Microsoft® Jump Start

M11: Implementing Active Directory Domain Services

Rick Claus | Technical Evangelist | Microsoft
Ed Liberman | Technical Trainer | Train Signal

Microsoft

Jump Start Target Agenda | Day One

Day 1	Day 2
Module 1: Installing and Configuring Servers Based on Windows Server 2012	Module 7: Implementing Failover Clustering
Module 2: Monitoring and Maintaining Windows Server 2012	Module 8: Implementing Hyper-V
Module 3: Managing Windows Server 2012 by Using PowerShell 3.0	Module 9: Implementing Failover Clustering with Hyper-V
- MEAL BREAK -	- MEAL BREAK -
Module 4: Managing Storage for Windows Server 2012	Module 10: Implementing Dynamic Access Control
Module 5: Implementing Network Services	Module 11: Implementing Active Directory Domain Services
Module 6: Implementing Direct Access	Module 12: Implementing Active Directory Federation Services

Module Overview

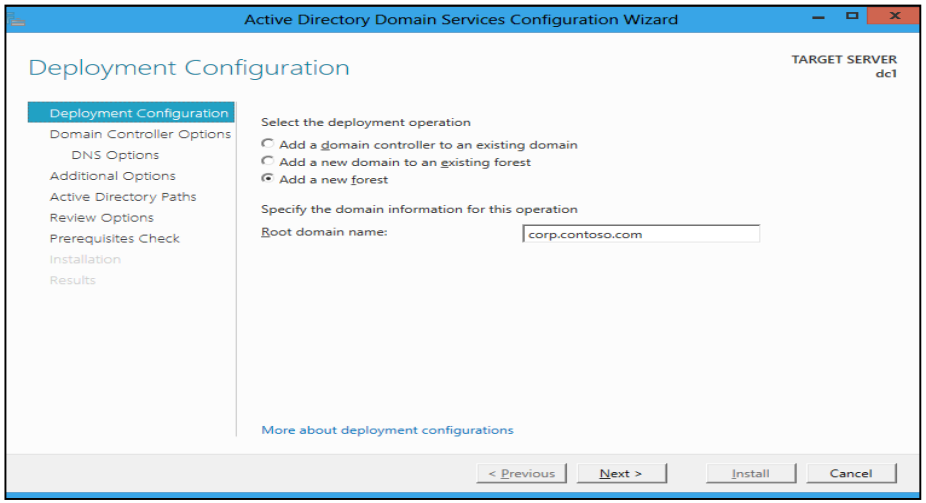
- Deploying AD DS Domain Controllers
- Configuring AD DS Domain Controllers
- Implementing Service Accounts
- Implementing Group Policy in AD DS
- Maintaining AD DS

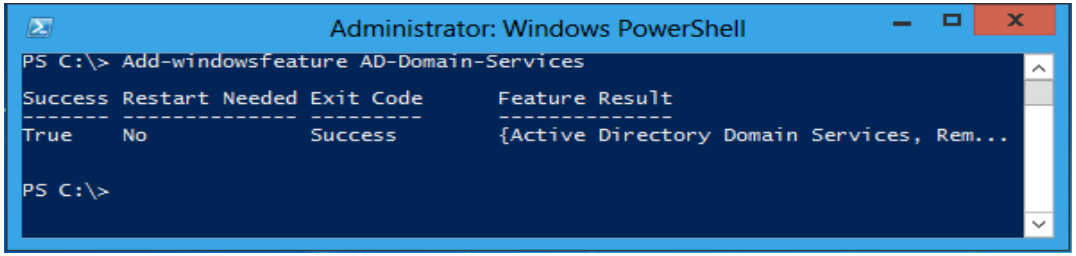
What's New in AD DS in Windows Server 2012?

- New deployment methods
- Simplified administration
- Virtualized domain controllers
- Active Directory module for Windows PowerShell
- Windows PowerShell History Viewer
- Active Directory Federated Services
- Active Directory Based Activation

Deploying AD DS Domain Controllers

- All configuration of domain controllers can be done through a wizard in Server Manager
- AD DS binaries can be installed using Windows PowerShell
- Dism.exe is more complex to use
- Active Directory Installation Wizard is only supported in Unattended mode





Deploying AD DS Domain Controllers on Server Core

You can install AD DS:

- Locally using Windows PowerShell cmdlets
- Remotely using either Windows PowerShell cmdlets or Server Manager

Deploying AD DS Domain Controllers by using Install From Media (IFM)

