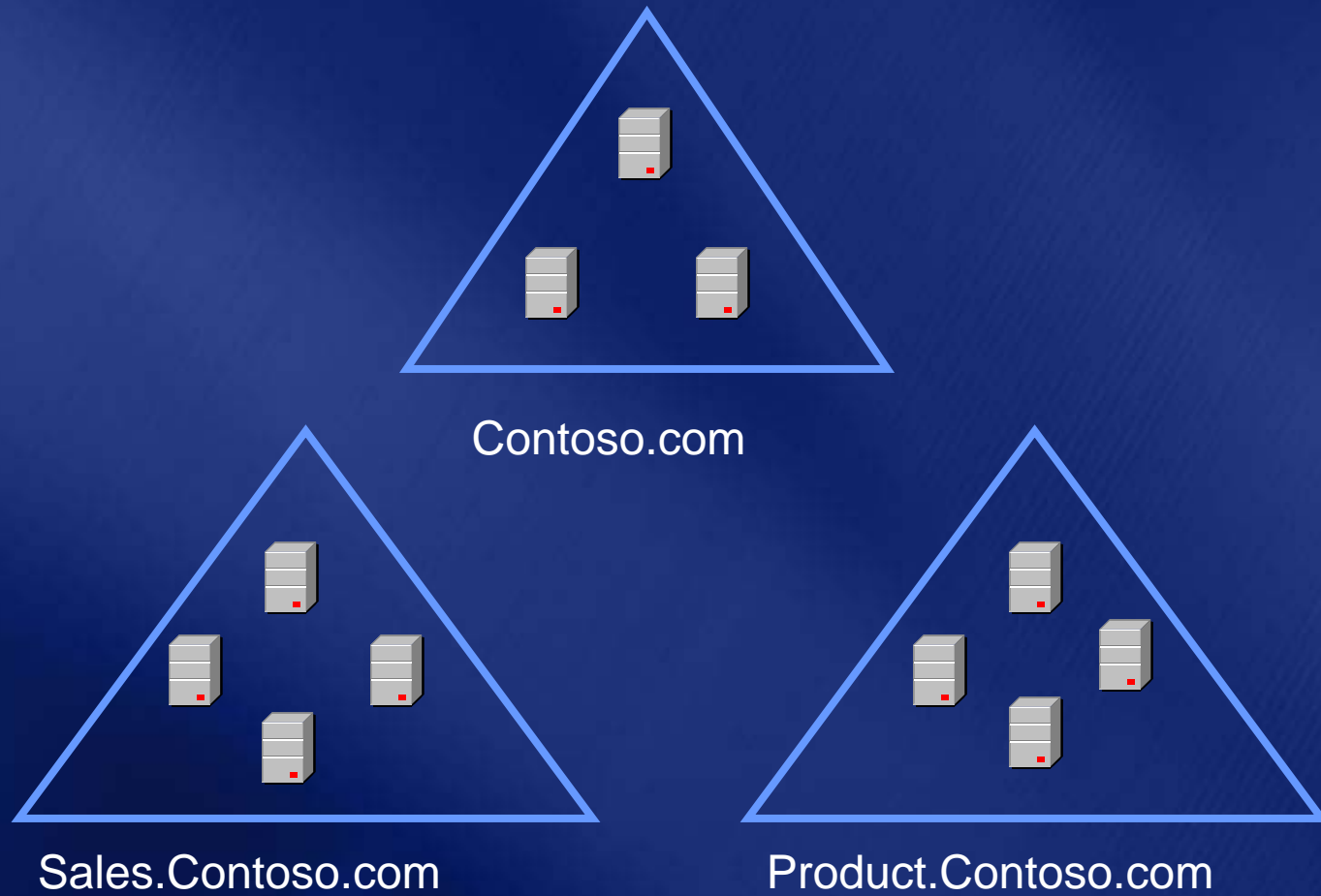


# Forest Recovery

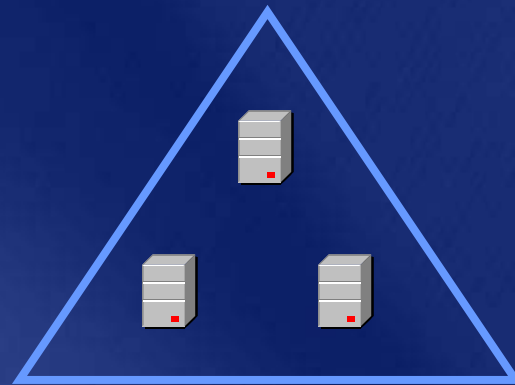
## Check your boundaries

- This type of disaster may warrant calling in outside help
- Remember my 'severed finger' analogy

