Microsoft

Administering Windows Server 2012

Training Guide

Orin Thomas

Administering Windows Server 2012

Designed to help enterprise administrators develop real-world, job-role-specific skills—this *Training Guide* focuses on deploying and managing Windows Server 2012. Build hands-on expertise through a series of lessons, exercises, and suggested practices—and help maximize your performance on the job.

This Microsoft *Training Guide:*

- Provides in-depth, hands-on training you take at your own pace
- Focuses on job-role-specific expertise for deploying and managing Windows Server 2012 core services
- Creates a foundation of skills which, along with on-the-job experience, can be measured by Microsoft Certification exams such as 70-411

Sharpen your skills. Increase your expertise.

- Deploy and update Windows Server 2012
- Manage account policies and service accounts
- Configure name resolution
- Administer Active Directory
- Manage Group Policy application and infrastructure
- Work with Group Policy settings and preferences
- Administer network policies
- Configure the network to enable remote access
- Manage file services
- Monitor and audit Windows Server 2012

About You

This *Training Guide* will be most useful to IT professionals who have at least three years of experience administering previous versions of Windows Server in midsize to large environments.

About the Author

Orin Thomas is a consultant, writer, and Microsoft MVP whose books include Microsoft Press *Training Kits* for Exams 70-646, 70-647, 70-662, and 70-680. He is also a contributing editor for *Windows IT Pro* magazine.

About the Practices

For most practices, we recommend using a Hyper-V virtualized environment.

For *system requirements*, see the Introduction.

Preparing for Microsoft Certification?

Get the official exam-prep guide for Exam 70-411.

Exam Ref 70-411: Administering Windows Server 2012
ISBN 9780735673557

microsoft.com/mspress

ISBN: 978-0-7356-7413-4

90000

9 780735 674134

U.S.A. $59.99
Canada $62.99
[*Recommended*]

Operating Systems/Windows

Microsoft

Microsoft

Training Guide: Administering Windows Server 2012

Orin Thomas

ISBN: 978-0-735-67413-4

2 3 4 5 6 7 8 9 10 LSI 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author’s views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation,
nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Michael Bolinger

Developmental Editor: Troy Mott

Production Editor: Holly Bauer

Editorial Production: Box Twelve Communications

Technical Reviewer: Randall Galloway

Copyeditor: Nancy Sixsmith

Indexer: Angie Martin

Cover Design: Twist Creative • Seattle

Cover Composition: Karen Montgomery

Illustrator: Rebecca Demarest

[2013-09-27]

Contents at a glance

Contents

Chapter 4 Administering Active Directory 177

Chapter 5 Managing Group Policy application and infrastructure 237

Chapter 6 Group Policy settings and preferences 275

Introduction

When Microsoft Learning puts together exam objectives for an exam, it doesn't randomly select pages from TechNet. Instead, in conjunction with subject matter experts and representatives of the product team, it puts together a list of tasks and areas of knowledge that represents what someone in a specific job role would do and need to know on a day-to-day, a weekly, or even a monthly basis.

Each exam maps to a different job role. The objectives for the 70-411 exam are a list of tasks and areas of knowledge that describe what an administrator of the Windows Server 2012 operating system with several years of on-the-job experience (managing other server operating systems as well as Windows Server 2012) does and understands. The objectives don't cover everything that a Windows Server 2012 systems administrator would know, and there will be tasks and areas that will be relevant to one person's real world role and not another, but the exam objectives provide a reasonable approximation of that role.

This book covers the majority of the topics and skills that are the subject of the Microsoft certification exam 70-411. The idea behind this book is that by reading it, you can learn how to perform tasks you may need to perform on a day-to-day basis in your role as a Windows Server 2012 administrator. Using the exam objectives as a working definition of that role has the additional benefit of giving you a better understanding of the topics and tasks listed on the 70-411 exam objectives. This book will assist you in preparing for the exam, but it's not a complete exam preparation solution. If you are preparing for the exam, you should use additional study materials, such as practice tests and *Exam Ref 70-411: Administering Windows Server 2012* (Microsoft Press, 2013) to help bolster your real-world experience. For your reference, a mapping of the topics in this book to the exam objectives is included in the back of the book in the Objectives Map.

By using this training guide, you will learn how to do the following:

- Deploy, manage, and maintain servers
- Configure file and print services
- Configure network services and access
- Configure a network policy server infrastructure
- Configure and manage Active Directory
- Configure and manage Group Policy

System requirements

The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. This book is designed assuming you will be using Hyper-V—either the client version available with some editions of Windows 8 or the version available in Windows Server 2012. You can use other virtualization software instead, such as VirtualBox or VMWare Workstation, but the practice setup instructions in the Appendix assume that you are using Hyper-V.

Hardware and software requirements

This section presents the hardware requirements for Hyper-V and the software requirements.

Virtualization hardware requirements

If you choose to use virtualization software, you need only one physical computer to perform the exercises in this book. That physical host computer must meet the following minimum hardware requirements:

- x64-based processor that includes both hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection. (On AMD systems, the data execution protection feature is called the No Execute or NX bit. On Intel systems, this feature is called the Execute Disable or XD bit.) These features must also be enabled in the BIOS. (Note: You can run Windows Virtual PC without Intel-VT or AMD-V.) If you want to use Hyper-V on Windows 8, you need a processor that supports Second Level Address Translation (SLAT).
- 8 GB of RAM (more is recommended).
- 80 GB of available hard disk space.
- Internet connectivity.

Software requirements

The following software is required to complete the practice exercises:

- Windows Server 2012 evaluation. You can download an evaluation edition of Windows Server 2012 in iso format from the Windows Server and Cloud Platform website at *http://www.microsoft.com/server*.

Virtual Machine setup instructions

The instructions for building the virtual machine environment that allow you to perform the exercises in this book are located in the Appendix.

Acknowledgments

I'd like to thank the following people for their dedication and help in getting this book written: Troy Mott, Randall Galloway, Nancy Sixsmith, Holly Bauer, and Jeff Riley.

Errata & book support

We made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://aka.ms/TGAdminWinServer2012/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, send an email to Microsoft Press Book Support at *mspinput@microsoft.com.*

Please note that product support for Microsoft software is not offered through the previous addresses.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback is our most valuable asset. Please tell us what you think of this book at:

http://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 5

Managing Group Policy application and infrastructure

There is far more to managing Group Policy than knowing the location of specific policy items. After your environment has more than a couple of Group Policy Objects (GPOs), you have to start thinking about issues such as how they apply, who can edit them, what to do if substantive changes in policy need to be rolled back, and how you can track changes in Group Policy over time. In this chapter, you'll learn how to back up, restore, import, and export GPOs. You'll learn how to delegate the process of editing and applying GPOs and how to resolve configuration problems related to the application of Group Policy.

Lessons in this chapter:

- Lesson 1: Group Policy Object maintenance
- Lesson 2: Managing the application of Group Policy

Before you begin

To complete the practice exercises in this chapter, you need to have deployed computers DC, SYD-A, and SYD-B, as described in the Appendix, using the evaluation edition of Windows Server 2012.

Lesson 1: Group Policy Object maintenance

As an experienced systems administrator pursuing certification, you have a reasonable idea of how to use Group Policy. The administration of Group Policy doesn't just occur at the level of configuring individual policies. In large organizations with many policies, it's necessary to have a maintenance strategy. Ensuring that important Group Policy Objects (GPOs) are backed up and recoverable is as important as backing up and recovering other critical services such as DNS and Dynamic Host Configuration Protocol (DHCP). In this lesson, you'll learn how to back up, restore, import, and copy GPOs. You'll also learn how to delegate the management of GPOs.

After this lesson, you will be able to:

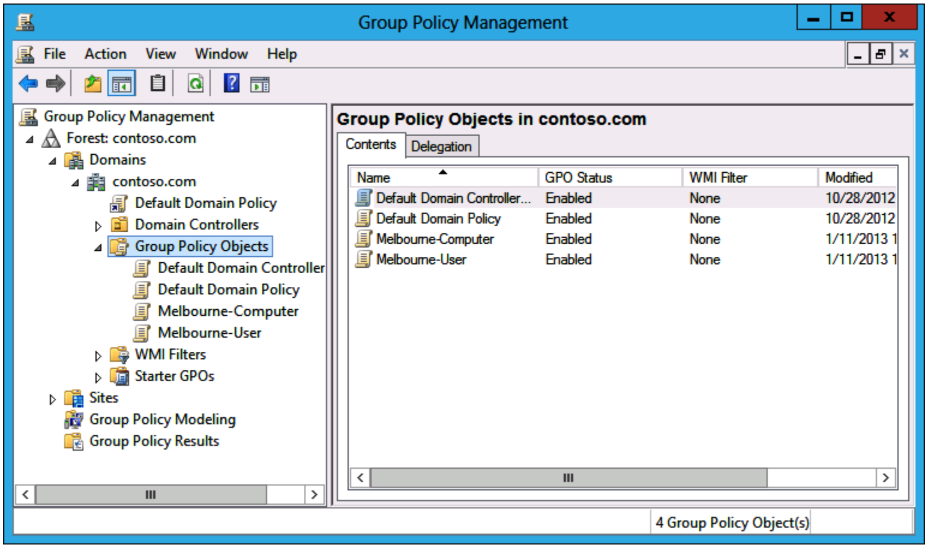
- Back up, import, copy, and restore GPOs.
- Migrate GPOs between domains and forests.
- Delegate GPO management.

Estimated lesson time: 45 minutes

Managing Group Policy Objects

As an experienced systems administrator, you are aware that GPOs enable you to configure settings for multiple users and computers. After you get beyond editing GPOs to configure settings, you need to start thinking about issues such as GPO maintenance. For example, if an important document is lost, you need to know how to recover it from backup. Do you know what to do if someone accidentally deletes a GPO that has hundreds of settings configured over a long period of time?

The main tool you'll use for managing GPOs is the *Group Policy Management Console (GPMC)*, shown in Figure 5-1. You can use this console to back up, restore, import, copy, and migrate. You can also use this console to delegate GPO management tasks.



Group Policy Objects in contoso.com

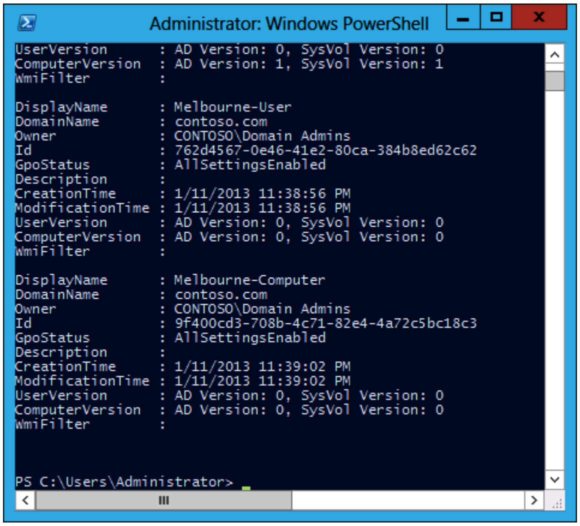
Name	GPO Status	WMI Filter	Modified
Default Domain Controller...	Enabled	None	10/28/2012
Default Domain Policy	Enabled	None	10/28/2012
Melbourne-Computer	Enabled	None	1/11/2013 1
Melbourne-User	Enabled	None	1/11/2013 1

FIGURE 5-1 GPMC

There are also a substantial number of cmdlets available in the Windows PowerShell Group Policy module, including the following:

- **Get-GPO** Enables you to view GPOs. The output of this cmdlet is shown in Figure 5-2.
- **Backup-GPO** Enables you to back up GPOs.

- **Import-GPO** Enables you to import a backed-up GPO into a specified GPO.
- **New-GPO** Enables you to create a new GPO.
- **Copy-GPO** Enables you to copy a GPO.
- **Rename-GPO** Enables you to change a GPO's name.
- **Restore-GPO** Enables you to restore a backed-up GPO to its original location.
- **Remove-GPO** Enables you to remove a GPO.



```
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 1, SysVol Version: 1
WmiFilter        :

DisplayName      : Melbourne-User
DomainName       : contoso.com
Owner            : CONTOSO\Domain Admins
Id               : 762d4567-0e46-41e2-80ca-384b8ed62c62
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 1/11/2013 11:38:56 PM
ModificationTime : 1/11/2013 11:38:56 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :

DisplayName      : Melbourne-Computer
DomainName       : contoso.com
Owner            : CONTOSO\Domain Admins
Id               : 9f400cd3-708b-4c71-82e4-4a72c5bc18c3
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 1/11/2013 11:39:02 PM
ModificationTime : 1/11/2013 11:39:02 PM
UserVersion      : AD Version: 0, SysVol Version: 0
ComputerVersion  : AD Version: 0, SysVol Version: 0
WmiFilter        :


PS C:\Users\Administrator> _
```

FIGURE 5-2 Output of the Get-GPO cmdlet

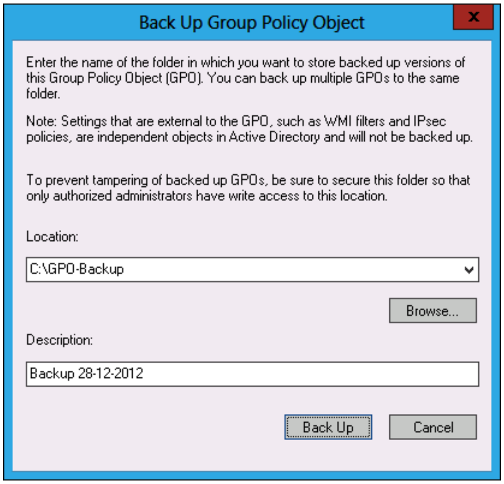
Backing up a GPO enables you to create a copy of a GPO as it exists at a specific point in time. A user must have read permission on a GPO to back it up. When you back up a GPO, the backup version of the GPO is incremented. It is good practice to back up GPOs prior to editing them so that if something goes wrong, you can revert to the unmodified GPO.

REAL WORLD **BACKING UP GPOS**

If your organization doesn't have access to the Microsoft Desktop Optimization Pack (MDOP), you should back up GPOs before you or other people modify them. If a problem occurs, it's quicker to restore a backup than it is to reconfigure the modified GPO with the existing settings.

To back up a GPO, perform the following steps:

1. Open the GPMC.
2. Right-click the GPO that you want to back up and click Back Up.In the Back Up Group Policy Object dialog box, shown in Figure 5-3, enter the location of the backup and a description for the backup.



Back Up Group Policy Object

Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.

Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.

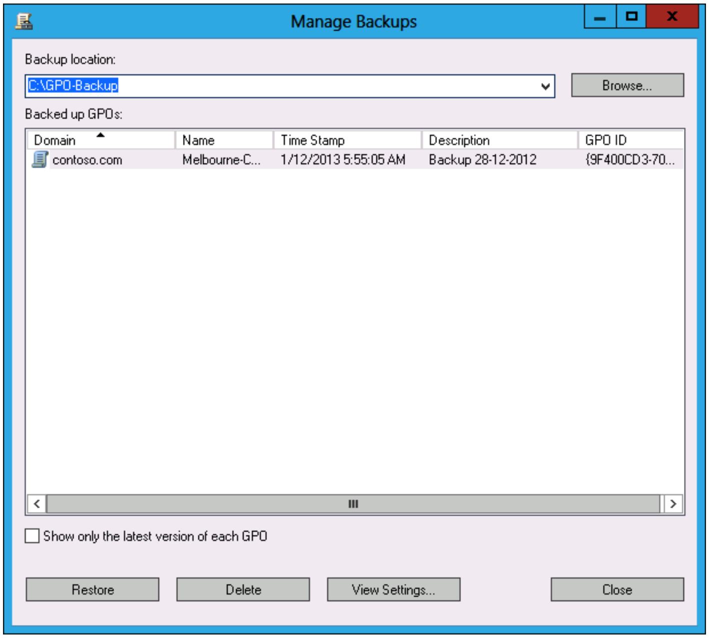
To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.

Location: C:\GPO-Backup

Description: Backup 28-12-2012

FIGURE 5-3 Backing up a GPO

You can restore a GPO using the Restore-GPO cmdlet. Restoring a GPO overwrites the current version of the GPO if one exists or re-creates the GPO if the GPO has been deleted. To restore a GPO, right-click the Group Policy Objects node in the GPMC and click Manage Backups. In the Manage Backups dialog box, shown in Figure 5-4, select the GPO that you want to restore and click Restore. If multiple backups of the same GPO exist, you can select which version of a GPO to back up.



Manage Backups

Backup location: C:\GPO-Backup

Backed up GPOs:

Domain	Name	Time Stamp	Description	GPO ID
contoso.com	Melbourne-C...	1/12/2013 5:55:05 AM	Backup 28-12-2012	{9F400CD3-70...

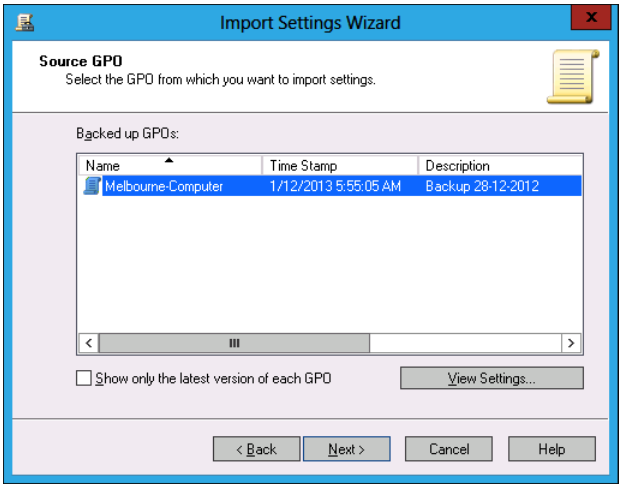
□ Show only the latest version of each GPO

FIGURE 5-4 Restoring a GPO from backup

Import and copy GPOs

Importing a GPO enables you to take the settings in a backed-up GPO and import them into an existing GPO. To import a GPO, perform the following steps:

1. Right-click an existing GPO in the GPMC and click Import Settings.
2. In the Import Settings Wizard, you are given the option of backing up the destination GPO's settings. This enables you to roll back the import.
3. Specify the folder that hosts the backed-up GPO.
4. On the Source GPO page of the Import Settings Wizard, shown in Figure 5-5, select the source GPO. You can view the settings that have been configured in the source GPO prior to importing it. Complete the wizard to finish importing the settings.


Import Settings Wizard
Source GPO
Select the GPO from which you want to import settings.
Backed up GPOs:
□ Show only the latest version of each GPO
View Settings...
< Back
Next >
Cancel
Help

Name	Time Stamp	Description
Melbourne-Computer	1/12/2013 5:55:05 AM	Backup 28-12-2012

FIGURE 5-5 Importing GPO settings

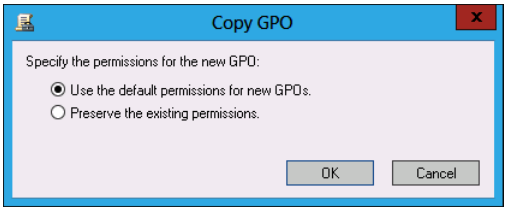
Remember that when you import settings from a backed-up GPO, the settings in the backed-up GPO overwrite the settings in the destination GPO.

Copying a GPO creates a new GPO and copies all configuration settings from the original to the new. You can copy GPOs from one domain to another. You can also use a *migration table* when copying a GPO to map security principals referenced in the source domain to security principals referenced in the destination domain.

To copy a GPO, perform the following steps:

1. Right-click the GPO that you want to copy and click Copy.
2. Right-click the location that you want to copy the GPO to and click Paste.

3. In the Copy GPO dialog box, choose between using the default permissions and preserving the existing permissions assigned to the GPO (see Figure 5-6).



Copy GPO

Specify the permissions for the new GPO:

● Use the default permissions for new GPOs.

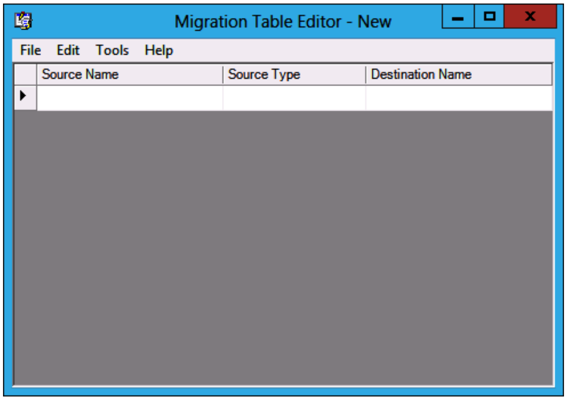
○ Preserve the existing permissions.

FIGURE 5-6 Copying a GPO

Migrate Group Policy Objects

When moving GPOs between domains or forests, you need to ensure that any domain-specific information is accounted for, so locations and security principals in the source domain aren't used in the destination domain. You can account for these locations and security principals using migration tables. You use migration tables when copying or importing GPOs.

Migration tables enable you to alter references when moving a GPO from one domain to another or from one forest to another. An example is when you are using GPOs for software deployment and need to replace the address of a shared folder that hosts a software installation file so that it is relevant to the target domain. You can open the Migration Table Editor (MTE), shown in Figure 5-7, by right-clicking Domains in the GPMC and clicking Open Migration Table Editor.



