What's new in AD for Windows Server 2008 R2

M.S.Anand
Technology Specialist
Microsoft Corp

msdn Microsoft® Developer Network

Microsoft TechNet

What's new in AD DS

- Active Directory Recycle Bin
- Active Directory module for Windows PowerShell
- Active Directory Administrative Center
- Active Directory Best Practices Analyzer
- Active Directory Web Services
- Authentication mechanism assurance
- Offline domain join
- Managed Service Accounts

Recycle Bin for AD

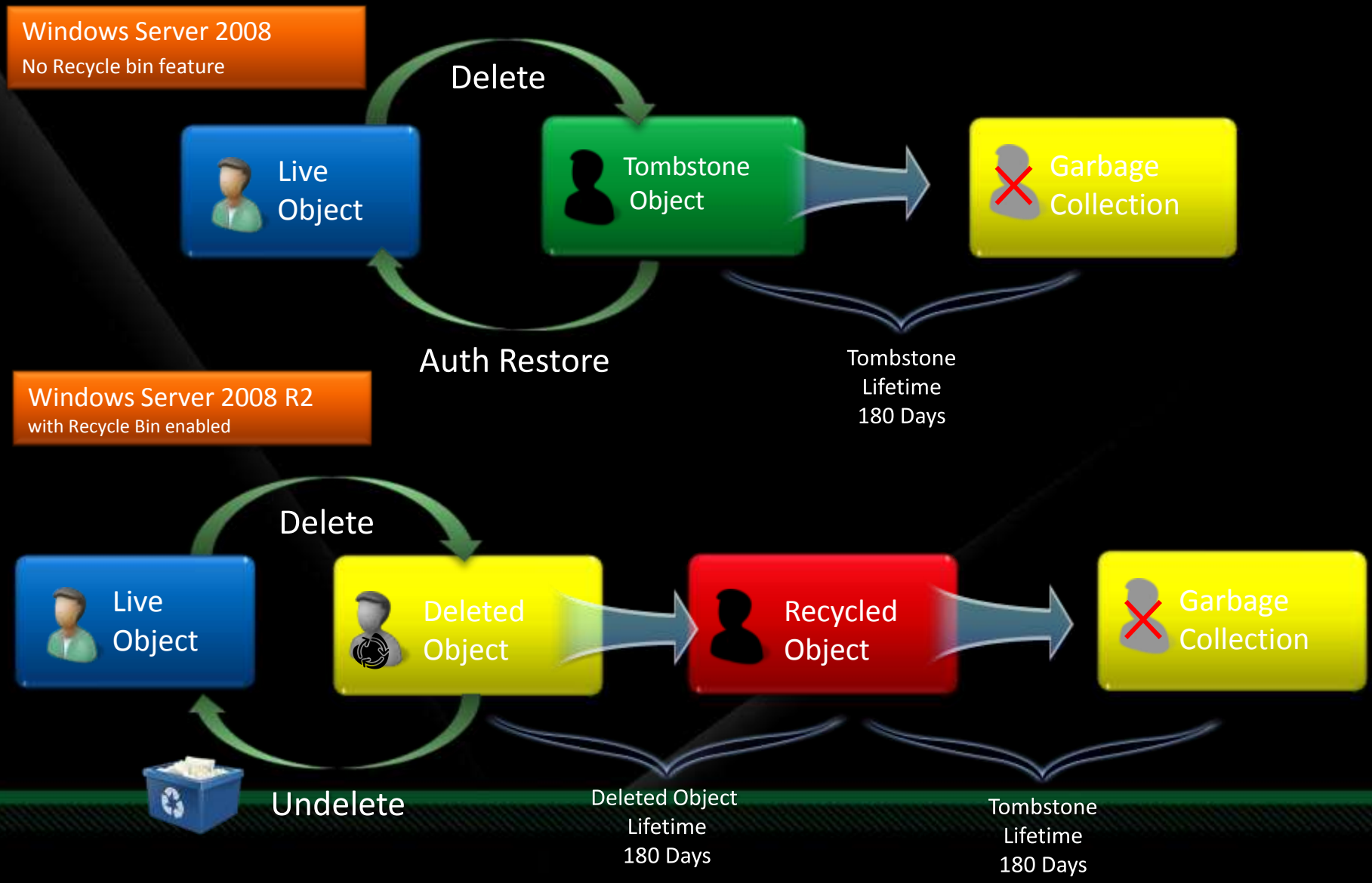
Recover from accidental deletion in Active Directory

