

Active Directory Best Practices Ten Years Later

Dan Holme, MVP, SharePoint

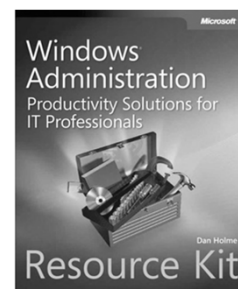
Author, *Windows Administration Resource Kit* (Microsoft Press)
Trainer & Consultant, *Microsoft Technologies Consultant*, *NBC Olympics*
Contributing Editor, *Windows IT Pro* magazine (www.windowsitpro.com)
Chief SharePoint Evangelist, *AvePoint*
Founding Partner, *Aptillon* (www.aptillon.com)

@danholme
dan.holme@avepoint.com
Slides: <http://bit.ly/gPH8hn> (Case Sensitive)



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
- Slides & scripts: <http://bit.ly/gPH8hn>



ACTIVE DIRECTORY DESIGN

Domain Controllers

- Keep them “clean”
- Virtualization
- Read-Only Domain Controllers (RODCs)
 - *TEST* against applications in production

Forest and Domain Design

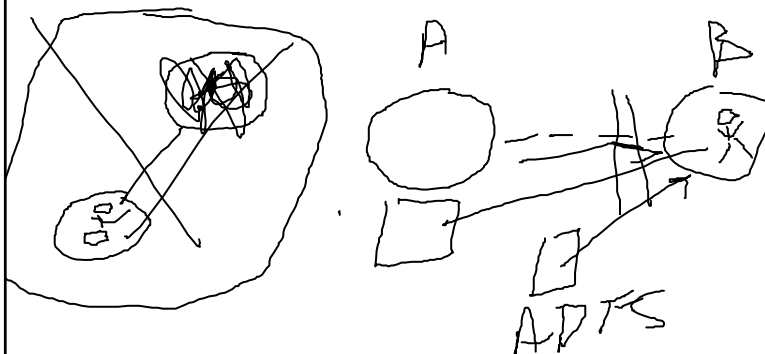
Out

- Multi-domain forests out
- Trust relationships

In

- Single-domain forests
- Federated identity & claims-based authentication with Active Directory Federated Services (ADFS)

Multi-domain forests



Trust relationships

Federation

OU Design

- Design *first* for security (delegation/administration/ACLs)
- Object-based models are most typical
 - Users: ACLed the same
 - Administrative identities: separated from standard users
 - Client computers: typically by site – who can *add computers to domain*?
 - Servers: typically by role
 - Groups: highly varied

