Troubleshooting Techniques for Microsoft Active Directory

Renato Pereira
Support Escalation Engineer
Microsoft Corporation

Humberto Rosas
Support Escalation Engineer
Microsoft Corporation

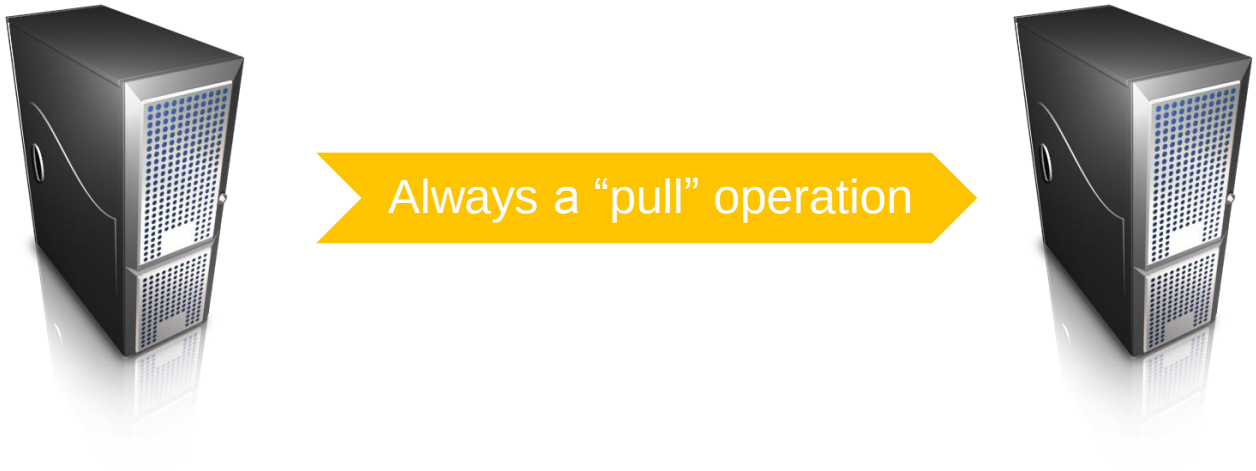
Microsoft | Services

Active Directory Troubleshooting Fundamental Concepts

AD Fundamental Concepts

- **Active Directory Replication**

The process of propagating updates between domain controllers



AD Fundamental Concepts

Up-to-Dateness Vector

The *up-to-dateness vector* is a value that the destination domain controller maintains for tracking the originating updates that are received from all source domain controllers.

Domain Controller	USN	Time Stamp
DC1	100	2009-04-15 9:00:00
DC2	200	2009-04-15 10:00:00

AD Fundamental Concepts

- **Tombstone Lifetime**

Determines the useful lifetime of a backup and how long will deleted objects be preserved before they are completely removed.

Operating System	Default Tombstone Lifetime
Windows 2000 (any SP)	60 days
Windows 2003 (after SP1)	180 days
Windows 2008 (any SP)	180 days

Active Directory Troubleshooting
Replication failures

AD Replication Failures

Common Issues

- Network restrictions (Firewalls, Routers, etc)
- DNS incorrect configuration (missing records, zones, etc)