Migration Table Editor - New

Source Name	Source Type	Destination Name

FIGURE 5-7 Opening the MTE

When you use the MTE, you can choose to populate from a GPO that is in the current domain or choose to populate the MTE from a backed-up GPO. When you perform this action, the MTE will be populated with settings that reference local objects. If, when you perform this action, there are no results, then no local locations are referenced in the GPO that you are going to migrate.

MORE INFO **WORKING WITH MIGRATION TABLES**

You can learn more about working with migration tables at *http://technet.microsoft.com/en-us/library/cc754682.aspx*.

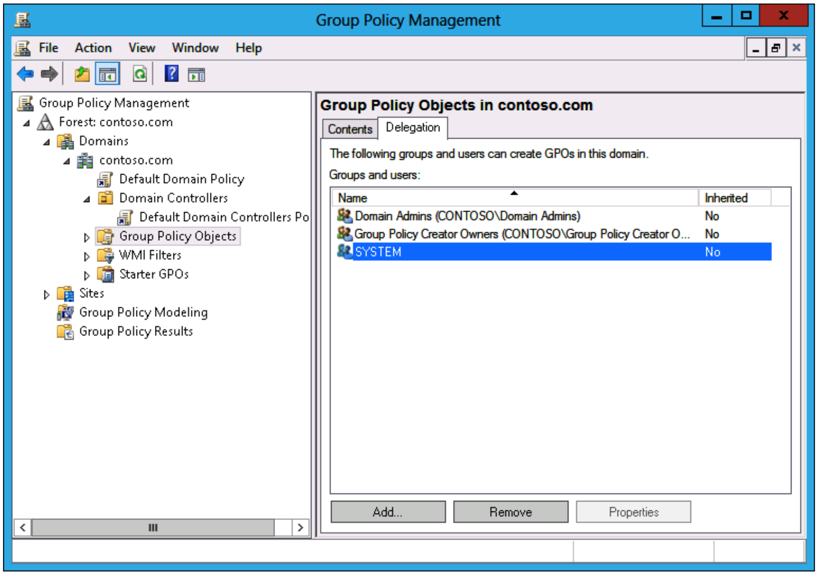
Delegate GPO management

In larger environments, there is more than one person in the IT department. In very large organizations, one person's entire job responsibility might be creating and editing GPOs. *Delegation* enables you to grant the permission to perform specific tasks to a specific user or group of users. You can delegate some or all of the following Group Policy management tasks:

- GPO creation
- GPO modification
- GPO linking to specific sites, organizational units (OUs), or domainsPermission to perform Group Policy Modeling analysis at the OU or domain levelPermission to view Group Policy Results information at the OU or domain levelWindows Management Instrumentation (WMI) filter creation

Users in the Domain Admins and Enterprise Admins groups can perform all Group Policy management tasks. Users that are members of the Group Policy Creator Owners domain group can create GPOs. They also have the right to edit and delete any GPOs that they have created.

You can delegate permissions to GPOs directly using the GPMC, as shown in Figure 5-8.



Group Policy Objects in contoso.com

The following groups and users can create GPOs in this domain.

Groups and users:

Name	Inherited
Domain Admins (CONTOSO\Domain Admins)	No
Group Policy Creator Owners (CONTOSO\Group Policy Creator O...	No
SYSTEM	No

FIGURE 5-8 Group Policy permissions

Creating GPOs

If you want to delegate the ability for users to create GPOs, you can add them to the Group Policy Creator Owners group. You can also explicitly grant them permission to create GPOs using the GPMC. To do this, perform the following steps:

1. Open the GPMC from the Tools menu of Server Manager.
2. Expand the domain in which you want to delegate the ability to create GPOs, click Group Policy Objects, and click the Delegation tab.
3. Click Add and select the group or user that you want to give the ability to create GPOs in that domain.

✓ **Quick check**

- **What group should you add users to if you want to enable them to create GPOs in the domain, but not add them to the Domain Admins or Enterprise Admins groups?**

Quick check answer

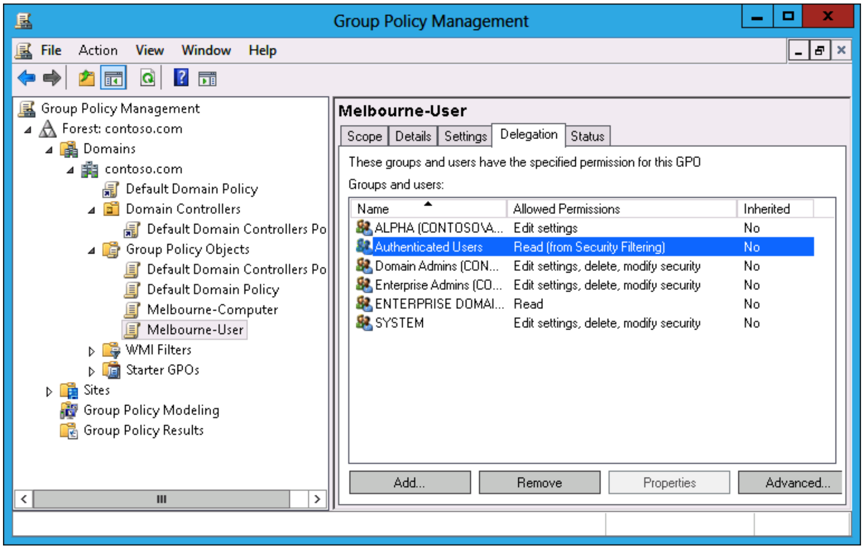
- **Add them to the Group Policy Creator Owner group.**

Editing GPOs

To edit a GPO, users must be either a member of the Domain Admins or Enterprise Admins group. They can edit a GPO if they created it. They can also edit a GPO if they have been given Read/Write permissions on the GPO through the GPMC.

To grant a user permission to edit a GPO, perform the following steps:

1. Click the GPO in the GPMC.
2. Click the Delegation tab, as shown in Figure 5-9.
3. Click Add, specify the user or group that should have permission to edit the GPO, and then specify the permissions that you want to give this user or group. You can choose from one of the following permissions:
   - Read
   - Edit Settings
   - Edit Settings, Delete, Modify Security



Melbourne-User

These groups and users have the specified permission for this GPO

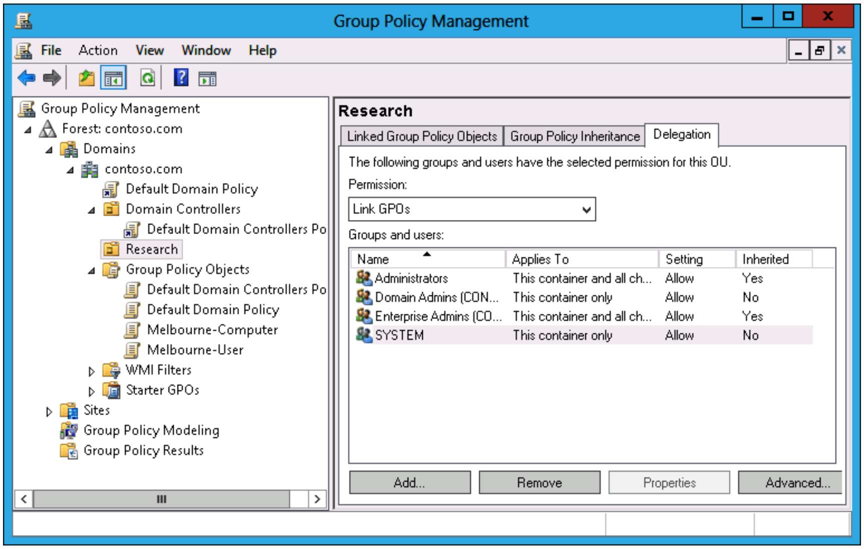
Groups and users:

Name	Allowed Permissions	Inherited
ALPHA (CONTOSO\A...	Edit settings	No
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (CON...	Edit settings, delete, modify security	No
Enterprise Admins (CO...	Edit settings, delete, modify security	No
ENTERPRISE DOMAI...	Read	No
SYSTEM	Edit settings, delete, modify security	No

FIGURE 5-9 Delegating permissions

Linking GPOs

To enable a user to link a GPO to a specific object, you need to edit the permission on that object. You can perform this task in the GPMC, as shown in Figure 5-10. For example, to grant a user or group permission to link a GPO to an OU, select the OU in the GPMC, select the Delegation tab, click Add, and then select the user or group to which you want to grant this permission.



Research

The following groups and users have the selected permission for this OU.

Permission: Link GPOs

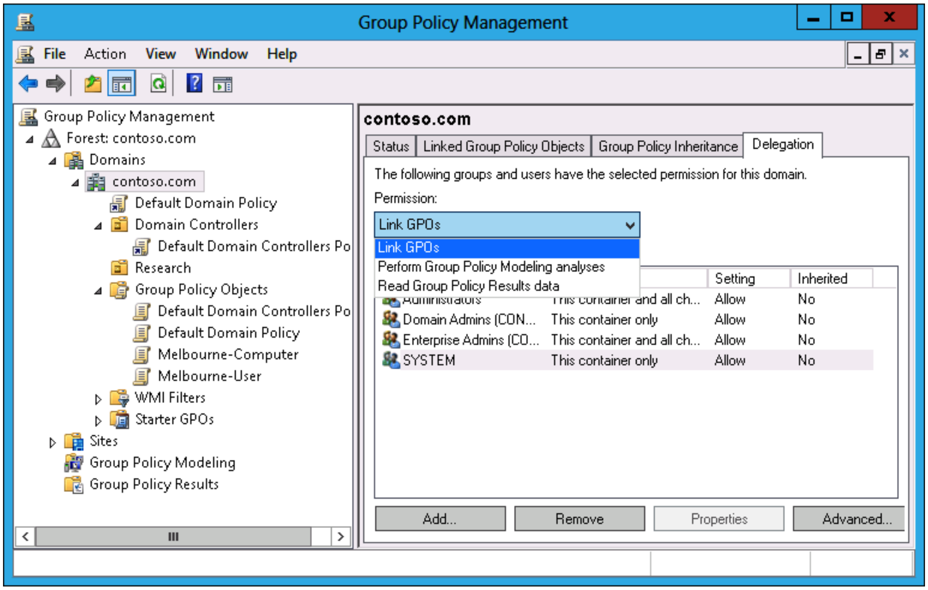
Groups and users:

Name	Applies To	Setting	Inherited
Administrators	This container and all ch...	Allow	Yes
Domain Admins (CON...	This container only	Allow	No
Enterprise Admins (CO...	This container and all ch...	Allow	Yes
SYSTEM	This container only	Allow	No

FIGURE 5-10 Delegating link GPO permission

Modeling, results, and WMI filters

Delegating permissions to perform tasks related to Group Policy Modeling and Group Policy Results is performed at the domain level, as shown in Figure 5-11. You can delegate the ability to create *WMI filters* by selecting the WMI Filters node in the GPMC and granting the permission on the Delegation tab.



The following groups and users have the selected permission for this domain.

Permission: Link GPOs

- Link GPOs
- Perform Group Policy Modeling analyses
- Read Group Policy Results data

		Setting	Inherited
Administrators	This container and all ch...	Allow	No
Domain Admins (CON...	This container only	Allow	No
Enterprise Admins (CO...	This container and all ch...	Allow	No
SYSTEM	This container only	Allow	No

FIGURE 5-11 Delegating Group Policy Modeling and Group Policy Results permissions

Lesson summary

- Each time you back up a GPO, it creates a copy of that GPO at a particular point in time.
- Restoring a GPO overwrites the existing GPO if it still exists or recovers it if it has been deleted.
- Importing a GPO overwrites the settings in the destination GPO with the settings from the imported GPO.
- Copying a GPO creates a duplicate of the GPO.
- You use migration tables when moving GPOs between domains and forests to account for local references in the source domain.
- You can delegate the permission to create, edit, and link using the GPMC. Non-administrative users can then perform some Group Policy tasks, such as editing policies, without giving them unnecessary privileges.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You have 200 individual GPO settings in a backed-up GPO named Melbourne-2012 that you want to include in an existing GPO named Sydney-2013. Which of the following Windows PowerShell cmdlets should you use to accomplish this goal?

   A. Backup-GPO

   B. Import-GPO

   C. Restore-GPO

   D. Copy-GPO

2. Prior to editing a Group Policy, your assistant makes a backup of the GPO that she is going to edit. Unfortunately, she makes a mistake in configuring the GPO. You need to revert the GPO to the state it was in prior to your assistant's edits. Which of the following Windows PowerShell cmdlets should you use to accomplish this goal?

   A. Copy-GPO

   B. Restore-GPO

   C. Import-GPO

   D. Backup-GPO

3. You want to copy a GPO from one domain to another in a forest. Which tool should you use to ensure that references to objects in the source domain updated are relevant to the destination domain? (Choose all that apply.)

   A. Active Directory Sites And Services

   B. Active Directory Users And Computers

   C. Migration Table Editor

   D. Group Policy Management Editor

4. Which of the following security groups have the right to create GPOs by default? (Choose all that apply.)

   A. Group Policy Creator Owners

   B. Enterprise Admins

   C. Domain Admins

   D. Domain Controllers

5. You are about to make substantial modifications to the default domain GPO. You want to ensure that you can return to the current state of the GPO if the modifications cause problems. Which of the following Windows PowerShell cmdlets should you use?

   A. Copy-GPO

   B. Restore-GPO

   C. Import-GPO

   D. Backup-GPO

Lesson 2: Managing Group Policy application

For environments in which you need to apply more than one Group Policy, understanding the rules of precedence is critical. Not only do you need to understand that where you apply a Group Policy determines its overall influence but also that GPOs may or may not apply due to inheritance blocks, security filtering, or loopback processing. In this lesson, you'll learn the rules on Group Policy application and how to determine which Group Policy settings have precedence in complex environments.

After this lesson, you will be able to:

- Determine policy processing order and precedence.
- Configure policy enforcement and blocking.
- Perform Group Policy security filtering.
- Configure WMI filtering.
- Enable loopback processing.
- Configure slow-link processing.

Estimated lesson time: 45 minutes

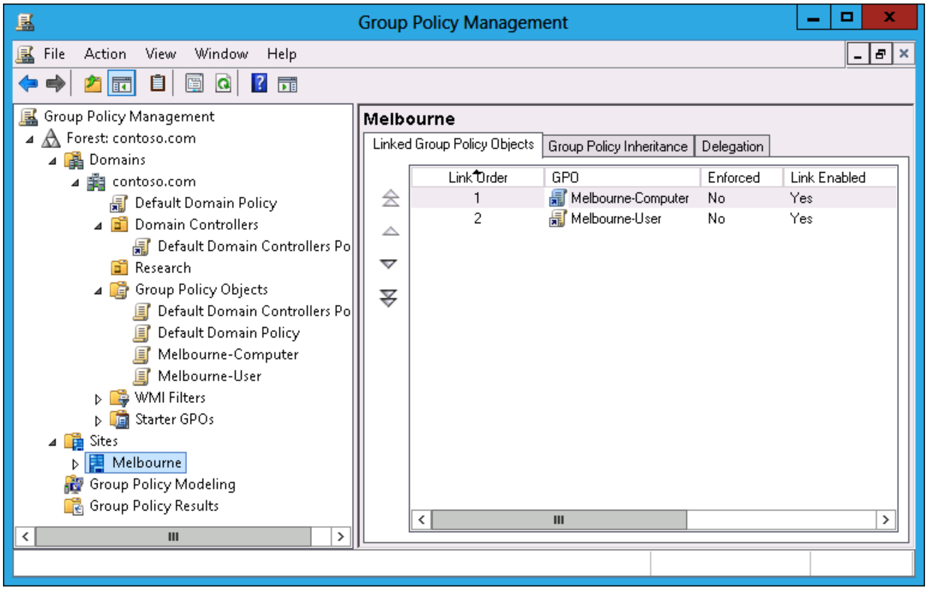
Policy processing precedence

In organizations with large Group Policy deployments, multiple GPOs might apply to a single user account or computer account; or when a user is signed on to a specific computer, to both. Group Policy processing *precedence* is the set of rules that determines which Group Policy items apply when multiple GPOs are configured.

Group Policies are processed in the following manner:

- **Local** Settings configured at the local level apply first. If multiple local policies apply, settings in machine policies apply first, settings in admin and nonadmin local policies override them, and settings in per-user policies override any configured at the machine and admin/nonadmin level.

- **Site** Policies based on location apply next. Any settings configured at the site level override settings configured at the local level. You can link multiple GPOs at the site level. When you do this, policies with a lower numerical link order override policies with a higher numerical link order. For example in Figure 5-12, settings in the Melbourne-Computer policy override settings configured in the Melbourne-User policy.



Link Order	GPO	Enforced	Link Enabled
1	Melbourne-Computer	No	Yes
2	Melbourne-User	No	Yes

FIGURE 5-12 GPO link order

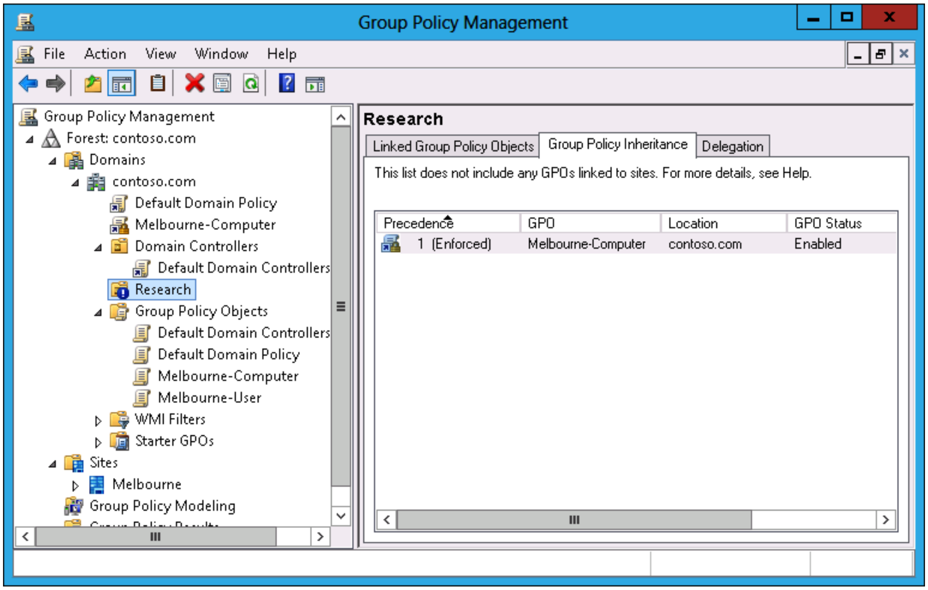
- **Domain** Settings applied at the domain level override settings applied at the site and local levels. You can link multiple GPOs at the domain level. The Default Domain Policy is linked at this level.
- **Organizational unit (OU)** Settings applied at the organizational unit level override settings applied at the domain, site, and local levels. When an account is a member of a child OU, policies applied at the child OU level override policies applied at the parent OU level. You can apply multiple GPOs at the OU level. Policies with a lower numerical link order override policies with a higher numerical link order.

Group Policy processing precedence is relevant only when there are conflicts in policies. If policy A applies at the domain level, and policy B applies at the OU level, both policy A and policy B apply.

Policy enforcement and blocking

When configuring a Group Policy, you can choose to enforce that policy. To enforce a Group Policy, right-click that policy at the location in which you link the policy and then click Enforced. When you choose to enforce a policy, that policy will apply and override settings configured at other levels. For example, normally a policy linked at the OU level would override a policy linked at the domain level. If you configure the policy at the domain level as Enforced, it instead overrides the policy linked at the OU level.

The *Block Inheritance* function enables you to block policies applied at earlier levels. For example, you can use Block Inheritance at the OU level to block policies applied at the domain and site level. Block Inheritance does not stop the application of policies configured as Enforced. For example, Figure 5-13 shows the Research OU configured with the Block Inheritance setting. The Melbourne-Computer policy, applied at the domain level as Enforced, still applies because a setting of Enforced overrides a setting of Block Inheritance.



- Group Policy Management
  - Forest: contoso.com
    - Domains
      - contoso.com
        - Default Domain Policy
        - Melbourne-Computer
        - Domain Controllers
          - Default Domain Controllers
        - Research
        - Group Policy Objects
          - Default Domain Controllers
          - Default Domain Policy
          - Melbourne-Computer
          - Melbourne-User
        - WMI Filters
        - Starter GPOs
    - Sites
      - Melbourne
  - Group Policy Modeling
  - Group Policy Results

Research

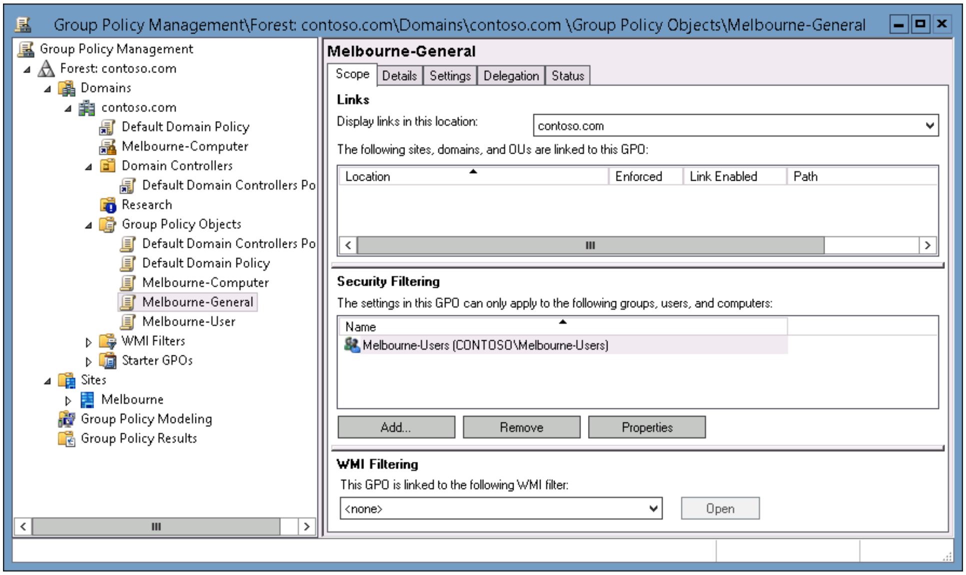
This list does not include any GPOs linked to sites. For more details, see Help.

