Test Lab Guide: Demonstrate Windows Server "8" Beta AD DS Simplified Administration

Microsoft Corporation

Published: February 2012

Abstract

This Microsoft Test Lab Guide (TLG) introduces Active Directory Domain Services Simplified Administration and provides step-by-step demonstration of new features in Windows Server "8" Beta.



Copyright Information

This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2012 Microsoft Corporation. All rights reserved.

Date of last update: February 22, 2012

Microsoft, Windows, Active Directory, Internet Explorer, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Introduction to Test Lab Guides 5](#_Toc317786782)

[What Is AD DS Simplified Administration? 5](#_Toc317786783)

[In this guide 6](#_Toc317786784)

[Test lab overview 6](#_Toc317786785)

[Hardware and software requirements 7](#_Toc317786786)

[User account control 8](#_Toc317786787)

[Windows PowerShell and remote pasting in Hyper-V virtual machines 8](#_Toc317786788)

[Steps for Upgrading the Existing AD DS Forest 9](#_Toc317786789)

[Step 1: Configure EXISTINGDC 9](#_Toc317786790)

[Install the operating system on EXISTINGDC 9](#_Toc317786791)

[Configure TCP/IP properties and computer name on EXISTINGDC 10](#_Toc317786792)

[Configure EXISTINGDC as a domain controller using Server Manager 10](#_Toc317786793)

[Step2: Configure NEWDC1 13](#_Toc317786794)

[Install the operating system on NEWDC1 13](#_Toc317786795)

[Configure TCP/IP properties on NEWDC1 13](#_Toc317786796)

[Rename the computer to NEWDC1 14](#_Toc317786797)

[Upgrade the existing forest using NEWDC1 and Server Manager 15](#_Toc317786798)

[Step 3: Complete Post-Upgrade Tasks on NEWDC1 16](#_Toc317786799)

[Create a user account in Active Directory on NEWDC1 16](#_Toc317786800)

[Move the PDC emulator FSMO role to NEWDC1 18](#_Toc317786801)

[Update the DNS client settings on EXISTINGDC 19](#_Toc317786802)

[Steps for adding a second Windows Server "8" Beta domain controller using Windows PowerShell 20](#_Toc317786803)

[Configure NEWDC2 20](#_Toc317786804)

[Install the operating system on NEWDC2 20](#_Toc317786805)

[Configure TCP/IP properties on NEWDC2 21](#_Toc317786806)

[Rename the computer to NEWDC2 22](#_Toc317786807)

[Promote NEWDC2 to a domain controller using Windows PowerShell 22](#_Toc317786808)

[Steps for adding a third Windows Server "8" Beta domain controller using remote management tools 24](#_Toc317786809)

[Step 1: Configure CLIENT1 24](#_Toc317786810)

[Install the operating system on CLIENT1 24](#_Toc317786811)

[Configure TCP/IP properties on CLIENT1 25](#_Toc317786812)

[Join CLIENT1 to the ROOT domain 25](#_Toc317786813)

[Install RSAT on CLIENT1 26](#_Toc317786814)

[Step 2: Configure NEWDC3 26](#_Toc317786815)

[Install the operating system on NEWDC3 27](#_Toc317786816)

[Configure TCP/IP properties on NEWDC3 27](#_Toc317786817)

[Rename and join NEWDC3 to the domain 27](#_Toc317786818)

[Configure NEWDC3 as a domain controller using Server Manager remotely from CLIENT1 28](#_Toc317786819)

[Decommission EXISTINGDC from the AD DS Forest 30](#_Toc317786820)

[Step 1: Move the remaining FSMO Roles 30](#_Toc317786821)

[Step 2: Reconfigure DNS client on NEWDC1 32](#_Toc317786822)

[Step 3: Demote EXISTINGDC 33](#_Toc317786823)

[Use New AD DS Simplified Administration Features in Windows Server "8" Beta 35](#_Toc317786824)

[Enable the Active Directory Recycle Bin using Active Directory Administrative Center 35](#_Toc317786825)

[Create, delete, and restore an object using Active Directory Administrative Center 36](#_Toc317786826)

[Create, delete, and restore an OU containing several objects using Active Directory Administrative Center 38](#_Toc317786827)

[Create Fine Grained Password Policies using Active Directory Administrative Center 40](#_Toc317786828)

[Use the Active Directory Administrative Center Windows PowerShell History Viewer to learn commands 42](#_Toc317786829)

[Use Server Manager to group and monitor domain controllers 43](#_Toc317786830)

[Appendix 46](#_Toc317786831)

[Set UAC behavior of the elevation prompt for administrators 46](#_Toc317786832)

[Pasting text to Hyper-V guests sometimes results in garbled characters 46](#_Toc317786833)

[Additional Resources 48](#_Toc317786834)

# Introduction to Test Lab Guides

Test Lab Guides (TLGs) allow you to get hands-on experience with new products and technologies using a pre-defined and tested methodology that results in a working configuration. When you use a TLG to create a test lab, instructions tell you what servers to create, how to configure the operating systems and platform services, and how to install and configure any additional products or technologies. A TLG experience enables you to see all of the components and the configuration steps on both the front-end and back-end that go into a single- or multi-product or technology solution.

# What Is AD DS Simplified Administration?

AD DS Simplified Administration is a reimagining of domain deployment and management in Windows Server "8" Beta. AD DS role deployment is now part of the new Server Manager architecture and allows remote installation, management, and monitoring. The AD DS deployment and configuration engine is now Windows PowerShell, even when using a graphical setup. The Active Directory Module for Windows PowerShell is now includes cmdlets for replication topology management, Dynamic Access Control, and other new operations.

The Active Directory Administrative Center includes a graphical Active Directory Recycle Bin, graphical Fine-Grained Password Policy management, and Windows PowerShell history viewer. Schema extension, forest preparation, and domain preparation are remote-capable, automatically part of domain controller promotion, and no longer require separate tasks on special servers such as the Schema Master. Promotion now includes prerequisite checking that validates forest and domain readiness for the new domain controller, lowering the chance of failed promotions. The Windows Server "8" Beta forest functional level and domain functional level do not implement new features, relieving administrators of the need for a homogenous domain controller environment.

There is an emphasis on Windows PowerShell in Windows Server "8" Beta. As distributed computing evolves, Windows PowerShell allows a single engine for configuration and maintenance from both graphical and command-line interfaces. It permits fully featured scripting of any component with the same first class citizenship for an IT Professional that an API grants to developers. As cloud-based computing becomes ubiquitous, Windows PowerShell also finally brings a true “headless server” capability, where a computer with no graphical interface has the same management capabilities as one with a monitor and mouse. This guide attempts to ease you into this by starting first with the more familiar graphical environment, then periodically demonstrating or requiring Windows PowerShell hands-on techniques.

A veteran AD DS administrator should find their previous knowledge highly relevant. A beginning administrator will find a far shallower learning curve. AD DS Simplified Administration improves the experience, based on the extensive feedback of customers like you.

Note

For more information about AD DS Simplified Administration, review [Understand and Troubleshoot ADDS Simplified Administration in Windows Server "8" Beta](http://go.microsoft.com/fwlink/p/?LinkId=237244)

In addition, there is full support for Virtualized Domain Controllers (VDC), to include automated deployment and rollback protection.

Note

For information about Virtualized Domain Controllers, see [Understand and Troubleshoot Virtualized Domain Controllers in Windows Server "8" Beta](http://go.microsoft.com/fwlink/p/?LinkId=236370) and [Test Lab Guide: Demonstrate Windows Server "8" Virtualized Domain Controller (VDC)](http://go.microsoft.com/fwlink/p/?LinkId=237261)

## In this guide

This document contains instructions for setting up the AD DS Simplified Administration test lab through:

* Graphically upgrading an existing Active Directory forest by adding the first Windows Server "8" Beta GUI domain controller
* Adding an additional Windows Server "8" Beta Core domain controller using Windows PowerShell
* Adding an additional Windows Server "8" Beta Core domain controller using Windows RSAT from a Windows 8 Consumer Preview computer
* Decommissioning the original legacy domain controller
* Using new AD DS graphical and Windows PowerShell features for further configuration and administration

Important

The following instructions are for configuring the Windows Server "8" Beta test lab. While this document tries to reinforce best practices, it does not always reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network.

## Test lab overview

The AD DS Simplified Administration test lab consists of the following:

* One computer running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 named EXISTINGDC that is configured as a domain controller and Domain Name System (DNS) server
* One computer running Windows Server "8" Beta named NEWDC1 that is configured as a GUI domain controller and DNS server
* One computer running Windows Server "8" Beta Core named NEWDC2 that is configured as a domain controller and DNS server
* One computer running Windows Server "8" Beta Core named NEWDC3 that is configured as a domain controller and DNS server
* One computer running Windows 8 Consumer Preview named CLIENT1 with the Windows Server "8" Beta Remote Server Administration Tools installed

The Windows 8 Consumer Preview Base Configuration test lab consists of one isolated lab subnet, referred to as the Corpnet subnet (10.90.0.0/24).