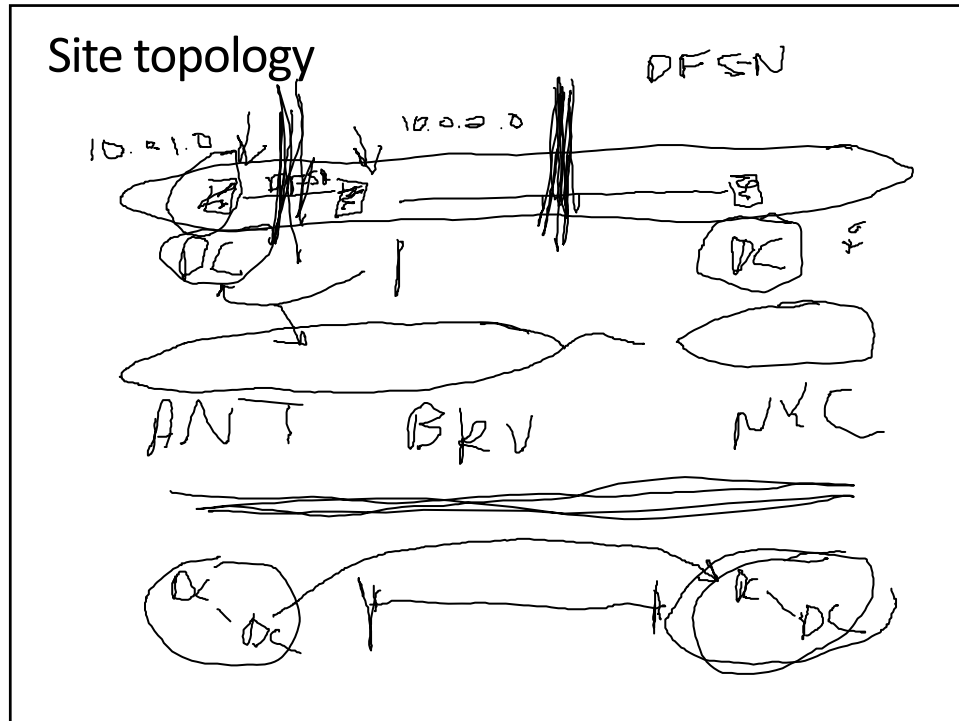
OU Design

Group Policy

- Policies
- Preferences
- Scoping Group Policies
 - WMI filters – use sparingly
 - Global security group filters – very effective!
 - Apply a GPO to a group
 - Remove Authenticated Users
 - Add the group
 - On the DELEGATION tab, click ADVANCED, and assign AUTHENTICATED USERS – ALLOW – READ permission
 - Facilitates troubleshooting
 - Deny a GPO to a group
 - On the DELEGATION tab, click ADVANCED, and assign Group – DENY – APPLY GROUP POLICY permission
 - ALWAYS include a “Deny” group
- Test group policies *in production*
 - Filter to apply GPO only to test users/computers

Site topology

- What's changed
 - Networks are good, need for sites to partition replication has decreased
 - Fewer sites
 - Increased use of replicated resources for performance, DR
- What's needed
 - More sites
 - Sites without domain controllers (domain controller-less sites)
 - Partition replicated resources (DFSN/DFSR)



Subnets

- What's changed
 - Multiple components, tools, technologies rely on AD sites
 - Domain controller location
 - Increased mobility: Where's ComputerX?
- What's needed
 - You *must* have a process by which IP subnets are synch'ed with AD DS
 - Ensure all IP addresses are associated with an AD subnet (therefore, site)
 - IP address provisioning
 - Use the LOCATION attribute of the AD subnet
 - US\LA\MSY\ConventionCenter\AudA

Replication

- What's changed
 - Networks are good
 - Increased need for convergence
 - People trust AD
- Notification-based replication
 - Change *intersite* replication to use notification-based replication
 - Same as intrasite
 - Reduce convergence of replication
 - Reduce issues related to password change, group change, lockout, etc.

ADMINISTRATIVE ROLES

Guidance: 2-3 accounts for admins

- Separate accounts for users vs. admins (“secondary logon” or “RunAs” accounts)
- User (non-privileged)
 - In “user identities” OU
- Administrative (privileged)
 - In “admin identities” OU
 - Client support (local Admin on clients)
 - Server support (local Admin on servers)
 - Service admins (e.g. SQL, Exchange)
 - AD data admin (can modify objects in AD)
- Administrative (super-privileged)
 - In “admin identities” OU
 - AD data admin (can create or delete or move objects)
 - AD service admin (physical access to DCs, restore AD)

Active Directory Administration & Delegation

- Domain’s Administrator account
 - Super-secured, never used, in-case-of-emergency-break-glass
- Domain Admins, Enterprise Admins, domain’s Administrators groups
 - E-M-P-T-Y (more or less): Custom accounts for use only as needed
 - Protected accounts: adminSDHolder
- Schema Admins
 - Empty. Add members when schema change needed.
- Builtin groups (Account/Server/Print/Backup Operators) empty
 - Over-delegated
 - Protected accounts (adminSDHolder)
- Audit changes to these groups using Directory Service Changes auditing

System Administration

- Remove Domain Admins from the local Administrators group
- Define scopes of computers
- Create (global or domain local) role groups defining scopes of administration
 - e.g. SYS_NYC_Clients_Admis, SYS_FileServer_Admis
- Use Group Policy Restricted Groups to specify Administrators membership
 - Use MemberOf setting – cumulative