Precedence	GPO	Location	GPO Status
1 (Enforced)	Melbourne-Computer	contoso.com	Enabled

FIGURE 5-13 Override versus Enforced

Group Policy security filtering

Security filtering enables you to configure permissions on GPOs. By default, Group Policies apply to the Authenticated Users group. By changing the default permissions, you can make the Group Policy apply only to a specific group. For example, if you remove the Authenticated Users group and add another security group such as the Melbourne-Users group (shown in Figure 5-14), the Group Policy applies to only that configured security group.



Melbourne-General

Links

Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Melbourne-Users (CONTOSO\Melbourne-Users)

WMI Filtering

This GPO is linked to the following WMI filter:

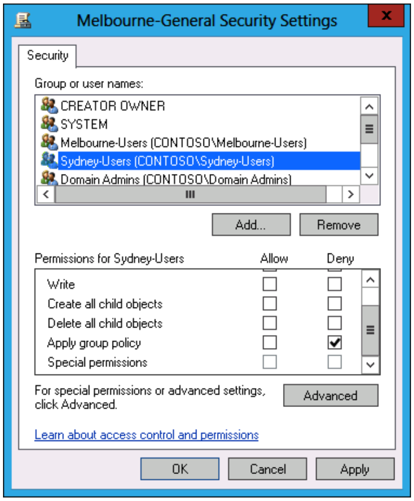
<none>

FIGURE 5-14 Security filtering

When considering whether to use security filtering, keep the following in mind:

- A security filter applies to the GPO, so it applies wherever the GPO is linked. You can't have one security filter apply to the GPO when linked at the domain level and another security filter apply to the GPO when linked at the OU level.
- Filtered policies still need to be checked during the Group Policy processing process, which can increase the amount of time spent on Group Policy processing. Startup and logon times may increase.

It is also possible to apply a Deny permission on the basis of security account or group. Deny permissions override Allow permissions. You block a particular security group from receiving a Group Policy by setting the Apply Group Policy (Deny) advanced permission, as shown for the Sydney-Users group for the Melbourne-General GPO in Figure 5-15. You can do this on the Delegation tab of a GPO's properties instead of the Scope tab.



Group or user names:

- CREATOR OWNER
- SYSTEM
- Melbourne-Users (CONTOSO\Melbourne-Users)
- Sydney-Users (CONTOSO\Sydney-Users)
- Domain Admins (CONTOSO\Domain Admins)

Permissions for Sydney-Users	Allow	Deny
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Apply group policy	□	☑
Special permissions	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

FIGURE 5-15 Security filtering

Quick check

- How would you block a GPO from applying to members of a particular security group?

Quick check answer

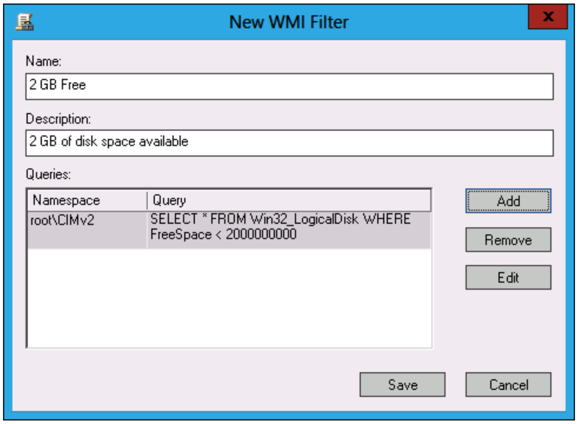
- Configure an Apply Group Policy (Deny) advanced permission on the Delegation tab of a GPO’s properties.

Group Policy WMI filtering

WMI filtering enables you to filter the application of policy based on the results of a WMI query. For example, you might write a WMI query to determine whether a computer has an x86 or x64 processor, or whether there is more than a certain amount of disk space available. WMI queries are often used with policies related to software deployment to determine whether the target computer has the appropriate system resources to support the installation of the application.

The drawback of WMI queries is that they are complicated for systems administrators who are unfamiliar with programming beyond simple scripting. WMI queries also cause significant delays in Group Policy processing. In environments in which sophisticated logic needs to be applied to targeted application distribution, products such as Microsoft System Center 2012 Configuration Manager are more appropriate. System Center 2012 Configuration Manager enables administrators performing software deployment to configure ways of checking hardware configuration prior to software deployment that do not require writing queries in WMI Query Language (WQL).

You can create WMI filters by using the New WMI Filter dialog box (shown in Figure 5-16).



Name:
2 GB Free

Description:
2 GB of disk space available

Queries:

Namespace	Query
root\CIMv2	SELECT * FROM Win32_LogicalDisk WHERE FreeSpace < 2000000000

FIGURE 5-16 Creating a WMI filter

MORE INFO **MORE INFO TITLE**

You can learn more about WMI queries at *http://msdn.microsoft.com/en-us/library/ms186146(VS.80).aspx*.

Loopback processing

As you are aware, each GPO has two distinct sections: Computer Configuration and User Configuration (see Figure 5-17). The resultant policies for a user are based on the cumulative user configuration settings in GPOs that apply to the user's accounts at the site, domain, and OU setting. The resultant computer policies are applied based on the cumulative computer configuration settings in GPOs that apply to the computer's account at the site, domain, and OU level.

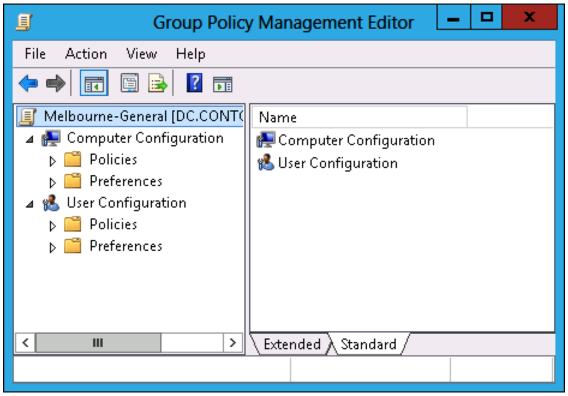
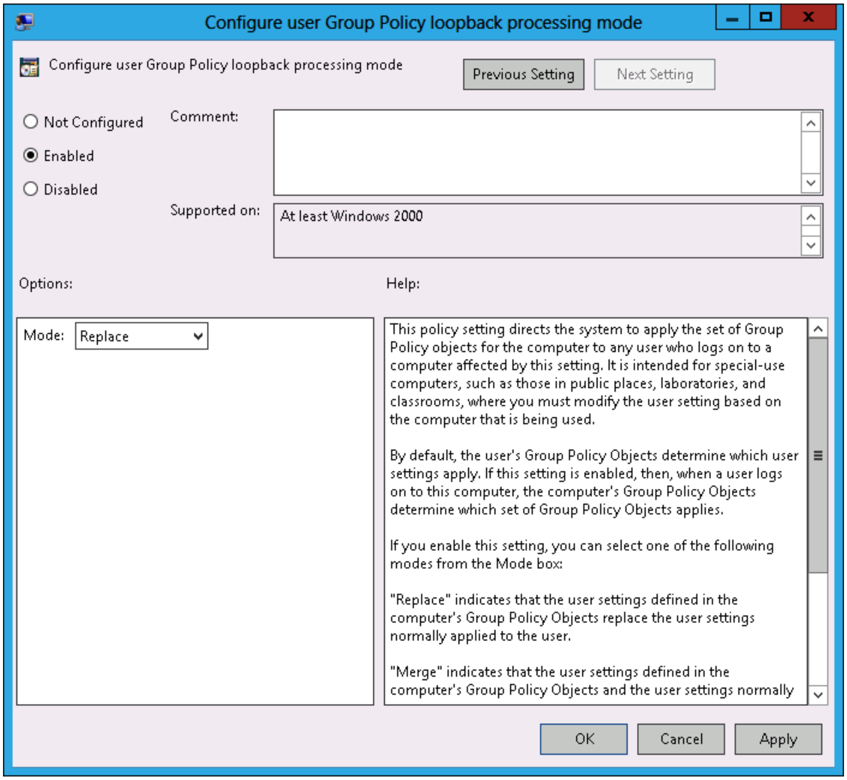


FIGURE 5-17 GPO structure

In some situations, you'll want only the GPOs that apply to the computer account to apply. You might want to do this with conference room computers, for which you want people to be able to sign on with domain accounts but to have a very controlled configuration. When you enable *loopback processing*, user settings are determined based on the settings in the User Configuration settings area of GPOs that apply to the computer account.

There are two types of loopback processing that you can configure by setting the Group Policy loopback processing mode policy, shown in Figure 5-18 and located under Computer Configuration\Administrative Templates\System\Group Policy: Replace And Merge.

- **Replace** When you configure Replace, only the GPOs that apply to the computer account will apply. Settings in the User Configuration area of the GPOs that apply to the computer account will apply.
- **Merge** The settings in the User Configuration area of GPOs that apply to the user account will still apply, but will be overridden by settings in the User Configuration area of GPOs that apply to the computer account.



Configure user Group Policy loopback processing mode

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Mode: Replace

Help:

This policy setting directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used.

By default, the user's Group Policy Objects determine which user settings apply. If this setting is enabled, then, when a user logs on to this computer, the computer's Group Policy Objects determine which set of Group Policy Objects applies.

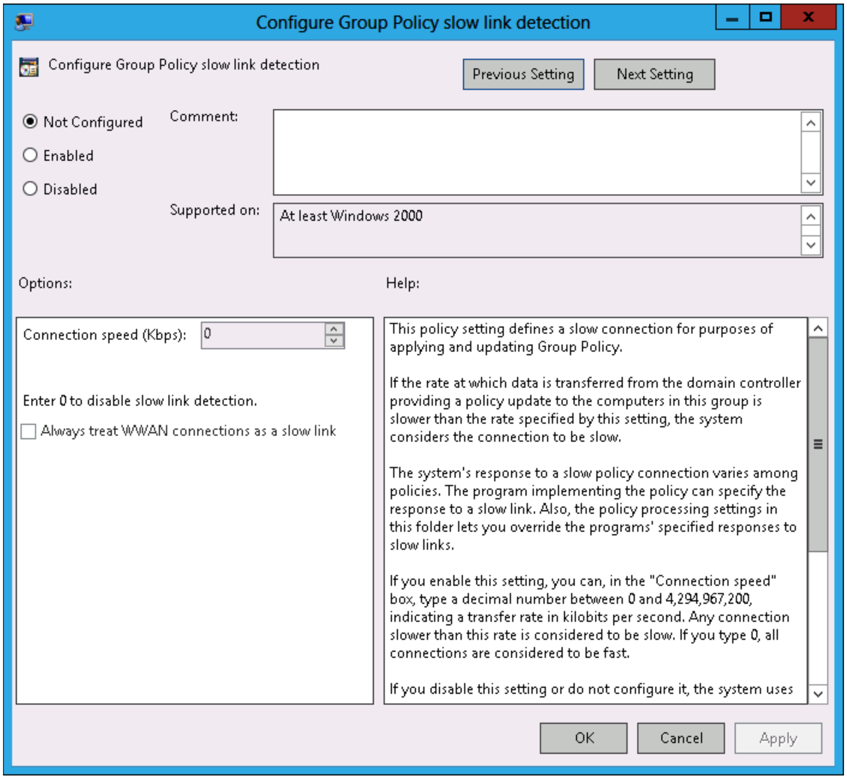
If you enable this setting, you can select one of the following modes from the Mode box:

"Replace" indicates that the user settings defined in the computer's Group Policy Objects replace the user settings normally applied to the user.

"Merge" indicates that the user settings defined in the computer's Group Policy Objects and the user settings normally

FIGURE 5-18 Loopback processing policy

Slow-link processing enables you to configure Group Policy application to be performed in a different manner, depending on the speed of the connection from the client to the domain controller. It enables you to block activities such as software deployment when the connection between Active Directory and the client is detected as falling below a particular threshold. You configure slow link detection by configuring the Group Policy slow link detection policy, as shown in Figure 5-19. This policy is located under Computer Configuration\Administrative Templates\System\Group Policy.



Configure Group Policy slow link detection

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Connection speed (Kbps): 0

Enter 0 to disable slow link detection.

□ Always treat WWAN connections as a slow link

Help:

This policy setting defines a slow connection for purposes of applying and updating Group Policy.

If the rate at which data is transferred from the domain controller providing a policy update to the computers in this group is slower than the rate specified by this setting, the system considers the connection to be slow.

The system's response to a slow policy connection varies among policies. The program implementing the policy can specify the response to a slow link. Also, the policy processing settings in this folder lets you override the programs' specified responses to slow links.

If you enable this setting, you can, in the "Connection speed" box, type a decimal number between 0 and 4,294,967,200, indicating a transfer rate in kilobits per second. Any connection slower than this rate is considered to be slow. If you type 0, all connections are considered to be fast.

If you disable this setting or do not configure it, the system uses

FIGURE 5-19 Slow link detection

Lesson summary

- Group policies are processed in the following order: local, site, domain, and OU. Policies processed later override policies processed earlier.
- When there are parent and child OUs, and the user or computer account is a member of the child OU, the policy applied at the child OU overrides policies applied at the parent OU.
- Policy processing order is important only when policies conflict.

- A policy with the Override setting will override other policies in the processing order, including when Block Inheritance has been configured.
- Security filtering applies on a GPO, no matter where it is linked.
- Loopback processing enables GPO settings applied to the computer account to override GPO settings applied to the user account.
- Slow-link processing enables you to configure policies not to be processed when low bandwidth connections to Active Directory are detected.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You want to ensure that a Group Policy applies only to computers that have more than 2 gigabytes (GB) of disk space. Which of the following should you configure to accomplish this goal?
   - **A.** Security filtering
   - **B.** WMI filtering
   - **C.** Loopback processing
   - **D.** Slow-link processing
2. A Group Policy named Alpha applies at the site level. A Group Policy named Beta is assigned link order 2 at the domain level. A Group Policy named Gamma is assigned link order 1 at the domain level. A Group Policy named Delta is assigned to the Research OU. A computer account is located in the Research OU. If the same setting is configured differently in the Alpha, Beta, Gamma, and Delta GPOs, which GPO's version of this setting will apply to the computer?
   - **A.** Alpha
   - **B.** Beta
   - **C.** Gamma
   - **D.** Delta
3. A Group Policy named Alpha applies at the site level. A Group Policy named Beta is assigned link order 2 at the domain level. A Group Policy named Gamma is assigned link order 1 at the domain level. A Group Policy named Delta is assigned to the Research OU. A computer account is located in the Research OU. GPO Gamma is configured with the No Override setting. If the same setting is configured differently in the Alpha, Beta, Gamma, and Delta GPOs, which GPO's version of this setting will apply to the computer?

A. Alpha

B. Beta

C. Gamma

D. Delta

4. A Group Policy named Alpha applies at the site level. A Group Policy named Beta is assigned link order 2 at the domain level. A Group Policy named Gamma is assigned link order 1 at the domain level. A Group Policy named Delta is assigned to the Research OU. A computer account is located in the Research OU. GPO Beta is configured with the No Override setting. OU Research is configured with the Block Inheritance setting. If the same setting is configured differently in GPOs Alpha, Beta, Gamma, and Delta, which GPO's version of this setting will apply to the computer?

   A. Alpha

   B. Beta

   C. Gamma

   D. Delta

5. You have a policy applied at the domain level that you don't want applied to five computers in your organization. Which of the following should you configure to accomplish this goal?

   A. Security filtering

   B. WMI filtering

   C. Loopback processing

   D. Slow-link processing

Practice exercises

The goal of this section is to provide you with hands-on practice with the following:

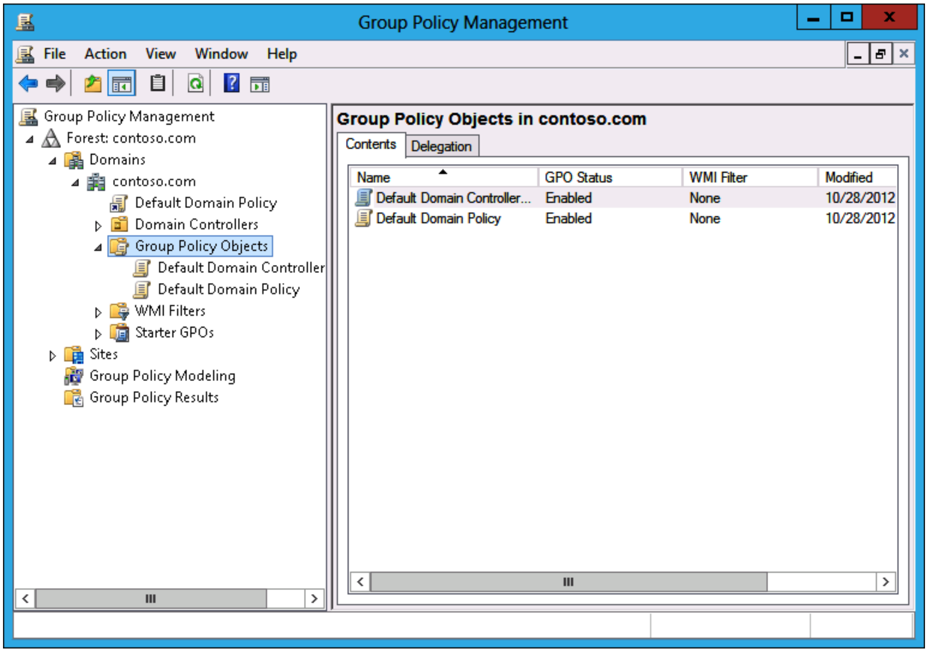
- Creating, backing up, and restoring GPOs
- Delegating GPO permissions
- Enabling loopback processing
- Configuring blocking and enforcement
- Configuring GPO security filtering

To perform the exercises in this section, you need access to the virtual machines you created by following the instructions in the Appendix. You should ensure that you have a snapshot of the virtual machines in their unaltered configuration so that you can revert to this snapshot after you have completed these exercises.

EXERCISE 1 Prepare GPOs, security groups, and OUs

In this exercise, you will prepare GPOs. To complete this exercise, perform the following steps:

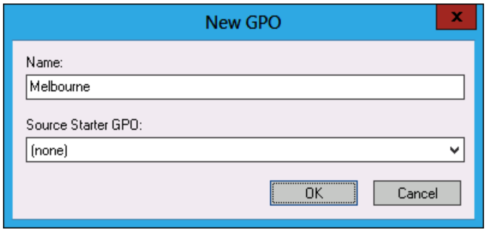
1. Sign in to DC with the Contoso\Administrator account.
2. In Server Manager, click the Tools menu and click Group Policy Management.
3. Expand the Forest: contoso.com\Domains\Contoso.com node and click Group Policy Objects, as shown in Figure 5-20.



Name	GPO Status	WMI Filter	Modified
Default Domain Controller...	Enabled	None	10/28/2012
Default Domain Policy	Enabled	None	10/28/2012

FIGURE 5-20 Clicking Group Policy Objects

4. In the Action menu, click New.
5. In the New GPO dialog box, type **Melbourne**, as shown in Figure 5-21, and click OK.