Important

The AD DS Simplified Administration TLG is *not* designed for use with the Windows Server "8" Beta Base Configuration guide. If you only need a simple pre-made Windows Server "8" Beta AD DS forest and are not interested in the AD DS scenarios of this lab, see [Test Lab Guide: Windows Server "8" Beta Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358).

The AD DS Simplified Administration TLG is a prerequisite for [Test Lab Guide: Demonstrate Windows Server "8" Virtualized Domain Controller (VDC)](http://go.microsoft.com/fwlink/p/?LinkId=237261). If planning to use to VDC test lab guide, deploy all computers in the AD DS Simplified Administration on a Windows Server "8" Beta server with Hyper-V installed or a third party hypervisor that supports VM-Generation ID (contact your vendor for details).

## Hardware and software requirements

The following are the minimum required components of the test lab:

* The product disc or files for Windows Server "8" Beta
* The product disc or files for Windows 8 Consumer Preview
* The product disc or files for Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2
* The Windows Server "8" Beta Remote Server Administration Toolkit
* One computer that meet the minimum hardware requirements for Windows Server 2003, Windows server 2008, or Windows Server 2008 R2
* Three computers that meet the minimum hardware requirements for Windows Server "8" Beta
* One computer that meets the minimum hardware requirements for Windows 8 Consumer Preview.

If you wish to deploy the AD DS Simplified Administration test lab in a virtualized environment, your virtualization solution must support Windows 8 Consumer Preview and Windows Server "8" Beta virtual machines. The server hardware must support the amount of RAM required to run all the virtual operating systems included in the lab simultaneously.

Important

Run Windows Update on all computers or virtual machines either during the installation or immediately after installing the operating systems. After running Windows Update, you can isolate your physical or virtual test lab from your production network.

### User account control

When you are logged in as an administrative user other than the built-in Administrator account, you are required to click Continue or **Yes** in the User Account Control (UAC) dialog box for some tasks. Several of the configuration tasks require UAC approval. When prompted, always click Continue or **Yes** to authorize these changes. Alternatively, see the [Appendix](#_Appendix_1) of this guide for instructions about how to set the UAC behavior of the elevation prompt for administrators.

### Windows PowerShell and remote pasting in Hyper-V virtual machines

This guide makes frequent use of Windows PowerShell samples in order to familiarize you with this robust command-line tool. In Windows Server "8" Beta, there is an issue where copying and pasting long lines of text into a remote virtual machine can lead to garbled text. See the [Appendix](#_Appendix_1) of this guide for instructions about mitigating this behavior.

# Steps for Upgrading the Existing AD DS Forest

There are three steps to create and upgrade the AD DS Forest.

1. Configure EXISTINGDC.
2. Configure NEWDC1
3. Complete post-upgrade tasks.

Note

You must logon as a member of the Administrators group to complete the tasks described in this section.

## Step 1: Configure EXISTINGDC

EXISTINGDC is a domain controller for the root.fabrikam.com. This simulates your current production AD DS environment. EXISTINGDC configuration consists of the following:

 Install the operating system

 Configure TCP/IP and computer name

 Install Active Directory and DNS

### Install the operating system on EXISTINGDC

Choose the operating system based on your current production domain infrastructure.

To install the operating system on EXISTINGDC

|  |
| --- |
| 1. Start the installation of Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. 2. Follow the instructions to complete the installation, specifying a strong password for the local Administrator account. Logon using the local Administrator account. 3. Install the latest service pack for the operating system if not already integrated in the installation media. 4. Connect EXISTINGDC to the Corpnet subnet. |

### Configure TCP/IP properties and computer name on EXISTINGDC

To configure TCP/IP and computer name on EXISTINGDC

|  |
| --- |
| 1. Click **Start**, then **Run** and type **Ncpa.cpl**. 2. In **Network Connections**, right-click **Local Area Connection**, and then click **Properties**. Note that the "Local Area Connection" interface name may be different on your computer. 3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 4. Select Use the following IP address. In IP address, type 10.90.0.100. In Subnet mask, type 255.255.255.0. In **Default gateway**, type **10.90.0.1**. Select Use the following DNS server addresses. In **Preferred DNS server**, type **127.0.0.1**. 5. Click **OK** then click **Close** to dismiss the **Local Area Connections** **Properties** dialog. Close the Network Connections window. 6. Click **Start**, then **Run** and type **Sysdm.cpl.** 7. On the **Computer Name** tab of the System Properties dialog, click **Change**. 8. In **Computer name**, type **EXISTINGDC**, click **OK** twice, and then click **Close**. When prompted to restart the computer, click **Restart Now**. 9. After restarting, login using the local Administrator account. |

### Configure EXISTINGDC as a domain controller using Server Manager

To configure EXISTINGDC as a domain controller and DNS server on *Windows Server 2003*

|  |
| --- |
| 1. Click **Start**, then **Run** and type **Dcpromo.exe**. Allow the active directory binary installation to complete. 2. On the Welcome to the Active Directory Installation Wizard page, click **Next**. 3. On the **Operating System Compatibility** page, review then click **Next**. 4. On the **Domain Controller Type** page, leave **Domain controller for a new domain** selected and click **Next**. 5. On the **Create New Domain** page, leave **Domain in a new forest** selected and click **Next**. 6. On the **New Domain** **Name** page, type **root.fabrikam.com** and click **Next**. 7. On the **NetBIOS Domain** **Name** page, leave **ROOT** as the selection and click **Next**. 8. On the **Database and Log Folders** page, leave the default database and log paths selected and click **Next**. 9. On the **Shared System Volume** page, leave the default SYSVOL path selected and click **Next**. 10. On the **DNS Registration Diagnostics** page, leave **Install and configure DNS server on this computer…** selected and click **Next**.   Note  The diagnostic failure warning is expected; the server points to itself for DNS, but DNS is not yet configured.   1. On the **Permissions** page, leave **Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems** selected and click **Next**. 2. On the **Directory Services Restore Mode Administrator** **Password** page, type and confirm a complex password, then click **Next**. 3. On the **Summary** page, review the proposed settings. If correct, click **Next**. 4. Allow the **Active Directory Installation Wizard** to complete the promotion. If prompted, provide the Windows Server 2003 source media to install the DNS service. Do *not* skip DNS installation if prompted. 5. On the **Completing the Active Directory Installation Wizard** page, click **Finish**. Click **Restart Now**. After the server restarts, logon using the ROOT\Administrator credentials. 6. Click **Start**, then **Run** and type **Domain.msc**. Right click the **root.fabrikam.com** node and click **Raise Domain Functional Level**. Set the dropdown to **Windows Server 2003** and click **Raise**. Click **OK** when prompted twice. Right click the **Active Directory Domains and Trusts** node and click **Raise Forest Functional Level**. Set the dropdown to **Windows Server 2003** and click **Raise**. Click **OK** when prompted twice. |

To configure EXISTINGDC as a domain controller and DNS server on *Windows Server 2008 or Windows Server 2008 R2*

|  |
| --- |
| 1. Click **Start**, then **Run** and type **Dcpromo.exe**. Allow the active directory binary installation to complete. 2. On the Welcome to the Active Directory Installation Wizard page, select **Use advanced mode installation** and click **Next**. 3. On the **Operating System Compatibility** page, review then click **Next**. 4. On the **Choose a Deployment Configuration** page, select **Create a new domain a new forest** and click **Next**. 5. On the **Name the Forest Root Domain** page, type **root.fabrikam.com** and click **Next**. 6. On the **Domain** **NetBIOS Name** page, leave **ROOT** as the selection and click **Next**. 7. On the **Set Forest Functional Level** page, set the dropdown to *at least* **Windows Server 2003**. You can set it higher as desired, especially if that matches your current production environment. Do *not* set it to **Windows 2000.** 8. On the optional **Set Domain Functional Level** page, set the dropdown to *at least* **Windows Server 2003**. You can set it higher as desired, especially if that matches your current production environment. Do *not* set it to **Windows 2000.** 9. On the **Additional Domain Controller Options** page, leave **the DNS Server** option selected and click **Next**. When prompted with **A delegation for this DNS server cannot be created…**, click **Yes**.   Note  The diagnostic failure warning is expected; the server points to itself for DNS, but DNS is not yet configured.   1. On the **Location for Database, Log Files, and SYSVOL** page, leave the default paths selected and click **Next**. 2. On the **Directory Services Restore Mode Administrator** **Password** page, type and confirm a complex password, then click **Next**. 3. On the **Summary** page, review the proposed settings. If correct, click **Next**. 4. Select **Reboot on completion**. 5. Allow the domain controller to restart. After the server restarts, logon using the ROOT\administrator credentials. |

## Step2: Configure NEWDC1

NEWDC1 is the first Windows Server "8" Beta domain controller in the domain. It updates the AD DS forest, schema, and domain to support subsequent Windows Server "8" Beta domain controllers and features.

