Windows Server 2008 R2 新しい機能あれこれ

小鮒 通成

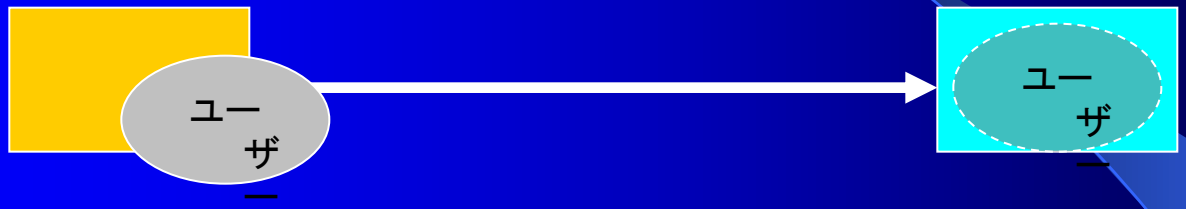
Windows Server 2008 R2 のActive Directory 新機能

- Active Directory ごみ箱
- Windows PowerShell の Active Directory モジュール
- Active Directory 管理センター
- ベスト プラクティス アナライザー
- Active Directory Web サービス
- 認証メカニズム保障
- オフライン ドメイン参加

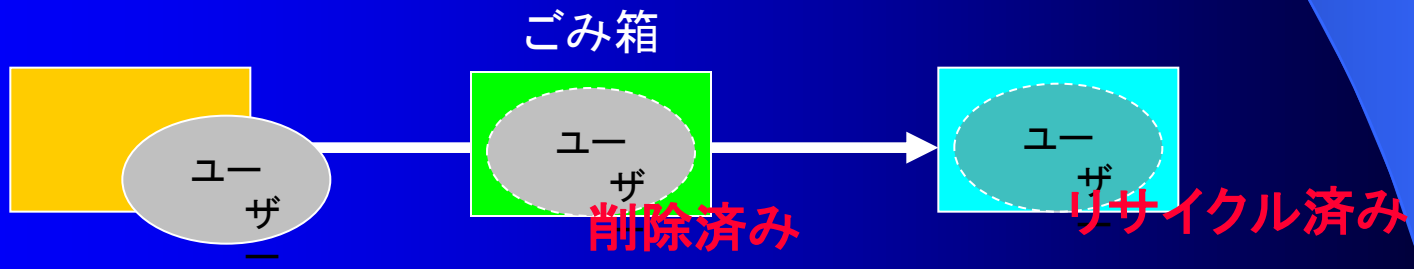
Active Directory ごみ箱

- 削除したオブジェクトをいったん貯めておく「ごみ箱」を実装
- ADUC 等で削除したオブジェクトをいったん「ごみ箱」に待避、180日間保存する
- 「ごみ箱」から元にもどすと、オブジェクト属性情報はそのまま元どおり
- 「ごみ箱」にあるオブジェクトは180日後、墓標化(廃棄状態)に移行する

Active Directory ごみ箱を絵にすると



アカウントを削除すると、削除フラグがつき、**属性はほとんど削除された状態**で、削除されたオブジェクト専用コンテナに格納される。



アカウントを削除すると、削除フラグがつき、**属性はそのままの状態で、専用コンテナに格納される。**墓標化されるとき、リサイクルフラグがつき、属性が削除される。

Active Directoryごみ箱のいいところ

- Authoritative Restoreを行なわなくても、アカウントを復旧できる
- Ldp.exeでアカウントを復旧したときのように、属性を再設定しなくていい
- アカウントの「属性」を元どおりにしたいときは、Authoritative Restoreで

Active Directory ごみ箱の要件

- フォレスト機能レベルがWindows Server 2008 R2である
- PowerShellで有効化する(再度無効にはできない)
- ごみ箱からの取り出しもPowerShellで(GUIツールはない)
  ＊PowerGUIを使う

Active Dirctory ごみ箱を有効にする

- Import-Module ActiveDirectory
- Enable-ADOptionalFeature 'Recycle Bin Feature' –Scope ForestOrConfigurationSet -Target 'example.com'
- ドメイン名前付けマスタに実行

Active Directoryごみ箱を操作する

- オブジェクトを確認する
- Get-ADObject -filter {msDS-lastKnownRDN -eq "yamakawa"} -IncludeDeletedObject
- オブジェクトを復元する
- Get-ADObject -filter {msDS-lastKnownRDN -eq "yamakawa"} -IncludeDeletedObject|Restore-ADObject

Active Directory ごみ箱の操作(2)