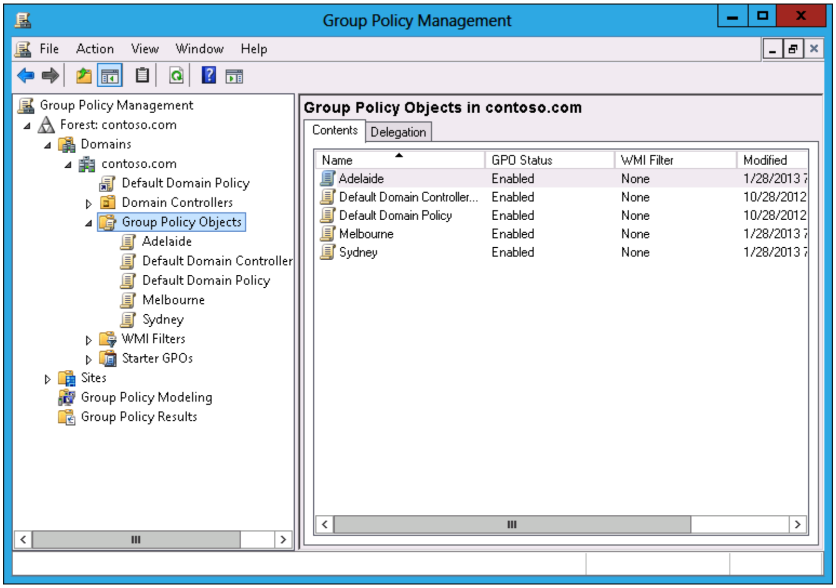
Name: Melbourne

Source Starter GPO: (none)

FIGURE 5-21 New GPO dialog box

6. Repeat steps 4 and 5 to create new GPOs named Sydney and Adelaide.

7. Verify that there are five GPOs listed, as shown in Figure 5-22.



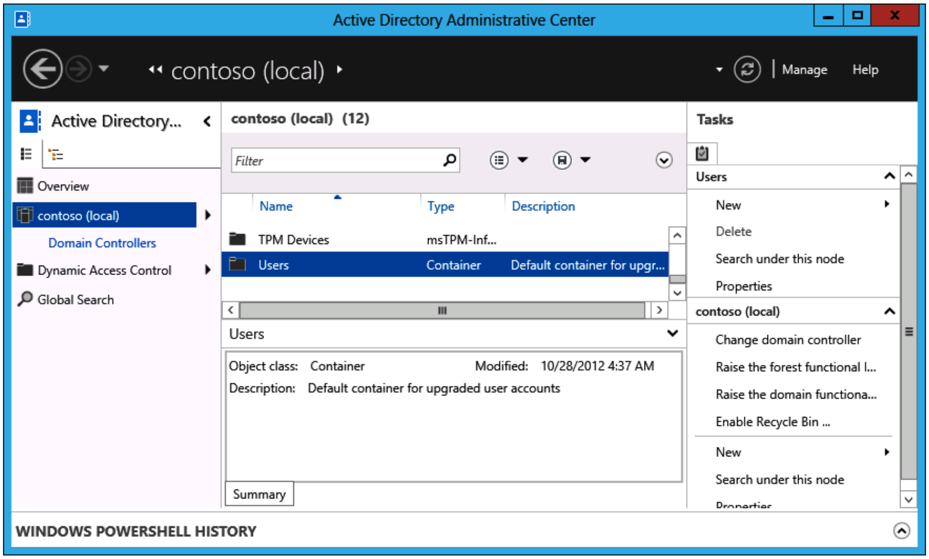
Group Policy Objects in contoso.com

Name	GPO Status	WMI Filter	Modified
Adelaide	Enabled	None	1/28/2013 7
Default Domain Controller...	Enabled	None	10/28/2012
Default Domain Policy	Enabled	None	10/28/2012
Melbourne	Enabled	None	1/28/2013 7
Sydney	Enabled	None	1/28/2013 7

FIGURE 5-22 Three new GPOs

8. In Server Manager, click Active Directory Administrative Center.

9. In Active Directory Administrative Center, click Contoso (Local) and then click Users, as shown in Figure 5-23.



contoso (local) (12)

Name	Type	Description
TPM Devices	msTPM-Inf...	
Users	Container	Default container for upgr...

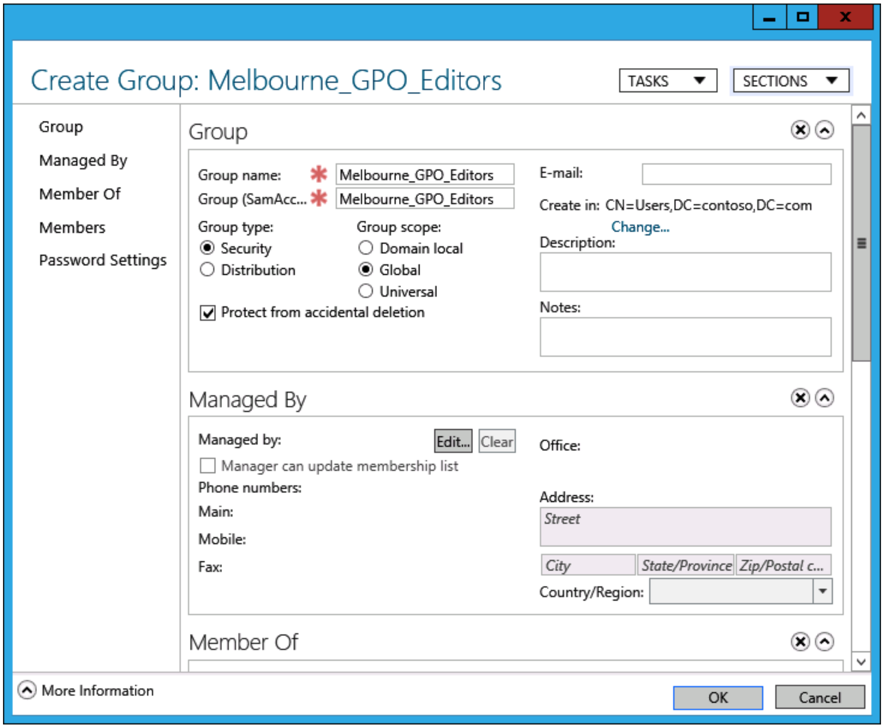
Users

Object class: Container Modified: 10/28/2012 4:37 AM
Description: Default container for upgraded user accounts

FIGURE 5-23 Users container

10. In the Tasks pane, click New and click Group.

11. In the Create Group dialog box, enter the group name **Melbourne_GPO_Editors**; click Security, Global, and Protect From Accidental Deletion, as shown in Figure 5-24; then click OK.



Create Group: Melbourne_GPO_Editors

Group

Group name: * Melbourne_GPO_Editors

Group (SamAcc... * Melbourne_GPO_Editors

E-mail:

Create in: CN=Users,DC=contoso,DC=com

Group type:
● Security
○ Distribution

Group scope:
○ Domain local
● Global
○ Universal

☑ Protect from accidental deletion

Description:

Notes:

Managed By

Managed by:

□ Manager can update membership list

Phone numbers:
Main:
Mobile:
Fax:

Office:

Address:
Street
City
State/Province
Zip/Postal c...
Country/Region:

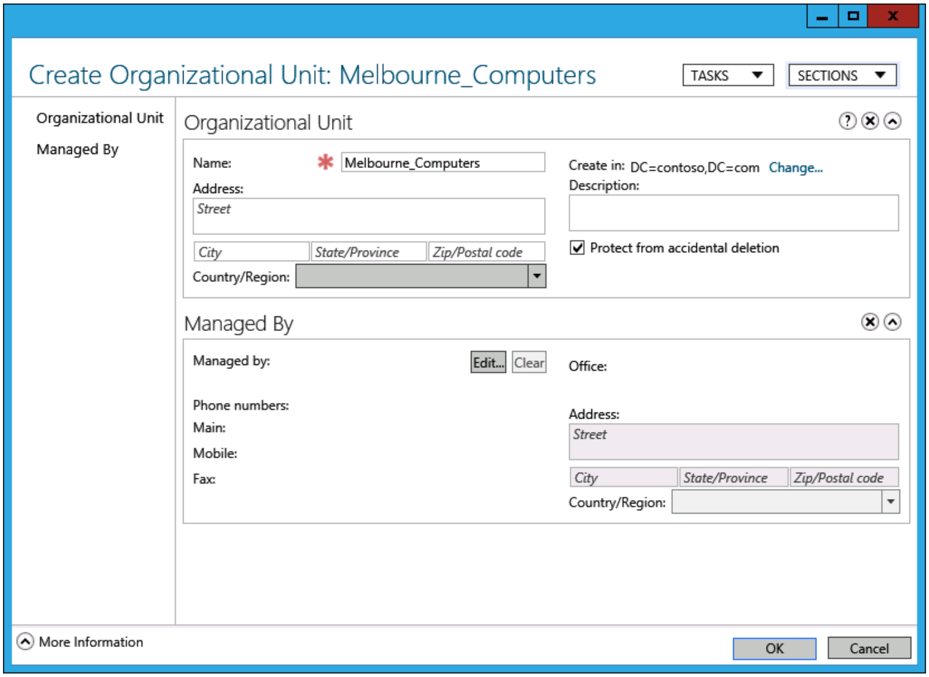
Member Of

FIGURE 5-24 Creating a security group

12. Repeat steps 10 and 11 to create the Adelaide_Computers security group.

13. In the Active Directory Administrative Center, in the Tasks pane, under Contoso (Local), click New and then click Organizational Unit.

14. In the Create Organizational Unit dialog box, enter the name **Melbourne_Computers**, as shown in Figure 5-25, and click OK.



Create Organizational Unit: Melbourne_Computers

Organizational Unit

Name: * Melbourne_Computers

Create in: DC=contoso,DC=com Change...

☑ Protect from accidental deletion

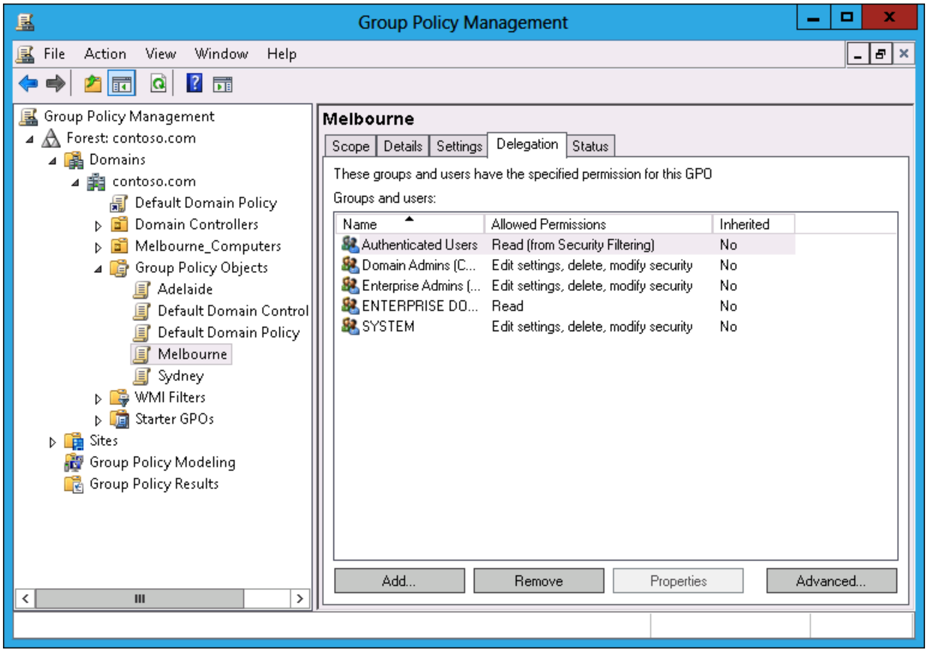
FIGURE 5-25 Create Organizational Unit dialog box

15. Close the Active Directory Administrative Center.
16. On the taskbar, click File Manager.
17. In File Manager, click Computer and then double-click Local Disk (C:) .
18. On the title bar of the Local Disk (C:) window, click the New Folder icon.
19. Name the new folder **GPO_Backup**.
20. Close the Local Disk (C:) window.

EXERCISE 2 Manage GPOs

In this exercise, you will perform several Group Policy management-related tasks. To complete this exercise, perform the following steps:

1. In the GPMC, click the Melbourne GPO.
2. When the Melbourne GPO is selected, click the Delegation tab, as shown in Figure 5-26.



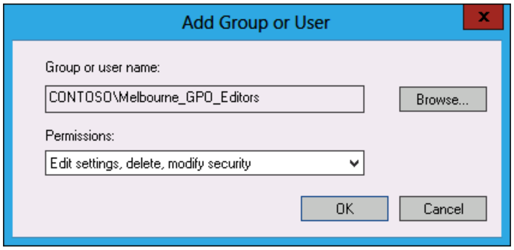
These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (C...	Edit settings, delete, modify security	No
Enterprise Admins (...	Edit settings, delete, modify security	No
ENTERPRISE DO...	Read	No
SYSTEM	Edit settings, delete, modify security	No

FIGURE 5-26 OU Delegation tab

3. On the Delegation tab, click Add.
4. In the Select User, Computer, Or Group dialog box, type **Melbourne_GPO_Editors**, click Check Names, and click OK.
5. In the Add Group Or User dialog box, use the drop-down menu to select Edit Settings, Delete, Modify Security, as shown in Figure 5-27, and click OK.

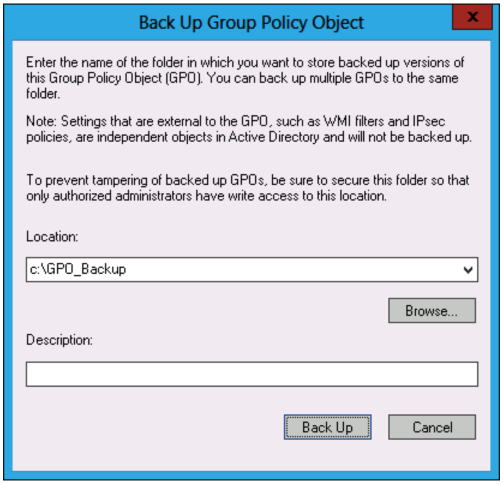


Group or user name: CONTOSO\Melbourne_GPO_Editors

Permissions: Edit settings, delete, modify security

FIGURE 5-27 OU Delegation tab

6. In the GPMC, click the Sydney GPO.
7. In the Action menu, click Back Up.
8. In the Back Up Group Policy Object dialog box, type **C:\GPO_Backup** as the location, as shown in Figure 5-28, and click Back Up.



Back Up Group Policy Object

Enter the name of the folder in which you want to store backed up versions of this Group Policy Object (GPO). You can back up multiple GPOs to the same folder.

Note: Settings that are external to the GPO, such as WMI filters and IPsec policies, are independent objects in Active Directory and will not be backed up.

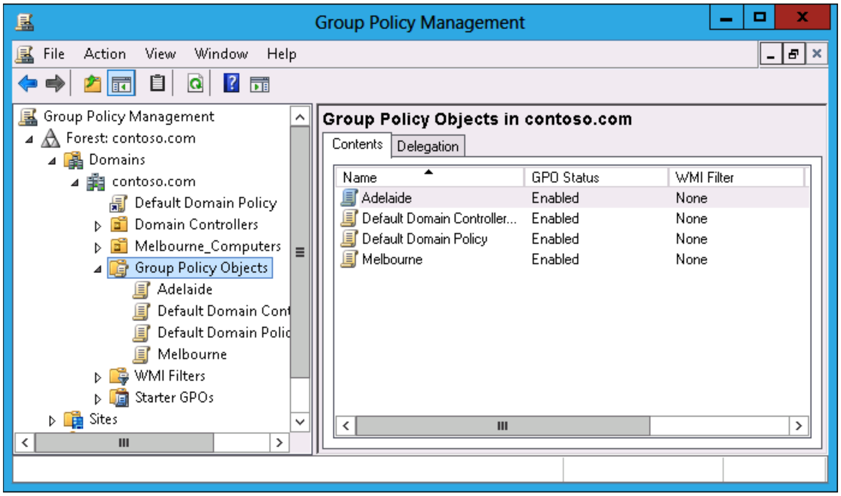
To prevent tampering of backed up GPOs, be sure to secure this folder so that only authorized administrators have write access to this location.

Location: c:\GPO_Backup

Description:

FIGURE 5-28 Back Up Group Policy Object dialog box

9. In the Backup dialog box, click OK.
10. In the GPMC, click the Sydney GPO.
11. In the Action menu, click Delete.
12. In the Group Policy Management dialog box, click Yes.
13. Verify that the Sydney GPO is no longer listed under Group Policy Objects, as shown in Figure 5-29.



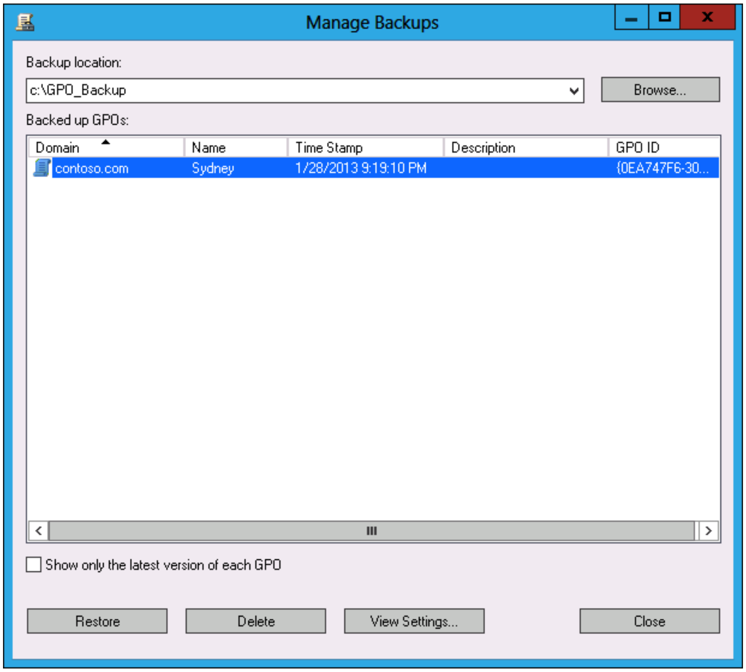
Group Policy Objects in contoso.com

Name	GPO Status	WMI Filter
Adelaide	Enabled	None
Default Domain Controller...	Enabled	None
Default Domain Policy	Enabled	None
Melbourne	Enabled	None

FIGURE 5-29 Verify deleted GPO

14. Click Group Policy Objects. In the Action menu, click Manage Backups.

15. In the Manage Backups dialog box, click the Sydney GPO, as shown in Figure 5-30, and click Restore.



Backup location: c:\GPO_Backup

Backed up GPOs:

Domain	Name	Time Stamp	Description	GPO ID
contoso.com	Sydney	1/28/2013 9:19:10 PM		{0EA747F6-30...

☐ Show only the latest version of each GPO

FIGURE 5-30 Manage Backups dialog box

16. In the Group Policy Management dialog box, click OK.

17. In the Restore dialog box, click OK.

18. In the Manage Backups dialog box, click Close.

19. Verify the presence of the Sydney GPO in the list of Group Policy Objects.

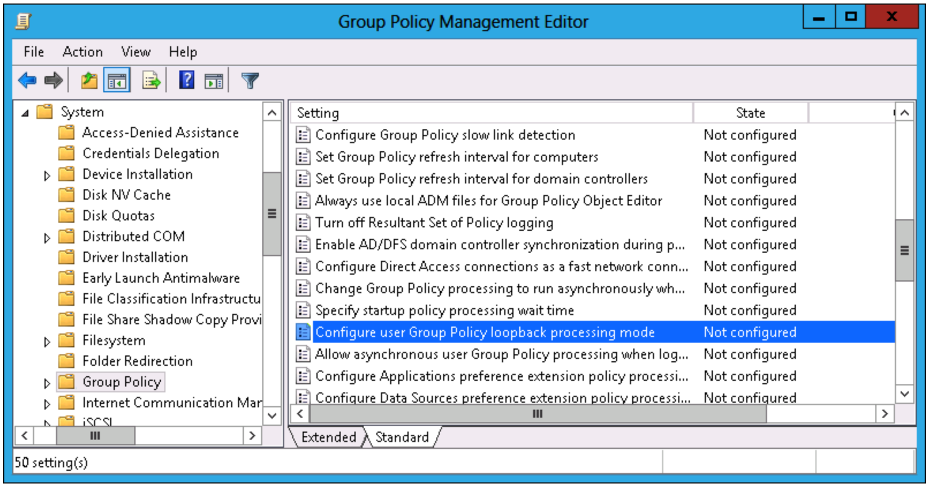
EXERCISE 3 Manage Group Policy processing

In this exercise, you will perform Group Policy management tasks related to Group Policy processing. To complete this exercise, perform the following steps:

1. In the GPMC, click the Adelaide GPO.

2. In the Action menu, click Edit.

3. In the Group Policy Management Editor, expand the Computer Configuration\Administrative Templates\System\Group Policy node and select the Configure User Group Policy loopback processing mode policy, as shown in Figure 5-31.



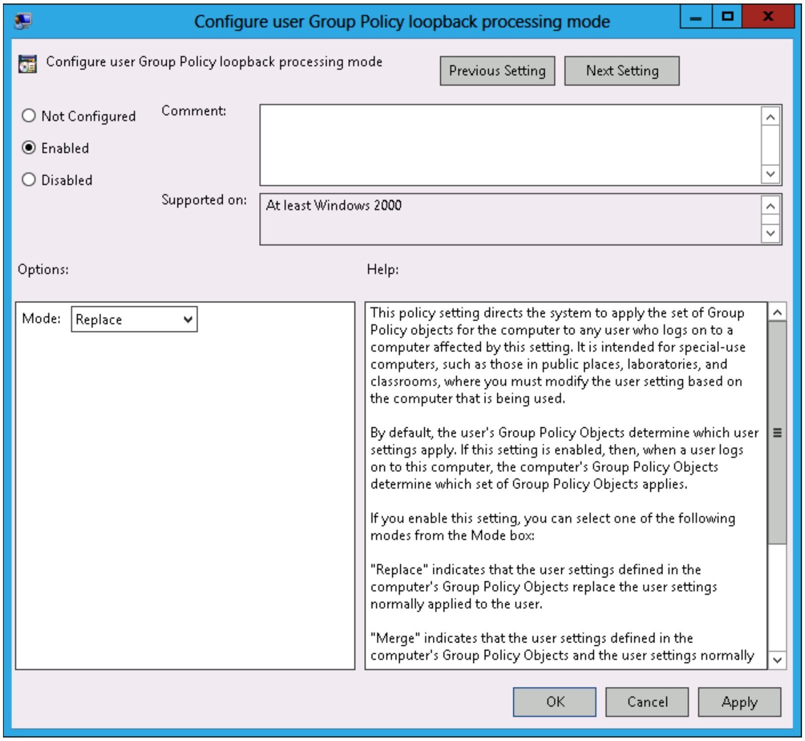
Setting	State
Configure Group Policy slow link detection	Not configured
Set Group Policy refresh interval for computers	Not configured
Set Group Policy refresh interval for domain controllers	Not configured
Always use local ADM files for Group Policy Object Editor	Not configured
Turn off Resultant Set of Policy logging	Not configured
Enable AD/DFS domain controller synchronization during p...	Not configured
Configure Direct Access connections as a fast network conn...	Not configured
Change Group Policy processing to run asynchronously wh...	Not configured
Specify startup policy processing wait time	Not configured
Configure user Group Policy loopback processing mode	Not configured
Allow asynchronous user Group Policy processing when log...	Not configured
Configure Applications preference extension policy processi...	Not configured
Configure Data Sources preference extension policy processi...	Not configured

50 setting(s)

FIGURE 5-31 Select Group Policy loopback processing mode policy

4. In the Action menu, click Edit.

5. In the Configure User Group Policy Loopback Processing Mode dialog box, click Enabled. Set the mode to Replace, as shown in Figure 5-32, and click OK.