# Working Forest

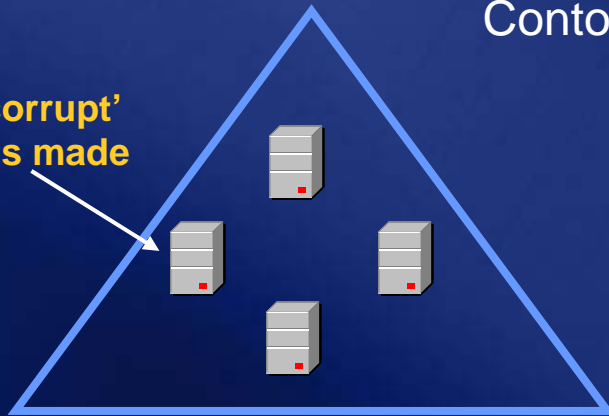


# Disaster Strikes

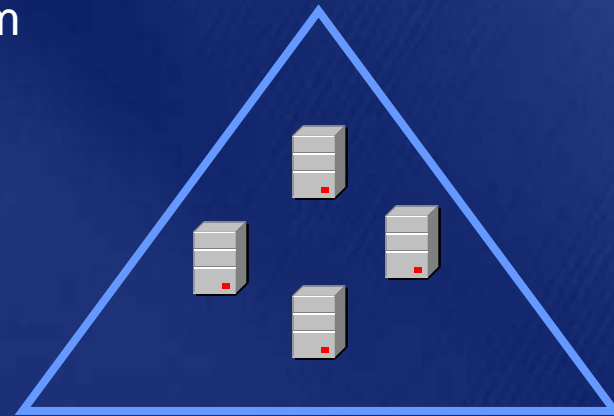


Contoso.com

Some 'corrupt' update is made



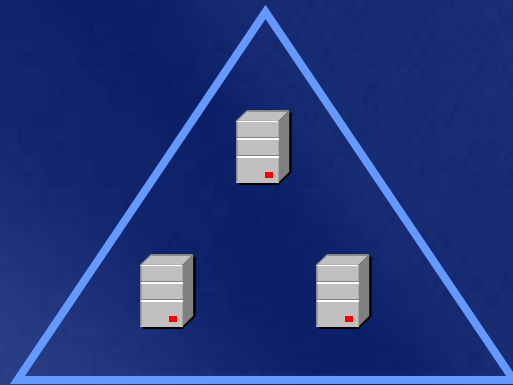
Sales.Contoso.com



Product.Contoso.com

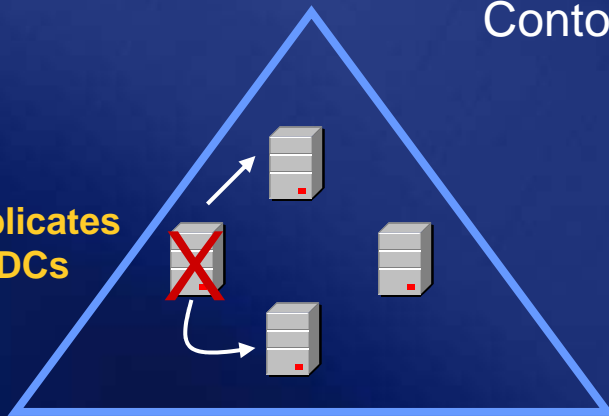
# “Corruption” Replicates

**X** Affected DCs

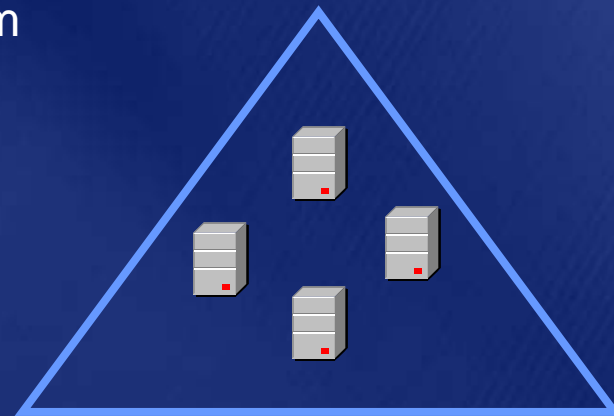


Contoso.com

Update replicates to partner DCs



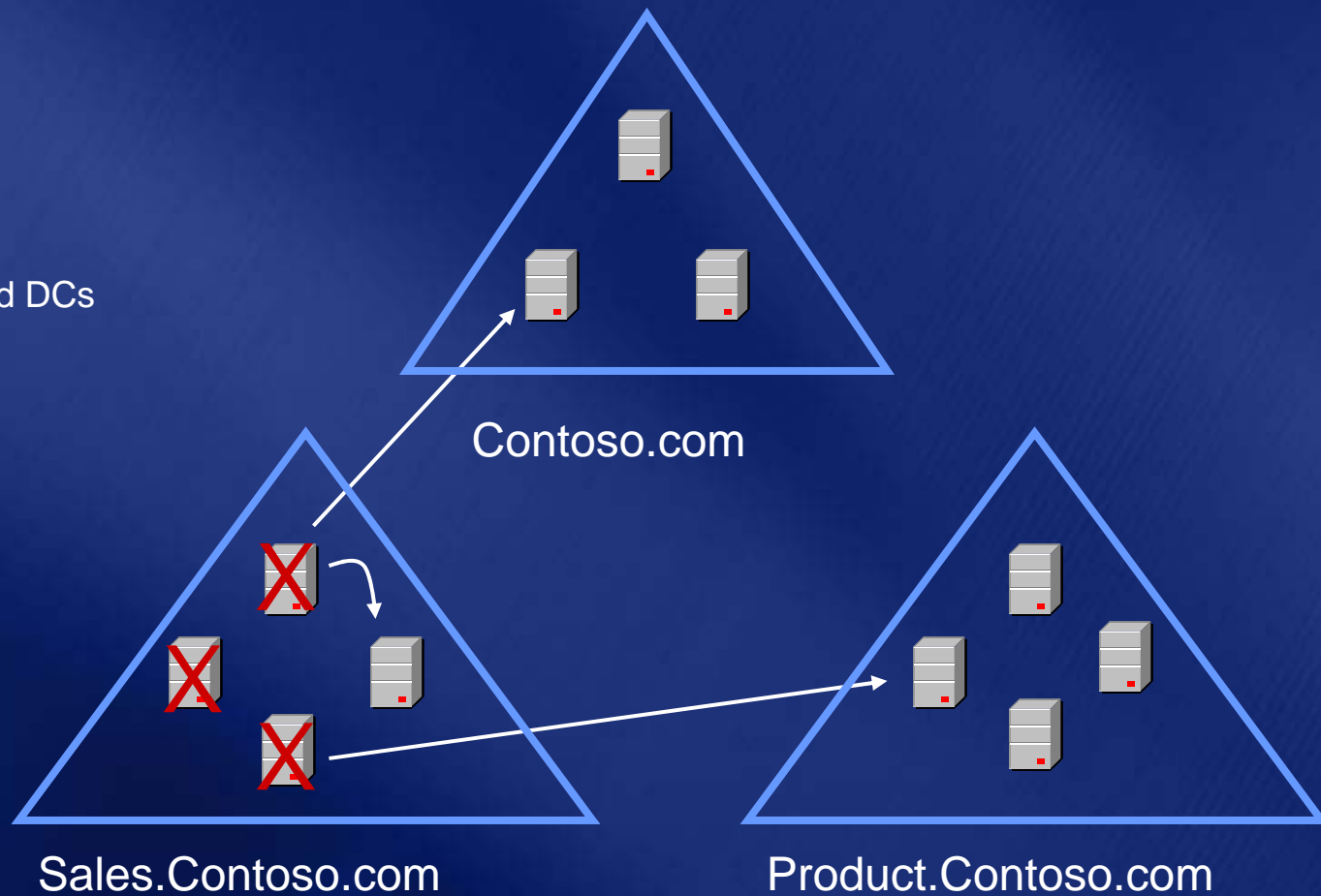
Sales.Contoso.com



Product.Contoso.com

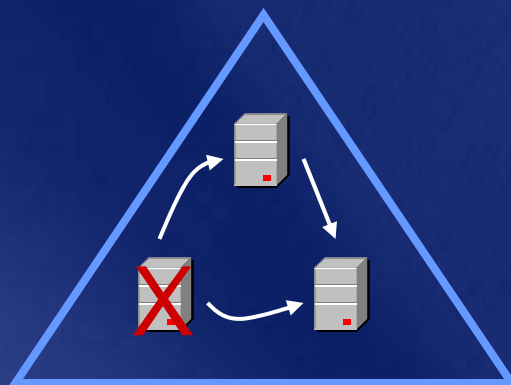
# “Corruption” Replicates

 Affected DCs

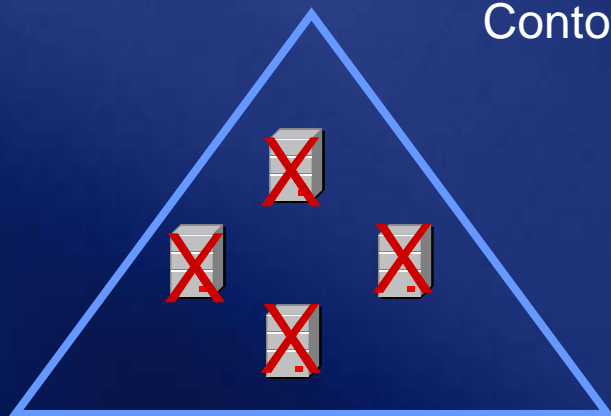


# “Corruption” Replicates

 Affected DCs