Use Ntdsutil.exe to create the installation media

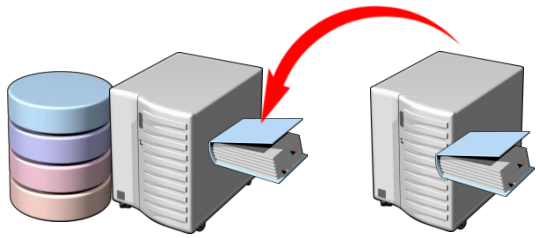
Ntdsutil.exe can create the following types of installation media:

- Full (or writable) domain controller
- Full (or writable) domain controller with SYSVOL data
- Read-only domain controller with SYSVOL data
- Read-only domain controller
- Create full no defrag
- Create sysvol full no defrag

Deploying AD DS Read-Only Domain Controllers

RODCs provide:

- Unidirectional replication
- Credential caching
- Administrative role separation
- Read-only DNS
- RODC filtered attribute set



Cloning Virtual AD DS Domain Controllers

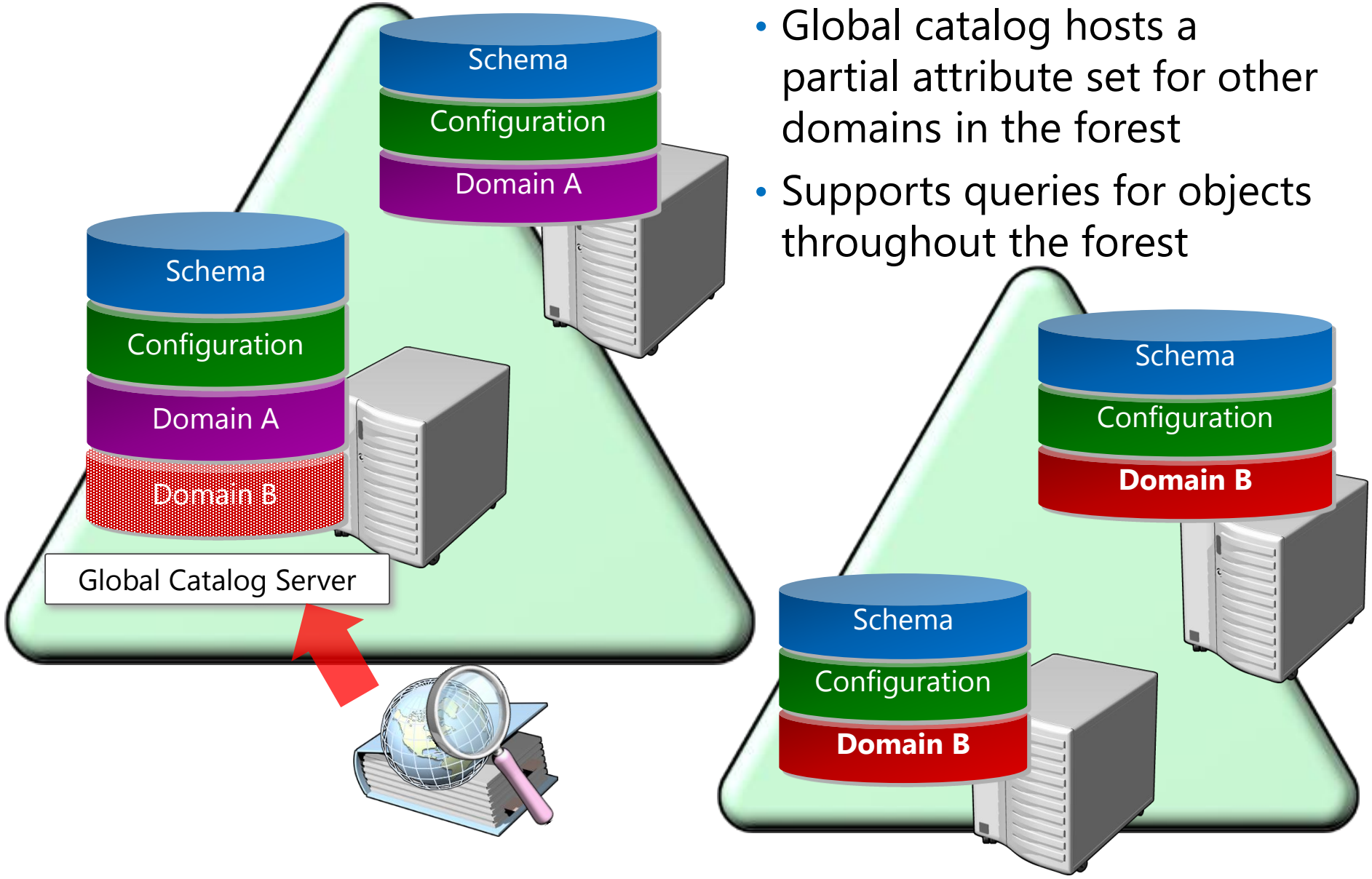
You can safely clone existing Virtual Domain Controllers (VDC) by:

- Creating a DcCloneConfig.xml file and storing it in the AD DS database location.
- Taking the VDC offline and exporting it.
- Creating a new virtual machine by importing the exported VDC.