- Accidental deletions are the number #1 cause of AD Disaster\Recovery scenarios
- Recycle Bin for AD:
  - Allows recovery of deleted users, groups, etc
    - Locate deleted object:

      Get-ADObject –Filter {} -IncludeDeletedObjects
    - Recover deleted object:

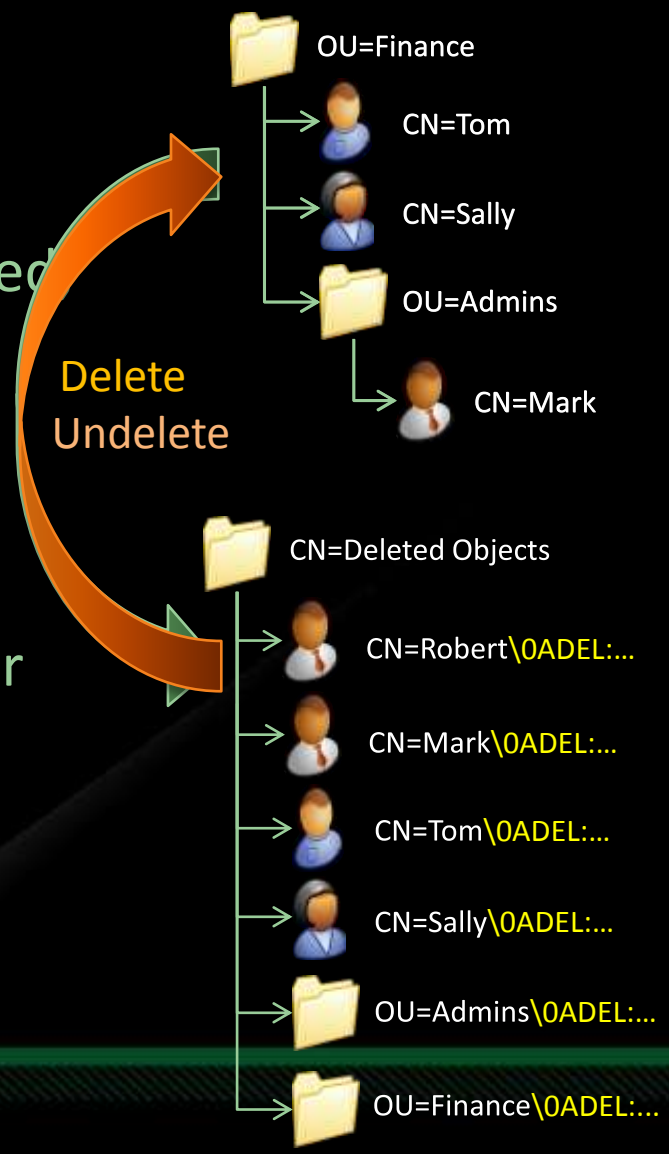
      Restore-ADObject -Identity {id}
  - All attributes are automatically restored
    - Including well known & problematic ‘Linked Attributes’
    - Description, password, group membership, managed by, etc.

Recycle Bin for AD Object Life-cycle



Recovering Multiple Objects

- Deleted Objects container
  - A flat list of all objects in the Deleted state
  - DN is mangled, attributes preserved, lastKnownParent
- Restore objects to live parent
  - Deleted objects must be restored to a live parent
  - Perform restore in top-down order
  - lastKnownParent and lastKnownRDN properties useful in rebuilding hierarchy
  - RDN over 128 chars truncated



Recycle Bin Considerations

- What's the impact on DIT size?
  - Anticipate growth of 5-10% when new DC is installed
  - Subsequent growth depends on size and frequency of object deletions
- Deleted Object Lifetime (DOL)
  - DOL = TSL = 180 days (by default)
  - Both can be modified independently
  - Attributes: msDS-deletedObjectLifetime , tombstoneLifetime
- How does this affect my back up strategy?
  - Backups remain valid for the lesser of DOL or TSL
- How do I permanently delete an object?
  - Delete the object from the Deleted Objects container

```
Get-ADObject –Filter {} –IncludeDeletedObjects | Remove-ADObject
```

demo

AD Recycle Bin

PowerShell for AD

Command line scripting for administrative, configuration and diagnostic tasks

- PowerShell V1:
  - Hodgepodge of command line tools for administration and configuration
  - Difficult to compose to achieve complex tasks
- PowerShell V2 with AD module:
  - Comprehensive set of AD cmdlets for AD DS and AD LDS administration and configuration
  - Brings the power and flexibility of PowerShell core to AD
  - Consistency with other server roles