Contoso.com



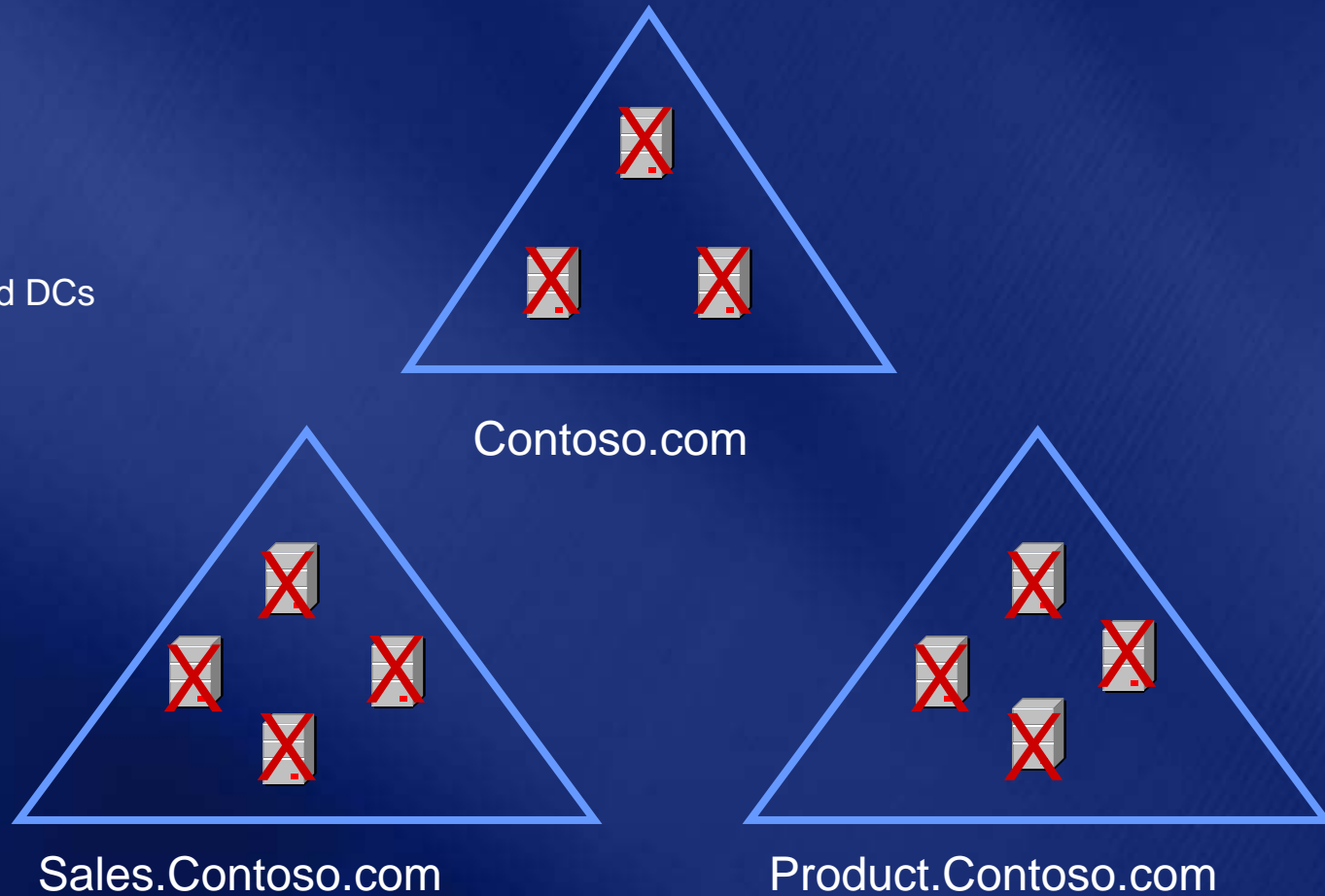
Sales.Contoso.com



Product.Contoso.com

# Entire Forest Is Affected

 Affected DCs



# Forest Recovery Considerations

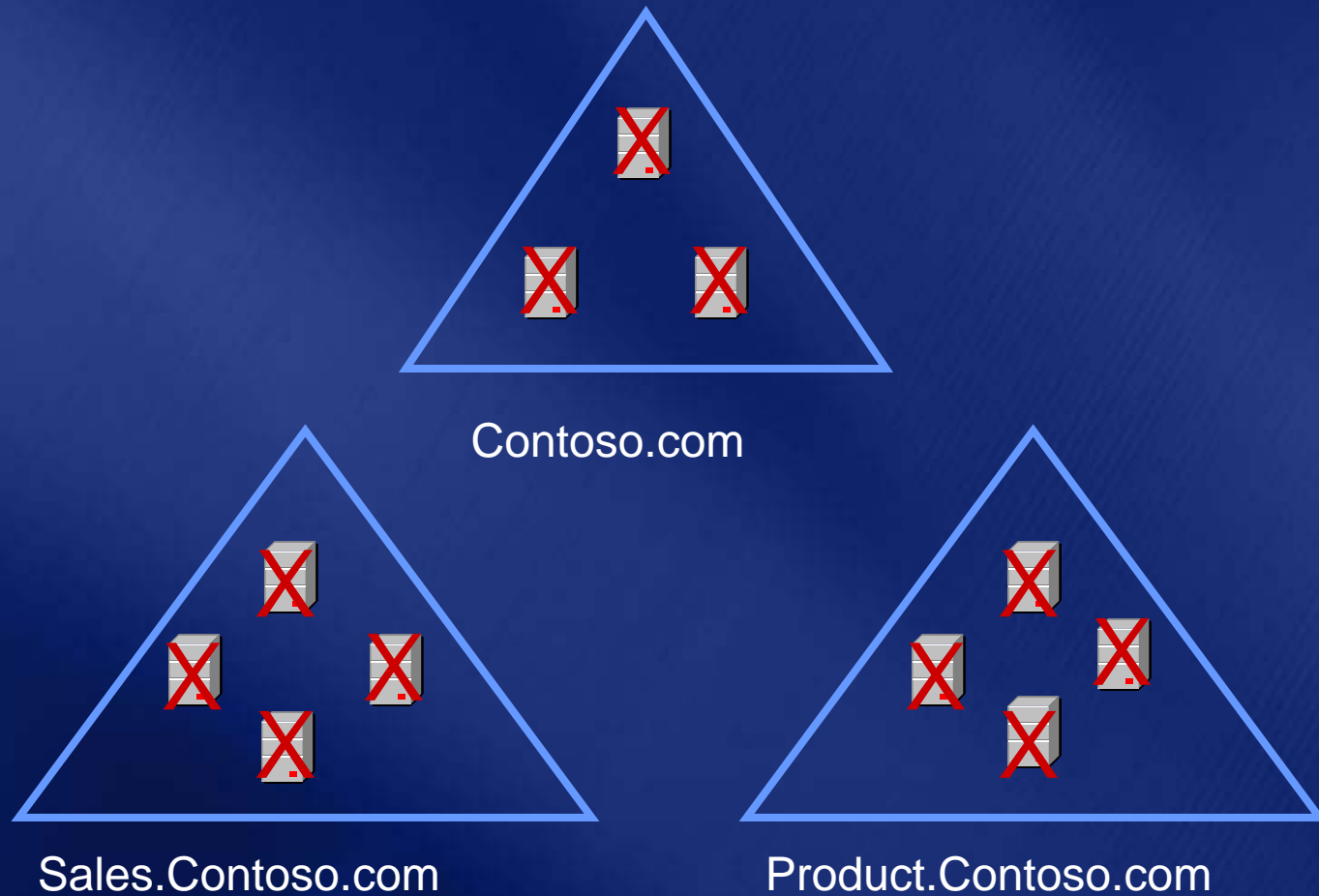
- Corruption can replicate from “affected” DCs to restored DCs
- Can’t shutdown all “affected” DCs before restored DCs are brought online
- Restore exactly 1 DC per domain from backup, because
  - The only thing worse than having to perform a forest recovery is having to perform it twice
  - Backups need to be tested for each DC you restore
  - Multiple DCs will have to be booted into isolation
  - You would have to perform the right recovery steps on each DC you restore



