Managing the User Experience

Across Physical and Virtual Environments

Dan Holme
Author, *Windows Administration Resource Kit (Microsoft Press)*
Trainer & Consultant, *Microsoft Technologies Consultant, NBC Olympics*
Contributing Editor, *Windows IT Pro* magazine (*www.windowsitpro.com)*
Chief SharePoint Evangelist, *AvePoint*
Founding Partner, *Aptillon* (www.aptillon.com)

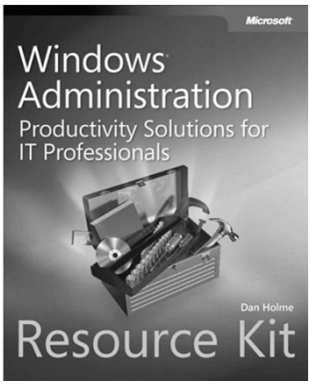
@danholme
dan.holme@intelliem.com
http://bit.ly/gPH8hn

Dan Holme

- Consultant, Trainer, Author
  - Fortune-caliber business, academic & government
  - Microsoft Technologies Consultant, NBC Olympics
  - Director of Training & Consulting, Intelliem
  - Founding partner, Aptillon
- Chief SharePoint Evangelist, AvePoint
- Microsoft Press
  - Windows Server 2008 R2 Active Directory Training Kit, Exam 70-640
  - Windows Administration Resource Kit
- *Windows IT Pro* and *SharePoint Pro* magazines
- @danholme
- dan.holme@avepoint.com
- Download slides from: http://bit.ly/gPH8hn (case sensitive)

Resources

- Windows Administration Resource Kit: Productivity Solutions for IT Professionals
  - Solutions Collection 3: Managing User Data and Settings
- Windows IT Pro magazine
  - February & March 2008 issues



Define the business requirements

Security
- Business data created by users will be secure

Mobility
- Users can access UDS from any computer
  - Physical or virtual

Availability
- UDS will be fully available at first logon

Resiliency
- Replacement of failed system with all UDS in *x* hours
- Loss of UDS will be limited in the event of client disk failure

What are your business requirements?

User profile

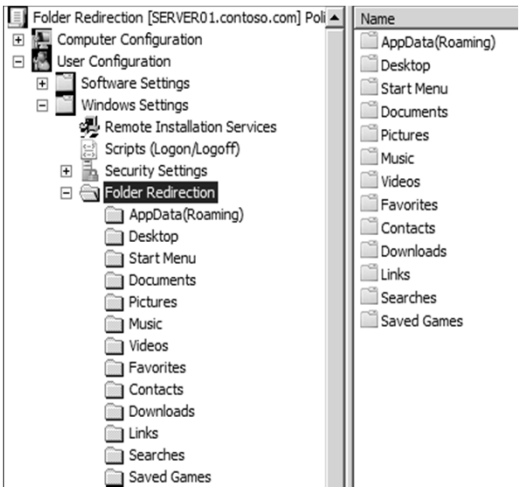
Components of UDS framework

- Redirected folders
  - Users access data in standard UI folders
  - Redirected to network data stores
- Offline files
  - Laptop users – disconnected scenarios
  - Encrypted cache – reduce risk of data loss
- Roaming profiles
  - Limited to users' registry hives (ntuser.dat), AppData & small folders
  - Small profile size – supported very well by roaming
- DFS namespaces
  - Abstract physical location of UDS data stores for easy management
- Configuration management: Group Policy
- Managing user data
  - Quotas, file screens, storage management, etc.
- Unmanaged data
  - Classes of data that aren't subject to requirements, so not on network