Configure user Group Policy loopback processing mode

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 2000

Options:

Mode: Replace

Help:

This policy setting directs the system to apply the set of Group Policy objects for the computer to any user who logs on to a computer affected by this setting. It is intended for special-use computers, such as those in public places, laboratories, and classrooms, where you must modify the user setting based on the computer that is being used.

By default, the user's Group Policy Objects determine which user settings apply. If this setting is enabled, then, when a user logs on to this computer, the computer's Group Policy Objects determine which set of Group Policy Objects applies.

If you enable this setting, you can select one of the following modes from the Mode box:

"Replace" indicates that the user settings defined in the computer's Group Policy Objects replace the user settings normally applied to the user.

"Merge" indicates that the user settings defined in the computer's Group Policy Objects and the user settings normally

FIGURE 5-32 Configure replace mode

6. Close the Group Policy Management Editor.

7. In the GPMC, click the Adelaide GPO and click the Scope tab.

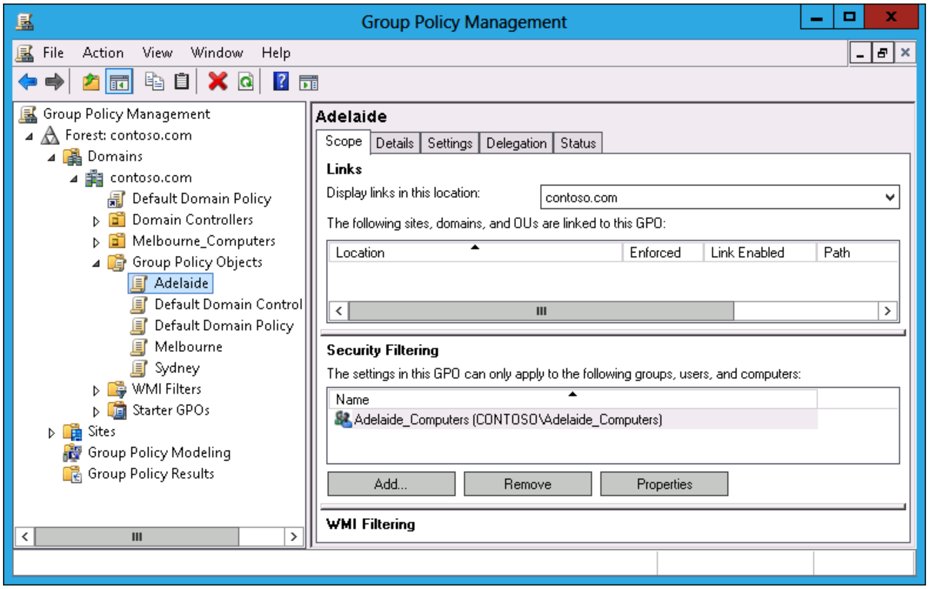
8. On the Scope tab, click the Authenticated Users group and click Remove.

9. In the Group Policy Management dialog box, click OK.

10. Under Security Filtering, click Add.

11. In the Select User, Computer, Or Group dialog box, type **Adelaide_Computers**, click Check Names, and click OK.

12. Verify that the security filtering properties of the Adelaide GPO match those in Figure 5-33.



Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

The settings in this GPO can only apply to the following groups, users, and computers:

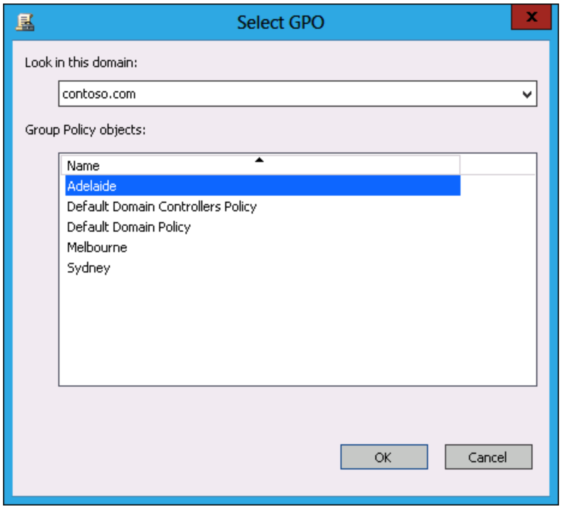
Adelaide_Computers (CONTOSO\Adelaide_Computers)

FIGURE 5-33 Configuring security filtering properties

13. In the GPMC, click Contoso.com and click the Linked Group Policy Objects tab.

14. Click contoso.com. In the Action menu, click Link An Existing GPO.

15. In the Select GPO dialog box, click Adelaide, as shown in Figure 5-34, and click OK.



Look in this domain:

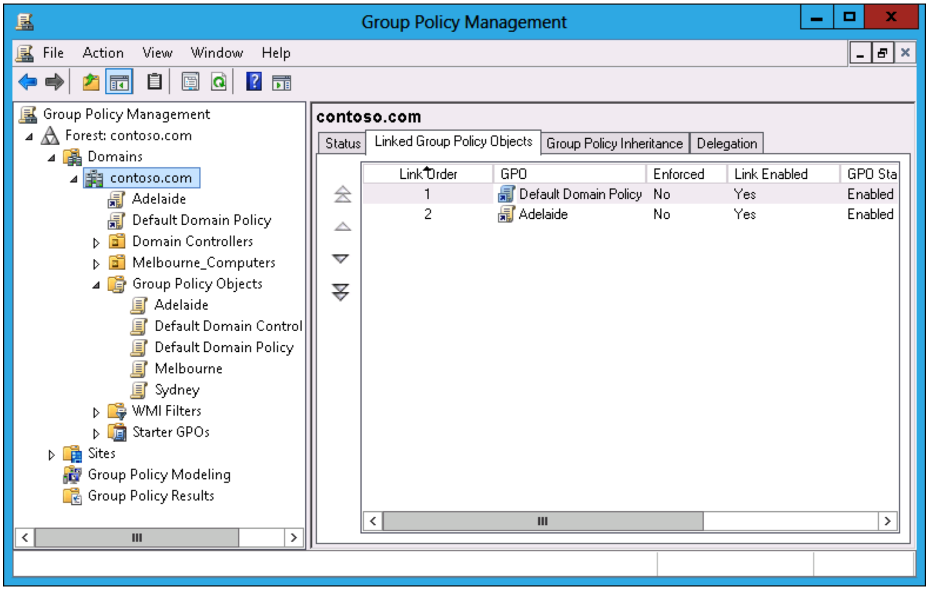
contoso.com

Group Policy objects:

Name
Adelaide
Default Domain Controllers Policy
Default Domain Policy
Melbourne
Sydney

FIGURE 5-34 Selecting the GPO to link

16. In the GPMC, verify that the Adelaide GPO and the Default Domain Policy GPO are linked to the domain, as shown in Figure 5-35.



- Group Policy Management
  - Forest: contoso.com
    - Domains
      - contoso.com
        - Adelaide
        - Default Domain Policy
        - Domain Controllers
        - Melbourne_Computers
        - Group Policy Objects
          - Adelaide
          - Default Domain Control
          - Default Domain Policy
          - Melbourne
          - Sydney
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

contoso.com

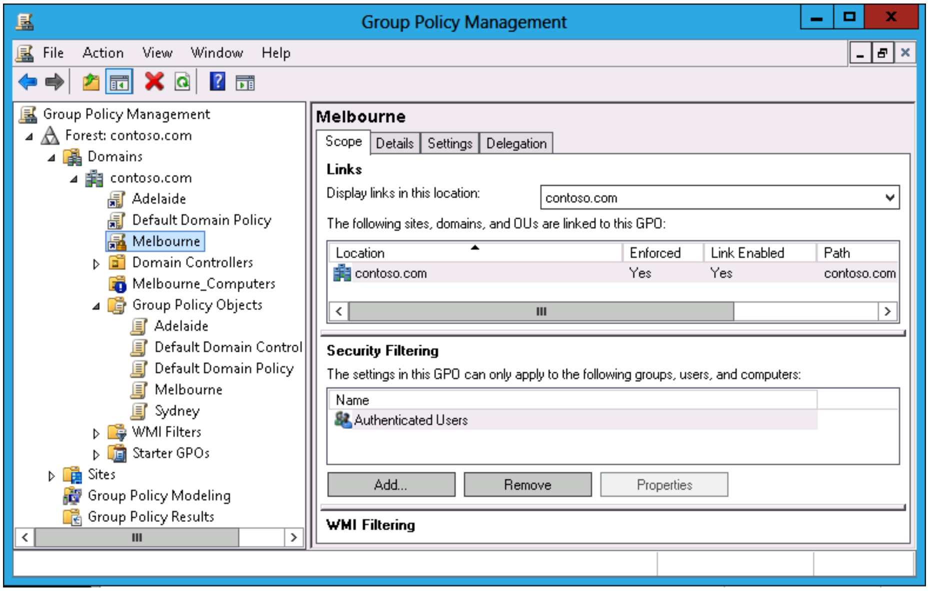
Link Order	GPO	Enforced	Link Enabled	GPO Sta
1	Default Domain Policy	No	Yes	Enabled
2	Adelaide	No	Yes	Enabled

FIGURE 5-35 GPOs linked to the domain

EXERCISE 4 Group Policy Inheritance and Enforcement

In this exercise, you will perform Group Policy management tasks related to Group Policy processing. To complete this exercise, perform the following steps:

1. In the GPMC, click the Melbourne_Computers OU.
2. In the Action menu, click Block Inheritance.
3. In the GPMC, click contoso.com.
4. In the Action menu, click Link An Existing GPO.
5. In the Select GPO dialog box, click Melbourne and then click OK.
6. Click the Melbourne GPO under contoso.com.
7. In the Action menu, click Enforced.
8. Verify that the GPMC shows the Melbourne policy as Enforced and the Melbourne_Computers OU set to Block Inheritance, as shown in Figure 5-36.



Links

Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
contoso.com	Yes	Yes	contoso.com

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

FIGURE 5-36 Block Inheritance and Enforced GPOs

9. In the GPMC, click the Group Policy Modeling node.

10. In the Action menu, click Group Policy Modeling Wizard.

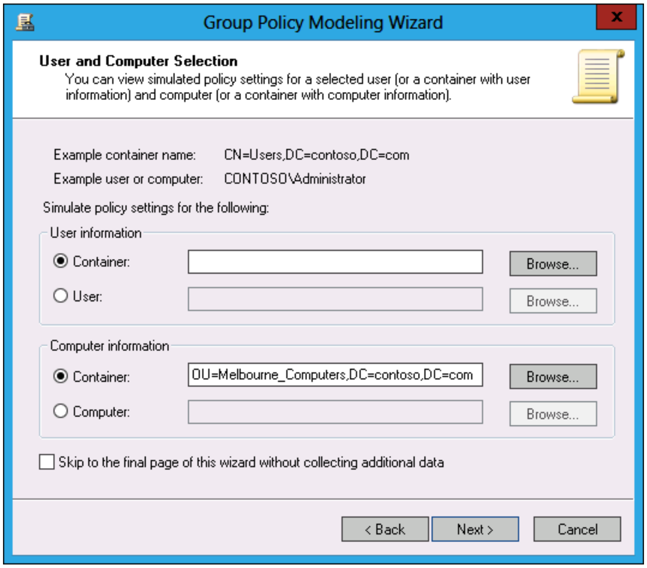
11. In the Welcome page of the Group Policy Modeling Wizard, click Next.

12. In the Domain Controller Selection page, click This Domain Controller and click DC.contoso.com. Click Next.

13. In the User And Computer Selection page, click Browse next to Container in the Computer Information section.

14. In the Choose Computer Container dialog box, click Melbourne_Computers and click OK.

15. Verify that the User And Computer Selection page matches Figure 5-37 and click Next.



Group Policy Modeling Wizard

User and Computer Selection
You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=contoso,DC=com
Example user or computer: CONTOSO\Administrator

Simulate policy settings for the following:

User information
● Container: [ ] Browse...
○ User: [ ] Browse...

Computer information
● Container: OU=Melbourne_Computers,DC=contoso,DC=com Browse...
○ Computer: [ ] Browse...

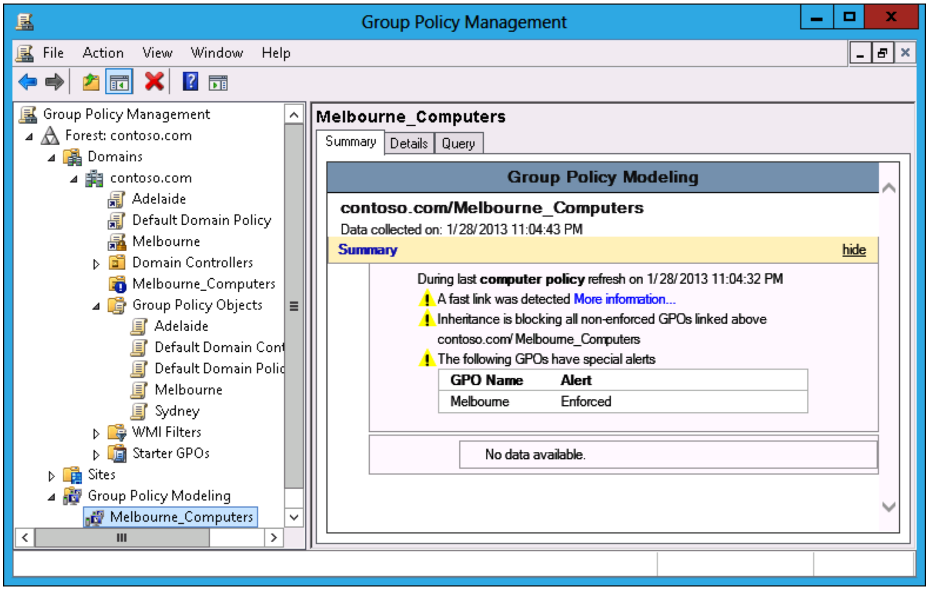
□ Skip to the final page of this wizard without collecting additional data

FIGURE 5-37 Group Policy Modeling Wizard

16. In the Summary Of Selections page, click Next and then click Finish.

17. In the Warning dialog box, click OK.

18. Verify that the report for the Melbourne_Computers OU matches Figure 5-38 and that only the Melbourne GPO is listed.



contoso.com/Melbourne_Computers

Data collected on: 1/28/2013 11:04:43 PM

Summary hide

During last **computer policy** refresh on 1/28/2013 11:04:32 PM

⚠ A fast link was detected More information...

⚠ Inheritance is blocking all non-enforced GPOs linked above contoso.com/Melbourne_Computers

⚠ The following GPOs have special alerts

GPO Name	Alert
Melbourne	Enforced

No data available.

FIGURE 5-38 Group Policy Modeling results

Suggested practice exercises

The following additional practice exercises are designed to give you more opportunities to practice what you've learned and to help you successfully master the lessons presented in this chapter.

- **Exercise 1** Configure GPO settings in the Melbourne GPO. Import these settings into the Sydney GPO.
- **Exercise 2** Configure the Melbourne GPO so that it will not apply to members of the Adelaide_Computers group.

Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct answer: B**
   - A. **Incorrect:** You use the Backup-GPO cmdlet to back up an existing GPO.
   - B. **Correct:** You use the Import-GPO cmdlet to import settings from a backed-up GPO to an existing target GPO.
   - C. **Incorrect:** You use the Restore-GPO cmdlet to restore a backed-up GPO to a previous state.
   - D. **Incorrect:** You use the Copy-GPO cmdlet to create a copy of an existing GPO.
2. **Correct answer: B**
   - A. **Incorrect:** You use the Copy-GPO cmdlet to create a copy of an existing GPO.
   - B. **Correct:** You use the Restore-GPO cmdlet to restore a backed-up GPO to a previous state.
   - C. **Incorrect:** You use the Import-GPO cmdlet to import settings from a backed-up GPO to an existing target GPO. Although it would import the settings from the backed-up GPO, it is possible that other settings not included in the original backed-up GPO were configured by your assistant.
   - D. **Incorrect:** You use the Backup-GPO cmdlet to back up an existing GPO.
3. **Correct answer: C**
   - A. **Incorrect:** You use the Active Directory Sites And Services console to manage Active Directory sites. You can't use this console to configure GPO migration settings.
   - B. **Incorrect:** You use this console to manage Active Directory security principals and containers. You can't use this console to configure GPO migration settings.
   - C. **Correct:** You use this tool to configure the migration table, which is necessary when migrating objects from one domain or forest to another.
   - D. **Incorrect:** You use this to edit GPOs. You can't use this console to configure GPO migration settings.

4. **Correct answers: A, B, and C**
   - **A. Correct:** Members of the Group Policy Creator Owners group can create GPOs by default.
   - **B. Correct:** Members of the Enterprise Admins group can create GPOs by default.
   - **C. Correct:** Members of the Domain Admins group can create GPOs by default.
   - **D. Incorrect:** The Domain Controllers group is a group for the accounts of domain controllers. It does not grant any permissions on GPOs.

5. **Correct answer: D**
   - **A. Incorrect:** You use the Copy-GPO cmdlet to create a copy of an existing GPO. It does not allow you to revert the default domain GPO to its original state.
   - **B. Incorrect:** You use the Restore-GPO cmdlet to restore a backed-up GPO to a previous state. You need to create the backup first.
   - **C. Incorrect:** You use the Import-GPO cmdlet to import settings from a backed-up GPO to an existing target GPO.
   - **D. Correct:** You use the Backup-GPO cmdlet to back up an existing GPO.

Lesson 2

1. **Correct answer: B**
   - **A. Incorrect:** You use Security Filtering to filter GPO application based on security group membership.
   - **B. Correct:** You can use a WMI query to filter GPO application based on the properties of a target computer, such as how much disk space it has available.
   - **C. Incorrect:** You use loopback processing to enforce settings that apply to the computer account rather than the user account.
   - **D. Incorrect:** You use slow-link processing to configure Group Policy not to apply across low-bandwidth connections.

2. **Correct answer: D**
   - **A. Incorrect:** In this scenario, GPO Delta has precedence over the other GPOs.
   - **B. Incorrect:** In this scenario, GPO Delta has precedence over the other GPOs.
   - **C. Incorrect:** In this scenario, GPO Delta has precedence over the other GPOs.
   - **D. Correct:** In this scenario, GPO Delta has precedence over the other GPOs.

3. **Correct answer: C**

   A. **Incorrect:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.

   B. **Incorrect:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.

   C. **Correct:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.

   D. **Incorrect:** In this scenario, the No Override setting on GPO Gamma means that it has precedence.

4. **Correct answer: B**

   A. **Incorrect:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.

   B. **Correct:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.

   C. **Incorrect:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.

   D. **Incorrect:** No Override settings override Block Inheritance, so the setting in GPO Beta applies to the computer.

5. **Correct answer: A**

   A. **Correct:** You use Security Filtering to filter GPO application based on security group membership. In this case, you configure the Apply Group Policy (Deny) advanced permission.

   B. **Incorrect:** You can use a WMI query to filter GPO application based on the properties of a target computer, such as how much disk space it has available.

   C. **Incorrect:** You use loopback processing to enforce settings that apply to the computer account rather than the user account.

   D. **Incorrect:** You use slow-link processing to configure Group Policy not to apply across low-bandwidth connections.

CHAPTER 10

Monitoring and auditing Windows Server 2012

Properly monitoring servers is a critical component in administering them. If you monitor servers correctly, you'll know well in advance if the server is under resource pressure from lack of disk space, RAM, or processor resources. You'll be able to deal with those issues before they start to affect the people that use the servers on a day-to-day basis. Auditing servers enables you to track object access and configuration changes, from modifications to security settings to users who are accessing a particularly sensitive spreadsheet.

In this chapter, you will learn how to monitor and configure auditing for computers running the Windows Server 2012 operating system.

Lessons in this chapter:

- Lesson 1: Monitor servers
- Lesson 2: Configure advanced audit policies

Before you begin

To complete the practice exercises in this chapter, you need to have deployed computers DC, SYD-A, and SYD-B, as described in the Appendix, using the evaluation edition of Windows Server 2012.

Lesson 1: Monitor servers

Unwatched servers, like unwatched children, invariably end up in a chaotic state. Monitoring a server using data collector sets, alerts, and events enables you to keep an eye on the server's performance and configuration. Although effective monitoring is unlikely to stop a server from ever experiencing problems, it often provides warning signs about developing problems, giving you a chance to resolve them before they cause a service disruption. In this lesson, you will learn how to configure data collector sets, manage alerts, monitor events, and perform network monitoring.