Upgrading to Windows Server 2012 AD DS

- Only domain controllers running Windows Server 2008 x64 or Windows Server 2008 R2 can be upgraded
- You cannot perform an in-place upgrade on a Windows Server 2003 domain controller
- Forestprep and Domainprep must both be run manually prior to upgrading

Configuring the Global Catalog



- Global catalog hosts a partial attribute set for other domains in the forest
- Supports queries for objects throughout the forest

Configuring Universal Group Membership Caching

- Universal group membership replicated in the global catalog:
  - Normal logon: User's token built with universal groups from global catalog
  - Global catalog not available at logon: domain controller denies authentication
- If every domain controller is a global catalog, this is never a problem
- If connectivity to a global catalog is not reliable:
  - Domain controllers can cache universal group membership for a user when user logs on
  - Global catalog later not available: User authenticated with cached universal groups
- In sites with unreliable connectivity to global catalog, enable universal group membership caching
- Right-click NTDS Settings for site, and select Properties:
  - Enables Universal Group Membership Caching for all domain controllers on the site

Configuring Operations Masters

- Forest-wide:
  - Domain naming: Adds/removes domains to/from the forest
  - Schema: Makes changes to the schema
- Domain-wide:
  - RID: Provides "pools" of RIDs to domain controllers, which use them for SIDs
  - Infrastructure: Tracks changes to objects in other domains that are members of groups in this domain
  - PDC: Plays several very important roles:
    - Emulates a Primary Domain Controller (PDC): compatibility
    - Special password update handling
    - Default target for Group Policy updates
    - Master time source for domain
    - Domain master browser

Managing Domain and Forest Functional Levels

- Domain functional levels
- Forest functional levels
- New functionality requires that domain controllers run:
  - Windows 2000
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
- Active Directory Domains and Trusts
- Cannot raise functional level while domain controllers are running previous Windows versions
- Cannot add domain controllers running previous Windows versions after raising functional level

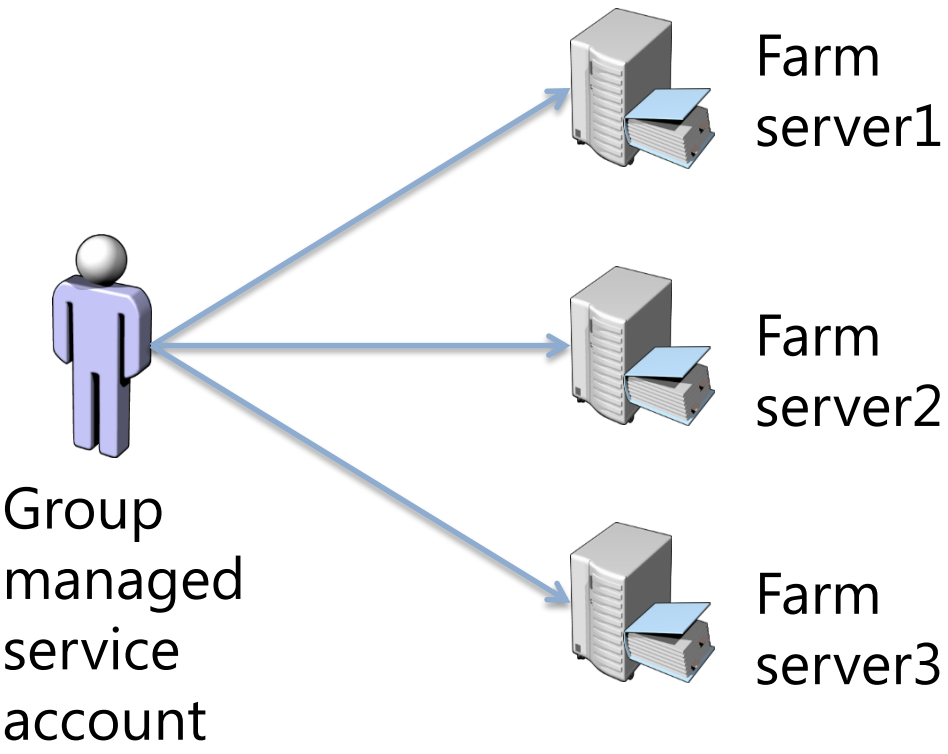
What Are Managed Service Accounts

- Used to automate password and SPN management for service accounts used by services and applications
- Requires a Windows Server 2008 R2 server with:
  - Microsoft .NET Framework 3.5.x
  - Active Directory module for Windows PowerShell
- Recommended to run with AD DS configured at the Windows Server 2008 R2 functional level
- Can be used in a Windows Server 2003 or Windows Server 2008 AD DS environment:
  - With Windows Server 2008 R2 schema updates
  - With Active Directory Management Gateway Service

What Are Group Managed Service Accounts?