* Install the operating system
* Configure TCP/IP
* Rename to NEWDC1
* Install the Active Directory Domain Services role
* Promote to a domain controller

### Install the operating system on NEWDC1

 To install the operating system on NEWDC1

|  |
| --- |
| 1. Start the installation of Windows Server "8" Beta. 2. Follow the instructions to complete the installation, specifying Windows Server "8" Beta GUI (i.e. *Server with a GUI* installation, not *Server Core Installation*) and a strong password for the local Administrator account. Logon using the local Administrator account. 3. Connect NEWDC1 to the Corpnet subnet. |

### Configure TCP/IP properties on NEWDC1

To configure TCP/IP properties on NEWDC1

|  |
| --- |
| 1. If not already running, start Server Manager from the taskbar or **Start** page. In Server Manager, click **Local Server** in the console tree. Click the link next to **Wired Ethernet Connection** in the Properties tile. 2. In **Network Connections**, right click **Wired Ethernet Connection**, and then click **Properties**. Note that the "Wired Ethernet Connection" interface name may be different on your computer. 3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 4. Select Use the following IP address. In IP address, type 10.90.0.101. In Subnet mask, type 255.255.255.0. In **Default gateway**, type **10.90.0.1**. 5. Select Use the following DNS server addresses. In Preferred DNS server, type 10.90.0.100. In **Alternate DNS server**, type **127.0.0.1**. 6. Click **OK**, and then click **Close**. Close the **Network Connections** window. 7. Open the Start page, type **CMD**, and then hit ENTER. 8. To check name resolution and network communication between NEWDC1 and EXISTINGDC, type **ping EXISTINGDC.root.fabrikam.com** in the command prompt windowand hit **ENTER**. 9. Verify that there are four replies from 10.90.0.100. 10. Close the Command Prompt window. |

### Rename the computer to NEWDC1

To rename the computer to NEWDC1

|  |
| --- |
| 1. In Server Manager, click **Local Server** in the console tree. Click the link next to **Computer name** in the **Properties** tile. 2. In the System Properties dialog box, click Change on the **Computer Name** tab. 3. In Computer Name, type **NEWDC1**. Click OK. 4. When prompted to restart the computer, click OK. 5. On the System Properties dialog box, click Close. 6. When prompted to restart the computer, click Restart Now. 7. After the computer restarts, logon with the local Administrator account. |

### Upgrade the existing forest using NEWDC1 and Server Manager

To configure NEWDC1 as a domain controller and upgrade the forest with Server Manager

|  |
| --- |
| 1. If not already running, start Server Manager from the taskbar or **Start** page. In Server Manager, click **Manage** then **Add Roles and Features**. 2. Review the **Before you begin** page and click **Next**. 3. On the **Select installation type** page, leave **Role-Based or Feature-based installation** selected and click **Next**. 4. On the **Select destination server** page, verify that **NEWDC1** is already highlighted and click **Next**. 5. On the **Select server roles** page, select **Active Directory Domain Services**. When prompted to **Add features that are required for Active Directory Domain Services** click **Add Features**. Click **Next**. 6. On the **Select features** page, click **Next**. 7. Review the **Active Directory Domain Services** page and click **Next**. 8. On the **Confirm installation selections** page, click **Install**. Allow role installation to complete. If you click **Close** on the **Installation progress** page before completion, click the **Notification Flag** on the Server Manager dashboard to see the installation status. 9. When installation is complete, click **Promote this server to a domain controller**. If you already closed the **Installation progress** page, click the **Notification Flag** (which now has an orange bang icon) and in the **Post-deployment configuration** menu, click **Promote this server to a domain controller**. The **Active Directory Domain Services Configuration Wizard** starts. 10. On the **Deployment Configuration** page, leave **Add a domain controller** **to an existing domain** selected. Click the **Select** button and provide the Root\Administrator account credentials when prompted. Select the **root.fabrikam.com** domain and click **OK**. Click **Next**. 11. On the **Domain Controller Options** page, leave **DNS** and **GC** selected. Type and confirm a strong DSRM password, then click **Next**. 12. On the **DNS Options** page, leave **Update DNS delegation** unselected and click **Next**. 13. On the **Additional Options** page, leave all defaults unchanged and click **Next**. 14. On the **Paths** page, leave the default paths unchanged and click **Next**. 15. Review the **Preparation Options** page and click **Next**. 16. Review your previous choices on the **Review Options** page. Optionally, click **View script** to save off the Windows PowerShell version of this promotion. Click **Next**. 17. Allow the **Prerequisites Check** page to complete validating the forest is ready for upgrade and the computer is ready for promotion. Review the results. If you see "All prerequisite checks passed successfully" then you are ready to promote. If there are any errors, follow the instructions shown to correct them, then click **Rerun prerequisites check** until you pass. Click **Install**. 18. Allow the **Installation** page to complete. When the **Results** page displays, the computer reboots automatically. After the server restarts, logon using the root\administrator credentials. |

## Step 3: Complete Post-Upgrade Tasks on NEWDC1

After promotion of NEWDC1, there are several post-upgrade tasks required:

* Create an alternative domain administrator user account
* Move the PDC emulator FSMO role to NEWDC1
* Update the DNS client settings on EXISTINGDC

### Create a user account in Active Directory on NEWDC1

Create a user account in Active Directory to use when performing administrative tasks that do not require the Enterprise Admins and Schema Admins groups. Avoid using the built-in Administrator account when possible, as it is difficult to tell which person actually made changes in a domain. The Administrator account also does not use UAC by default, which inhibits certain Windows Server "8" Beta features.

Note

Perform these steps while logged on to NEWDC1 as root\administrator

To create a user account using Active Directory Administrative Center  
[Do this step using Windows PowerShell](#PS4)



|  |
| --- |
| 1. Open the **Start** page, and then type **DSAC** and hit ENTER. 2. In the Active Directory Administrative Center console tree, click **root (local)**, and then double-click **Users**. This adds Users as a recent navigation link in the console tree. 3. In the **Tasks** pane, click **New**, and then click **User**. 4. In the **Create User** dialog, type **AdminUser1** next to **Full name** and type **AdminUser1** next to **User SamAccountName logon: root\** 5. In Password, type the password that you want to use for this account, and in Confirm password, type the password again. 6. Under **Password options**, select **Other password options**. 7. Scroll down to the **Member of** section and click **Add**. Type **Domain Admins**, and then click **OK**. 8. Click **Add** and then click **OK**. 9. Click **OK** to close the Create User dialog. 10. Exit the Active Directory Administrative Center. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlets perform the same function as the preceding procedure. Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.    **New-ADUser -SamAccountName AdminUser1 -AccountPassword (read-host "Set user password" -assecurestring) -name "AdminUser1" -enabled $true -PasswordNeverExpires $true -ChangePasswordAtLogon $false**  **Add-ADPrincipalGroupMembership -Identity "CN=AdminUser1,CN=Users,DC=root,DC=fabrikam,DC=com" -MemberOf "CN=Domain Admins,CN=Users,DC=root,DC=fabrikam,DC=com"** |

### Move the PDC emulator FSMO role to NEWDC1

Move the PDC emulator FSMO role to a Windows Server "8" Beta domain controller in order to create new built-in groups and well-known security identifiers.

To move the PDCE FSMO role to NEWDC1  
[Do this step using Windows PowerShell](#PS5)



Note  
 Perform these steps while logged on to NEWDC1 as root\administrator

|  |
| --- |
| 1. Open the **Start** page, and then type **DSA.MSC** and hit ENTER. 2. In the Active Directory Users and Computers snap-in console tree, right click the **root.fabrikam.com** node and then click **Operations Masters...** 3. In the **Operations Masters** dialog, click the **PDC** tab. Click the **Change** button to move the PDC FSMO role to **NEWDC1**. Click **Yes** to confirm.   Note  If the target is not already **NEWDC1**, click **Close**, right click **root.fabrikam.com**, click **change domain controller**, select **NEWDC1**, and click **OK**. Then repeat step 3.   1. Click **OK** when successfully transferred. Click **Close**. 2. Click on the **Users** node under the **root.fabrikam.com** node. Validate that the PDC emulator created the new Windows Server "8" Beta groups (example: **Cloneable Domain Controllers**). You may have to refresh by hitting F5. 3. Exit the Active Directory Users and Computers snap-in. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet performs the same function as the preceding procedure. Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.    **Move-ADDirectoryServerOperationMasterRole -Identity "NEWDC1" -OperationMasterRole PDCEmulator** |

### Update the DNS client settings on EXISTINGDC

Change the DNS client IP address to point primarily to NEWDC1 and avoid potential DNS islanding.