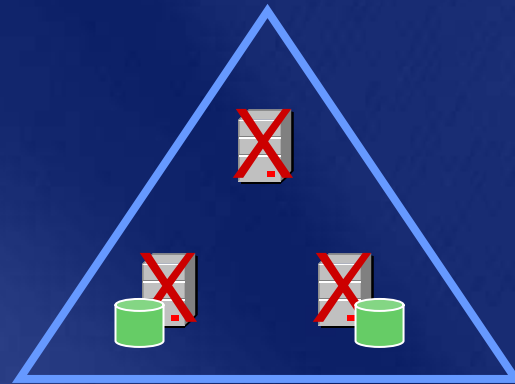
# Forest Recovery Considerations

- **Select a backup that is unaffected by the “corruption”**
- **If using AD integrated DNS, then preferably backup should be that of a DNS server**
- **Restore at least 1 GC, because without a GC:**
  - **Users/computers can't authenticate**
  - **Can't install a DC**
  - **Secure dynamic updates of DNS records fail**
  - **MS Exchange would not function**
- **Restoring a GC could result in lingering objects which would have to be cleaned later**

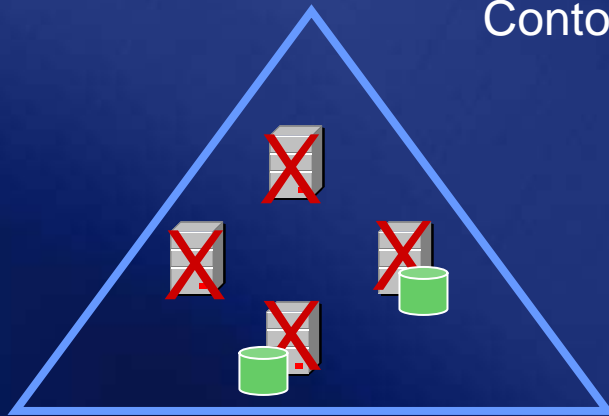