Powershell Advantages

- Consistent vocabulary and syntax
  - Verbs – Add, New, Get, Set, Remove, Clear…
  - Nouns – ADObject, ADUser, ADComputer, ADDomain, ADForest, ADGroup, ADAccount, ADDomainController, …
- Easily discovered
  - No need to find, install, or learn other tools, utilities or commands
- Flexible output
  - Output from one cmdlet easily consumed by another
- Easily composed
  - Create higher level tools for complex operations
- Leverage .Net Framework
  - All the capabilities of .Net Framework
- End-to-End manageability
  - With other roles such as Exchange, Group Policy, etc

PowerShell Provider Model

- Brings file system like navigation to the directory
- Use familiar file system commands within the directory
  - Copy, Move, Rename, Delete, etc
- Map drives to containers in AD DS, ADLDS or AD Snapshots
- Enables best practice sharing across connections

demo

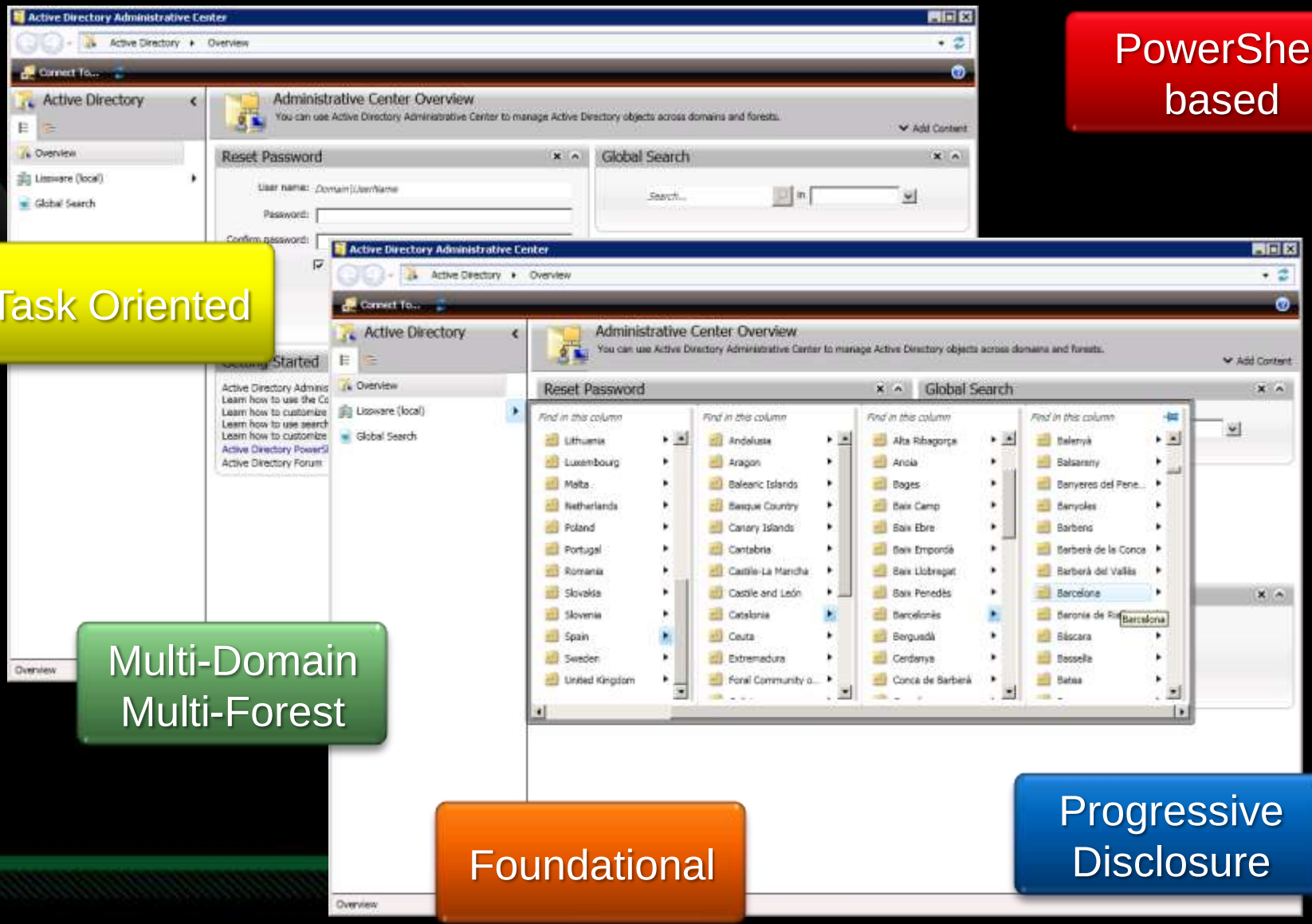
PowerShell for AD

AD Administrative Center

Increase productivity by providing a scalable, task-oriented UX for managing Active Directory