Keeping it simple

- Create a shared folder with correct ACLs (KB 274443)
  - \\server01\users$
- Use Group Policy to redirect folders to the shared folder
  - Basic Redirection
  - Target: \\server01\users$\%username%
- Use ProfilePath attribute to roam user profile settings
  - ProfilePath: \\server01\users$\%username%\Profile[.V2]
    - .V2 extension added automatically by Windows Vista and Windows 7
  - Redirected folders automatically excluded
- User logs on
  - Redirection may require two logons unless Always Wait for the Network…
- Windows creates user specific folders automatically
- Documents migrated at logon, settings at logoff
- All data and settings are available offline
  - Redirected folders are automatically cached by Offline Files
  - Roaming profile is synchronized at logon and logoff

Folder redirection policy settings



Offline files

- Allow redirected folders to be available offline
  - Redirected folders made available offline automatically
  - *Bad idea* for most enterprises!
    - Think about users logging on in a conference room.
  - *You must turn this behavior off!*
    - User Configuration\Administrative Templates\System\
      Folder Redirection\
      Do not automatically make redirected folders available offline
- "Pin" files offline on the user's primary computer(s)
  - As part of system provisioning

Offline files

- Eliminate errors from blocked file types
  - Default blocked types: *.slm; *.mdb; *.ldb; *.mdw; *.mde; *.pst; *.db?
  - Computer Configuration\Administrative Templates\Network\Offline Files\Files Not Cached: Set to *blank*
- Update cache if files moved in network namespace
- Know how to *reset the cache*
  - A registry entry and a restart
- Encrypt the offline files cache
  - Unless using BitLocker or another full disk encryption

Application Data

- %AppData% = %userprofile%\AppData\Roaming
- Some applications store useful data in AppData\Local
  - Microsoft Outlook *.pst files
- Some applications do not respect redirection of AppData
- Some applications do not survive state change (online to offline)

- Guidance
  - *Roam* AppData until you have completely tested redirection
  - Redirect AppData only in highly managed, tested environments

Permissions

- Permissions granted on root are not least privilege
  - Microsoft documentation (KB 274443)
    - *http://support.microsoft.com/kb/274443*
  - Least privilege ACLs
- User is granted exclusive access to redirected folders
  - Can change this in the policy setting for the redirected folder
- User is granted exclusive access to profile folders
- Must test functionality in production
  - Some apps behave badly and will break without greater permissions

DFS-N

- Redirected folder targets are tied to server and share names
  - \\server01\users$\%username%\foldername...
  - Cannot move store to new server without reconfiguation
    - Group Policy redirected folder settings, Active Directory ProfilePath
    - Offline files cache
    - User links and shortcuts
  - Cannot manage users as groups of related users
    - Relocate some users to another office and datacenter
- Solution: DFS Namespace (DFS-N)
  - DFS-N domain namespace
    - \\contoso.com\users
  - DFS-N folder and target
    - \\contoso.com\users\jfine --> \\server01\users$\jfine
  - Group Policy redirected folder targets
    - \\contoso.com\users\%username%
  - ProfilePath
    - \\contoso.com\users\%username%\Profile

What happens when a user's data moves?

- Paths of targets to redirected folders
  - Group Policy object settings
  - Registry redirection paths
- Roaming profile path
  - User account setting
- Source paths of offline files
  - Requires resetting & resynching, or re-targeting
- Paths used in applications, by shortcuts, by mapped drives, etc. (yuck!)
- Paths for links within and between documents (super yuck!)
  - between Excel worksheets in the user's Documents folder

Provisioning

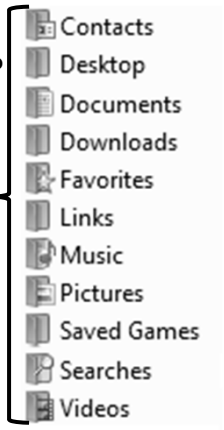
- Must provision (pre-create) folders, ACLs, and DFS-N folders

Physical (NTFS) Namespace

- Flat namespace – all folders are subfolders of *username* folder
  - Problematic because data management requirements are *not* flat