Group managed service accounts provide:

- Automatic password and SPN management to multiple servers in a farm
- A single identity for services running on a farm



DEMO: Configuring Group Managed Service Accounts

In this demonstration you will see how to create a group managed service account and associate the account with a server

What's New: Group Policy in Windows Server 2012?

- Group Policy Infrastructure Status
- Remote Policy Refresh
- New RSOP Logging Data

Managing GPOs

- The GPMC is the main Group Policy management tool. It is used to:
  - Create GPOs
  - Edit GPOs through the GPO Editor
  - Link GPOs
  - Back up GPOs
  - Restore GPOs
  - Copy GPOs
  - Import GPOs

Configuring Group Policy Processing

- GPOs are applied in an order known as precedence. When multiple policies apply to the same container the precedence can be set.
- GPO settings inherit down and merge to provide the cumulative effect of all settings. Inherited GPOs can be viewed on the **Inheritance** tab.
- Inheritance can be blocked. Inheritance cannot be blocked for only selected GPOs – it is all or none.
- GPOs can be enforced. Enforcement overrides blocking inheritance and conflicting settings.
- Loopback applies the user settings from the policy that applied the loopback setting. It is typically used for Remote Desktop Services and special cases.
- Security filtering. Permissions on the GPOs can control which object receive settings.
- WMI Filters. WMI can query for conditions under which the GPO settings are applied.

Group Policy Client Side Extensions

- How GPOs and their settings are applied
- Group Policy Client retrieves ordered list of GPOs
- GPOs are downloaded, and then cached
- Components called CSEs process the settings to apply the changes:
  - One for each major category of policy settings: Security, registry, script, software installation, mapped drive preferences, and so on.
  - Most CSEs apply settings only if GPO as a whole changed
    - Improves performance
    - Security CSE applies changes every 16 hours
  - GPO application is client computer driven (pull)

Troubleshooting Group Policy

Group Policy issues can be caused by Group Policy-specific issues, or they can be caused by unrelated issues like network connectivity or authentication problems.

Key Group Policy troubleshooting areas:

- Inheritance
- Security group or WMI filtering
- Replication
- Policy refresh

Best Practices for Implementing Group Policy

- Plan the Group Policy deployment
- Create standard desktop configurations
- Do not use the Default GPOs for other purposes
- Use inheritance modifications sparingly
- Employ Loopback processing for special case scenarios
- Implement a change request process

Options for AD DS Backup

- Windows Server Backup snap-in
- Wbadmin.exe
- Backups can be manual or automated
- Back up to CD/DVD/HDD
- You must back up all critical volumes for AD DS
  - System volume
  - Boot volume
  - Volumes hosting SYSVOL, AD DS database (NTDS.dit), logs

Options for AD DS Restore

- Non-authoritative (normal) restore
  - Restore domain controller to previously known good state of Active Directory
  - Domain controller is updated by using standard replication from up-to-date partners
- Authoritative restore
  - Restore domain controller to previously known good state of Active Directory
  - "Mark" objects that you want to be authoritative
  - Windows sets the version numbers very high
  - Domain controller is updated from its up-to-date-partners
  - Domain controller sends authoritative updates to its partners
- Full Server Restore
  - Typically performed in Windows Recovery Environment
- Alternate Location Restore

How does the Active Directory Recycle Bin Work?