Complex Issues

- USN Rollback
- Time Synchronization
- Lingering Objects

AD Replication Failures

Tool of Choice

REPADMIN.EXE

The “Swiss army knife” for troubleshooting AD replication issues

Strong points

- Very complete
- Extremely reliable

Weak points

- Command line tool
- May require a complex syntax

AD Replication Failures

Common Issues

Error code examples returned by REPADMIN /SHOWREPL

- **Network restrictions (Firewalls, Routers, etc)**

1722 (0x6ba) - RPC_S_SERVER_UNAVAILABLE
1753 (0x6d9) - EPT_S_NOT_REGISTERED
1256 (0x4e8) - ERROR_HOST_DOWN

- **DNS incorrect configuration (missing records, zones, etc)**

8524 (0x214c) - ERROR_DS_DNS_LOOKUP_FAILURE

AD Replication Failures

- **Complex Issues**

Error code examples returned by REPADMIN /SHOWREPL

› **Potential USN Rollback detected (+)**

8456 (0x2108) - ERROR_DS_DRA_SOURCE_DISABLED

› **Replication occurred more than a TSL period ago (+)**

8614 (0x216a) - ERROR_DS_REPL_LIFETIME_EXCEEDED

› **Lingering Object(s) detected (+)**

8606 (0x219e) - ERROR_DS_INSUFFICIENT_ATTR_TO_CREATE_OBJECT

demo

Demo 1 – Active Directory
Common Replication Failures

AD Replication Failures

- **Complex Issues**

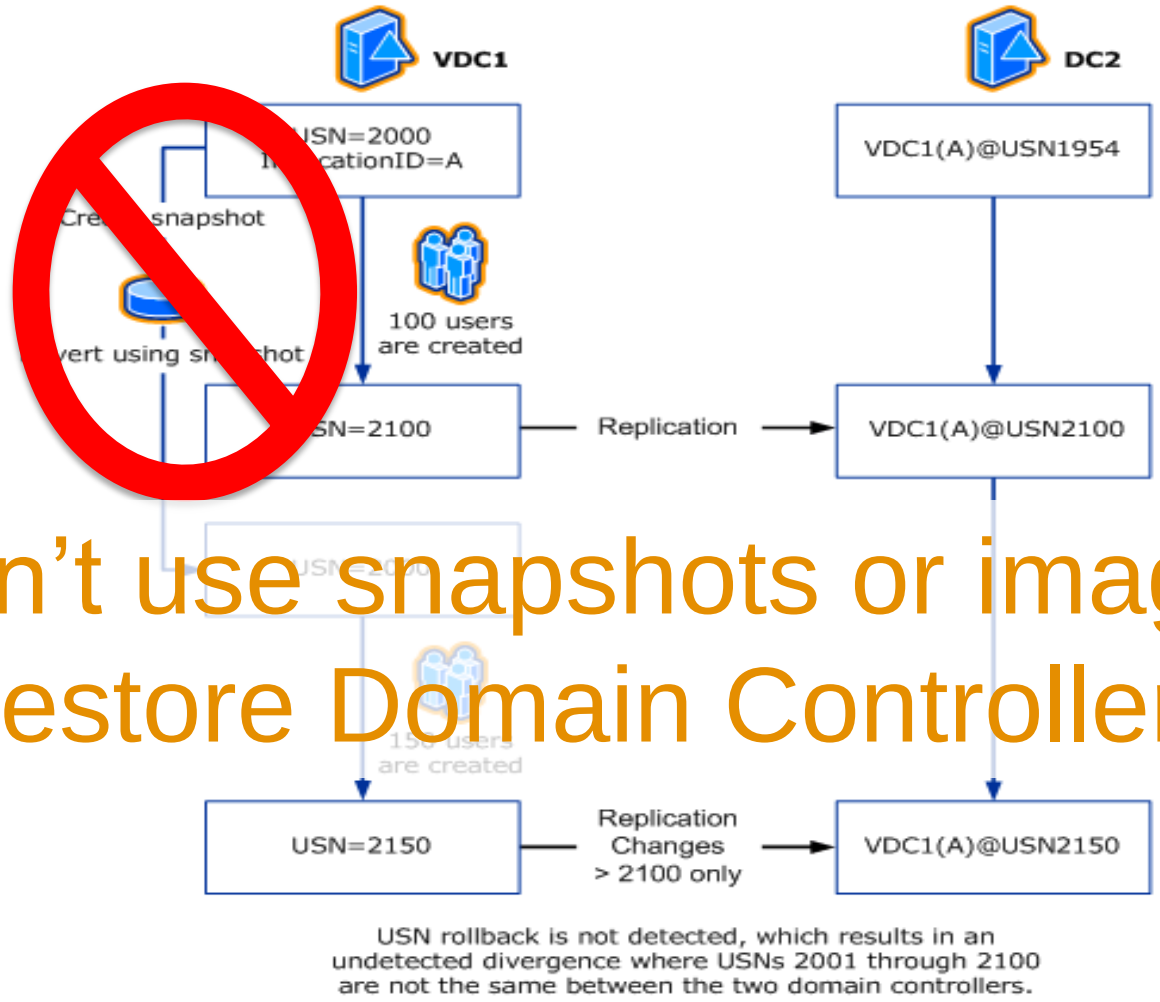
› **USN Rollback - Definition**

Occurs when an Active Directory database is incorrectly “restored “ or copied into place.

When a USN rollback occurs, modifications to objects and attributes that get committed on one domain controller do not replicate to other domain controllers in the forest

AD Replication Failures

USN Rollback scenario



Don’t use snapshots or images to restore Domain Controllers!!!

USN rollback is not detected, which results in an undetected divergence where USNs 2001 through 2100 are not the same between the two domain controllers.