To change the DNS client settings on EXISTINGDC



Note  
Perform these steps while logged on to EXISTINGDC as root\administrator



|  |
| --- |
| 1. Click **Start**, then **Run** and type **Ncpa.cpl** 2. In **Network Connections**, right click **Local Area Connection**, and then click **Properties**. Note that the "Local Area Connection" interface name may be different on your computer. 3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 4. In **Preferred DNS server**, type **10.90.0.101**. In **Alternate DNS server**, type **127.0.0.1**. 5. Click **OK** then click **Close** to dismiss the **Local Area Connections** **Properties** dialog. 6. Close the Network Connections window. |

# Steps for adding a second Windows Server "8" Beta domain controller using Windows PowerShell

Note

You must logon to NEWDC2 as a member of the Administrators group to complete the tasks described in this section.

## Configure NEWDC2

NEWDC2 is the second Windows Server "8" Beta domain controller in the domain, and the first one configured as the default Server Core Installation (no graphical interface) installation. This demonstrates how to deploy a Windows Server "8" Beta Core domain controller using nothing but Windows PowerShell.

 Install the operating system

 Configure TCP/IP

 Install the Active Directory Domain Services role

 Promote to a domain controller

### Install the operating system on NEWDC2

 To install the operating system on NEWDC2

|  |
| --- |
| 1. Start the installation of Windows Server "8" Beta. 2. Follow the instructions to complete the installation, specifying Windows Server "8" Beta running Core (i.e. choose *Server Core Installation,* not *Server with a GUI* installation) and a strong password for the local Administrator account. Logon using the local Administrator account. 3. Connect NEWDC2 to the Corpnet subnet. |

### Configure TCP/IP properties on NEWDC2

To configure TCP/IP properties on NEWDC2 using Windows PowerShell

|  |  |  |
| --- | --- | --- |
| 1. Start Windows PowerShell by typing **powershell.exe.** 2. In Windows PowerShell:  |  | | --- | | Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** | | Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that the "Wired Ethernet Connection" interface name may be different on your computer. Use **ipconfig /all** to list out the interfaces. Always run Windows PowerShell as an elevated administrator.    **Netsh interface ipv4 set address "wired ethernet connection" static 10.90.0.102 255.255.255.0 10.90.0.1 1**  **Netsh interface ipv4 set dnsservers "wired ethernet connection" static 10.90.0.101 validate=no**  **Netsh interface ipv4 add dnsservers "wired ethernet connection" 127.0.0.1 index=2 validate=no** |  1. To check name resolution and network communication between NEWDC2 and NEWDC1, type **ping NEWDC1.root.fabrikam.com** and hit **ENTER**. 2. Verify that there are four replies from 10.90.0.101. 3. Close the Command Prompt window. |

### Rename the computer to NEWDC2

To rename the computer to NEWDC2

|  |  |  |
| --- | --- | --- |
| 1. In Windows PowerShell:  |  | | --- | | Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** | | Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.  **Rename-computer -NewName NEWDC2**  **Restart-computer** |  1. Allow the server to reboot. After the server restarts, logon using the local Administrator credentials. |

### Promote NEWDC2 to a domain controller using Windows PowerShell

To configure NEWDC2 as a domain controller using Windows PowerShell

|  |  |  |
| --- | --- | --- |
| 1. Start Windows PowerShell by typing **powershell.exe.** 2. In Windows PowerShell:  |  | | --- | | Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** | | Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that the "Wired Ethernet Connection" interface name may be different on your computer. Use **ipconfig /all** to list out the interfaces. Always run Windows PowerShell as an elevated administrator.    **Install-WindowsFeature -name ad-domain-services -includemanagementtools**  **Install-AddsDomainController -DomainName root.fabrikam.com -credential (get-credential)** |  1. Type in the root\adminuser1 credentials when prompted and click **OK**. 2. Type and confirm the **safemodeadministratorpassword** (i.e. DSRM). 3. When prompted to begin, hit ENTER. 4. Allow the server to reboot. After the domain controller restarts, logon using the Root\Adminuser1 credentials. |

# Steps for adding a third Windows Server "8" Beta domain controller using remote management tools

There are two steps to remotely deploying the third Windows Server "8" Beta domain controller:

1. Configure CLIENT1.
2. Configure NEWDC3

Note

You must logon as a member of the Administrators and Domain Admins group to complete the tasks described in this section.

## Step 1: Configure CLIENT1

CLIENT1 configuration consists of the following:

 Install the operating system

 Join CLIENT1 to the ROOT domain

 Add the Remote Server Administration Tools

### Install the operating system on CLIENT1

To install the operating system on CLIENT1

|  |
| --- |
| 1. Start the installation of Windows 8 Consumer Preview. 2. When prompted for a computer name, type CLIENT1. 3. When prompted by the Settings dialog, click Use express settings. 4. At the Logon prompt, click **Don't want to sign in with a Microsoft account?** Click **Local account**. 5. When prompted for a local user name, type **User1**. Type a strong password twice, and type a password hint. Click **Finish**. 6. Connect CLIENT1 to the Corpnet subnet. Click **Yes, turn on sharing and connect to devices** when prompted. |

### Configure TCP/IP properties on CLIENT1

To configure TCP/IP properties on CLIENT1

|  |
| --- |
| 1. Open the **Start** page and type **ncpa.cpl** then hit ENTER. 2. In **Network Connections**, right-click **Wired Ethernet Connection**, and then click **Properties**. Note that the "Wired Ethernet Connection" interface name may be different on your computer. 3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 4. Select Use the following IP address. In IP address, type 10.90.0.201. In Subnet mask, type 255.255.255.0. In **Default gateway**, type **10.90.0.1**. 5. Select Use the following DNS server addresses. In Preferred DNS server, type 10.90.0.101. In the **Alternate DNS server**, type **10.90.0.102**. 6. Click **OK**, and then click **Close**. Close the **Network Connections** window. 7. Open the **Start** page, type **CMD**, and then hit ENTER. 8. To check name resolution and network communication between CLIENT1 and NEWDC1, type **ping NEWDC1.root.fabrikam.com** in the command prompt windowand hit **ENTER**. 9. Verify that there are four replies from 10.90.0.101. 10. Close the Command Prompt window. |

### Join CLIENT1 to the ROOT domain

To join CLIENT1 to the ROOT domain

|  |
| --- |
| 1. Open the **Start** page and type **sysdm.cpl**, then hit ENTER. 2. On the **System** page, click **Advanced system settings**. 3. In the System Properties dialog box, click the **Computer Name** tab. On the **Computer Name** tab, click Change. 4. In the Computer Name/Domain Changes dialog box, click Domain, type root.fabrikam.com, and then click OK. 5. When prompted for a user name and password, type the user name and password for the **AdminUser1** domain account, and then click OK. 6. When you see a dialog box that welcomes you to the root.fabrikam.com domain, click OK. 7. When you see a dialog box that prompts you to restart the computer, click OK. 8. In the System Properties dialog box, click Close. Click **Restart Now** when prompted. 9. After the computer restarts, click the **Switch User arrow icon**, and then click **Other User**. Logon to the ROOT domain with the **AdminUser1** account. |

### Install RSAT on CLIENT1

To install RSAT

|  |
| --- |
| 1. Download the Windows Server "8" Beta Remote Server Administration Tools for Windows 8 Consumer Preview ([Windows6.2-KB958830-x64.msu](http://go.microsoft.com/fwlink/?LinkId=242077)). Copy it to the CLIENT1 computer. 2. Double-click the MSU file and click **Yes** to install. Click **I Accept** for the **License terms**. 3. Click **OK** when completed. |

## Step 2: Configure NEWDC3

NEWDC3 is the third Windows Server "8" Beta domain controller in the domain, and the second one configured as the default Core (no graphical interface) installation. This demonstrates how to manage and deploy a Windows Server "8" Beta Core domain controller using remote Server Manager running on a Windows 8 Consumer Preview computer. In this example, you use the SConfig tool, rather than Windows PowerShell, as a demonstration of an alternative method.

* Install the operating system
* Configure TCP/IP
* Join to the domain
* Install the Active Directory Domain Services role remotely
* Promote to a domain controller remotely

### Install the operating system on NEWDC3

 To install the operating system on NEWDC3

|  |
| --- |
| 1. Start the installation of Windows Server "8" Beta. 2. Follow the instructions to complete the installation, specifying Windows Server "8" Beta Core (i.e. choose *Server Core Installation,* not *Server with a GUI* installation) and a strong password for the local Administrator account. Logon using the local Administrator account. 3. Connect NEWDC3 to the Corpnet subnet. |

### Configure TCP/IP properties on NEWDC3

To configure TCP/IP properties on NEWDC3 using SCONFIG

|  |
| --- |
| 1. Type **SConfig** 2. Type **8** (i.e. **Network Settings**) and hit ENTER. 3. When prompted to select the **Network Adaptor Index#**, type the appropriate one shown and hit ENTER. 4. Type **1** and hit ENTER, then **S** and ENTER. 5. Type the **static IP address** of **10.90.0.103**, the **subnet mask** of **255.255.255.0**, and the **default gateway** of **10.90.0.1**. 6. Type **2** and hit ENTER. For the new **preferred DNS server**, type **10.90.0.101** and hit ENTER. For the **alternate DNS server,** type **127.0.0.1** and hit ENTER. Type **4** and hit ENTER to return to the **server configuration** menu. |

### Rename and join NEWDC3 to the domain

To rename the computer and join the domain

|  |
| --- |
| 1. Type **1** (i.e. **Domain/Workgroup**) and hit ENTER. Type **D** and hit ENTER. 2. For the **domain to join**, type **root.fabrikam.com** and hit ENTER. For **specify an authorized domain\user** type **root\adminuser1** and then the correct password. 3. When prompted to change the computer name, click **Yes**. Type **NEWDC3** and hit ENTER. When prompted for credentials, type **root\adminuser1** and the password. Click **Restart** when prompted. 4. Allow the server to reboot. After the domain controller restarts, logon using the Root\Adminuser1 credentials. |

### Configure NEWDC3 as a domain controller using Server Manager remotely from CLIENT1

Perform these steps from CLIENT1.