# Affected Forest



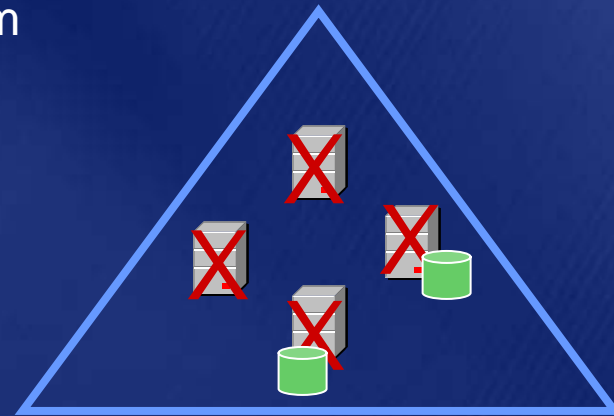
# 1. Identify Backups



Contoso.com

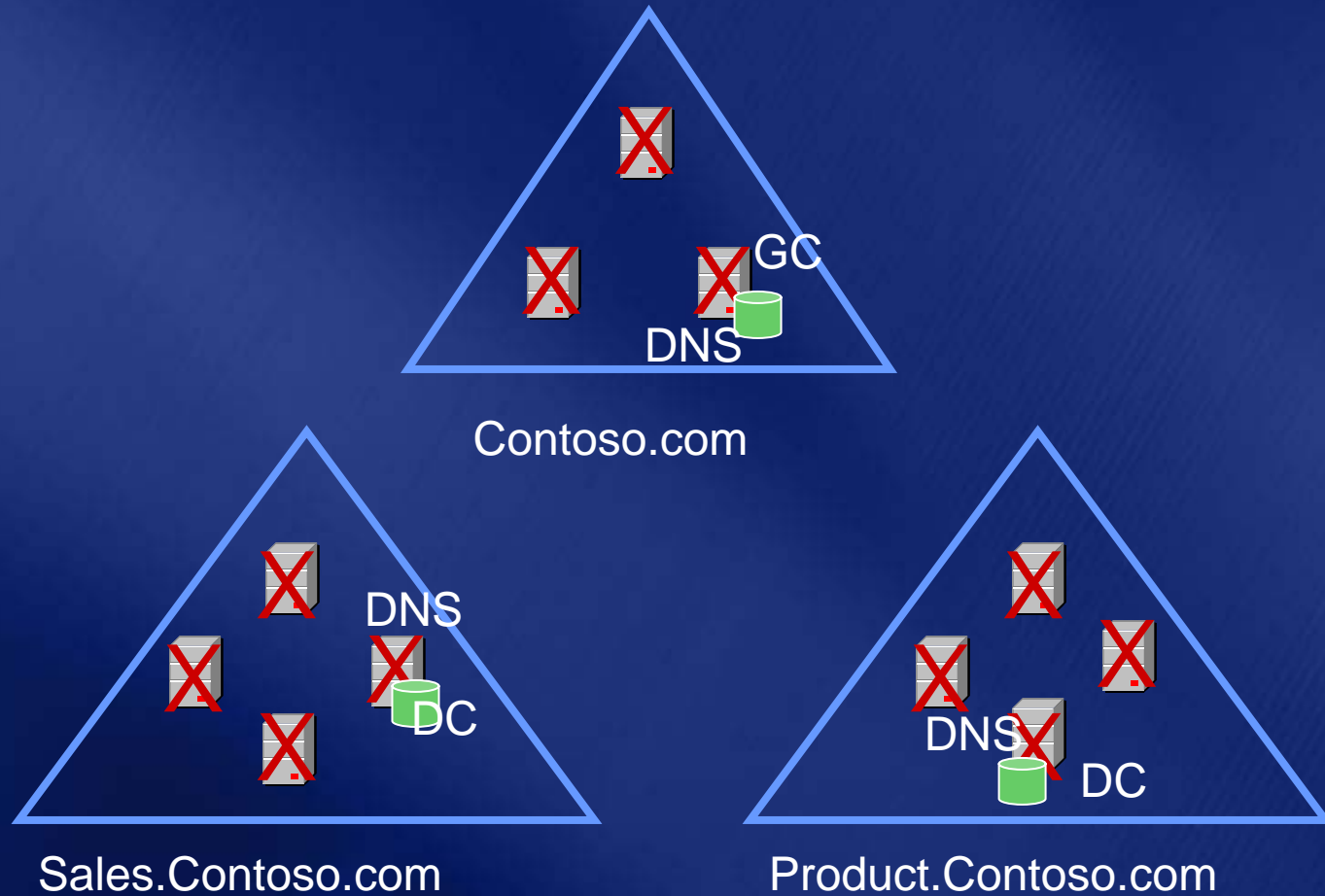


Sales.Contoso.com

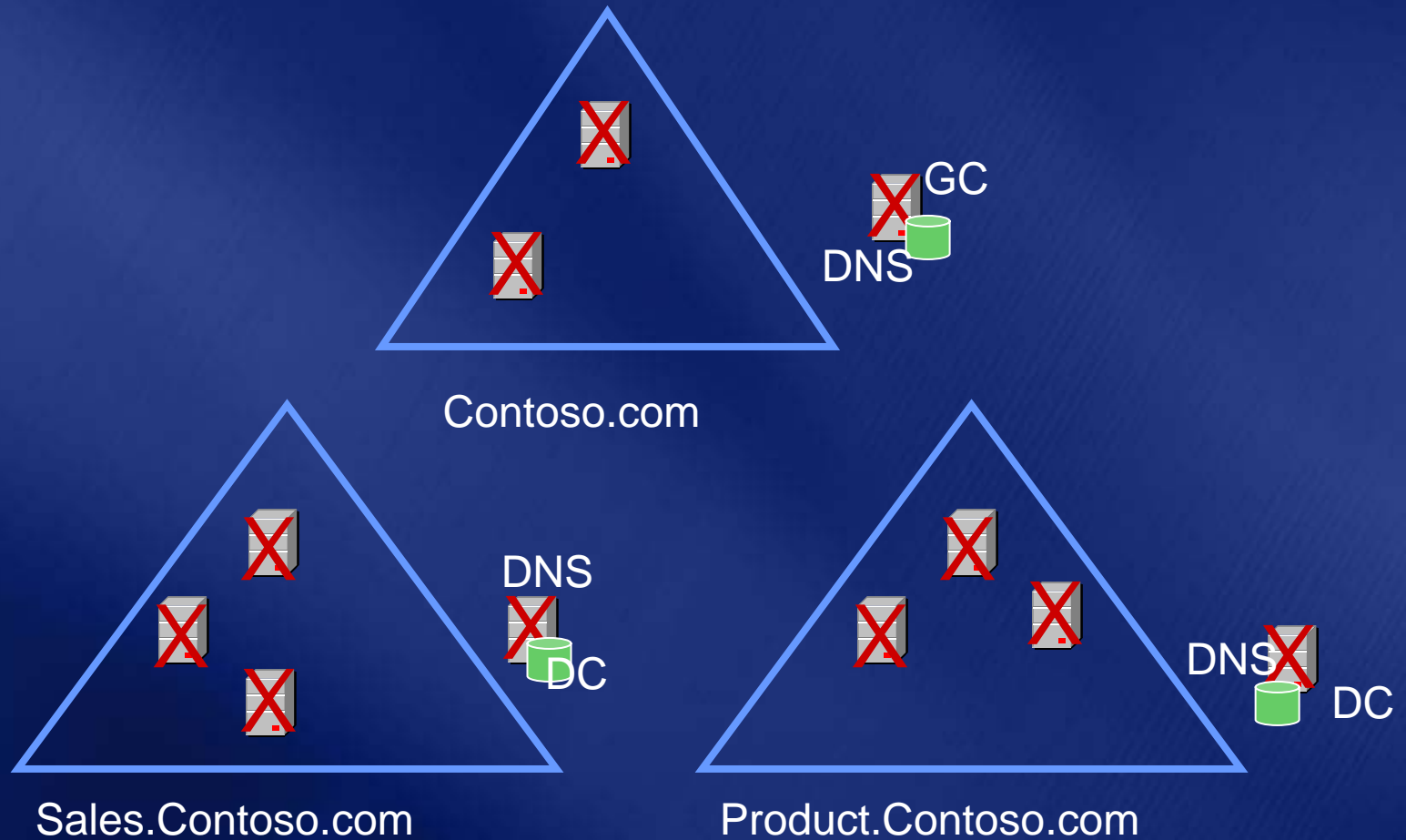


Product.Contoso.com

## 2. Select a Backup



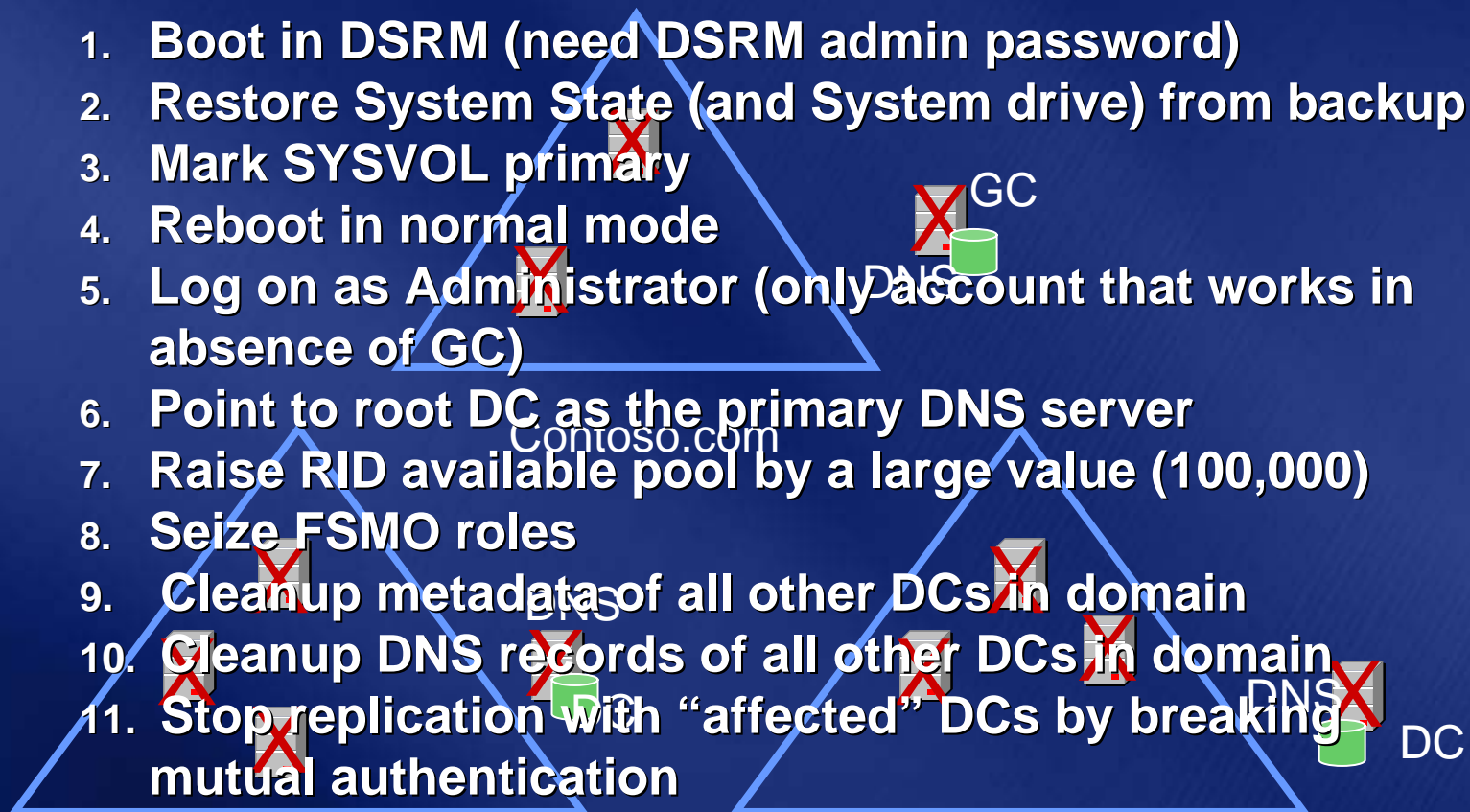
# 3. Isolate DC to Be Restored



# 4. Recover Isolated DC

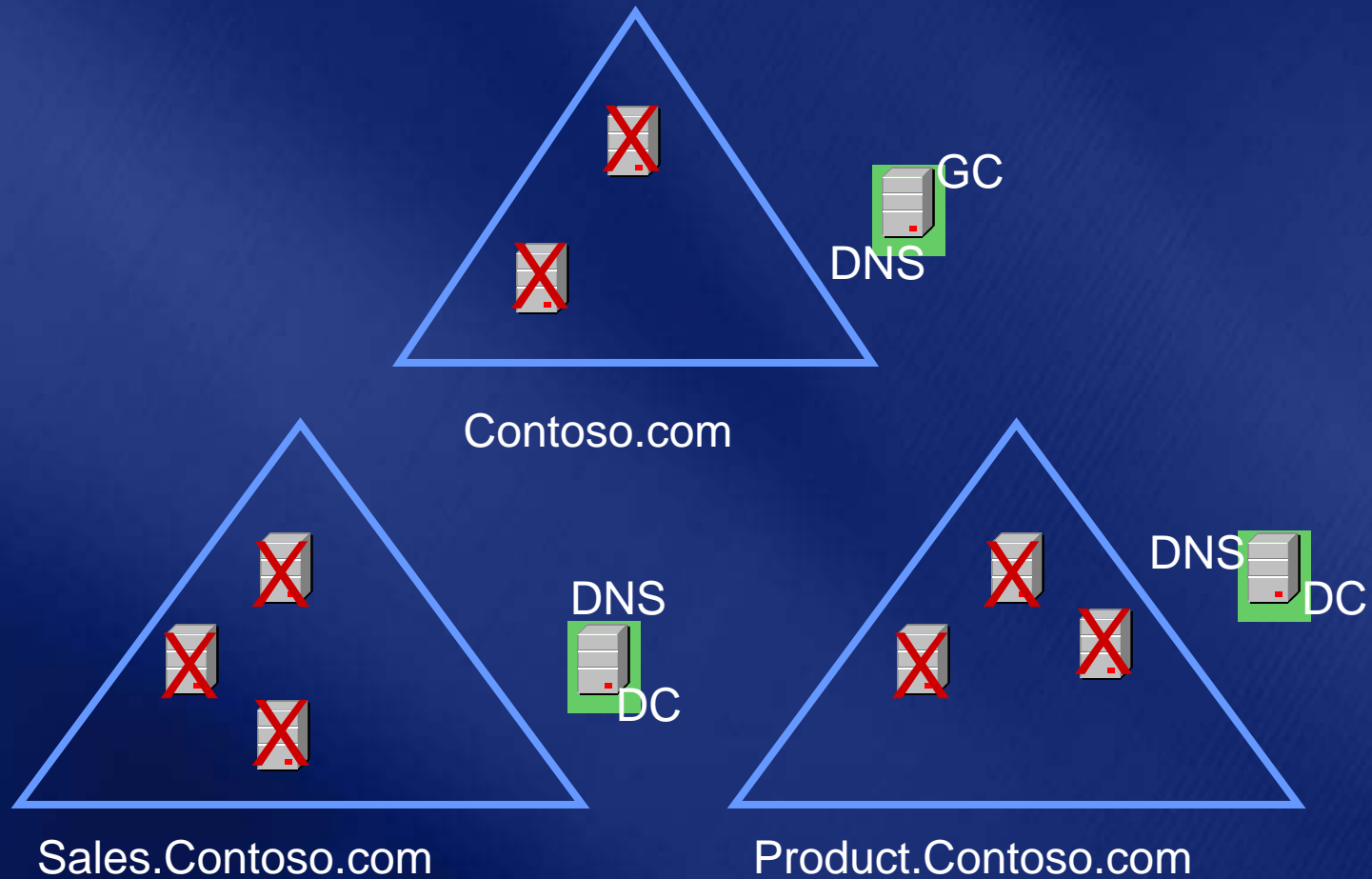
1. Boot in DSRM (need DSRM admin password)
2. Restore System State (and System drive) from backup
3. Mark SYSVOL primary
4. Reboot in normal mode
5. Log on as Administrator (only account that works in absence of GC)
6. Point to root DC as the primary DNS server
7. Raise RID available pool by a large value (100,000)
8. Seize FSMO roles
9. Cleanup metadata of all other DCs in domain
10. Cleanup DNS records of all other DCs in domain
11. Stop replication with "affected" DCs by breaking mutual authentication

- Reset computer account password (twice)
- Reset krbtgt password
- Delete computer accounts of all other DCs in domain
- Reset trust password on one side of the trust (twice)