AD Replication Failures

Complex Issues

› **USN Rollback - Resolution**

The only supported method is to perform a:

- *DCPROMO /FORCEREMOVAL*
- *METADATA CLEANUP*
- *DELETE all snapshots and VHD's associated with the problematic DC.*

demo

Demo 2 – Active Directory
USN ROLLBACK

AD Replication Failures

- **Complex Issues**

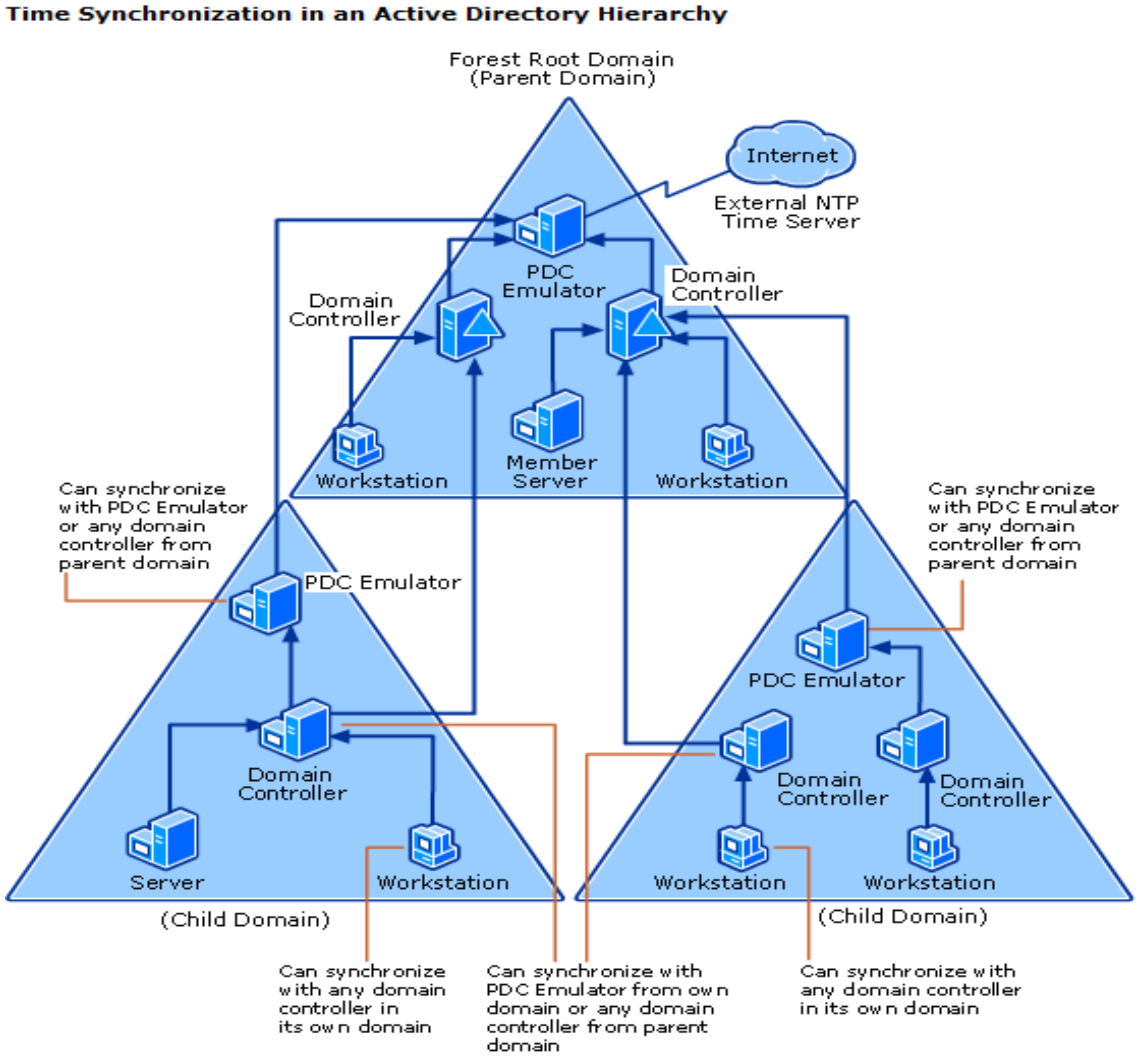
› **Time Synchronization - Definition**

The Windows Time Service is responsible for maintaining time synchronized across the domain or forest.

Synchronized time is critical in Window because the default authentication protocol (MIT Kerberos version 5) uses workstation time as part of the authentication ticket generation process.

Any mechanism that uses timestamps will be affected by time sync issues.

AD Replication Failures



AD Replication Failures

Complex Issues

- **Time Synchronization - Scenarios**

Time Jump Forward

- *Garbage Collection occurs*
- *Machine account passwords are changed*
- *Changes that occur at this time, will be stamped with that date*

Time Jump Backwards

- *Authentication breaks*
- *Quarantine protection kicks in (replication occurred >TSL)*
- *Deletion that occur in the “past” can be immediately garbage collected*

AD Replication Failures

- **Complex Issues**

› **Time Jump – Prevention**

Prevention against large time offsets

- **How to configure the Windows Time service against a large time offset**
  http://support.microsoft.com/kb/884776/en-us