To configure NEWDC3 as a domain controller with Server Manager from CLIENT1

|  |
| --- |
| 1. Open the **Start** page and type **servermanager**, then hit ENTER. 2. Click **Manage** then **Add Servers** (alternatively, right-click **All Servers** and click **Add Servers**). 3. In the **Add Servers** dialog box on the **Active Directory** tab, click **Find Now**. Select the **NEWDC3** server then click the arrow to add it to the **Selected** pane. Optionally, added all other Windows Server "8" Beta domain controllers. Click **OK**. 4. Click **Manage** and then **Add Roles and Features**. 5. Review the **Before you begin** page and click **Next**. 6. On the **Select installation type** page, leave **Role-Based or Feature-based installation** selected and click **Next**. 7. On the **Select destination server** page, select the **NEWDC3** server and click **Next**. 8. On the **Server Roles** page, select **Active Directory Domain Services**. When prompted to **Add features that are required for Active Directory Domain Services** click **Add Features**. Click **Next**. 9. On the **Select features** page, click **Next**. 10. Review the **Active Directory Domain Services** page and click **Next**. 11. On the **Confirm installation selections** page, click **Install**. Allow role installation to complete. If you click **Close** on the **Installation progress** page before completion, click the **Notification Flag** on the Server Manager dashboard to see the installation status. 12. When installation is complete, click **Promote this server to a domain controller**. If you already closed the **Installation progress** page, click the **Notification Flag** (which now has an orange bang icon) and in the **Post-deployment configuration** menu, click **Promote this server to a domain controller**. The Active Directory Domain Services Configuration Wizard starts. 13. On the **Deployment Configuration** page, leave **Add a domain controller to an existing domain** selected. Click the **Change** button and provide the Root\Adminuser1 account credentials when prompted. Leave the **root.fabrikam.com** domain default and click **OK**. Click **Next**. 14. On the **Domain Controller Options** page, leave **DNS** and **GC** selected. Type and confirm a strong DSRM password, then click **Next**. 15. On the **DNS Options** page, leave **Update DNS delegation** unselected and click **Next**. 16. On the **Additional Options** page, leave all defaults unchanged and click **Next**. 17. On the **Paths** page, leave the paths unchanged and click **Next**. 18. Review your previous choices on the **Review Options** page. Optionally, click **View script** to save off the Windows PowerShell version of this promotion. Click **Next**. 19. Allow the **Prerequisites Check** page to complete validating the computer is ready for promotion. Review the results. If you see "All prerequisite checks passed successfully" then you are ready to promote. If there are any errors, follow the instructions shown to correct them, then click **Rerun prerequisites check** until you pass. Click **Install**. 20. Allow the **Installation** page to complete. When the **Results** page displays the computer reboots automatically. |

# Decommission EXISTINGDC from the AD DS Forest

Now that the forest and domain support Windows Server "8" Beta, you will demote the legacy domain controller. For the purposes of this lab, this is required if the EXISTINGDC runs Windows Server 2003 or Windows Server 2008. If EXISTINGDC runs Windows Server 2008 R2, there is no requirement to demote, as the Windows Server 2008 R2 domain functional level and forest functional levels are the minimum required for Windows Server "8" Beta features.

There are three steps to decommissioning EXISTINGDC:

1. Move the remaining FSMO roles off EXISTINGDC
2. Reconfigure DNS client on NEWDC1
3. Demote EXISTINGDC

Important

Do not skip this section, regardless of the operating system on EXISTINGDC; there are several steps required for the management and configuration section later in this guide.

Note

You must logon as a member of the Administrators and Domain Admins group to complete the tasks described in this section.

## Step 1: Move the remaining FSMO Roles

As the first domain controller in the domain, EXISTINGDC contains all of the Flexible Single Master Operations roles except the PDC emulator (which you transferred previously). FSMO roles are critical to AD DS operation. While demotion will automatically move the FSMO roles, it is better to manually perform this step and ensure the specific domain controllers you want to hold a role become the new owners. This step also demonstrates just how much simpler and easier Windows PowerShell can be, compared to graphical tools.

Note

Perform these steps on NEWDC1

To move the remaining FSMO role  
[Do this step using Windows PowerShell](#PS6)

|  |
| --- |
| 1. Open the **Start** page, and then type **DSA.MSC** and hit ENTER. 2. In the **Active Directory Users and Computers** snap-in console tree, right click the **root.fabrikam.com** node and then click **Operations Masters...** 3. In the **Operations Masters** dialog, click the **Infrastructure** tab. Click the **Change** button to move the Infrastructure Master FSMO role to **NEWDC1**.   Note  If not already targeting **NEWDC1**, click **Close**, right click **root.fabrikam.com**, click **change domain controller**, select **NEWDC1**, and click **OK**. Then repeat step 3.   1. Click **OK** when successfully transferred. Click **Close**. 2. Repeat for the **RID** tab (and the **PDC** tab if you did not perform that step earlier in the guide). 3. Exit the **Active Directory Users and Computers** snap-in. 4. Open the **Start** page, and then type **DOMAIN.MSC** and hit ENTER. 5. In the **Active Directory Domains and Trusts** snap-in console tree, right click the **Active Directory Domains and Trusts** node and then click **Operations Master...** 6. In the **Operations Master** dialog, click the **Change** button to move the Domain Naming Master FSMO role to **NEWDC1**. Click **Yes** to confirm.   Note  If not already targeting **NEWDC1**, click **Close**, right click **root.fabrikam.com**, click **change domain controller**, select **NEWDC1**, and click **OK**. Then repeat step 3.   1. Click **OK** when successfully transferred. Click **Close**. 2. Exit the **Active Directory Domains and Trusts** snap-in. 3. Open the **Start** page, and then type **regsvr32 schmmgmt.dll** and hit ENTER. Click **OK** when you see the succeeded message. 4. Open the **Start** page, and then type **mmc** and hit ENTER. In the **Console1** dialog, click **File** then click **Add/Remove Snap-in**. 5. In the **Available snap-ins** pane, select **Active Directory Schema** then click **Add >**. Click **OK**. 6. Right click the **Active Directory Schema** node then click **Change Active Directory Domain Controller**. Select **NEWDC1** and click **OK**. Accept the warning by clicking **OK**. 7. Right click **Active Directory Schema** and click **Operations Master…** In the **Change Schema Master** dialog, click the **Change** button to move the Schema Master FSMO role to **NEWDC1**. Click **Yes** to confirm. 8. Click **OK** when successfully transferred. Click **Close**. 9. Close the **Console1** dialog. You do not have to save settings. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet performs the same function as the preceding procedure. Enter the command on a single line, even though it appears word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.    **Move-ADDirectoryServerOperationMasterRole -Identity "NEWDC1" -OperationMasterRole PDCEmulator,RidMaster,InfrastructureMaster,SchemaMaster,DomainNamingMaster** |

## Step 2: Reconfigure DNS client on NEWDC1

Change the DNS client IP address to point primarily to NEWDC2 and avoid potential DNS islanding.

Note

Perform these steps on NEWDC1

To change the DNS client settings on NEWDC1  
[Do this step using Windows PowerShell](#PS7)



|  |
| --- |
| 1. If not already running, start Server Manager from the taskbar or **Start** page. In Server Manager, click **Local Server** in the console tree. Click the link next to **Wired Ethernet Connection** in the Properties tile. 2. In **Network Connections**, right-click **Wired Ethernet Connection**, and then click **Properties**. Note that the "Wired Ethernet Connection" interface name may be different on your computer. 3. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 4. In Preferred DNS server, type 10.90.0.102. 5. Click **OK**, and then click **Close**. Close the **Network Connections** window. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** |
| Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that the "Wired Ethernet Connection" interface name may be different on your computer. Use **ipconfig /all** to list out the interfaces. Always run Windows PowerShell as an elevated administrator.  **Netsh interface ipv4 set dnsservers "wired ethernet connection" static 10.90.0.102**  **Netsh interface ipv4 add dnsservers "wired ethernet connection" 127.0.0.1 index=2 validate=no** |

## Step 3: Demote EXISTINGDC

If EXISTINGDC is a Windows Server 2003 or Windows Server 2008 domain controller, you *must* demote it to gain access to certain Windows Server "8" Beta features in this lab. If EXISTINGDC is a Windows Server 2008 R2 domain controller, demotion is optional but still recommended.