Identify and classify data

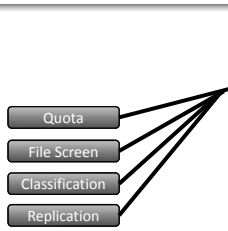
- What "stores" of data exist?
  Which ones are related—variations on a theme?
- What types of data should be managed similarly?
- Proposal: four classes of data
- Settings: Application Data (AppData\Roaming)
- User data
- E-mail archives
  - Outlook: AppData\Local\Microsoft\Outlook*.pst
  - Notes: Program Files\Lotus\Notes\Data
- Archives, backups, long-term storage

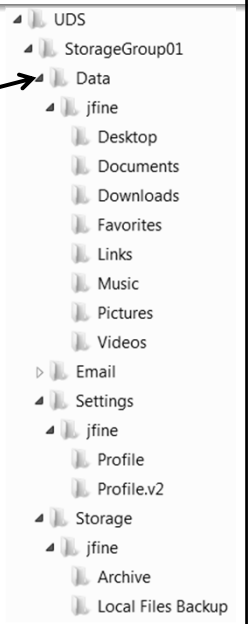


Which data types are, or are not, subject to each of the business requirements?
What are the *information management* characteristics of each data type?

Represent data classes in NTFS namespace

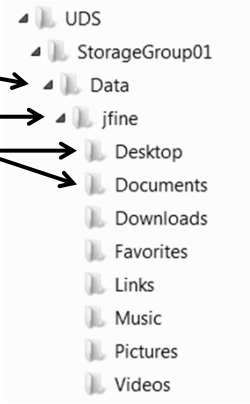
- *DataClass* folders for each class of data
  - Business data
  - Email
  - Settings
  - Storage (Archived files)
  - You may have more or fewer *DataClass* folders based on your business requirements
- Provide a *management scope*
  - Quotas
  - File screens
  - File classification
  - Storage management
    - e.g. Archives on slower/cheaper storage
    - Different replication policies





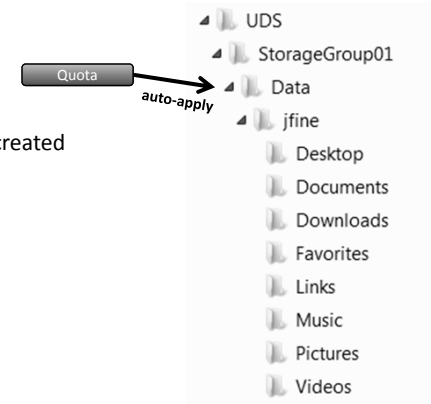
Data: Physical (NTFS) namespace

- **Data** folder
  - Contains user data stores
  - Provides a scope to manage *all* users' data
  - ***username*** folder
    - **Subfolders** are data stores equivalent to those in the user profile
    - You may or may not redirect all profile folders, based on business requirements
- Security
  - User is the only one with access to the *contents* of the data stores
  - Support/Admin can see to (but not into) the data stores
  - Role-based access into user data stores
    - Auditing (Read Only)
    - Administration (Full Control)
      - Virus scanner
      - Security group for "emergency" access



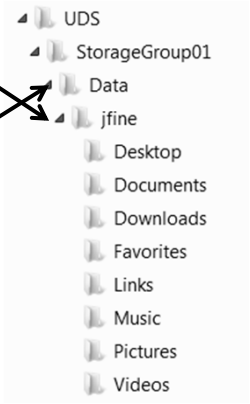
Quotas

- Default quota
  - Applied to *DataClass* folder
  - Configured to auto-apply
    - Applies to all existing folders
    - Applies to each new folder when created
- Exception quotas
  - Apply directly to user folder



Security

- User is the only one with access to the *contents* of the data stores
- Support/Admin can see to (but not into) the data stores
- Role-based access into user data stores
  - Auditing (Read Only)
  - Administration (Full Control)
    - Virus scanner
    - Security group for "emergency" access



Create the data class folder

- Create data class root folder ("Data")
- Apply least privilege permissions to folders
  - System::Allow:Full Control
    - Apply To: This folder, subfolder, and files
  - Administrators::Allow:Full Control
    - Apply To: This folder and subfolders
    - Apply permissions within this container only
    - Segregate roles between *system* Administrator and *data* administrators
  - UDS Data Admins::Allow::Full Control
    - Apply To: Subfolders and files
    - This is the limited group that should have full control of all UDS
  - UDS Data Audit::Allow::Read & Execute
    - Apply To: This folder, subfolder, and files
    - This is the limited group that should have read access to all UDS

What's missing?