After this lesson, you will be able to:

- Configure data collector sets.
- Manage alerts.
- Monitor events.
- Configure event subscriptions.
- Perform network monitoring.

Estimated lesson time: 45 minutes

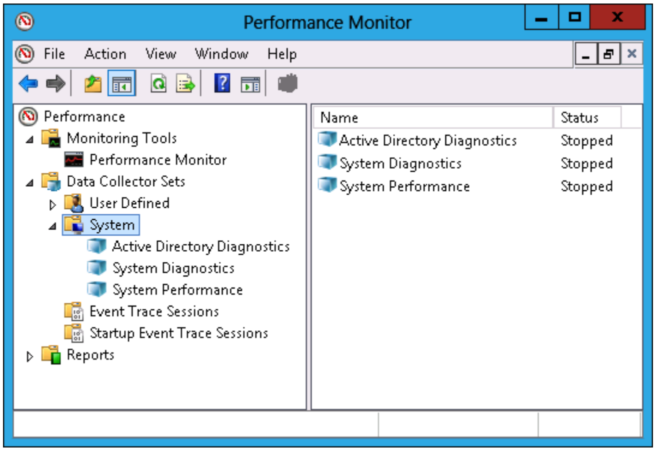
Data collector sets

Data collector sets enable you to collect performance data, system configuration information, and statistics into a single file. You can use Performance Monitor or other third-party tools to analyze this information to make a determination about how well a server is functioning against an assigned workload.

You can configure data collector sets to include the following:

- **Performance counter data** The data collector set not only includes specific performance counters but also the data generated by those counters.
- **Event trace data** Enables you to track events and system activities. Event trace data can be useful when troubleshooting misbehaving applications or services.
- **System configuration information** Enables you to track the state of registry keys and record any modifications made to those keys.

Windows Server 2012 includes the following built-in data collector sets, as shown in Figure 10-1.



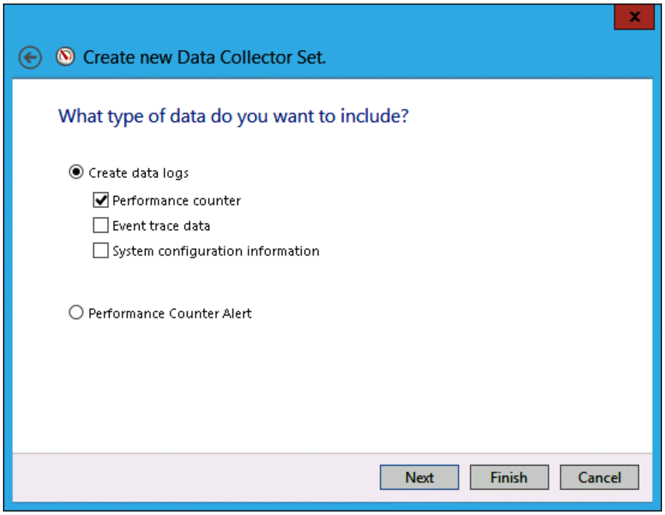
Name	Status
Active Directory Diagnostics	Stopped
System Diagnostics	Stopped
System Performance	Stopped

FIGURE 10-1 Built-in data collector sets

- **Active Directory Diagnostics** Available if you have installed the computer as a domain controller; it provides data on Active Directory health and reliability.
- **System Diagnostics** Enables you to troubleshoot problems with hardware, drivers, and STOP errors.
- **System Performance** Enables you to diagnose problems with sluggish system performance. You can determine which processes, services, or hardware may be causing performance bottlenecks.

To create a data collector set, perform the following steps:

1. Open Performance Monitor from the Tools menu of the Server Manager console.
2. Expand Data Collector Sets.
3. Click User Defined. On the Action menu, click New and click Data Collector Set.
4. You are given the option of creating the data collector set from a template, which enables you to select from an existing data collector set, or to create a data collector set manually. If you choose to create a data collector set manually, you have the option of creating a data log, which can include a performance counter, event trace data, and system configuration information; or a performance counter alert. This choice is shown in Figure 10-2.



Create new Data Collector Set.

What type of data do you want to include?

● Create data logs

☑ Performance counter

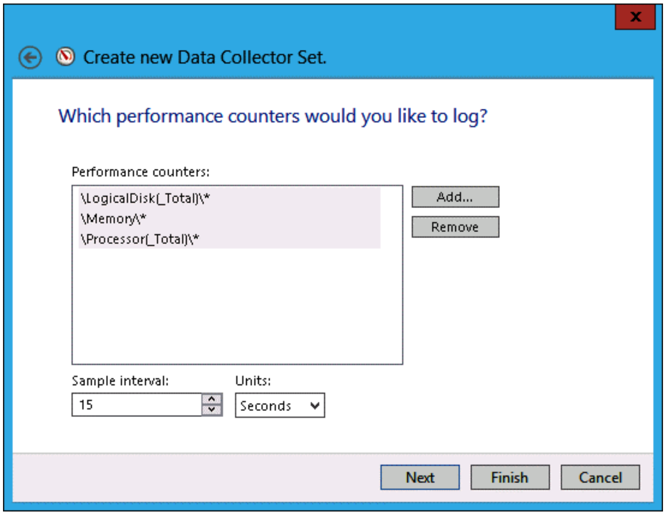
□ Event trace data

□ System configuration information

○ Performance Counter Alert

FIGURE 10-2 Creating a new data collector set

5. If you select Performance Counter, you then choose which performance counters to add to the data collector set. You also specify how often Windows should collect data from the performance counters. Figure 10-3 shows data being collected once every 15 seconds.


Create new Data Collector Set.

Which performance counters would you like to log?

Performance counters:

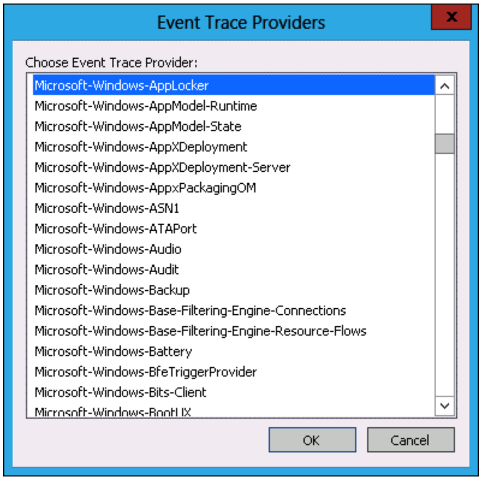
\LogicalDisk(_Total)*
\Memory*
\Processor(_Total)*

Sample interval: 15

Units: Seconds

FIGURE 10-3 Setting an interval for the data collector set

6. If you choose to include event trace data, you need to enable event trace providers. As Figure 10-4, shows, a large number of event trace providers are available with Windows Server 2012. You use event trace providers when troubleshooting a specific problem. For example, the Microsoft Windows-AppLocker event trace provider helps you diagnose and troubleshoot issues related to AppLocker.

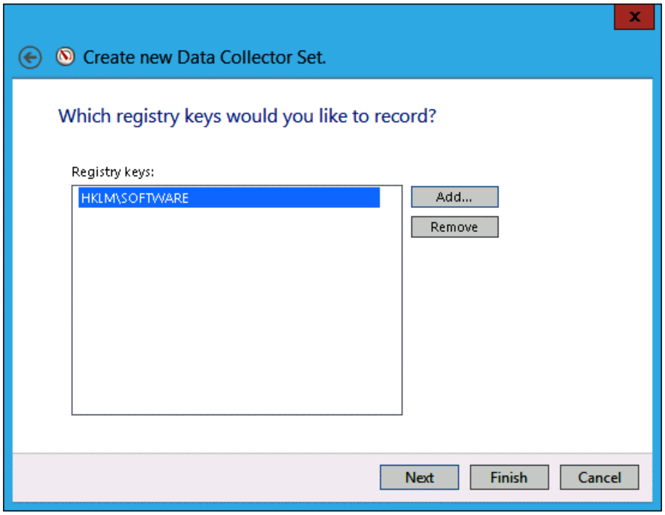

Event Trace Providers

Choose Event Trace Provider:

Microsoft-Windows-AppLocker
Microsoft-Windows-AppModel-Runtime
Microsoft-Windows-AppModel-State
Microsoft-Windows-AppXDeployment
Microsoft-Windows-AppXDeployment-Server
Microsoft-Windows-AppxPackagingOM
Microsoft-Windows-ASN1
Microsoft-Windows-ATAPort
Microsoft-Windows-Audio
Microsoft-Windows-Audit
Microsoft-Windows-Backup
Microsoft-Windows-Base-Filtering-Engine-Connections
Microsoft-Windows-Base-Filtering-Engine-Resource-Flows
Microsoft-Windows-Battery
Microsoft-Windows-BfeTriggerProvider
Microsoft-Windows-Bits-Client
Microsoft-Windows-BootUX

FIGURE 10-4 Event trace providers

7. If you choose to monitor system configuration information, you can select registry keys to monitor, as shown in Figure 10-5. Selecting a parent key enables you to monitor all registry changes that occur under that key while the data collector set is running.



Create new Data Collector Set.

Which registry keys would you like to record?

Registry keys:

HKLM\SOFTWARE

FIGURE 10-5 Setting registry keys to record

8. You then specify where you want data collected by the data collector set to be stored. The default location is the %systemdrive%\PerfLogs\Admin folder. If you intend to run the data collector set for an extended period of time, you should store the data on a volume separate from the one that hosts the operating system.

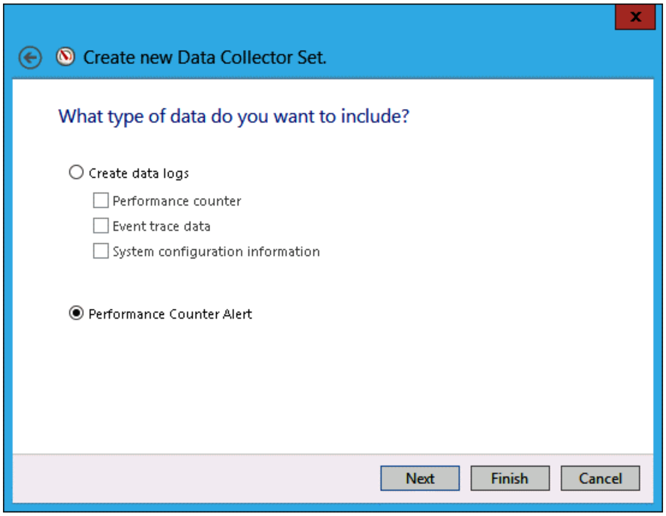
9. The final step in setting up a data collector set is to specify the account under which the data collector set runs. The default is Local System, but you can configure the data collector set to use any account for which you have the credentials.

MORE INFO **DATA COLLECTOR SETS**

For more information about data collector sets, consult the following TechNet link: ***http://technet.microsoft.com/en-us/library/cc749337.aspx*****.**

Alerts

Performance counter alerts enable you to configure a task to run when a performance counter, such as available disk space or memory, falls under or exceeds a specific value. To configure a performance counter alert, you create a new data collector set, choose the Create Manually option, and select the Performance Counter Alert option, as shown in Figure 10-6.



Create new Data Collector Set.

What type of data do you want to include?

○ Create data logs

□ Performance counter

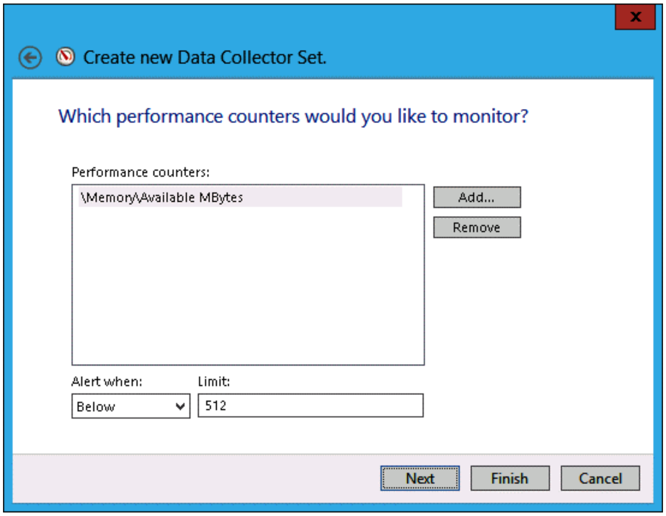
□ Event trace data

□ System configuration information

● Performance Counter Alert

FIGURE 10-6 Configuring the performance counter alert

You add the performance counter, threshold value, and whether the alert should be triggered if the value exceeds or falls below this value. Figure 10-7 shows an alert that is triggered when the amount of available memory falls below 512 megabytes.



Create new Data Collector Set.

Which performance counters would you like to monitor?

Performance counters:

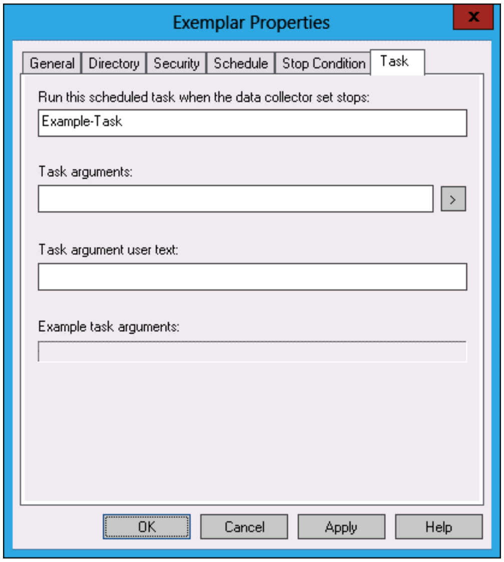
\Memory\Available MBytes

Alert when: Below

Limit: 512

FIGURE 10-7 Setting an alert threshold

When you create an alert, all it does when triggered is to add an event to the event log. You can also configure an alert to run a scheduled task when triggered. You do this by editing the properties of the alert and specifying the name of the scheduled task on the Task tab, as shown in Figure 10-8.



Run this scheduled task when the data collector set stops: Example-Task

Task arguments:

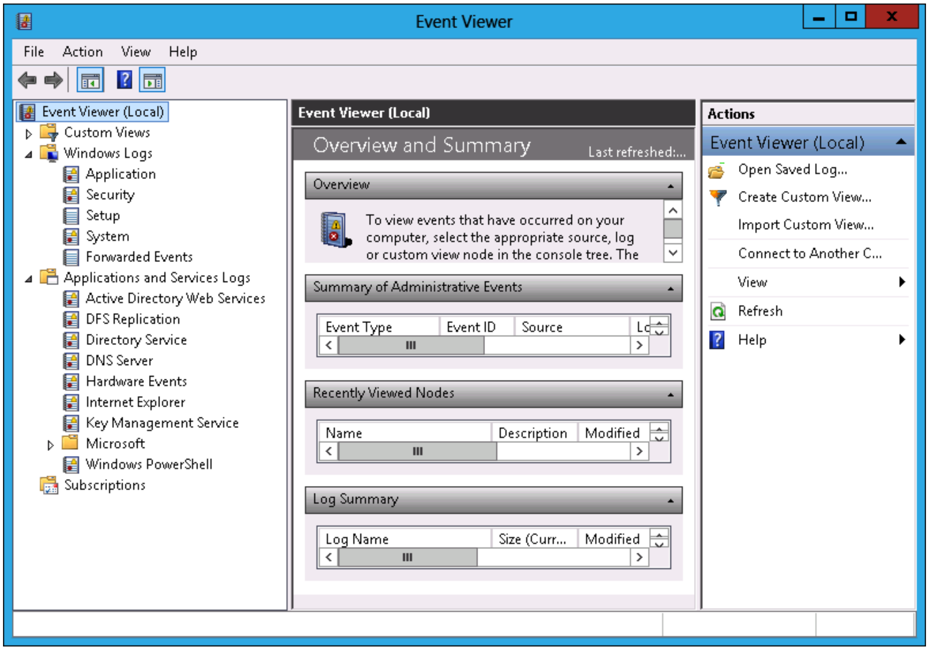
Task argument user text:

Example task arguments:

FIGURE 10-8 Running a scheduled task

Event Viewer

Event Viewer, shown in Figure 10-9, enables you to access recorded event information. The Windows Server 2012 Event Viewer differs from the Event Viewer in earlier versions of the Windows Server operating system, such as Windows Server 2003, in that it not only offers the application, security, setup and system logs but it also contains separate application and service Logs. These logs are designed to provide information on a per-role or per-application basis, rather than having all application and role service-related events funneled into the application log. When searching for events related to a specific role service, feature, or application, check to see whether that role service, feature, or application has its own application log.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The

FIGURE 10-9 Event Viewer

MORE INFO **EVENT VIEWER**

For more information about Event Viewer, consult the following TechNet link: ***http://technet.microsoft.com/en-us/library/cc766042.aspx*.**

Event log filters

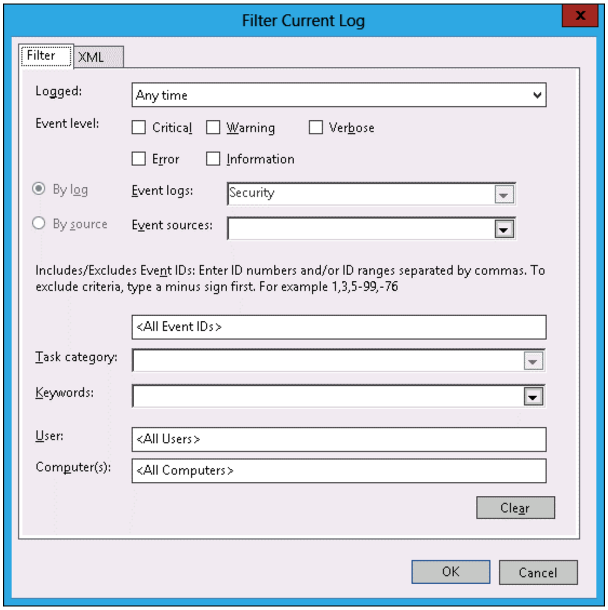
Filters and event logs enable you to view only those events that have specific characteristics. Filters apply only to the current Event Viewer session. If you constantly use a specific filter or set of filters to manage event logs, you should instead create a custom view. Filters apply only to a single event log. You can create filters on a log based on the following properties:

- **Logged** Enables you to specify the time range for the filter.
- **Event Level** Enables you to specify event levels. You can choose the following options: Critical, Warning, Verbose, Error, and Information.
- **Event Sources** Enables you to choose the source of the event.
- **Event IDs** Enables you to filter based on event ID. You can also exclude specific event IDs.
- **Keywords** Enables you to specify keywords based on the contents of events.

- **User** Enables you to limit events based on user.
- **Computer** Enables you to limit events based on the computer.

To create a filter, perform the following steps:

1. Open Event Viewer and select the log that you want to filter.
2. Determine the properties of the event that you want to filter.
3. On the Actions pane, click Filter Current Log.
4. In the Filter Current Log dialog box, shown in Figure 10-10, specify the filter properties.



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

FIGURE 10-10 Specifying filter properties

Event log views

Event log views enable you to create customized views of events across any event log stored on a server, including events in the forwarded event log. Rather than looking through each event log for specific items of interest, you can create event log views that target only those specific items. Event Viewer includes a custom view named Administrative Events. This view displays critical, warning, and error events from a variety of important event logs such as the application, security and system logs.

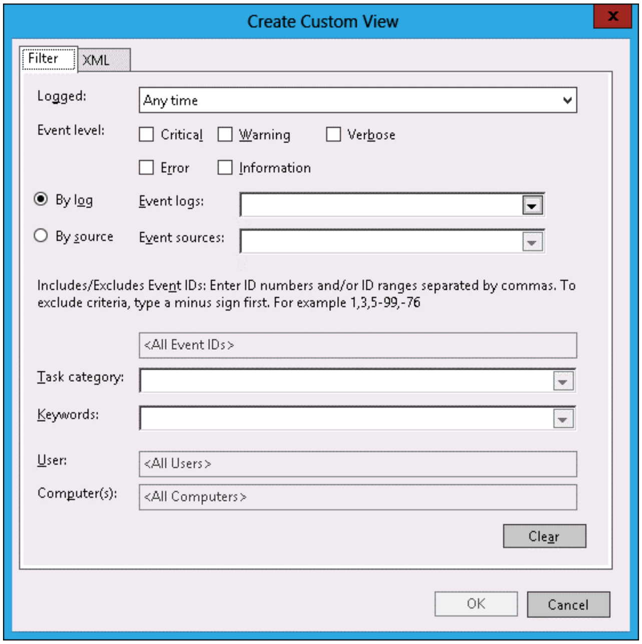
Views differ from filters in the following ways:

- **Persistent** You can use a view across multiple Event Viewer sessions. If you configure a filter on a log, it is not available the next time you open the Event Viewer.

- **Include multiple logs** A custom view can display events from separate logs. Filters are limited to displaying events from one log.
- **Exportable** You can import and export event log views between computers.