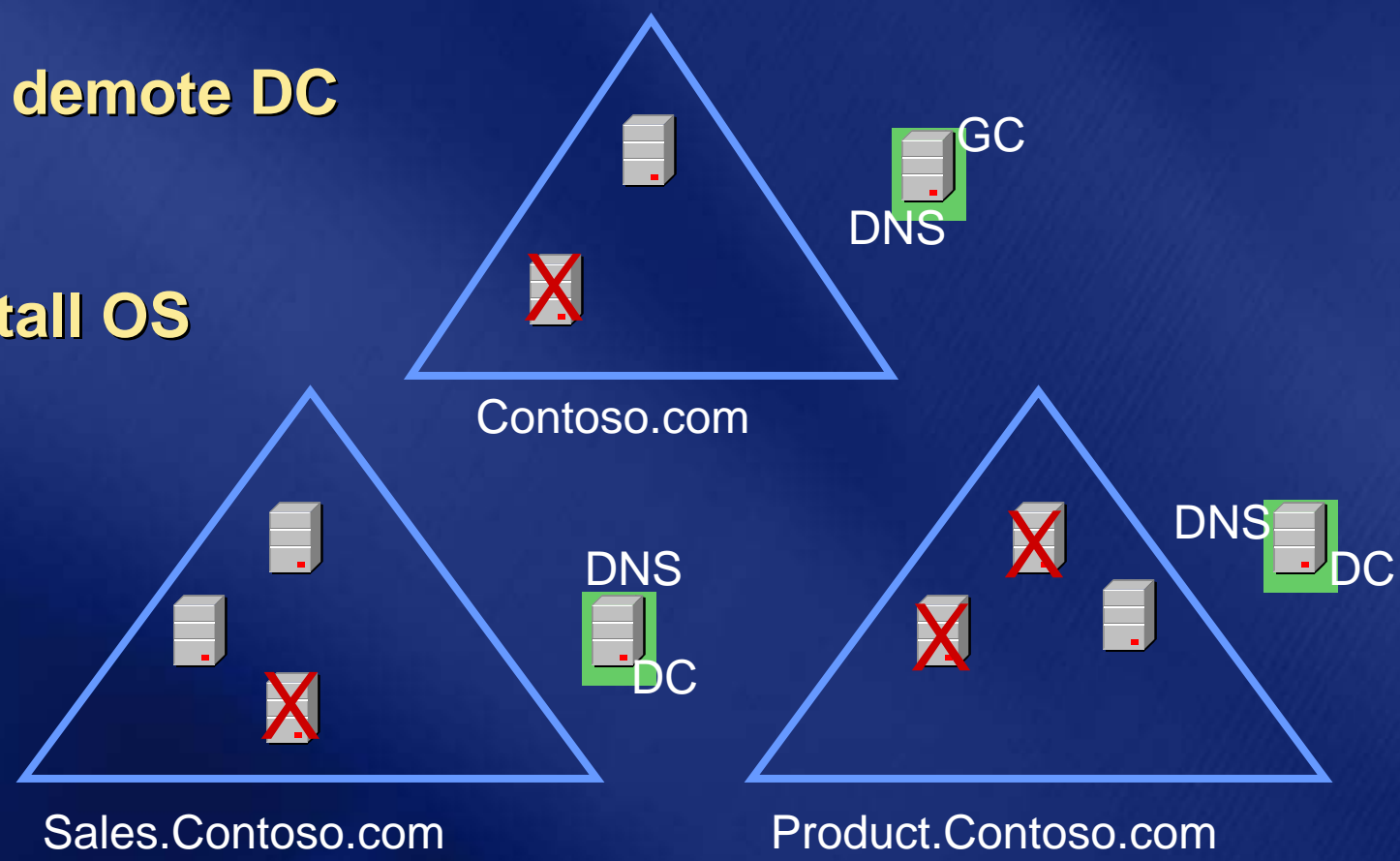
Sales.Contoso.com Product.Contoso.com

# 4. Recover Isolated DCs



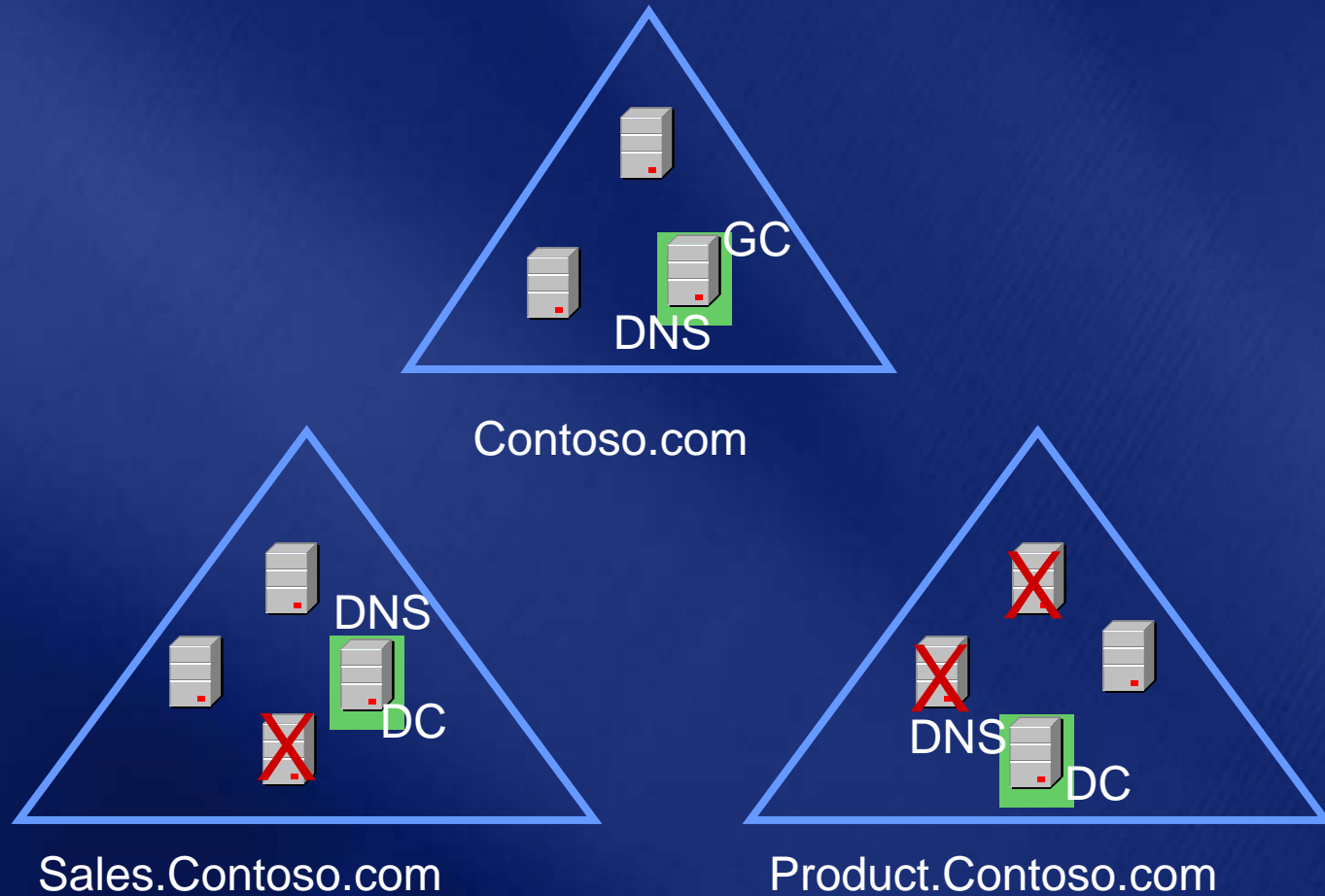
# 5. Remove AD From “Affected” DCs

Force demote DC  
or  
Reinstall OS

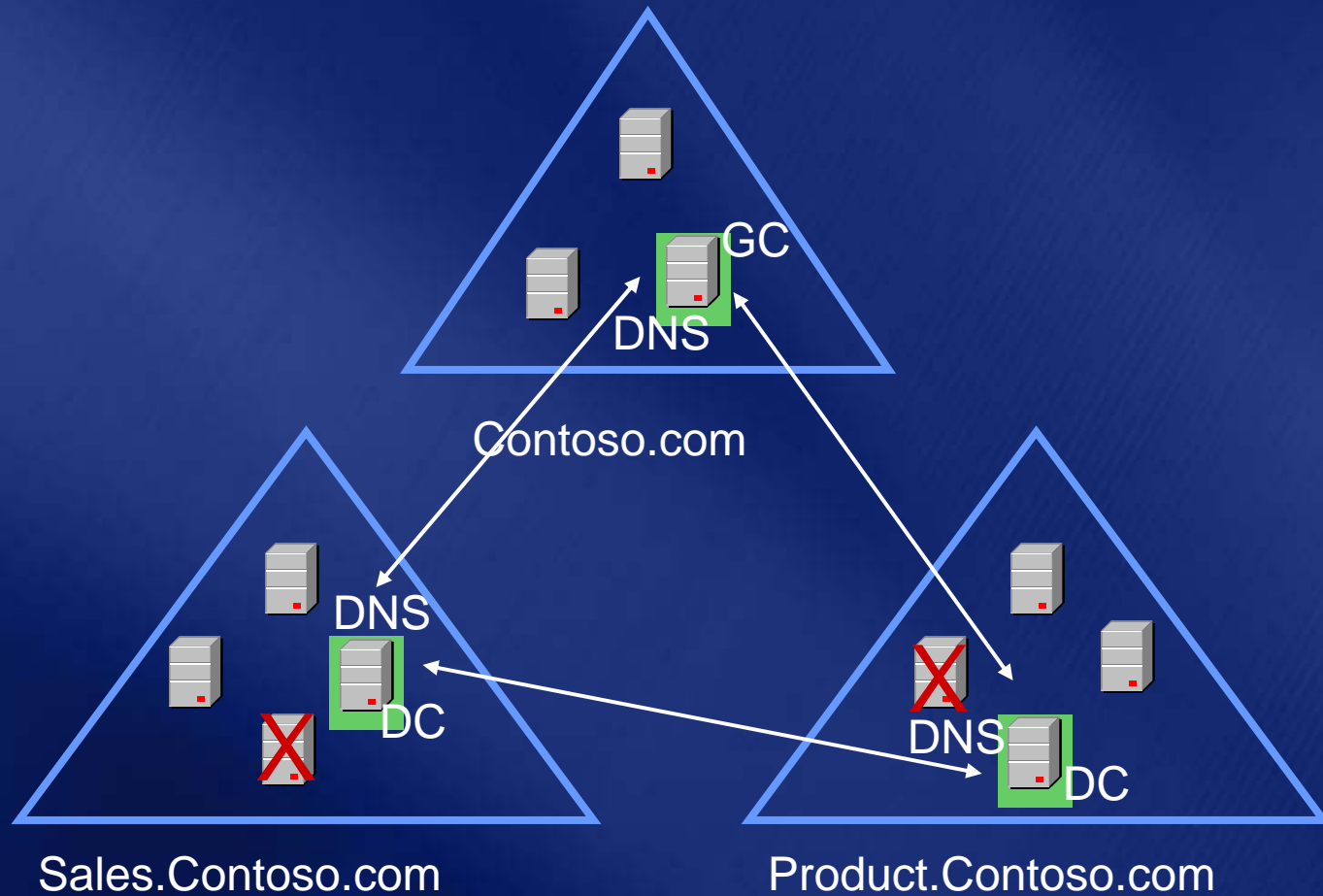




# 6. Bring Isolated DCs Online



# 7. Verify Replication

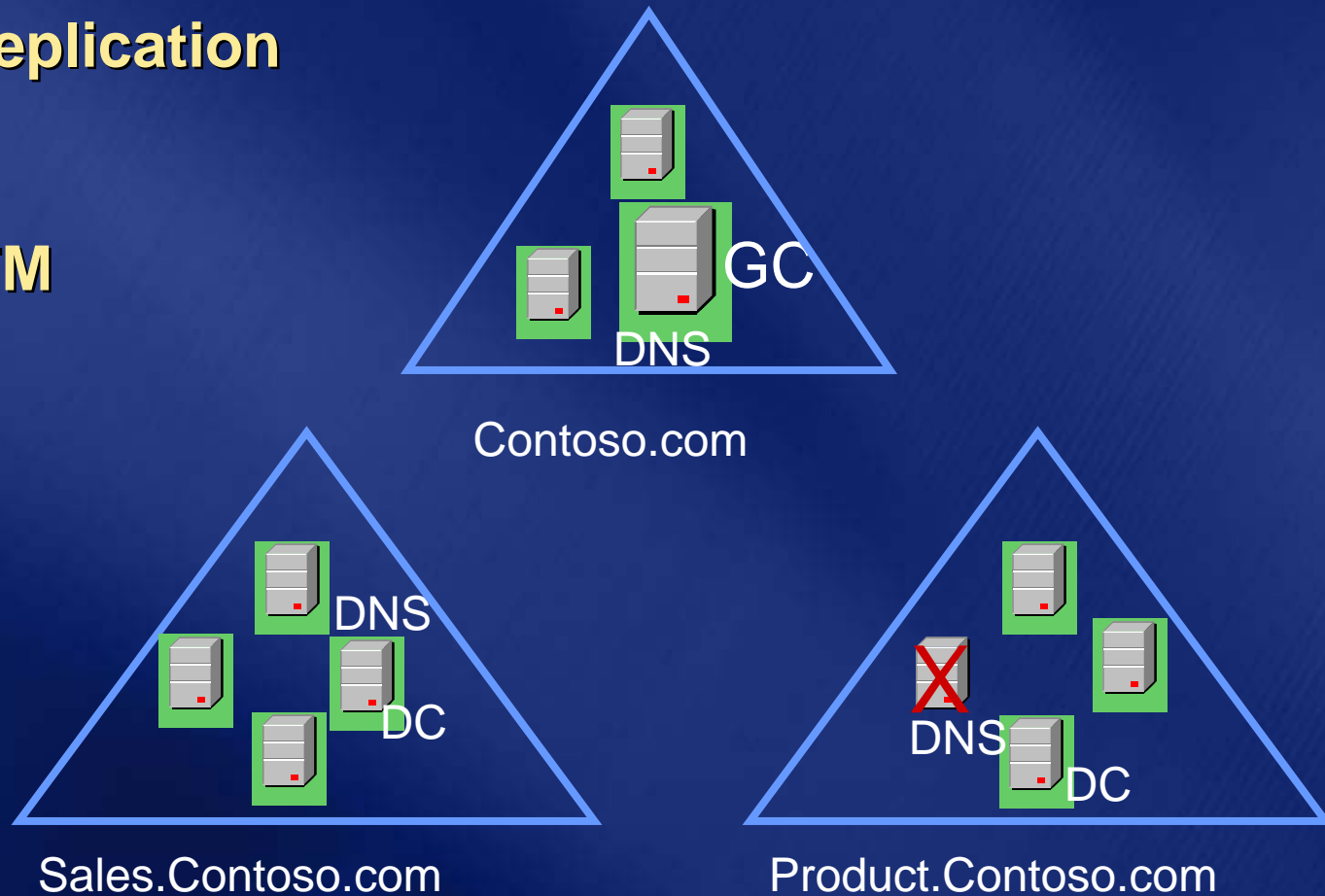


# 8. Promote Remaining DCs

Via Replication

or

Via IFM



# Forest Recovery

## Post-recovery steps

- Restore DNS to its original configuration
- Add additional GCs, DNS servers
- Fix up user/machine passwords that fail
- Transfer FSMO roles to appropriate DCs
- Recover missing objects
- Fix Exchange mailboxes for missing users
- Recover other AD dependent applications
- Remove lingering objects on GCs

# Agenda

- **Planning for the Worst**
- **Practical Recovery Examples**
- **Summary**
- **Questions**

# Summary

- To be able to restore from a backup requires having taken one
- Have you checked your spare tire?
  - While you're at it, check your smoke alarms also
- Remember the 'severed finger'...
  - Nothing wrong with knowing your boundaries and asking for help.
- Practice makes perfect

# Resources

**Forest Recovery Whitepaper:**

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=3EDA5A79-C99B-4DF9-823C-933FEBA08CFE>

**Windows Server 2003 Operation Guide:**

<http://www.microsoft.com/technet/itsolutions/cits/mo/winsrvmg/adpog/adpog1.msp>

**Windows Server 2003 SP1 authoritative restore help:**

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/Operations/690730c7-83ce-4475-b9b4-46f76c9c7c90.msp>

**Tombstone reanimation help:**

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/active\\_directory.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ad/ad/active_directory.asp)

**How to force demote a DC:**

<http://support.microsoft.com/default.aspx?scid=kb;en-us;332199>

**Group Policy Administration using GPMC:**

[http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC\\_Administering.doc](http://download.microsoft.com/download/a/9/c/a9c0f2b8-4803-4d63-8c32-3040d76aa98d/GPMC_Administering.doc)

# Resources

**Chewy Chong**

**Email: [chewyc@avanade.com](mailto:chewyc@avanade.com)**

**Blog: [firechewy.com/blog](http://firechewy.com/blog)**



questions?

# ***Your Feedback is Important!***



**Please write the number located in the bottom left hand corner of your name badge, on the top of the Evaluation Form. This number links back to your registration details so that we can contact you after TechEd.**

**When completing the Evaluation Form, please tick the number that best corresponds to your experience at TechEd. For additional comments, use the comments section at the end of each form.**

***Microsoft***<sup>®</sup>

*Your potential. Our passion.*<sup>™</sup>

© 2005 Microsoft Corporation. All rights reserved.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.