- AD Administration Today:
  - Non task-oriented UI
  - Representation in MMC not scalable for large datasets
  - Limited to managing one domain at a time
- AD Administrative Center in Windows Server 2008 R2:
  - Task oriented administration model, with support for larger datasets and progressive disclosure of data
  - Consistency between CLI and UI capabilities
  - Navigation experience designed to support multi-domain, multi-forest environments
  - Foundation for future UI enhancements

AD Administrative Center



PowerShell based

Task Oriented

Multi-Domain Multi-Forest

Foundational

Progressive Disclosure

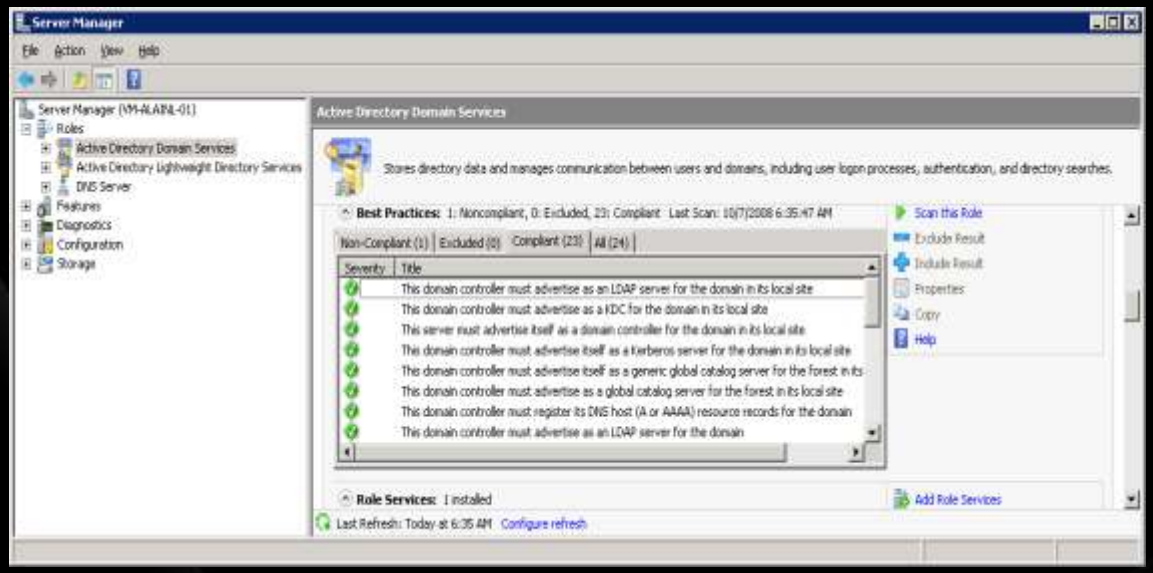
Best Practice Analyzer

Identify deviations from best practices to help better manage Active Directory deployments

- AD Best Practice Analyzer
  - Analyzes AD settings that cause most unexpected behavior
  - Flags settings/configurations that violate recommended best practices
  - Provides guidance only, does not modify settings
  - User initiates scan, not a monitoring solution
  - Scan can be initiated through Server Manager or from PowerShell directly
  - BPA scan can be initiated from client using PS remoting
  - Quarterly updates post RTM