- 親オブジェクトも削除されているなら、親オブジェクトを先に復旧する
- 復旧先パスはlastKnownParent属性を、復旧時の名前はmsDS-lastKnownRDN属性をデフォルトで利用するから
- Restore-ADObjectコマンドレットで-Newnameでオブジェクト名を、-Targetpathで復元先を変更できる

Active Directory ごみ箱の操作(3)

- 親OUを復旧する
- Get-ADObject -filter {msDS-lastKnownRDN -eq "Sales"} -IncludeDeletedObject|Restore-ADObject
- 子オブジェクトを復旧する
- Get-ADObject -filter {lastKnownParent -eq "OU=Sales,OU=Accounts,DC=example,DC=com" } -IncludeDeletedObject |Restore-ADObject

Demo:Active Directory ごみ箱を使う

- ごみ箱を有効にする
- ごみ箱から復旧する
- ツリー構成を復旧する

Active Directoryごみ箱の保存期間を変える

- Set-ADObject "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=example,DC=com" -Partition "CN=Configuration,DC=example,DC=com" -Replace:@{"msDS-DeletedObjectLifetime" = 10}

Active Directory廃棄状態の保存期間を変える

- Set-ADObject "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=example,DC=com" -Partition "CN=Configuration,DC=example,DC=com" -Replace:@{"tombstoneLifetime" = 30}

Active Directory PowerShell モジュール

- (数えた限り)76のコマンドレットがある
- [機能]-AD[対象]のコマンドレットが対象
- Get-Command –Module ActiveDirectoryコマンドレットで、一覧を取得できる
- Import-Module ActiveDirectoryコマンドレットを「毎回」実行して、モジュールを読み込む

Active Directory PowerShellの一例

- Get-ADObject
- Get-ADComputer
- Get-ADDomainController
- Get-ADUser
- New-ADUser
- Set-ADUser
- Search-ADAccount

細かい設定が可能なパスワードポリシーをPowerShellで

- New-ADFineGrainedPasswordPolicy -Instance $templatePSO -Name "AdminsPSO" -Precedence 200 -Description "The Domain Administrators Password Policy" -DisplayName "Domain Administrators PSO" -MaxPasswordAge "15.00:00:00" -MinPasswordLength 10
- Add-ADFineGrainedPasswordPolicySubject AdminsPSO -Subjects "Domain Admins"
- たった2行で、実現できる！

Demo:PowerShellを使う

- ユーザーを検索してみる
- ユーザーを追加してみる
- 細かい設定が可能なパスワードを設定してみる

Active Directory管理センター

- 管理用GUIツール(ADUCとは異なる)
- 新しいユーザー アカウント/コンピュータアカウント、グループの作成管理
- 新しい組織単位 (OU) およびコンテナーの作成管理
- １つ以上のドメインまたはドメイン コントローラーに接続し、ドメインまたはドメイン コントローラーのディレクトリ情報を表示管理
- クエリ作成検索を使用して、Active Directory データをフィルター

ベスト プラクティス アナライザー

- ドメインコントローラをスキャンして、最適設定(ベストプラクティス)項目の判定をしてくれる
- サーバマネージャ(GUI)
- PowerShell(別にBPAモデルが必要)

Active Directory Webサービス

- Active Dirctoryにアクセスするwebサービス
- WCFプロトコルを使う
- 9389/TCPが必要
- IISは不要

認証メカニズム保障

- 証明書(スマートカード)を使ってログオンしたユーザを、同じユーザが通常のパスワードでログオンした場合と区別する機能。
- スマートカードでログオンする場合ユニバーサルグループのメンバシップをアクセストークンに追加することで、区別する。
- Windows Server 2008 R2ドメイン機能レベルが必要

オフラインドメイン参加

- クライアントがドメインコントローラと接続していなくても、ドメイン参加を可能にする機能
- djoin.exeを使ってドメインコントローラ側でコンピュータアカウントを作成し、生成されたテキストデータを、クライアントに移動して、このデータでドメイン参加を行なう。
- Windows Serer 2008 R2およびWindow 7が必須

まとめ

- Windows Server 2008 R2 Acitve Directory はかゆいところに手が届くような、細かい機能が増えている。
- Active Directory PowerShellはほぼ必須。少しずつ慣れていこう。

参考

Active Directory ドメイン サービスの新機能

< http://technet.microsoft.com/ja-jp/library/dd378796(WS.10).aspx >

[まとめ]Windows Server 2008 R2 – Active Directory Recycle Bin に関する投稿

< http://blogs.technet.com/junichia/pages/Article-List-_2D00_-Windows-Server-2008-R2-Active-Directory-Recycle-Bin.aspx >