Note

Perform these steps on EXISTINGDC

To demote EXISTINGDC on *Windows Server 2003*

|  |
| --- |
| 1. Click **Start**, then **Run** and type **Dcpromo.exe**. 2. On the Welcome to the Active Directory Installation Wizard page, click **Next**. Click **OK** when warned that this is a global catalog. 3. On the **Remove Active Directory** page, review and then click **Next**. Do *not* select **This server is the last domain controller in the domain**. 4. On the **Administrator** **Password** page, type and confirm a complex password, then click **Next**. 5. On the **Summary** page, review the proposed demotion. If correct, click **Next**. 6. Allow the **Active Directory Installation Wizard** to complete the demotion. 7. On the **Completing the Active Directory Installation Wizard** page, click **Finish**. Click **Restart Now**. Allow the domain controller to restart. 8. This server is no longer needed in the lab and can be turned off or discarded. |

To demote EXISTINGDC on *Windows Server 2008 or Windows Server 2008 R2*

|  |
| --- |
| 1. Click **Start**, then **Run** and type **Dcpromo.exe**. 2. On the Welcome to the Active Directory Installation Wizard page, click **Next**. Click **OK** when warned that this is a global catalog. 3. On the **Delete the domain** page, review and then click **Next**. Do *not* select **This server is the last domain controller in the domain**. 4. On the **Administrator** **Password** page, type and confirm a complex password, then click **Next**. 5. On the **Summary** page, review the proposed demotion. If correct, click **Next**. 6. Select **Reboot on Completion** when presented. 7. Allow the **Active Directory Installation Wizard** to complete the demotion. 8. On the **Completing the Active Directory Installation Wizard** page, click **Finish**. Click **Restart Now**. Allow the domain controller to restart. 9. This server is no longer needed in the lab and can be turned off or discarded. |

# Use New AD DS Simplified Administration Features in Windows Server "8" Beta

Now that the forest and domain contains Windows Server "8" Beta domain controllers (and optionally, Windows Servers 2008 R2 domain controllers), you are ready to implement new Windows Server "8" Beta administrative features.

* Enable the Active Directory Recycle Bin using Active Directory Administrative Center
* Create, delete, and restore an object using Active Directory Administrative Center
* Create, delete, and restore an OU with several child objects using Active Directory Administrative Center
* Create Fine Grained Password Policies using Active Directory Administrative Center
* Use the Active Directory Administrative Center Windows PowerShell History Viewer to learn commands
* Use Server Manager to group and monitor domain controllers

Note

You can perform all tasks from either CLIENT1 or NEWDC1.

## Enable the Active Directory Recycle Bin using Active Directory Administrative Center

The Active Directory Administrative Center now supports enabling the Active Directory Recycle Bin feature first introduced in Windows Server 2008 R2.

Note

You must logon as a member of the Enterprise Admins and Domain Admins group to complete the task described in this section, which means the Root\Administrator account in this lab. You can perform the steps from any server or client.

To enable the Active Directory Recycle Bin  
[Do this step using Windows PowerShell](#PS8)



|  |
| --- |
| 1. Open the **Start** page, and then type **DSAC** and hit ENTER. 2. In theActive Directory Administrative Centerconsole tree, click **root (local)**. 3. In the Tasks pane, click **Raise the forest functional level**. 4. In the **Raise the forest functional level** dialog, select the **Windows Server "8" Beta** or **Windows Server 2008 R2** functional level.   Note  Windows Server "8" Beta forest and domain functional levels do not introduce any new features. This is an intentional design change, intended to make administering heterogeneous Windows environments easier while still allowing you to set a minimum domain controller operating system requirement.   1. Click **OK** when prompted with a warning. Click **OK** when shown the result. 2. Click the **Refresh** icon (two arrows within a circle in the **address bar**) to refresh the page and expose the **Enable Recycle Bin** option. 3. In the Tasks pane, click **Enable Recycle Bin**. 4. Click **OK** when prompted with a warning. Click **OK** when shown the result. 5. Click the **Refresh** icon to expose the **Deleted Objects** container. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** |
| Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. This example assumes you previously moved the Domain Naming Master FSMO role holder to NEWDC1. Always run Windows PowerShell as an elevated administrator.  **Set-AdForestMode -identity root.fabrikam.com -forestmode Win8**  **Enable-AdOptionalFeature -identity "recycle bin feature" -server NEWDC1 -scope forestorconfiguration -target root.fabrikam.com** |

## Create, delete, and restore an object using Active Directory Administrative Center

The Active Directory Administrative Center now supports graphically restoring deleted objects using the Active Directory Recycle Bin feature.

Note

You must logon as a member of the Domain Admins group to complete the task described in this section.

 Create, delete, and restore an object using Active Directory Administrative Center  
[Do this step using Windows PowerShell](#PS9)

|  |
| --- |
| 1. In theActive Directory Administrative Centerconsole tree, click **root (local)**, and then double-click **Users**. This adds **Users** as a recent navigation link in the console tree. 2. In the **Tasks** pane, click **New**, and then click **User**. 3. In the **Create User** dialog, type **Tony** next to **First name,** type **Wang** next to **Last name**, and type **twang** next to **User SamAccountName logon: root\** 4. In Password, type the password that you want to use for this account, and in Confirm password, type the password again. 5. Scroll down to the **Organization** section, type **Sales** next to **Department**. 6. Scroll down to access the **Member of** section of the Create User dialog, and click **Add**. Type **Allowed RODC Password Replication Group**, and then click **OK**. 7. Click **Add** and then click **OK**. 8. Click **OK** to close the Create User dialog. 9. Right click the **Tony Wang** user object and click **Delete**. Click **Yes** to accept the confirmation. 10. Click the **root (local)** node in the navigation pane and double click **Deleted Objects**. 11. Select the deleted **Tony Wang** user object and in the Tasks pane, click **Restore**. 12. Return to the **Users** container and note the restored **Tony Wang** user. Double click the **Tony Wang** object and note the department and group membership are also restored. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** |
| Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.  **New-ADUser -SamAccountName "twang" -AccountPassword (read-host "Set user password" -assecurestring) -name "Tony Wang" -enabled $true -givenname "Tony" -surname "Wang" -department "Sales"**  **Add-ADPrincipalGroupMembership -Identity "CN=tony wang,CN=Users,DC=root,DC=fabrikam,DC=com" -MemberOf "CN=** **Allowed RODC Password Replication Group,CN=Users,DC=root,DC=fabrikam,DC=com"**  **Remove-AdUser -identity "CN=tony wang,CN=Users,DC=root,DC=fabrikam,DC=com"**  **Get-AdObject -filter 'samaccountname -eq "twang"' -includedeletedobjects | Restore-AdObject** |

## Create, delete, and restore an OU containing several objects using Active Directory Administrative Center

The Active Directory Administrative Center does not restore all nested objects of a container recursively, requiring that you understand the order of operations when recovering deleted objects. In this demonstration, you will create an OU with a user and group, then delete the OU with its contents and restore them all.

Note

You must logon as a member of the Domain Admins group to complete the task described in this section.

 Create, delete, and restore multiple objects using Active Directory Administrative Center  
[Do this step using Windows PowerShell](#PS10)