Initiating a BPA Analysis

- From Server Manager



- From PowerShell

Import-Module BestPractices

Invoke-BpaModel Microsoft/BestPractices/DirectoryServices

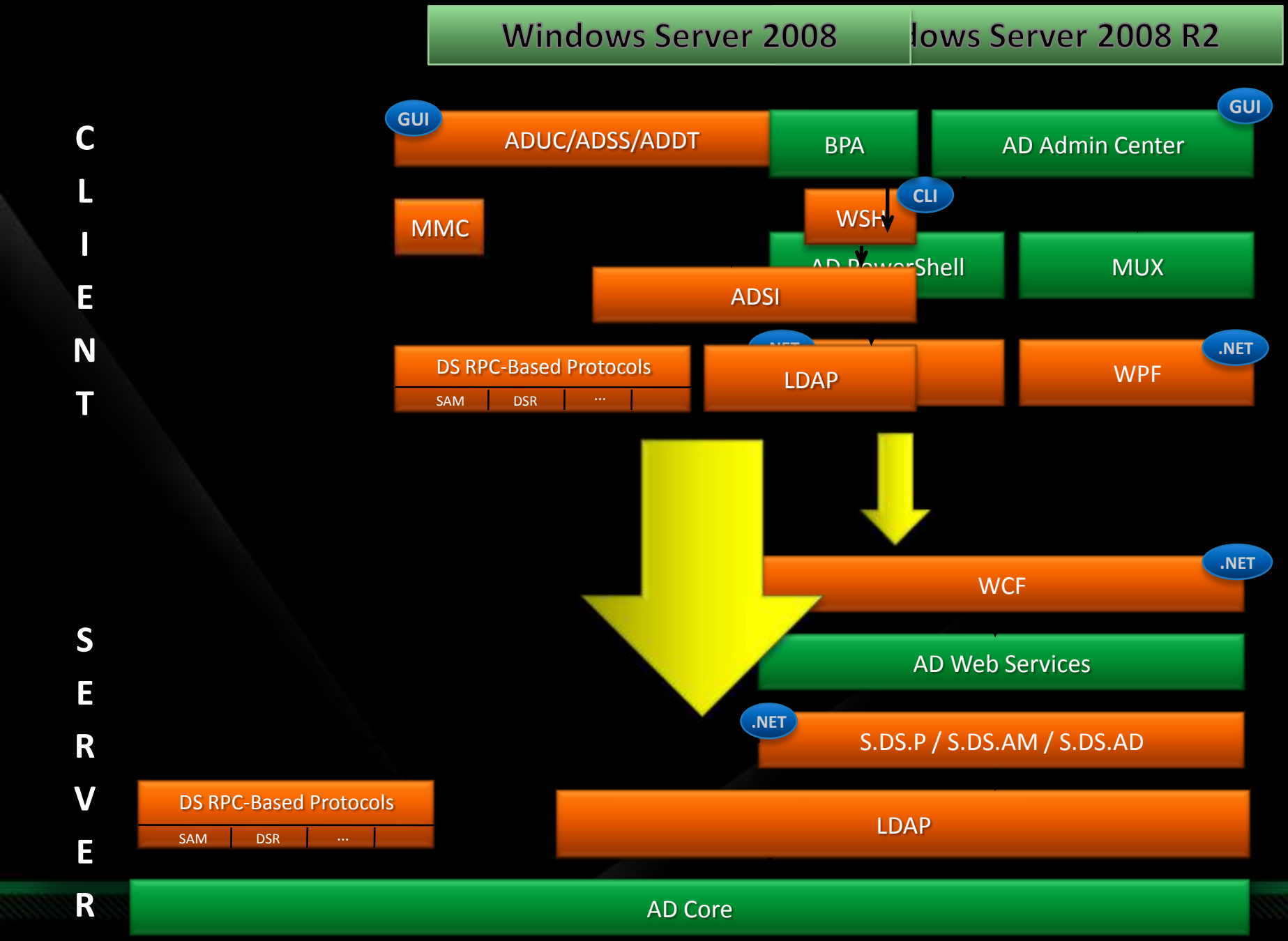
Get-BpaResult Microsoft/BestPractices/DirectoryServices

Best Practice Analyzer Rules

- DNS Registration/Discovery
  - SRV/A/AAA records registered
- Disaster Recovery
  - Multiple DC per domain
  - Resultant backup lifetime
- Replication
  - One GC per site
  - KCC enabled
  - VM Scenarios
- Topology/connectivity
  - FSMO role assignment
  - FSMO availability
- Lingering Object Prevention
  - Strict Replication Consistency
- Time Service
  - PDC time source
  - MaxPhaseCorrection limits

Active Directory Web Service

- AD Administration:
  - LDAP/RPC protocol used for administration and configuration
  - Lack of developer experience in Visual Studio
- AD Web Service:
  - Built using WCF and WS* protocols
    - WS-Enum, WS-Transfer, IMDA
  - Replaces LDAP and RPC for remote administration
  - Not intended for developer consumption in this release
  - Simpler firewall management
  - Web Service listening on port 9389
  - Download will be available for WS 2008 & 2003