AD Replication Failures

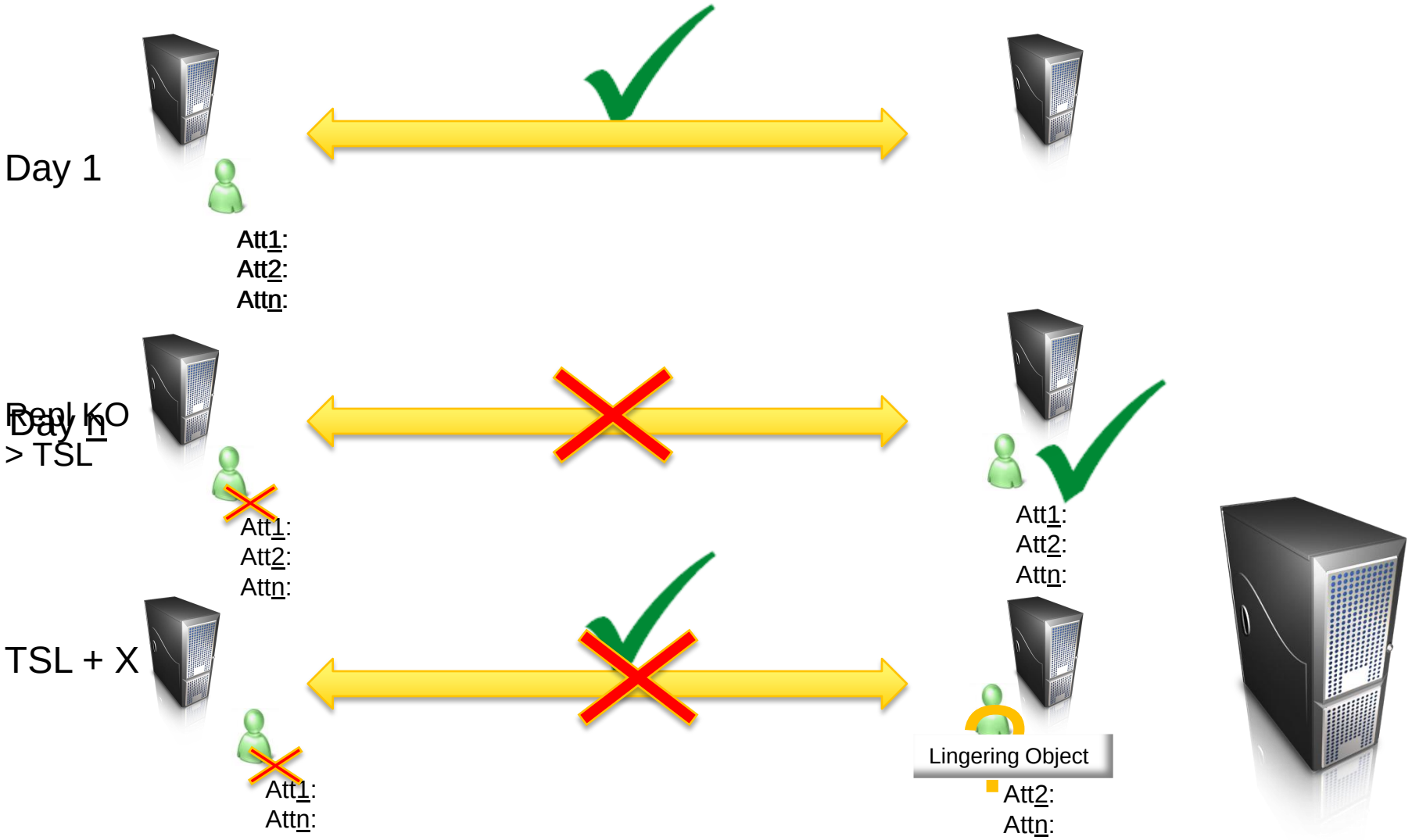
- **Complex Issues**

› **Lingering Objects - Definition**

Objects that have been deleted and garbage collected from an Active Directory partition but still exist in the writable partitions of other DCs in the same domain, or read-only partitions of global catalog servers in other domains in the forest are known as "lingering objects".

??? What ???

AD Replication Failures



AD Replication Failures

Complex Issues

- **Long time disconnections – Resolution**

  HKLM\System\CurrentControlSet\Services\NTDS\Parameters**Allow Replication With Divergent and Corrupt Partner**

  - **Must be created and enabled (1)**
  - **Allows replication between dc's that do not replicate for more than TSL**

AD Replication Failures

Complex Issues

› **Lingering Objects – Resolution**

- **Use REPADMIN /REMOVELINGERINGOBJECTS**

  - with /ADVISORY_MODE → detection
  - without /ADVISORY_MODE →removal

- **Replication Consistency**

  HKLM\System\CurrentControlSet\Services\NTDS\Parameters**Strict Replication Consistency**

  - **Default and recommended value → 1**
  - **Ensure the database consistency between DC's**

demo

Demo 3 – Active Directory
Lingering Objects

Questions?

Microsoft®

Your potential. Our passion.™