USER ACCOUNTS

User Logon Names: A Modest Proposal

- Pre-Windows 2000 Logon Name (*sAMAccountName*)
 - %username% - used in numerous places - unlikely to untangle
 - **Unique in the enterprise** (Employee ID or alias)
- User Principal Name (UPN)
 - Make it the same as the user's email address
- Cultural change: Log on with email address – users never forget it!
- Rename Administrator
 - Not for security – to reduce confusion and potential for lockout
 - Use Group Policy to scope name differently to different classes of computers

Passwords

- A short complex password is *not* secure and *not* usable
- A short *phrase* is secure!
 - Antwerp is fun!
- Fine-grained password policies
 - Domain administrators
 - Service accounts

Generic User Accounts

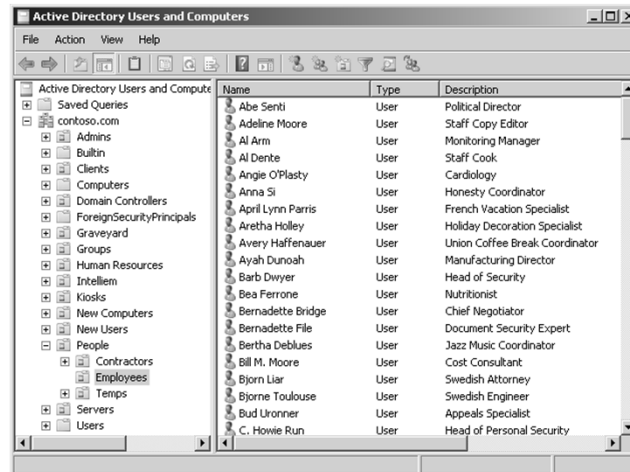
- Security death wish
- Typical scenarios
 - Internet access
 - Kiosk
- Consider *local* account
 - Unique password on each system where needed
 - So account cannot authenticate to other systems with the generic account
 - Create account with same name in the domain
- Better yet: unique accounts for each user, managed the same way
 - User name: Intern01, Intern02, Intern03 – Unique passwords
 - In a group, “INTERN” that defines user experience

best practices

LAST NAME, FIRST NAME



Scenario: User management

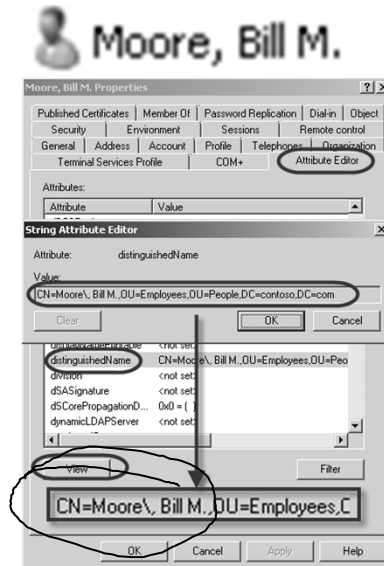


Problem: Finding users easily

Name	Type	Description
Bernadette Bridge	User	Chief Negotiator
Bernadette File	User	Document Security Expert
Bertha Deblues	User	Jazz Music Coordinator
Bill M. Moore	User	Cost Consultant
Bjorn Liar	User	Swedish Attorney
Bjorne Toulouse	User	Swedish Engineer
Bud Uronner	User	Appeals Specialist
C. Howie Run	User	Head of Personal Security
Candace Guy	User	Downsizing Consultant
Candy U Callback	User	Customer Complaints Specialist

Solution: The wrong solution

- Do not use <Last>, <First> as the common name
- LDAP distinguishedName is delimited by commas, so commas are 'escaped'
- Throws off many scripts and apps
- displayName can be <Last>, <First>