- Users!
- That's right, users require *zero* permissions on the root
  - User has Full Control of user's specific top-level folder (jfine)
  - Traverse Folders user right (assigned to Everyone by default) allows user to "jump through" to his or her folder even though (s)he doesn't have permission to root
- Now *that* is least privilege
- The catch: you must provision the user folders

Data: DFS-N Options

- DFS-N options
  - One DFS-N folder for all user profiles
    - DFS-N Folder: \\contoso.com\users\Data
    - Target: \\server01\Data$
    - ProfilePath: \\contoso.com\users\Data\%username%\Profile
  - One DFS-N folder per user data store
    - DFS-N Folder: \\contoso.com\users*username*\Desktop [Documents, etc.]
    - Target: \\server01\Data$*username*\Desktop [Documents, etc.]
    - ProfilePath: \\contoso.com\users\%username%\Profile
      - .V2 added automatically by Windows Vista and later clients

DFS namespace recommendations

- Goal: the location of the user's folders in the DFS namespace *never changes*
- Data class or fully enumerated DFS namespace
- Scalability: More than 5000 folders needed?
  - Upgrade to Windows Server 2008 domain functional level
    - 300,000 folders in a DFS namespace in R2

  or
  - Create "groupings" of users in the DFS namespace
    - Make grouping *arbitrary*, not based on sites or any other business construct
      - e.g. \\contoso.com\Users01, \\contoso.com\Users02, …
    - Tip: Groupings of employees by employee number

Folder redirection

- For Documents and Desktop
  - Not for Start Menu or Application Data*
  - For other folders based on requirements
- When configuring redirection policies, choose
  - "Redirect to the following location"
  - *namespace*\%username%*folder*
- Don't do advanced folder redirection
  - You will want to configure other policy settings that aren't multivalued
  - Instead, create one GPO per group
- Settings tab
  - Grant the user exclusive rights: CLEARED
  - Move the contents: CLEARED
  - Also apply redirection to XP: SELECTED (when available)
  - Removal: Leave the folder in the new location

Folder redirection

- Fix the UI
  - Vista leaves the default folders in place so you see "two of everything"
  - Applications ("bad" ones) will drop a user into the %userprofile% folder and/or re-create the folders if you delete them

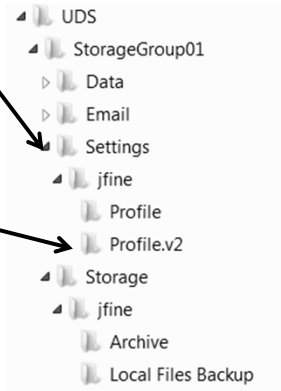
- Preference
  - Folder: Update the %userprofile%*foldername* folder
    - Set to Hidden
  - Shortcut: Put a shortcut in %userprofile%*foldername* that provides easy navigation to network folder
- *or* a *junction* (%username%*foldername*) for each folder
  - Requires Vista+ clients
  - Must be created per-user but requires admin credentials
  - I don't have an answer for you yet on this one

Settings: Physical (NTFS) Namespace

- Settings folder

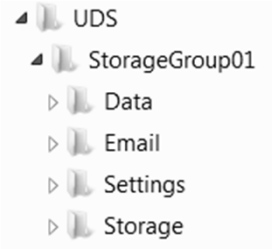
  Contains roaming profiles

  Provides a scope to manage *all* users' settings
  - *username* folder
    - Profile
      - Used by Windows XP
    - Profile.v2
      - Used by Vista, Windows 7 Windows Server 2008/R2
    - VDIProfile.V2 (not shown)
      - Used by virtual and remote infrastructure