Creating an event log view is a similar process to creating a filter. The primary difference is that you can select events from multiple logs and you give the event log view a name and choose a place to save it. To create an event log view, perform the following steps:

1. Open Event Viewer.
2. Click the Custom Views node and then click Create Custom View from the Actions menu.
3. In the Create Custom View dialog box, shown in Figure 10-11, select the properties of the view, including:
   - When the events are logged
   - The event level
   - Which event log to draw events from
   - Event source
   - Task category
   - Keywords
   - User
   - Computer



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs:

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

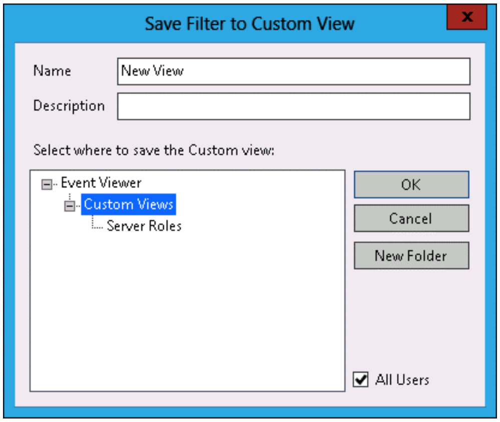
Keywords:

User: <All Users>

Computer(s): <All Computers>

FIGURE 10-11 Creating a custom view

4. In the Save Filter To Custom View dialog box, enter a name for the custom view and a location in which to save the view (see Figure 10-12). Click OK.



Name: New View

Description:

Select where to save the Custom view:

- Event Viewer
  - Custom Views
    - Server Roles

☑ All Users

FIGURE 10-12 Entering the custom view name

5. Verify that the new view is listed as its own separate node in the Event Viewer.

You can export a custom event log view by selecting the event log view and clicking Export Custom View. Exported views can be imported on other computers running Windows Server 2012.

MORE INFO **EVENT LOG VIEWS**

For more information about event log views, consult the following TechNet link: ***http://technet.microsoft.com/en-us/library/cc766522.aspx*****.**

Event subscriptions

Event log forwarding enables you to centralize the collection and management of events from multiple computers. Rather than having to examine the event log of each computer by making a remote connection to that computer, event log forwarding enables you to do one of the following:

- Configure a central computer to collect specific events from source computers. Use this option in environments in which you need to consolidate events from only a small number of computers.
- Configure source computers to forward specific events to a collector computer. Use this option when you have a large number of computers from which you want to consolidate events. You configure this method using Group Policy.

Event log forwarding enables you to configure the specific events that are forwarded to the central computer. This enables the computer to forward important events. It isn't necessary to forward all events from the source computer. If you discover something that warrants further investigation from the forwarded traffic, you can log on to the original source computer and view all the events from that computer in a normal manner.

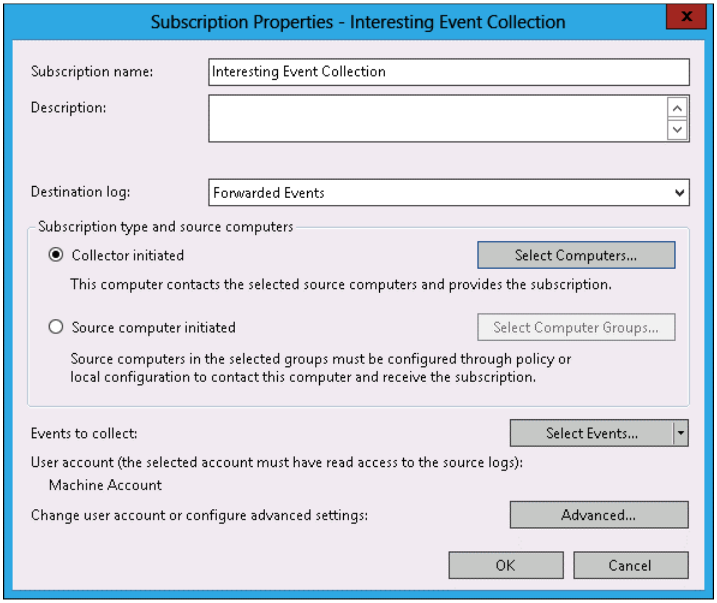
REAL WORLD **OPERATIONS MANAGER**

In large environments, you use Microsoft System Center 2012 Operations Manager as a way of monitoring large numbers of computers for important events instead of searching through the event log manually looking for events that require further investigation.

Event log forwarding uses Windows Remote Management (WinRM) and the Windows Event Collector (wecsvc). You need to enable these services on computers that function as event forwarders and event collectors. You configure WinRM using the winrm quickconfig command. You configure wecsvc using the wecutil qc command. If you want to configure subscriptions from the security event log, you need to add the computer account of the collector computer to the local Administrators group on the source computer.

To configure a collector-initiated event subscription, configure WinRM and Windows Event Collector on the source and collector computers. In the Event Viewer, configure the Subscription Properties dialog box, shown in Figure 10-13, with the following information:

- **Subscription Name** The name of the subscription.
- **Destination Log** The log where collected events will be stored.
- **Subscription Type And Source Computers: Collector Initiated** Use the Select Computers dialog box to add the computers that the collector will retrieve events from. The collector must be a member of the local Administrators group or the Event Log Readers group on each source computer, depending on whether access to the security log is required.
- **Events To Collect** Create a custom view to specify which events are retrieved from each of the source computers.



Subscription Properties - Interesting Event Collection

Subscription name: Interesting Event Collection

Description:

Destination log: Forwarded Events

Subscription type and source computers

● Collector initiated

This computer contacts the selected source computers and provides the subscription.

○ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

User account (the selected account must have read access to the source logs):
Machine Account

Change user account or configure advanced settings:

FIGURE 10-13 Configuring a collector-initiated event subscription

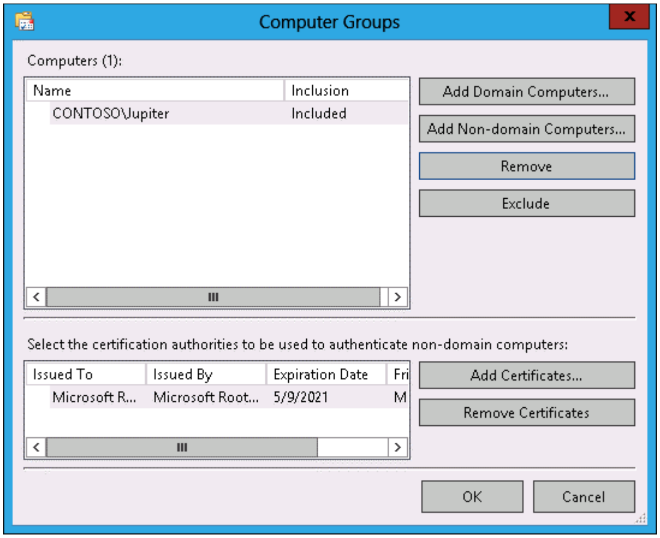
If you want to instead configure a source computer-initiated subscription, you need to configure the following group policies on the computers that will act as the event forwarders:

- **Configure Forwarder Resource Usage** This policy determines the maximum event forwarding rate in events per second. If this policy is not configured, events will be transmitted as soon as they are recorded.
- **Configure Target Subscription Manager** This policy enables you to set the location of the collector computer.

MORE INFO **EVENT SUBSCRIPTIONS**

For more information about event subscriptions, see *http://technet.microsoft.com/en-us/library/cc749183.aspx*.

Both these policies are located in the Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding node. When configuring the subscription, you must also specify the computer groups that hold the computer accounts of the computers that will be forwarding events to the collector. You do this in the Computer Groups dialog box, as shown in Figure 10-14.


Computer Groups

Computers (1):

Name	Inclusion
CONTOSO\Jupiter	Included

Select the certification authorities to be used to authenticate non-domain computers:

Issued To	Issued By	Expiration Date	Fri
Microsoft R...	Microsoft Root...	5/9/2021	M

FIGURE 10-14 Configuring subscription computer groups for the subscription

Quick check

- **You want to view specific events across multiple event logs. What tool should you use to accomplish this goal?**

Quick check answer

- **You should use custom views.**

Event-driven tasks

Event Viewer enables you to attach tasks to specific events. A drawback to the process of creating event-driven tasks is that you need to have an example of the event that triggers the task already present in the event log. Events are triggered based on an event having the same log, source, and event ID.

To attach a task to a specific event, perform the following steps:

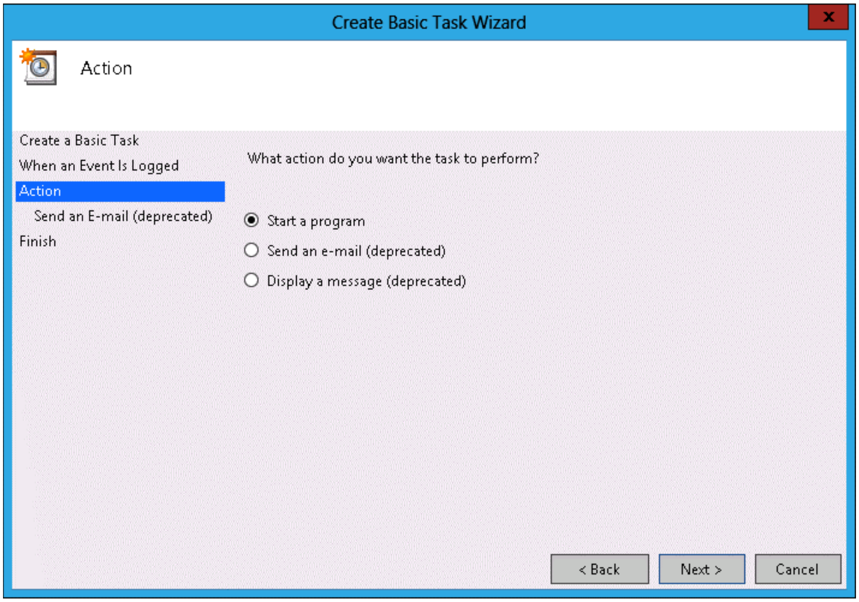
1. Open Event Viewer. Locate and select the event upon which you want to base the new task.

2. On the Event Viewer Actions pane, click Attach Task To This Event. The Create Basic Task Wizard displays.

3. On the Create A Basic Task page, review the name of the task that you want to create. By default, the task is named after the event. Click Next.

4. On the When An Event is Logged page, review the information about the event. This will list the log from which the event originates, the source of the event, and the event ID. Click Next.

5. On the Action page, shown in Figure 10-15, you can choose the task to perform. The Send An E-Mail and Display A Message tasks are deprecated, and you get an error if you try to create a task using these actions. Click Next.



Create Basic Task Wizard

Action

What action do you want the task to perform?

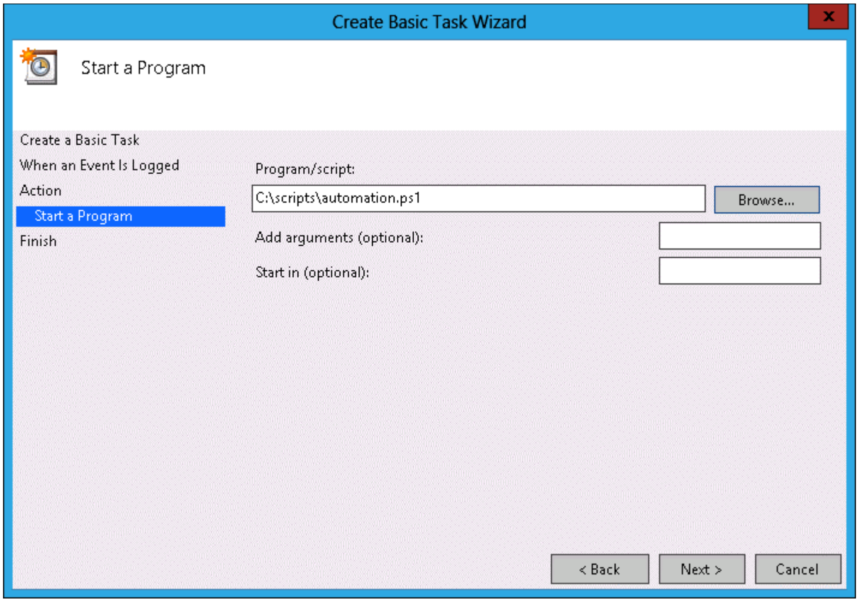
● Start a program

○ Send an e-mail (deprecated)

○ Display a message (deprecated)

FIGURE 10-15 Attaching a task to a specific event

6. On the Start A Program page, shown in Figure 10-16, specify the program or script that should be automatically triggered as well as additional arguments.



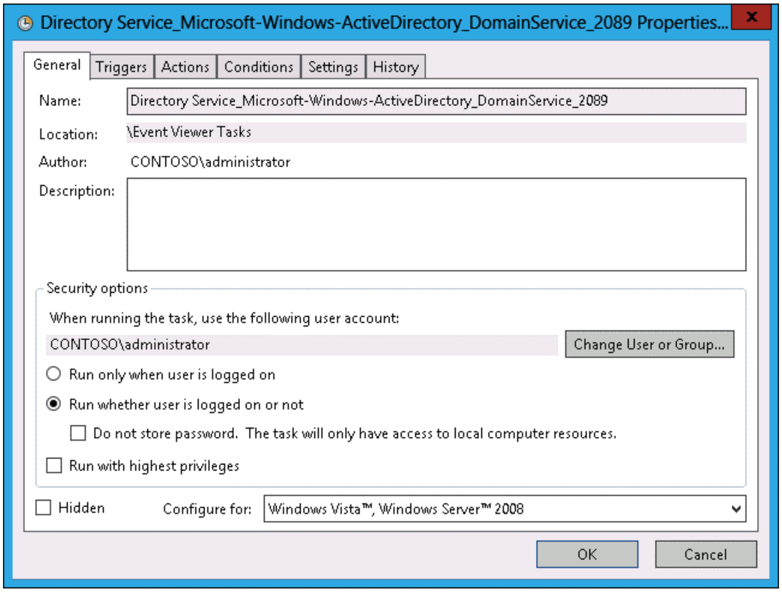
Program/script: C:\scripts\automation.ps1

Add arguments (optional):

Start in (optional):

FIGURE 10-16 Specifying a triggered script

7. After you complete task creation, you can modify the task to specify the security context under which the task executes. By default, event tasks run only when the user is signed on. You can configure the task to run whether the user is signed on or not, as shown in Figure 10-17.



Name: Directory Service_Microsoft-Windows-ActiveDirectory_DomainService_2089

Location: \Event Viewer Tasks

Author: CONTOSO\administrator

Description:

When running the task, use the following user account:

CONTOSO\administrator

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

□ Run with highest privileges

□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008

FIGURE 10-17 Run your task if the user is logged on or off

REAL WORLD **IT'S NOT ABOUT SENDING EMAIL, IT'S ABOUT SENDING A MESSAGE**

Even though the Send An Email task is deprecated, you can use the Start A Program option to execute a Windows PowerShell script that sends an email. In many cases, however, instead of sending a message to an administrator so the administrator can perform a task, it's better to have the task directly called wherever possible. Creating automated tasks that resolve problems without requiring direct intervention saves time and money. You should send email messages only when you need to notify yourself about an issue that cannot be resolved by running a script.

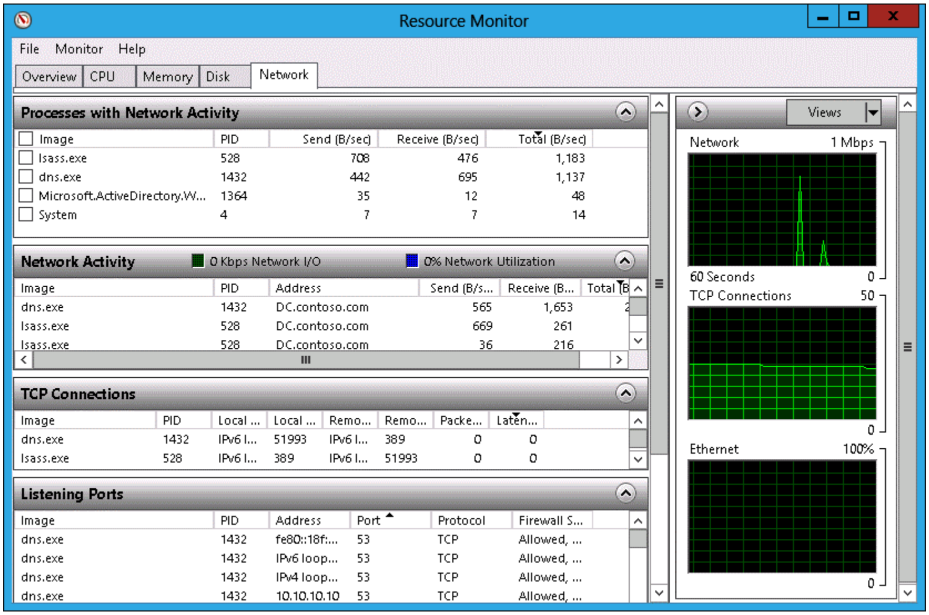
Network monitoring

Network monitoring enables you to track how a computer interacts with the network. Through network monitoring, you can determine which services and applications are using specific network interfaces, which services are listening on specific ports, and the volume of traffic that exists. There are two primary tools through which you can perform network monitoring on computers running Windows Server 2012:

- Resource Monitor
- Message Analyzer

Resource Monitor

Resource Monitor enables you to monitor how a computer running the Windows Server 2012 operating system uses CPU, memory, disk, and network resources. Resource Monitor provides real time information. You can't use Resource Monitor to perform a traffic capture and review activity that occurred in the past. You can use Resource Monitor to view activity that is currently occurring. The Network tab of Resource Monitor is shown in Figure 10-18.



Processes with Network Activity

□ Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ lsass.exe	528	708	476	1,183
□ dns.exe	1432	442	695	1,137
□ Microsoft.ActiveDirectory.W...	1364	35	12	48
□ System	4	7	7	14

Network Activity 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

Image	PID	Address	Send (B/s...	Receive (B...	Total (B
dns.exe	1432	DC.contoso.com	565	1,653	2
lsass.exe	528	DC.contoso.com	669	261	
lsass.exe	528	DC.contoso.com	36	216	

TCP Connections

Image	PID	Local ...	Local ...	Remo...	Remo...	Packe...	Laten...
dns.exe	1432	IPv6 l...	51993	IPv6 l...	389	0	0
lsass.exe	528	IPv6 l...	389	IPv6 l...	51993	0	0

Listening Ports

Image	PID	Address	Port	Protocol	Firewall S...
dns.exe	1432	fe80::18f:...	53	TCP	Allowed, ...
dns.exe	1432	IPv6 loop...	53	TCP	Allowed, ...
dns.exe	1432	IPv4 loop...	53	TCP	Allowed, ...
dns.exe	1432	10.10.10.10	53	TCP	Allowed, ...

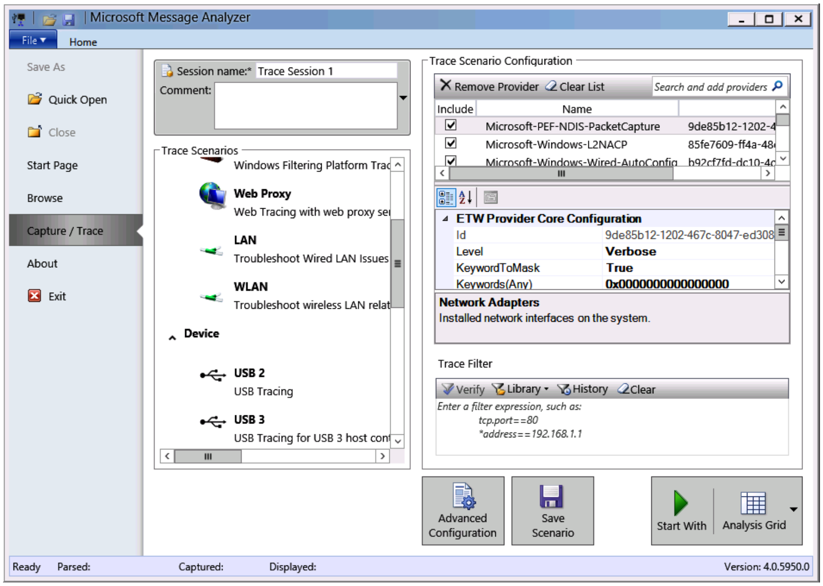
FIGURE 10-18 Resource Monitor Network tab

Resource Monitor provides the following information that is relevant to network monitoring:

- **Processes With Network Activity** This view lists processes by name and ID; and provides information on bits sent per second, bits received per second, and total bits per second.
- **Network Activity** Lists network activity on a per-process basis, but also lists the destination address, sent bits per second, received bits per second, and total bits per second.
- **TCP Connections** Provides information on connections on the basis of local address, port, and remote address and port.
- **Listening Ports** Lists the ports and addresses that services and applications are listening on. Also provides information about the firewall status for these roles and services.

Message Analyzer

Microsoft Message Analyzer is the successor to Network Monitor. You can use Message Analyzer to perform network traffic capture and analysis. Message Analyzer also functions as a replacement for LogParser, which enables you to manage system messages, events, and log files. When performing a capture, you select the scenario that best represents the type of event about which you are interested in capturing traffic. For example, the LAN scenario, shown in Figure 10-19, enables you to capture traffic on local area network (LAN) interfaces.