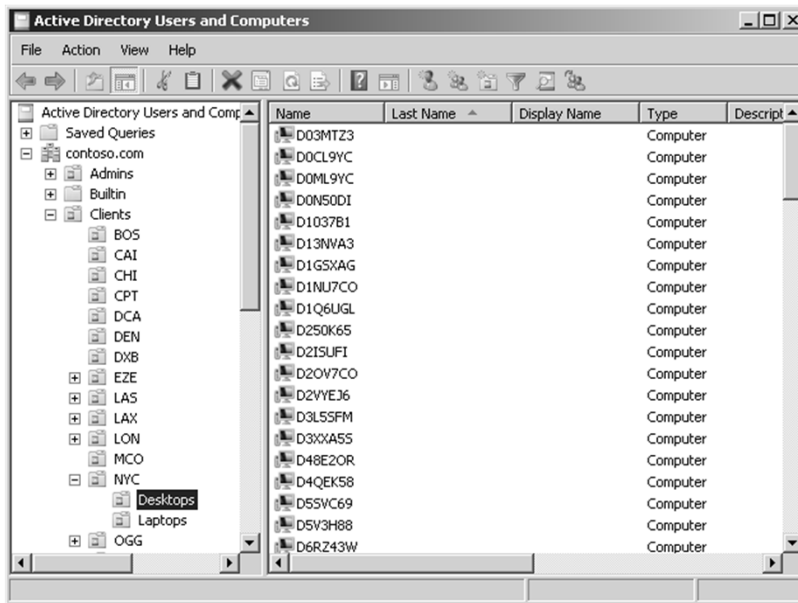


Solution: Customize MMC view

- View → Add / Remove Columns
 - Last Name or Display Name
- Sort by Last Name or Display Name

Name	Last Name ^	Display Name
Warren T. Mifutt	Mifutt	Mifutt, Warren T.
Maury Missions	Missions	Missions, Maury
Adeline Moore	Moore	Moore, Adeline
Bill M. Moore	Moore	Moore, Bill M.
Tara Neuwon	Neuwon	Neuwon, Tara
Hadley Newham	Newham	Newham, Hadley

New problem: View affects all OUs



EXTREME MMC CONSOLES

The MMC

- Simple custom consoles
 - Start → Run → mmc.exe
 - Add snap-ins (File menu)
 - Save
 - To (shared or local) location that is *accessible* by
 - Your (Run As Administrator) administrative credentials
 - Other administrators
 - **Recommendation**
 - **Remote Desktop Application** or
 - Deploy custom consoles & supporting tools/scripts to administrators in a local location, e.g.
c:\Program Files\RTN Admin Tools
Use Group Policy Preferences to keep it up-to-date
- RSAT required

Secure administration

- Maintain at least two accounts
 - A standard user account
 - An account with administrative privileges
- Log on to your computer as a standard user
 - Do not log on to your computer with administrative credentials
- Launch administrative consoles with Run As Administrator
 - Right-click → **Run as administrator**
- New in 2008R2/Win7
 - **Shift+Right-click → Run as different users**