|  |
| --- |
| 1. In theActive Directory Administrative Centerconsole tree, click **root (local)**. 2. In the **Tasks** pane, click **New**, and then click **Organizational Unit**. 3. In the **Create Organizational Unit** dialog, type **Vice Presidents** next to **name.** *De-*select the **Protect from accidental deletion** checkbox. 4. Click **OK** to close the **Create Organizational Unit** dialog. 5. Double click the new **Vice Presidents** OU to enter its context. 6. In the **Tasks** pane, click **New**, and then click **User**. 7. In the **Create User** dialog, type **Seth** next to **First name,** type **Grossman** next to **Last name**, and type **sgross** next to **User SamAccountName logon: root\** 8. In Password, type the password that you want to use for this account, and in Confirm password, type the password again. 9. Click **OK** to close the **Create User** dialog. 10. In the **Tasks** pane, click **New**, and then click **Group**. 11. In the **Create Group** dialog, type **Marketing Executives** next to **Group name** and **MarkExec** next to **Group (SamAccountName)**. 12. In the **Members** section, click **Add**. In the **Select Users, Contacts, Computers, Service Accounts or Groups** dialog, type **Seth Grossman** and click **OK**. 13. Click **OK** to close the **Create Group** dialog. 14. Click the **root (local)** node to enter its context. 15. Select the **Vice Presidents** OU and click **Delete** in the **Tasks** pane. Click **Yes** to confirm. Select the **Use delete subtree server control** and click **Yes** to force the deletion of the OU and all its child objects. 16. Double click the **Deleted Objects** container to enter its context. Drag and expand the **Last Known Parent** column so you can see its full path for each object. 17. Select the **Vice Presidents** OU and click **Restore** in the **Tasks** pane. 18. Click the **Refresh** icon and note that the **Last Known Parent** value on the deleted **Seth Grossman** and **Marketing Executives** objects changes to the restored **Vice Presidents** OU. 19. Hold down SHIFT and select both deleted objects, then click **Restore** in the **Tasks** menu. 20. Return to the restore **Vice Presidents** OU and note that the user and group restored along with their inter-related group membership information. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** |
| Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.  **New-AdOrganizationalUnit -name "Vice Presidents" -protectedfromaccidentaldeletion:$false**  **New-ADUser -SamAccountName "sgross" -AccountPassword (read-host "Set user password" -assecurestring) -enabled $true -givenname "Seth" -surname "Grossman" -name "Seth Grossman" -path "ou=vice presidents,DC=root,DC=fabrikam,DC=com"**  **New-ADGroup -name "Marketing Executives" -groupscope global -groupcategory security -samaccountname "markexec" -path "ou=vice presidents,DC=root,DC=fabrikam,DC=com"**  **Add-ADPrincipalGroupMembership -Identity "CN=Seth Grossman,ou=vice presidents,DC=root,DC=fabrikam,DC=com" -MemberOf "CN=Marketing Executives,OU=vice presidents,DC=root,DC=fabrikam,DC=com"**  **Remove-AdOrganizationalUnit -identity "ou=vice presidents,DC=root,DC=fabrikam,DC=com" -recursive**  **Get-ADObject -filter 'msds-lastKnownRdn -eq "Vice Presidents"' -includeDeletedObjects | Restore-ADObject**  **Get-AdObject -filter 'lastknownparent -like "ou=vice presidents,DC=root,DC=fabrikam,DC=com"' -includedeletedobjects | Restore-AdObject** |

## Create Fine Grained Password Policies using Active Directory Administrative Center

The Active Directory Administrative Center supports graphically creating and managing the Fine Grained Password Policies first introduced in Windows Server 2008. In this demonstration, you will create an FGPP for the built-in Administrator account and the Domain Admins accounts, so that they have stricter requirements than the rest of the low-privilege domain users.

Note

You must logon as a member of the Domain Admins group to complete the task described in this section.

Create fine-grained password policies using Active Directory Administrative Center  
[Do this step using Windows PowerShell](#PS11)



|  |
| --- |
| 1. In theActive Directory Administrative Centerconsole tree, click **root (local)**. Double click the **System** container, and then double click the **Password Settings Container** object. 2. In the **Tasks** pane, click **New**, and then click **Password Settings**. 3. In the **Create Passwords** dialog, type **Built-In Administrator** **FGPP** next to N**ame.** Type **1** next to **Precedence**. 4. Type **16** next to **Minimum Password length (characters)**. 5. Type **14** next to **User must change the password after (days)**. 6. Note the other default password requirements. 7. Under the **Directly Applies To** section, click **Add**. In the **Select Users or Groups** dialog, type **Administrator** and click **OK.** 8. Click **OK** to close the **Create Password Settings** dialog. 9. In the **Tasks** pane, click **New**, and then click **Password Settings**. 10. In the **Create Passwords** dialog, type **Domain Admins FGPP** next to N**ame.** Type **2** next to **Precedence**. 11. Type **12** next to **Minimum Password length (characters)**. 12. Note the other default password requirements. 13. Under the **Directly Applies To** section, click **Add**. In the **Select Users or Groups** dialog, type **Domain Admins** and click **OK.** 14. Click **OK** to close the **Create Password Settings** dialog. 15. In theActive Directory Administrative Centerconsole tree, click **root (local)**, and then double-click **Users**. 16. In the **Tasks** pane, click **New**, and then click **User**. 17. In the **Create User** dialog, type **AdminUser2** next to **Full name** and type **adminuser2** next to **User SamAccountName logon: root\** 18. In Password, type the password that you want to use for this account, and in Confirm password, type the password again. 19. Scroll down to access the **Member of** section of the Create User dialog, and click **Add**. Type **Domain Admins**, and then click **OK**. 20. Click **OK** to close the **Create User** dialog. 21. Open the **Start** page and click your user name in the upper right, then click **Lock**. 22. Click **Switch User,** then hit **CTRL+ALT+DEL** and then click the left arrow to choose **Other User.** Type **AdminUser2** for the user name and the password you set earlier. 23. When prompted to change your password before logging on the first time, click **OK**. Enter a new complex password that is more than 7 characters, but not more than 11 characters. You will receive the expected error that you do not meet the password requirements.   Note  The built-in default password policy of this domain requires only a 7-character password of all users, but because your user account is a member of the Domain Admins group, your account requires at least a 12-character password.   1. Log back on as the original user account. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell commands** |
| Enter each command on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Always run Windows PowerShell as an elevated administrator.  **New-ADFineGrainedPasswordPolicy -Name "Built-In Administrator FGPP" -Precedence 1 -ComplexityEnabled $true -MaxPasswordAge "14.00:00:00" -MinPasswordAge "1.00:00:00" -MinPasswordLength 16 -PasswordHistoryCount 24 -ReversibleEncryptionEnabled $false**  **Add-ADFineGrainedPasswordPolicySubject "Built-In Administrator FGPP" -Subjects "Administrator"**  **New-ADFineGrainedPasswordPolicy -Name "Domain Admins FGPP" -Precedence 2 -ComplexityEnabled $true -MaxPasswordAge "42.00:00:00" -MinPasswordAge "1.00:00:00" -MinPasswordLength 12 -PasswordHistoryCount 24 -ReversibleEncryptionEnabled $false**  **Add-ADFineGrainedPasswordPolicySubject "Domain Admins FGPP" -Subjects "Domain Admins"** |

## Use the Active Directory Administrative Center Windows PowerShell History Viewer to learn commands

The Active Directory Administrative Center contains a new Windows PowerShell history viewer that shows you all commands run to create, modify, or delete objects.

Note

You must logon as a member of the Domain Admins group to complete the task described in this section.

 Create, delete, and restore multiple objects using Active Directory Administrative Center

|  |
| --- |
| 1. In theActive Directory Administrative Centerconsole tree, click the **chevron** (arrow pointing up) in the lower right corner of the page, in the section called **Windows PowerShell History**. 2. Click **root (local)**. Double click the **Users** container. 3. In the **Tasks** pane click **New** then click **Group**. 4. Type **Support Team** next to **Group Name** and type **support** next to **Group (SamAccountName)**. Select a **group scope** of **Universal**. 5. In the **Members** section, click Add. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog, click **Advanced** then click **Find Now**. Add **AdminUser1** and **AdminUser2** and click **OK**. 6. Click **OK** to close the **Create Group** dialog. 7. Note how the Windows PowerShell History viewer has two new entries for cmdlets **New-Adgroup** and **Set-ADGroup**. Click the **+** sign next to **New-Adgroup** to expand the node and see all the arguments passed to the **Active Directory Windows PowerShell** module. 8. Right click **New-Adgroup** and click **Copy**. 9. On the Windows taskbar, right click the PowerShell icon and click **Run as Administrator**. 10. In the new Windows PowerShell console, right click and the Windows PowerShell commands will paste in. 11. Use the left arrow on your keyboard to backtrack to the **-Samaccountname** argument and change "Support" to "Research". Use the back arrow again to backtrack to the **-Name** argument and change "Support Team" to "Research Team". 12. Hit ENTER. The new group is created using Windows PowerShell. |

## Use Server Manager to group and monitor domain controllers

Server Manager in Windows Server "8" Beta is the new centralized, graphical management tool for domain controllers and other server roles. It is especially useful for remotely administering environments using Windows Server "8" Beta in its default Core installation, which has no graphical interface.

Note

You must logon as a member of the Domain Admins group to complete the task described in this section.