Windows Server 2008
lows Server 2008 R2
CLIENT
SERVER
GUI
ADUC/ADSS/ADDT
BPA
GUI
AD Admin Center
MMC
CLI
WSH
MUX
ADSI
DS RPC-Based Protocols
SAM
DSR
...
LDAP
.NET
WPF
.NET
WCF
AD Web Services
.NET
S.DS.P / S.DS.AM / S.DS.AD
DS RPC-Based Protocols
SAM
DSR
...
LDAP
AD Core

Authentication Mechanism Assurance

Applications can control resource access based on authentication strength and method

- Active Directory Federation Services:
  - Cannot use authentication type or authentication strength to protect corporate data
    - Example: control access to resources based on claims such as use of smartcard for logon or the certificate used 2048 bit encryption
- ADFS for Windows 2008 R2:
  - Administrators can map certificate issuance policies to groups which applications can then use to control access to resources
  - Based on information obtained during authentication, these additional credential attributes are added to Kerberos tickets and used by claims aware applications as authorization data
  - Requires Windows Server 2008 R2 domain functional level
    - All domain controllers in the domain need to be WS 2008 R2 DCs

Offline Domain Join

Enable easier provisioning of machines in the data center

- Domain Joins Today:
  - Not possible to prepare the machine to be domain joined while offline
- Domain Join in Windows Server 2008 R2:
  - Ability to pre-provision machine accounts in the domain to prepare OS images for mass deployment
  - Machines are domain joined on initial boot without network connectivity
  - Reduces steps and time needed to deploy in the data center
  - Requires Win7 client and only one WS08 R2 member server

Managed Service Accounts

Simple management of service accounts

- Service Accounts Today:
  - Running multiple services under Built in accounts do not provide service isolation
  - Running service under user account requires cumbersome password management
- Service Accounts in Windows 2008 R2:
  - Managed Service Accounts provide the isolation that services need along with automatic password management
  - Lowers TCO through reduced service outages (for manual password resets and related issues)
  - Use one Managed Service Account per Service per Server
    - Service account can not be shared by multiple machines
  - Better SPN management available with in WS08 R2 Domain Functional Mode
    - Allows server renaming with effect service account

Using Managed Service Accounts

- Requires one WS08 R2 domain controller
- Create necessary Managed Service Accounts

```
New-ADServiceAccount –Name {name} –Path {path}
```

- Optionally delegate management of service account
- Optionally associate server and service account

```
Add-ADServiceAccount –Identity {id} -ServiceAccount {msa}
```

- Install service accounts on local server

```
Install-ADServiceAccount –Identity {id}
```

- Configure services to use managed service accounts
- No need to manage service account passwords
  - Traditionally a reoccurring and time consuming operation
  - Service account are subject to the domains password policy

Forest Functional Levels

- Windows Server 2008 R2 introduces new Forest and Domain functional level
  - Raising functional level alone has no effect other than allowing optional features to be enabled
    - Can raise functional level without unforeseen side effects
  - Recycle bin requires WS08 R2 Forest Functional level
    - Required in order to ensure that all DCs preserve attributes necessary for complete object recovery
  - Functional level can be lowered only if all optional features are disabled (recycle bin cannot be disabled)
- Optional features can be enabled individually

```
Enable-ADOptionalFeature  'Recycle Bin Feature' -Scope Forest
   -Target {target}
```

The Journey to Windows Server 2008 R2

- Upgrading to Windows 7 client while keeping existing servers, you can use:
  - Offline domain join
- Once AD Web-service is available for existing servers, if you upgrade to Windows 7 client, you can use:
  - AD PowerShell and ADAC for remote management of your servers
- Upgrading to Windows 7 client while installing one or more Windows Server 2008 R2 (one per domain), you can use:
  - Managed Service Accounts
- If you change the domain functional level to Windows Server 2008 R2, you can use:
  - Authentication Mechanism Assurance
  - Managed service account with an enhanced SPN management experience
- If you change the Forest functional level to Windows Server 2008 R2, you can use:
  - Recycle Bin

question & answer

msdn Microsoft® Developer Network

Microsoft TechNet


આભાર
ধন্যবাদ
நன்றி
धन्यवाद
Thank You!
ధన్యవాదాలు
ಧನ್ಯವಾದಗಳು
ধন্যবাদ
ਧੰਨਵਾਦ
നിങ്ങൾക്ക് നന്ദി

Microsoft®

Your potential. Our passion.™