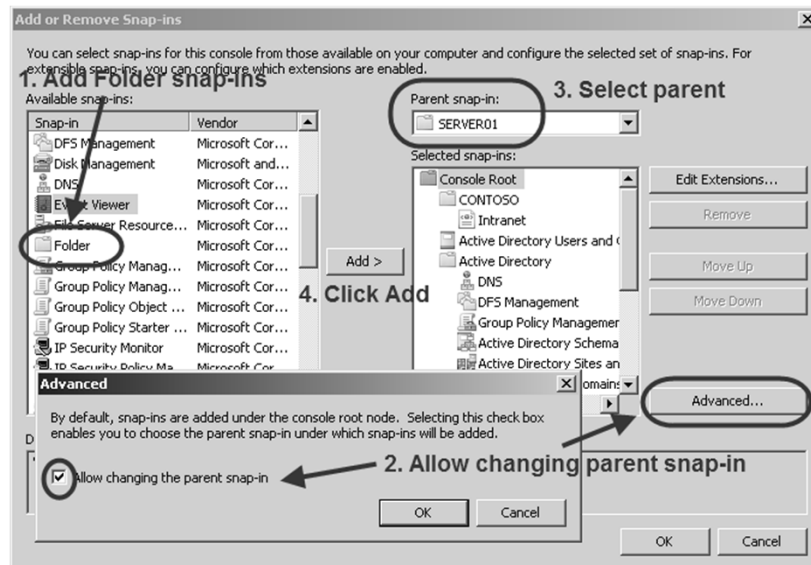
Security benefit of custom consoles

- One tool with multiple snap-ins makes enforcing Run As Administrator easier
 - One shortcut configured to Run As Administrator
 - Shortcut Properties → Advanced
 - Put shortcut in Startup group
 - Custom console launches immediately after logon, prompting you for your admin credentials.

Customized MMC consoles

- Rename the root (Console Root)
- Create folders to organize your snap-ins
 - Folder per server or per task group
 - In the Add or Remove Snap-Ins dialog, click Advanced
 - Select “Allow changing the parent snap-in”
 - When adding a snap-in, select the parent before clicking Add


Creating a hierarchical console



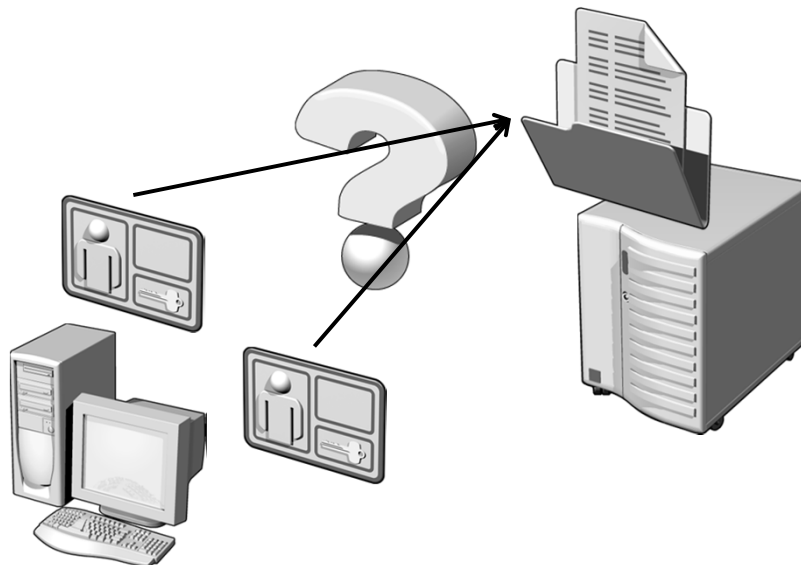
Snap-ins that rock

- Remote Desktops snap-in
 - Connect to console
 - Not available in stand-alone RDP client!
 - Windows Server 2008, you no longer connect to console
 - One snap-in with connections to all servers
 - One snap-in per server folder with connection to that server

Snap-ins that rock

- Link to Web Address 
 - Expose in MMC an external web resource
 - <http://support.microsoft.com/search/?adv=1>
 - Exposing in the MMC an intranet web resource
 - Policies and procedures documentation
 - Performance and monitoring reports
 - Environment documentation & diagrams
 - Admin Web applications, e.g. your help desk ticket system
 - SharePoint site for admins (or other collaboration site)
- Note: connection uses MMC's credentials

Two accounts to same server?