 Create, delete, and restore multiple objects using Active Directory Administrative Center

|  |
| --- |
| 1. If not already running, start Server Manager from the taskbar or **Start** page. 2. Click **Manage** then **Add Servers** (alternatively, right-click **All Servers** and click **Add Servers**). 3. In the **Add Servers** dialog box on the **Active Directory** tab, click **Find Now**. Type **NEW** next to **Name(CN)** and click **Find Now**. This returns all servers starting with a name of NEW. 4. Select the three domain controllers and click the **arrow** to add them to the server pool. Click **OK**. Wait for Server Manager to refresh the dashboard. 5. When done refreshing, the AD DS thumbnail now shows the number **3** in the upper right, meaning that it is monitoring three computers with the AD DS role installed. 6. Click the **AD DS** linkand the AD DS details page opens. The **Servers** tile shows all three servers being monitored. Their status will be **Online - Performance Counters not started**. 7. Right click **NEWDC2** and note the menu options. From here, you can add roles, restart the server, perform computer management, make an RDP connection, run a Windows PowerShell session, or run the most common AD DS management tools. Click **Start Performance Counters**. Repeat this with the other two domain controllers. 8. Select all three domain controllers using the CTRL key and clicking, and then scroll down to the **Events** tile. Note how all ASD DS-related errors and warnings show from the past 24 hours. Click several to see their details. 9. Click the **Tasks** menu and click **Configure Event Data**. Change the **Get events that have occurred within the past** to **3 days** and click **OK**. 10. Click the **Dashboard** link then click the **Events** link on the **AD DS** thumbnail. Click the dropdown next to Event **severity** **levels** and select **Error**. Note how all error events show now from the past three days in addition to critical events. Click OK and note how the **AD DS** thumbnail now has a red numbered alert next to **Services** that matches the number of events. 11. Click the **AD DS** link. 12. Scroll down to the **Services** tile and now how all AD DS-related services are monitored. On **NEWDC2**, right-click the **Netlogon** service and click **Stop Service**. 13. Click the **Dashboard** link and note how the AD DS thumbnail now has a red **1** alert next to **Services**. Click **Services** and note why the Netlogon service is making Server Manager report an alert: its **start type** is **automatic** but its **status** is **stopped**. Right click the **Netlogon** service and click **Start Service**. Click **OK** to close the **Services** dialog. 14. Click the **AD DS** link. 15. Right click **NEWDC2** in the **Servers** tile and click **Windows PowerShell**. Note how the Windows PowerShell opens in the context of **NEWDC2**. 16. Type **stop-computer** and hit ENTER. This shuts down **NEWDC2**. Close the Windows PowerShell console. 17. Click the **Dashboard** link and either wait up to 10 minutes or click the **Refresh** icon. Now how an alert appears for **Manageability** on the **AD DS** thumbnail, meaning that a server is offline. 18. Click **Manageability**. Note that the name and IP address of the server shows, as well as the last time Server Manager received a heartbeat response. Click OK to close the **Manageability** dialog. 19. Boot **NEWDC2** back up from its virtual machine or hardware power switch and allow it to reach the Lock Screen. 20. Refresh Server Manager or wait up to 10 minutes and note how the **Manageability** alert disappears. 21. Click the **AD DS** link. 22. Now that some time has passed, scroll down to the Performance tile and examine the CPU and Memory usage patterns. Click **Tasks** and **Configure Performance Alerts**. 23. Change the **Graph display period** **(days)** to **7**, so that when you look at the server in the future you have a longer point of comparison. If high CPU alerts were to start occurring later, you now have reference points for the behavior. |

# Appendix

## Set UAC behavior of the elevation prompt for administrators

By default, UAC is enabled in Windows Server "8" Beta and Windows 8 Consumer Preview. This service will prompt for permission to continue during several of the configuration tasks described in this guide. In all cases, you can click Continue in the UAC dialog box to grant this permission, or you can use the following procedure to change the UAC behavior of the elevation prompt for administrators.

To set UAC behavior of the elevation prompt for administrators

|  |
| --- |
| * 1. Click **the Search** charm**.** Click **Apps.**   2. Type secpol.msc, and press ENTER.   3. In the console tree, open Local Policies, and then click Security Options.   4. In the contents pane, double-click User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode.   5. Click Elevate without prompting in the list, and then click OK.  1. 6. Close the Local Security Policy window. |

## Pasting text to Hyper-V guests sometimes results in garbled characters

When using a Hyper-V Virtual Machine Connection console to a running virtual machine on Windows Server "8" Beta Hyper-V and then using **Type Clipboard Text** menu option, the characters pasted may appear out of order or garbled. This makes copying and pasting Windows PowerShell commands difficult.

To work around this issue:

* Use the **mstsc.exe** RDP client to connect directly to virtual machines. Note that this requires attaching your client computer to the corpnet network described in this guide
* Increase the keyboard class buffer size in the virtual machine
* Disable the synthetic keyboard in the virtual machine to force using the emulated keyboard, which does not have this issue

 To Increase the keyboard class buffer size in the virtual machine

|  |
| --- |
| 1. Logon to a running virtual machine as a member of the Administrators group. 2. Open the **Start** page, type **regedit**, and hit ENTER. 3. Locate and then click the following registry entry:   **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\kbdclass\Parameters**   1. In the details page, double click:   **KeyboardDataQueueSize**   1. Select **Decimal** and type a **value data** of:   **1024**   1. Click **OK**. Close the Registry Editor and restart the virtual machine. |

To disable the synthetic keyboard for a virtual machine

|  |
| --- |
| 1. Logon to a running virtual machine as a member of the Administrators group. 2. Open the **Start** page and type **devmgmt.msc** then hit ENTER. 3. Click **Keyboards**, right click **Microsoft Hyper-V Virtual Keyboard** and click **Disable**. 4. Close the Device Manager snap-in.  * Note  On Windows Server "8" Beta Core, download [DevCon.exe](http://social.technet.microsoft.com/wiki/contents/articles/182.aspx) from the Windows Driver Kit to [disable](http://msdn.microsoft.com/en-us/library/windows/hardware/ff544722(v=vs.85).aspx) this driver using the command-line. |

# Additional Resources

For a list of all of the Windows Server "8" Beta TLGs, see [Windows Server "8" Beta Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=243062) in the TechNet Wiki.

For more information about Windows Server "8" Beta AD DS Simplified Administration, see:

* [Understand and Troubleshoot ADDS Simplified Administration in Windows Server "8" Beta](http://go.microsoft.com/fwlink/p/?LinkId=237244)
* [Active Directory Administrative Center Enhancements (FGPP UI, Recycle Bin UI, and Windows PowerShell Script Viewer)](http://go.microsoft.com/fwlink/p/?LinkID=238331)
* [Active Directory Replication and Topology Management Using Windows PowerShell](http://go.microsoft.com/fwlink/p/?LinkID=238337)
* [AD DS Deployment Guide](http://go.microsoft.com/fwlink/p/?LinkID=238318)

For information about Windows Server "8" Beta Virtualized Domain Controllers, see:

* [Understand and Troubleshoot Virtualized Domain Controllers in Windows Server "8" Beta](http://go.microsoft.com/fwlink/p/?LinkId=236370)
* [Test Lab Guide: Demonstrate Windows Server "8" Beta Virtualized Domain Controller (VDC)](http://go.microsoft.com/fwlink/p/?LinkId=237261)
* [AD DS Virtualization (Cloning and Virtualization safe improvements)](http://go.microsoft.com/fwlink/p/?LinkID=238316)

For more information about Windows Server Hyper-V, see:

* [Windows Server Hyper-V](http://www.microsoft.com/en-us/server-cloud/windows-server/hyper-v.aspx) (Portal)
* [Hyper-V](http://technet.microsoft.com/en-us/library/cc753637(v=WS.10).aspx) (Windows Server 2008 R2 TechNet Portal)
* [Virtualization Team](http://blogs.technet.com/b/virtualization/) (Official Microsoft Product Team Blog)

For more information about Active Directory Domain services, see:

* [Active Directory Domain Services](http://technet.microsoft.com/en-us/library/cc770946(WS.10).aspx)  (TechNet Portal)
* [Active Directory Domain Services for Windows Server 2008 R2](http://technet.microsoft.com/en-us/library/dd378801(WS.10).aspx)
* [Active Directory Domain Services for Windows Server 2008](http://technet.microsoft.com/en-us/library/dd378891(WS.10).aspx)
* [Windows Server Technical Reference](http://technet.microsoft.com/en-us/library/cc739127(WS.10).aspx) (Windows Server 2003)
* [Active Directory Administrative Center: Getting Started](http://technet.microsoft.com/en-us/library/dd560651(WS.10).aspx) (Windows Server 2008 R2)
* [Running Adprep](http://technet.microsoft.com/en-us/library/dd464018(WS.10).aspx) (Windows Server 2008 R2)
* [Active Directory Recycle Bin, see Active Directory Recycle Bin Step-by-Step Guide](http://technet.microsoft.com/en-us/library/dd392261(WS.10).aspx) (Windows Server 2008 R2)
* [AD DS Fine-Grained Password and Account Lockout Policy Step-by-Step Guide](http://technet.microsoft.com/en-us/library/cc770842(WS.10).aspx) (Windows Server 2008 R2)
* [Active Directory Administration with Windows PowerShell](http://technet.microsoft.com/en-us/library/dd378937(WS.10).aspx) (Windows Server 2008 R2)
* [Ask the Directory Services Team](http://blogs.technet.com/b/askds/) (Official Microsoft Commercial Technical Support Blog)

To provide the authors of this guide with feedback or suggestions for improvement, send email to [tlgfb@microsoft.com](mailto:tlgfb@microsoft.com).