- Cannot be disabled once it is enabled
- Now has a user interface to simplify restoration of objects
- Is enabled and accessed through the Active Directory Administration Center
- Cannot restore sub-trees of object in a single operation
- Requires forest level be at least Windows Server 2008 R2
- Requires Enterprise Admins
- Increases the size of the Active Directory database
- Objects are preserved in the recycle bin for the tombstone lifetime: 180 days by default
- Deleted object can be viewed in the Deleted Object folder
- Objects can be restored by selecting them and choosing Restore

DEMO: Restoring AD DS Objects Using the Active Directory Recycle Bin

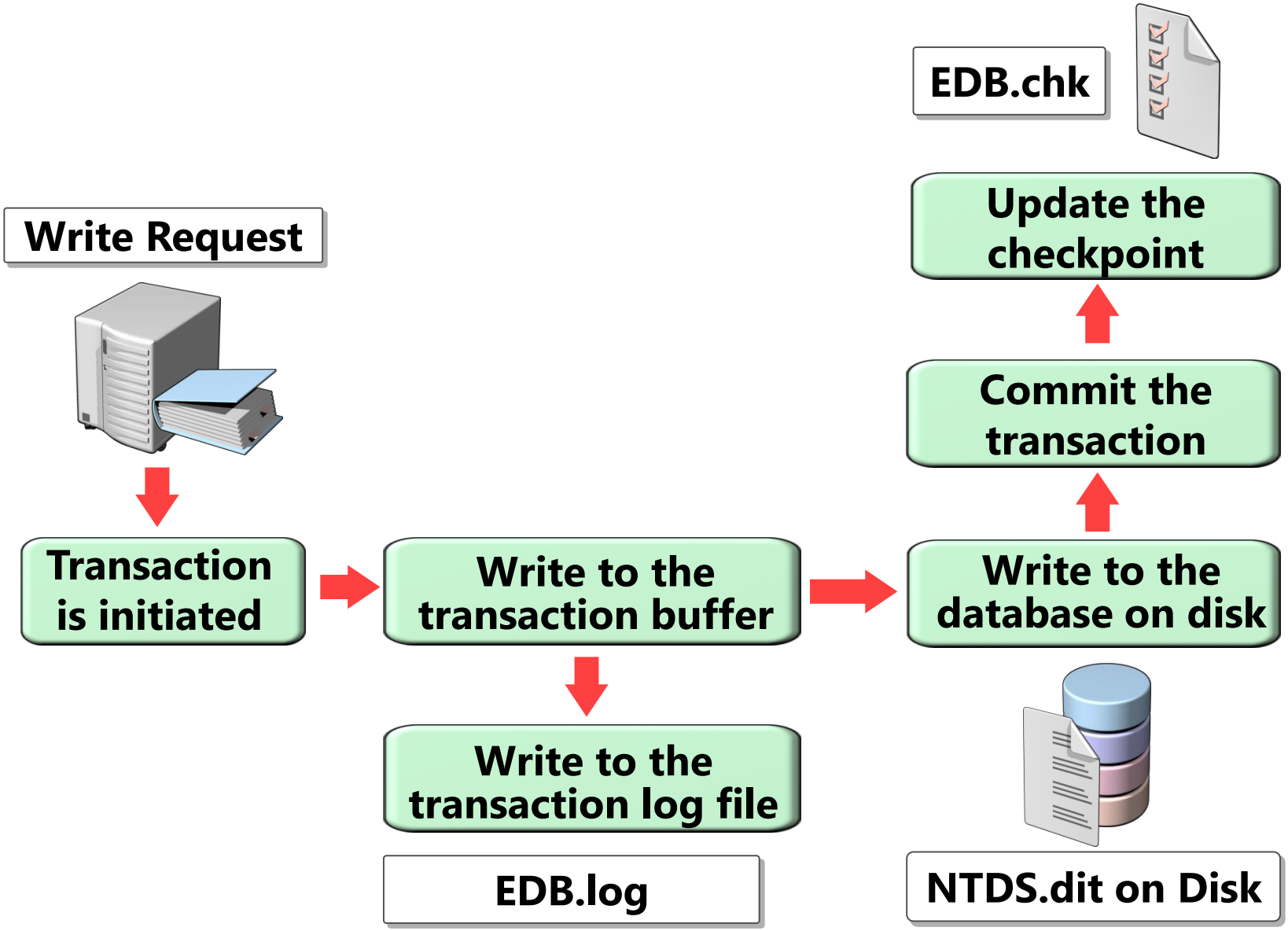
In this demonstration you will see how to:

- Enable the Active Directory Recycle Bin
- Use the Recycle Bin to restore a deleted object

What are AD DS Snapshots?

- Create a snapshot of Active Directory:
  - NTDSUtil
- Mount the snapshot to a unique port:
  - NTDSUtil
- Expose the snapshot:
  - Right-click the root node of Active Directory Users and Computers and select **Connect to Domain Controller**
  - Enter serverFQDN:port
- View (read-only) snapshot:
  - Cannot directly restore data from the snapshot
- Recover data:
  - Manually reenter data, or
  - Restore a backup from the same date as the snapshot

AD DS Database Maintenance



Microsoft