Snap-ins that rock

- Link to Web Address
 - Exposing a share on a server (totally under-documented!)
 - Use a UNC (\\server\share) instead of a URL
 - Add server to IE Local Intranet or Trusted Sites zone
 - Add it as \\server. IE will change it to file:// syntax
 - Connection uses MMC's (admin) credentials
 - Similar to "map drive using another account"

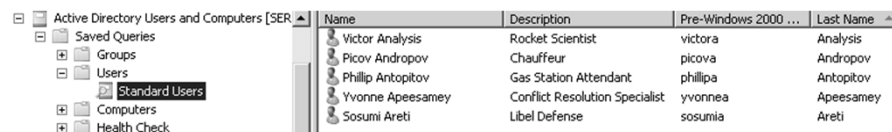
demo

SAVED QUERIES

Saved queries

- Use SAVED QUERIES for administrative views
 - Don't even try using actual OUs/nodes in ADUC
- Benefits
 - Columns (View → Columns) unique to saved query
 - Add Last Name column to a saved query ☺
 - In an OU you get Last Name in *every* OU ☹
 - “Virtualizes” complex AD structure
 - Efficient administrative views
 - e.g. disabled users, locked out users, users with passwords set to not expire
 - Manage users by group

Unique views per query



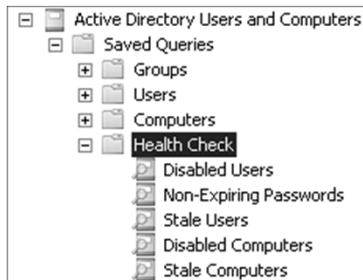
The screenshot shows the 'Active Directory Users and Computers' console tree on the left. The 'Standard Users' query is selected. The main pane displays a table of users with columns: Name, Description, Pre-Windows 2000 ..., and Last Name.

Name	Description	Pre-Windows 2000 ...	Last Name
Victor Analysis	Rocket Scientist	victora	Analysis
Picov Andropov	Chauffeur	picova	Andropov
Phillip Antopitov	Gas Station Attendant	phillipa	Antopitov
Yvonne Apeesamey	Conflict Resolution Specialist	yvonnea	Apeesamey
Sosumi Areti	Libel Defense	sosumia	Areti

Virtualized view of your enterprise hides the complexity of OU design



Efficient administrative views



Manage users by *group* (not OU)

- Create a saved query that lists the (direct) members of a group
(&(objectCategory=user)
(memberOf=*DN of Group*))
no wildcards—DN must be exact

demo

TASKPADS

Create a taskpad

Create a custom MMC console:

1. Click Start and choose the Run command (Windows XP), or click in the Search box (Windows Vista/Windows Server 2008) type **mmc.exe**, and then press Enter.
An empty MMC console appears.
2. Choose File → Add/Remove Snap-In.
3. Add the Active Directory Users and Computers snap-in.
4. Save the console: File → Save.
 - Save in a location accessible by *both* your user and administrative credentials

Now you must create what is called a *taskpad*:

1. Expand the details pane of the console to an OU that contains users.
2. Right-click the OU, and choose New Taskpad View.
3. The New Taskpad View Wizard appears. Click Next.
4. On the Taskpad Style page, accept all defaults and click Next.
5. On the Taskpad Reuse page, select Selected Tree Item and click Next.
6. On the Name And Description page, accept or change the default name and description and click Next.
7. On the Completing page, be sure the check box is selected and click Finish.

Create a taskpad menu command

You have actually finished creating the taskpad, and a second wizard launches to help you create the task on the taskpad:

1. Launch the New Task Wizard. Either:
 - Continue to the New Task Wizard from the New Taskpad Wizard, or
 - Right-click the container to which the taskpad is associated → Edit Taskpad View → Tasks → New
2. The New Task Wizard appears. Click Next.
3. On the Command Type page, choose Menu Command and click Next.
4. In the Menu Command box, select the command.
 - See important note on next slide
5. Click Next.
6. On the Name And Description page, in the Task Name box, type a name.
7. Optionally, enter a description.
8. Click Next.
9. On the Task Icon page, select an icon.
Custom icons: c:\windows\system32\shell32.dll (XP or later) or
c:\windows\system32\imageres.dll (Vista / 2008)
10. Click Next.
11. Click Finish.