Physical namespace

- Storage Group folder
  - Provides management scope for all users contained in the storage group
    - Replication
    - Permissions & policies
    - Auditing
    - SLAs

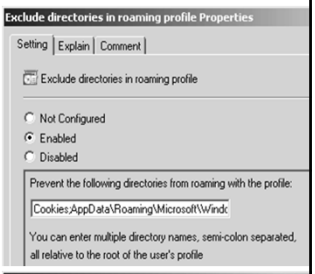


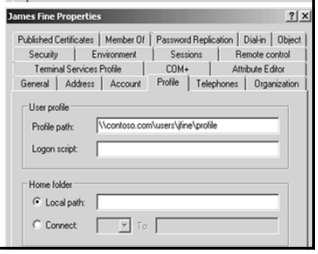
Settings: DFS-N Options

- DFS-N options
  - One DFS-N folder for all user profiles
    - DFS-N Folder: \\contoso.com\users\Settings
    - Target: \\server01\Settings$
    - ProfilePath: \\contoso.com\users\Settings\%username%\Profile
  - One DFS-N folder per user profile
    - DFS-N Folder: \\contoso.com\users*username*\Profile.V2
    - Target: \\server01\Settings$*username*\Profile.V2
    - ProfilePath: \\contoso.com\users\%username%\Profile
      - .V2 added automatically by Windows Vista and later clients

User profiles: Managing roamed folders

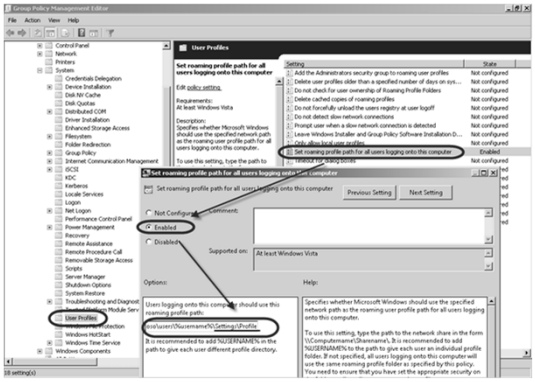
- Configure the folders that will not roam
  - User Configuration\Administrative Templates\System\User Profiles\ Exclude directories in roaming profiles except…
- What *will* roam
  - ntuser.dat
    - Roaming profile is the only real option for meeting requirements for this UDS store
  - Application Data
    - Can redirect (technically)
    - Requires *lots* of validation
      - Applications looking for %userprofile%\Application Data
      - Access from network
      - Offline state transition
  - Links*
  - Other shell folders not redirected





User profiles: Physical vs. Virtual

- Profile configuration with Group Policy
  - Applies to Windows Vista, Windows 7, Windows Server 2008 & R2
  - Computer Configuration policy setting
    - Can use %username% in the path
  - Allow "segregation" of profiles between environments
    - Physical vs. virtual



User profiles

- Setting synchronization
  - Some apps put settings in bad places
    - %userprofile%\AppData\Local\...
    - c:\programdata\...
  - "Manual" roaming
  - Script that copies settings at logon & logoff
  - A *junction* that redirects the folder to the desired location

Storage: Physical (NTFS) namespace

- Storage folder
  - Not a subfolder of data
    - Provides a unique scope for quotas & other management
  - Archive folder
    - Data that isn't needed regularly and therefore doesn't need to be available offline for laptop users
    - User and/or enterprise manages what goes in, when and how
  - Local Files Backup folder
    - Backup of Local Files folder
    - Enterprise manages what data goes in, when, and how
  - You might split these two into separate *DataClass* folders

38

Resources

- Windows Administration Resource Kit: Productivity Solutions for IT Professionals
  - Solutions Collection 3: Managing User Data and Settings
- Windows IT Pro magazine
  - February & March 2008 issues
- dan.holme@avepoint.com
- @danholme
- Questions & Answers
- Please fill in your feedback forms!