Taskpad menu command tips

- Menu commands are what you see when you right-click an object
 - Major “trap”: to create a task in a task pad, there must be an object upon which the task can be performed, and you must have rights to perform the task. For example, if you want to add a task to unlock a user account, there must be a LOCKED user account in the node in order for you to add the task to the taskpad. If you want to add tasks for “enable user account” there must be a disabled user account; etc.
- Find cool icons in system32\shell32.dll

Taskpads as an "Admin Launch Pad"

- Create tasks for Shell commands
 - Can be any command you can run from Start → Run
 - For command-line commands, prefix with cmd.exe /c
- Anything that launches will launch with same credentials as MMC (admin/alternate creds)
- Suggestion
 - Add a folder snap-in
 - Rename the folder Tools
 - Create a taskpad view with "No List" view
 - Add shell command tasks

Create a taskpad shell command

You have actually finished creating the taskpad, and a second wizard launches to help you create the task on the taskpad:

1. Launch the New Task Wizard. Either
 - Continue to the New Task Wizard from the New Taskpad Wizard, or
 - Right-click the container to which the taskpad is associated → Edit Taskpad View → Tasks → New
2. The New Task Wizard appears. Click Next
3. On the Command Type page, choose Shell Command and click Next
4. In the Command box, type the command
5. In the Parameters box, type the parameters
6. Click Next
7. On the Name And Description page, in the Task Name box, type a name
8. Optionally, enter a description
9. Click Next
10. On the Task Icon page, select an icon
Custom icons: c:\windows\system32\shell32.dll (XP or later) or
c:\windows\system32\imageres.dll (Vista / 2008)
11. Click Next
12. Click Finish

Taskpads for simplified admin

- Navigation between taskpad nodes in a console
 1. Create a 'home page' snap-in with a taskpad view
 - e.g. Link To Web Address snap-in showing IT intranet site
 2. Add taskpad nodes to Favorites (Favorites menu)
 3. Add tasks to the home page taskpad that are “Navigation tasks” to other nodes
 4. Add tasks to each node that are Navigation tasks back to home page
 5. After linking each node you can hide the MMC tree
- View → Customize and lock down the MMC UI
- File → Options, save in a user mode

demo

CUSTOM COMMANDS

Integrate a custom command

- Locate a useful command, script, or tool
 - `mstsc /v:ComputerName`
`[/h:WindowHeight /w:WindowWidth | /full]`
`[/console | /admin]`
- Identify *parameters* that can be passed
 - *ComputerName*
- Add the command as a *shell task* to an MMC taskpad

Create a taskpad task

1. Launch the New Task Wizard. Either
 - Continue to the New Task Wizard from the New Taskpad Wizard, or
 - Right-click the container to which the taskpad is associated → Edit Taskpad View → Tasks → New
2. The New Task Wizard appears. Click Next.
3. On the Command Type page, choose Shell Command and click Next
4. In the Command box, type **mstsc.exe**
5. In the Parameters box, type **/v:**
6. With the cursor positioned after the colon, click the arrow (browse button)
7. Select Name as a parameter for computers
 - Most computer-related tasks will use NAME as the parameter
 - Most user and group related tasks will use PRE-WINDOWS 2000 LOGON NAME as the parameter

Create a taskpad task

8. The Parameters box should look like this: **/v:\$COL<0>**
For a user or group, it will look like this: *parameters \$COL<9>*
9. Click Next
10. On the Name And Description page, in the Task Name box, type **Connect with Remote Desktop**. Optionally, enter a description
11. Click Next
12. On the Task Icon page, select an icon
Custom Icon: c:\windows\system32\shell32.dll (XP or later) or
c:\windows\system32\imageres.dll (Vista / 2008)
13. Click Next
14. Click Finish

Open remote command prompt

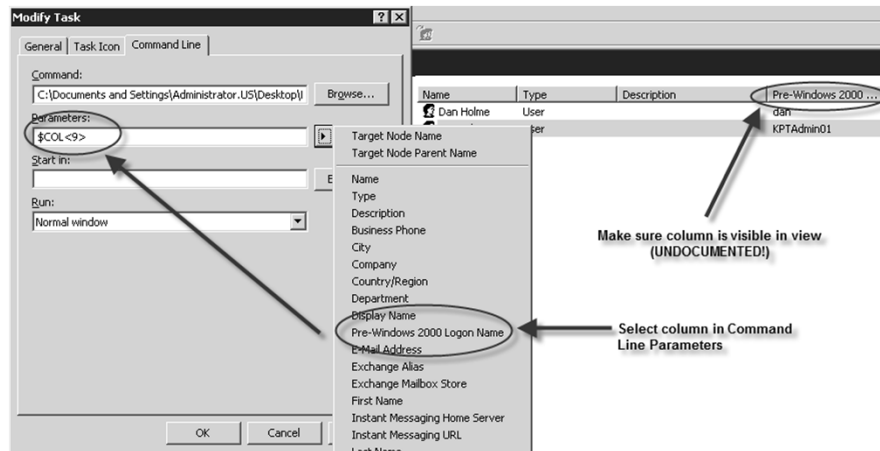
- PSEXec for remote command execution
 - Download from <http://technet.microsoft.com/sysinternals>
 - Put in system path (e.g. SYSTEM32)
or include full path in task command
- psexec `\\computername cmd.exe`
- Create shell command task
 - Command: **psexec.exe**
 - Parameters: `\\NAME cmd.exe`
`\\$COL<0> cmd.exe`

Critical custom task step

Now there's one more *very* important step. This step is *so easy to forget* and *so confusing to solve if you forget it* that I recommend you *don't forget this step!* **Any column referenced as a parameter for the task *must* be visible.** Otherwise, the task won't appear when you select an object.

1. Click View and then click Add/Remove Columns.
2. Select Pre-Windows 2000 Logon Name, and click Add.
3. Click OK to close the Add/Remove Columns dialog box.
4. Save the console.

A custom shell task

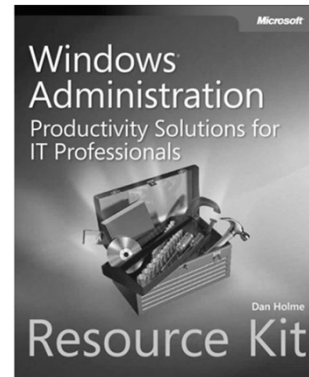


Remove a task or taskpad

- Remove a task
 - Right-click OU → Edit Taskpad View → Tasks tab → *task* → Remove
- Remove taskpad view
 - Right-click OU → Delete Taskpad View

Resources

- Windows Administration Resource Kit: Productivity Solutions for IT Professionals
- Windows IT Pro magazine
- dan.holme@avepoint.com
- @danholme
- Questions & Answers
- Please fill in your feedback forms!



Stay up to date with TechNet Belux

Microsoft | TechNet



Register for our newsletters and stay up to date:

<http://www.technet-newsletters.be>

- Technical updates
- Event announcements and registration
- Top downloads



Join us on Facebook

<http://www.facebook.com/technetbe>

<http://www.facebook.com/technetbelux>



LinkedIn: <http://linkd.in/technetbelux/>



Twitter: [@technetbelux](https://twitter.com/technetbelux)

Download

MSDN/TechNet Desktop Gadget

<http://bit.ly/msdntngadget>



TechDays 2011 On-Demand



- **Watch** this session on-demand via TechNet Edge
<http://technet.microsoft.com/fr-be/edge/>
<http://technet.microsoft.com/nl-be/edge/>
- Download to your favorite MP3 or video player
- Get access to slides and recommended resources by the speakers



THANK YOU

Dan Holme, MVP, SharePoint
Chief SharePoint Evangelist, AvePoint
Author, *SharePoint 2010 Training Kit* (Microsoft Press)
Trainer & Consultant, *Microsoft Technologies Consultant*, *NBC Olympics*
Community Lead, www.sharepointpromag.com
Founding Partner, *Aptillon* (www.aptillon.com)

@danholme
dan.holme@avepoint.com
Slides: <http://bit.ly/gPH8hn> (Case Sensitive)