Session name:* Trace Session 1

Comment:

Include	Name	
☑	Microsoft-PEF-NDIS-PacketCapture	9de85b12-1202-4
☑	Microsoft-Windows-L2NACP	85fe7609-ff4a-48
☑	Microsoft-Windows-Wired-AutoConfig	b92cf7fd-dc10-4c

ETW Provider Core Configuration

Id	9de85b12-1202-467c-8047-ed308
Level	**Verbose**
KeywordToMask	**True**
Keywords(Any)	**0x0000000000000000**

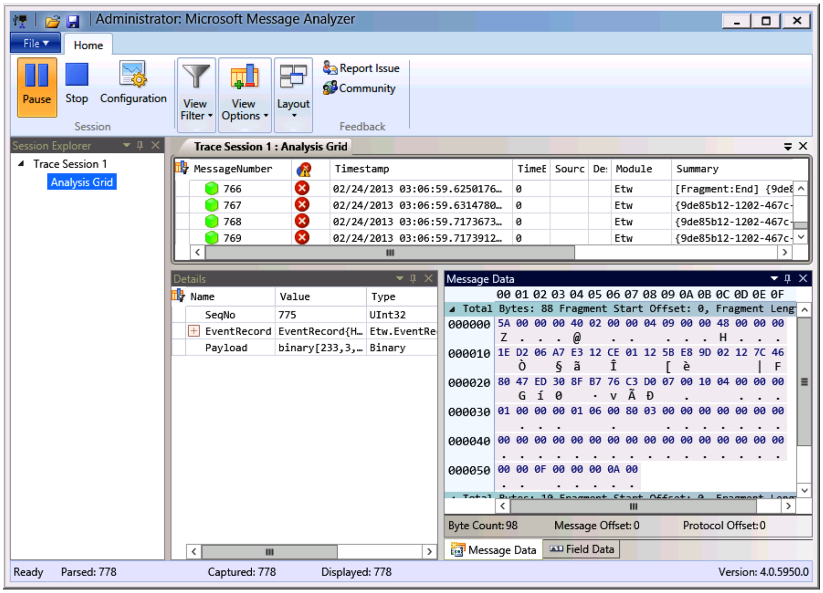
Network Adapters
Installed network interfaces on the system.

Enter a filter expression, such as:
tcp.port==80
**address==192.168.1.1*

Ready Parsed: Captured: Displayed: Version: 4.0.5950.0

FIGURE 10-19 LAN scenario

When performing certain types of network traffic capture, you need to run Message Analyzer using an account that is a member of the local Administrators group. After the capture has been performed, you can analyze the content of each message, as shown in Figure 10-20. By applying appropriate filters, you can locate network traffic that has specific characteristics, such as using a particular TCP port, source, or destination address.



MessageNumber		Timestamp	TimeE	Sourc	De:	Module	Summary
766	☒	02/24/2013 03:06:59.6250176…	0			Etw	[Fragment:End] {9de8
767	☒	02/24/2013 03:06:59.6314780…	0			Etw	{9de85b12-1202-467c-
768	☒	02/24/2013 03:06:59.7173673…	0			Etw	{9de85b12-1202-467c-
769	☒	02/24/2013 03:06:59.7173912…	0			Etw	{9de85b12-1202-467c-

Name	Value	Type
SeqNo	775	UInt32
EventRecord	EventRecord{H…	Etw.EventRe
Payload	binary[233,3,…	Binary

```
        00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
◢ Total Bytes: 88 Fragment Start Offset: 0, Fragment Leng
000000  5A 00 00 00 40 02 00 00 04 09 00 00 48 00 00 00
        Z  .  .  .  @     .  .     .  .  .  H  .  .  .
000010  1E D2 06 A7 E3 12 CE 01 12 5B E8 9D 02 12 7C 46
           Ò     §  ã     Î        [  è           |  F
000020  80 47 ED 30 8F B7 76 C3 D0 07 00 10 04 00 00 00
           G  í  0     ·  v  Ã  Ð     .        .  .  .
000030  01 00 00 00 01 06 00 80 03 00 00 00 00 00 00 00
           .  .  .        .        .  .  .  .  .  .  .
000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
        .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
000050  00 00 0F 00 00 00 0A 00
        .  .     .  .  .  .  .
```

Byte Count: 98 Message Offset: 0 Protocol Offset: 0

Ready Parsed: 778 Captured: 778 Displayed: 778 Version: 4.0.5950.0

FIGURE 10-20 Message Analyzer

NOTE **MESSAGE ANALYZER**

At the time of writing, Message Analyzer is still beta software. There is a blog on TechNet that describes the features and functionality of the new product: *http://blogs.technet.com/b/messageanalyzer/archive/2012/09/17/meet-the-successor-to-microsoft-network-monitor.aspx*.

Lesson summary

- Data collector sets enable you to collect performance counter data, event trace data, and system configuration information.
- Performance counter alerts enable an event to be written to the event log and a command to be run when a specified performance counter exceeds or falls below a configured value.
- Event log filters apply to a single event log and are not persistent.
- Event log views are persistent, can include items from multiple event logs, and can be imported and exported.
- Event subscriptions enable you to configure one computer to consolidate the event logs of multiple computers.
- Event-driven tasks enable you to configure a program or script to be run when a specific event is written to the event log.
- Message Analyzer, which is the successor to Network Monitor, enables you to capture and analyze network traffic.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You want to collect processor, memory, and network interface utilization data over the course of several hours. You need to be able to review the data at a later period in time. Which of the following tools should you use to accomplish this goal?

   A. Resource Monitor

   B. Task Manager

   C. Data collector set

   D. Message Analyzer

2. A particular network service on a computer running Windows Server 2012 that you are responsible for managing is not functioning correctly. You suspect that the service is listening on a TCP port that Windows Firewall is configured to block, but you don't know which TCP port the service uses. Which of the following tools should you use to determine this information?
   - **A.** Task Manager
   - **B.** Resource Monitor
   - **C.** Message Analyzer
   - **D.** Data collector set
3. Which of the following tools can you use to capture and analyze network traffic?
   - **A.** Data collector set
   - **B.** Message Analyzer
   - **C.** Resource Monitor
   - **D.** Task Manager
4. You are configuring event log subscriptions. Computer SYD-A will function as the event log collector, and computers MEL-A, MEL-B, and MEL-C will function as the event log sources. You want SYD-A to collect events from the security logs on computers MEL-A, MEL-B, and MEL-C. To which of the following security groups on MEL-A, MEL-B, and MEL-C should you add the computer account of SYD-A?
   - **A.** Backup operators
   - **B.** Power users
   - **C.** Event log readers
   - **D.** Administrators

Lesson 2: Advanced audit policies

Auditing enables you to track both actual and attempted access and changes to objects and policies. Auditing enables you to verify that the policies that you've put in place to secure your organization's network infrastructure are actually being enforced, from tracking modifications to sensitive user accounts through to access to sensitive files and folders. In this lesson, you will learn about advanced audit policy, how to configure expression-based audit policies, and how you can use auditpol.exe to manage auditing.

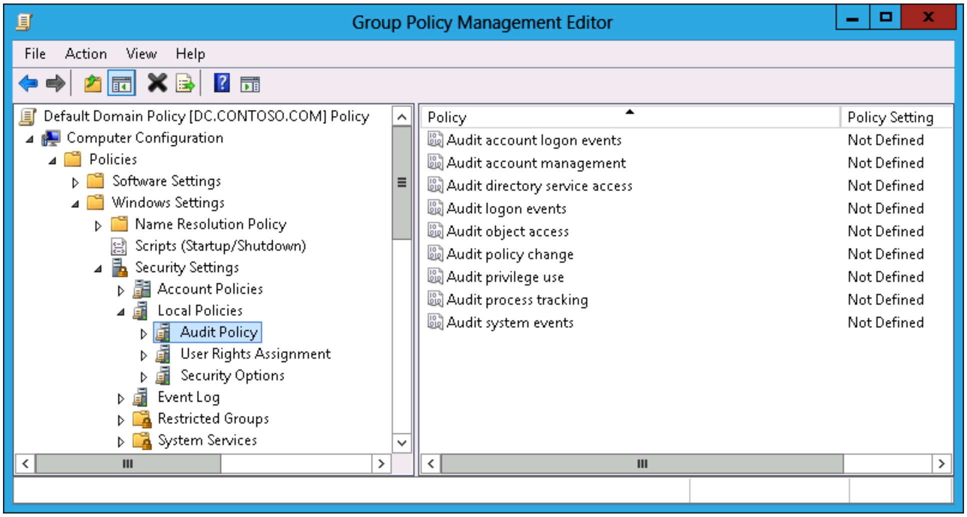
After this lesson, you will be able to:

- Understand advanced audit policies.
- Configure auditing using Group Policy.
- Use auditpol.exe to manage auditing.

Estimated lesson time: 45 minutes

Advanced auditing

There are two sets of audit policies in a Group Policy Object (GPO): traditional audit policies and *advanced audit policies*. The traditional audit policies are located in the Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policies node and are shown in Figure 10-21. They are the audit policies that have been available with the Windows Server operating system since Windows 2000. The drawback of these policies is that they are general, and you can't be specific in the way you configure auditing. When you use these policies, you'll not only audit the events that you're interested in but you'll also end up auditing many events that you don't need to know about.



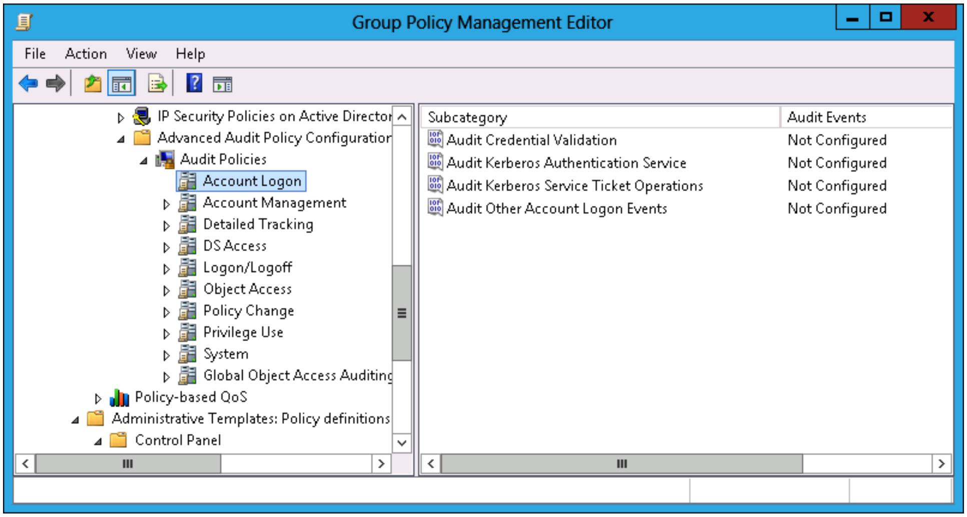
Policy	Policy Setting
Audit account logon events	Not Defined
Audit account management	Not Defined
Audit directory service access	Not Defined
Audit logon events	Not Defined
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Not Defined

FIGURE 10-21 General auditing policies

REAL WORLD **NEEDLES AND HAYSTACKS**

The trick of implementing a successful audit policy is to reduce the size of the haystack so that finding the needles is easier. An audit policy that records only activity that you are interested in produces fewer events than a more general audit policy, in which interesting events can get lost in the clutter.

The advanced audit policies enable you to be more specific in the types of activity you audit. The advanced audit policies are located under the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration node, as shown in Figure 10-22.


Group Policy Management Editor
File
Action
View
Help
IP Security Policies on Active Director
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions
Control Panel

Subcategory	Audit Events
Audit Credential Validation	Not Configured
Audit Kerberos Authentication Service	Not Configured
Audit Kerberos Service Ticket Operations	Not Configured
Audit Other Account Logon Events	Not Configured

FIGURE 10-22 Advanced audit policies

There are 10 groups of audit policy settings and 58 individual audit policies available through Advanced Audit Policy Configuration. The audit policy groups contain the following settings:

- **Account Logon** You can audit credential validation and Kerberos-specific operations.
- **Account Management** You can audit account management operations, such as changes to computer accounts, user accounts, and group accounts.
- **Detailed Tracking** You can audit encryption events, process creation, process termination, and RPC events.
- **DS Access** You can audit Active Directory access and functionality.
- **Logon/Logoff** You can audit logon, logoff, and other account activity events, including IPsec and Network Policy Server (NPS) events.
- **Object Access** You can audit access to objects including files, folders, applications, and the registry.
- **Policy Change** You can audit changes to audit policy.
- **Privilege Use** You can audit the use of privileges.
- **System** You can audit changes to the security subsystem.
- **Global Object Access Auditing** You can configure expression-based audit policies for files and the registry.

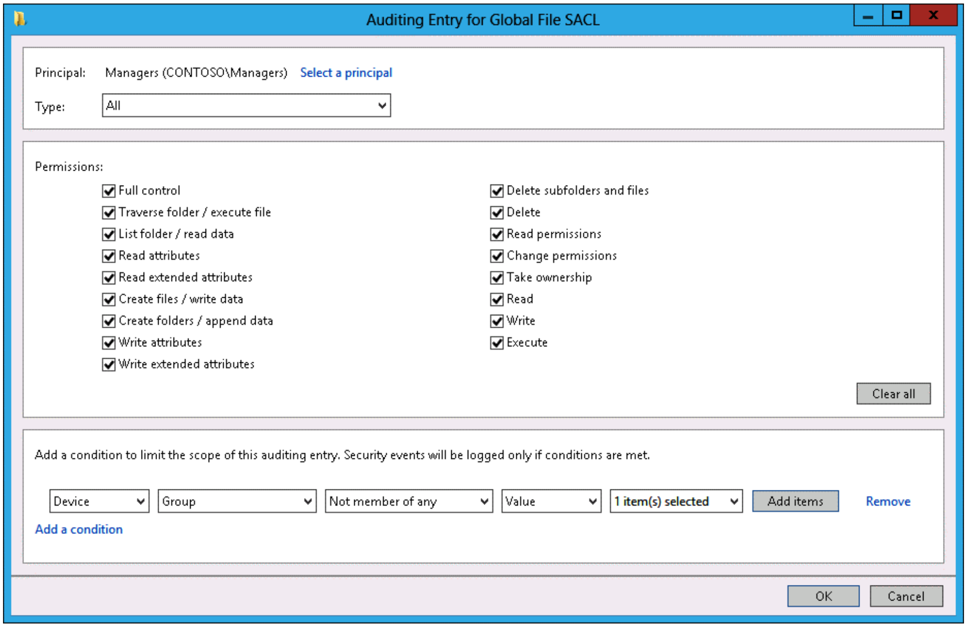
REAL WORLD **CONFIGURE AN AUDIT POLICY**

Determine what you want to audit first and then enable the policies to audit that type of activity. A mistake that many administrators make is that they aren't entirely sure what they should be auditing, so they audit everything. They become frustrated with the process because the auditing events that they might be interested get lost in the vast sea of auditing events that they are not interested in.

Expression-based audit policies

Traditional object audit policies involve specifying a group and configuring the type of activities that will trigger an event to be written to the security log. Specifying that an audit event will be written each time a member of the Managers group accesses a file in a specific folder is a good example.

Expression-based audit policies enable you to go further. These policies enable you to put conditions as to when auditing might occur. For example, you might want to configure auditing so that members of the Managers group have access to sensitive files tracked only when they access files from computers that aren't part of the Managers_Computers group. Figure 10-23 shows auditing configured in this way. This way, you don't bother tracking access when members of this group access sensitive files from within the office, but you do track all access to those sensitive files when members of this group are accessing them from an unusual location.



Auditing Entry for Global File SACL

Principal: Managers (CONTOSO\Managers) Select a principal

Type: All

Permissions:

☑ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☑ Read permissions
☑ Change permissions
☑ Take ownership
☑ Read
☑ Write
☑ Execute

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Device | Group | Not member of any | Value | 1 item(s) selected

FIGURE 10-23 Expression-based audit policies

You can integrate expression-based audit policies with Dynamic Access Control (DAC) to create targeted audit policies that are based on user, computer, and resource claims. Instead of just adding claims based on user or device group membership, the claim can be based on document metadata such as confidentiality settings and site location. You can configure expression-based audit policies at the file or folder level, or apply them through Group Policy using policies in the Global Object Access Auditing node of Advanced Audit Policy Configuration.

✓ **Quick check**

- **What type of auditing should you configure if you want to audit file access by a specific group of people only when they aren't signed on to a specific group of computers?**

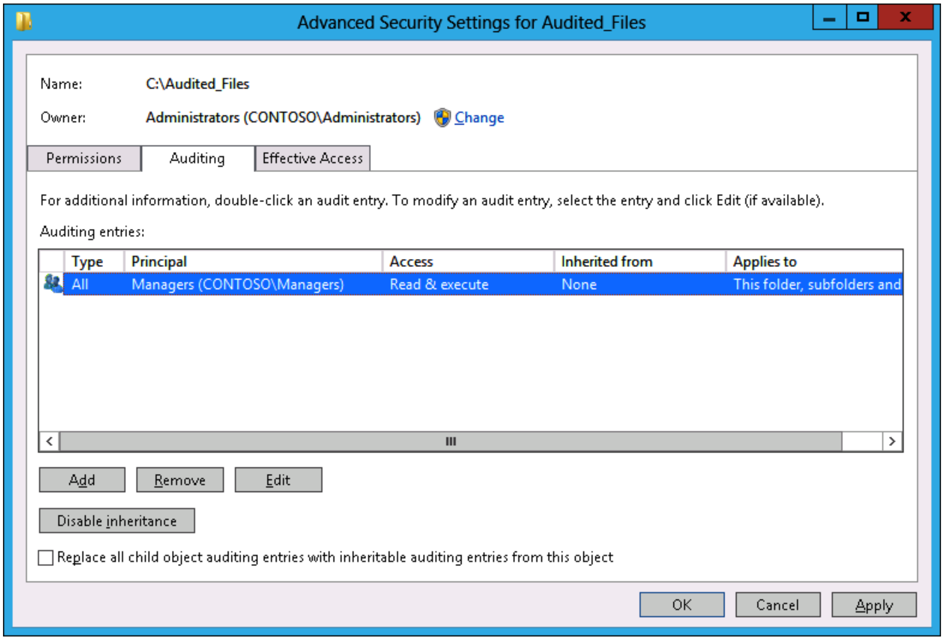
Quick check answer

- **You configure an expression-based audit policy to audit file access by a specific group of people who are accessing files from computers other than those in a specific group.**

Configuring file and folder auditing

After you configure auditing of object access, either through the traditional or advanced audit policies, you can configure auditing at the file and folder level. The simplest way to configure auditing is at the folder level because you can then configure all folders and subfolders to inherit those auditing settings. If you change the auditing settings at the folder level, you can use the Replace All Child Object Auditing Entries option to apply the new auditing settings to the folder's child files and folders.

You can configure auditing for a specific file and folder through the Advanced button on the Security tab of the object's properties. You can configure basic success and failure auditing, as shown in Figure 10-24. You can also configure expression-based auditing so that activity by members of a specific security group are audited only if other conditions, such as membership of other security groups, are also met.


Advanced Security Settings for Audited_Files

Name: C:\Audited_Files

Owner: Administrators (CONTOSO\Administrators) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
All	Managers (CONTOSO\Managers)	Read & execute	None	This folder, subfolders and

□ Replace all child object auditing entries with inheritable auditing entries from this object

FIGURE 10-24 Configuring basic success and failure auditing

The advantage of using Global Object Access Auditing is that when you have it configured, you can use file classification to apply metadata to files and then automatically have auditing enabled for those files. For example, using file classification and DAC, you can configure a Windows Server 2012 file server so that all files that contain the phrase “code secret” are marked as Sensitive. You can then configure Global Object Access Auditing so that all access to files marked as Sensitive are automatically audited. Instead of having an administrator track down all the files that are sensitive and configuring auditing on those files, the process is automatic. All that needs to happen to trigger it is the inclusion of the phrase “code secret” in the file.

Using auditpol with auditing

Auditpol.exe is a command-line utility that you can use to configure and manage audit policy settings from an elevated command prompt. You can use auditpol.exe to perform the following tasks:

- View the current audit policy settings with the /get subcommand
- Set audit policy settings with the /set subcommand
- Display selectable policy elements with the /list subcommand

- Back up and restore audit policies using the /backup and /restore subcommands
- Delete all per-user audit policy settings and reset the system policy settings using the /clear subcommand
- Remove all per-user audit policy settings and disable all system policy settings using the /remove subcommand

For example, to enable success and failure auditing for the File System subcategory of Object Access, execute this command:

```
Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable
```

To view the current audit policy settings for all audit policies, issue this command:

```
Auditpol.exe /get /category:*
```

To view the current audit policy settings for a specific category, such as Object Access, issue this command:

```
Auditpol.exe /get /category:"Object Access"
```

MORE INFO **AUDITPOL.EXE**

To learn more about auditpol.exe, consult the following TechNet article at: *http://technet.microsoft.com/en-us/library/cc731451(v=ws.10).aspx*.

Lesson summary

- Advanced audit policies enable you to perform more granular auditing than is possible with the traditional auditing policies available in earlier versions of Windows server.
- Expression-based audit policies enable you to configure auditing based on object metadata. You can also use expression-based audit policies to perform conditional auditing.
- After you have enabled the auditing of object access, you can configure auditing at the file and folder level. File- and folder-level auditing supports expression-based audit policies.
- You can use the auditpol.exe command-line utility from an elevated command prompt to configure and manage audit policy settings.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following commands should you use to enable success and failure auditing for all audit policies under the Object Access category on a computer running Windows Server 2012?
   - **A.** Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.
   - **B.** Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable
   - **C.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable.
   - **D.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable.
2. You want to enable failure auditing, but not success auditing, for all audit policies under the Object Access category on a computer running Windows Server 2012. Which of the following commands should you use to accomplish this goal?
   - **A.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable.
   - **B.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable.
   - **C.** Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable.
   - **D.** Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.
3. You want to enable success and failure auditing only for the File System subcategory. Which of the following commands should you use to accomplish this goal?
   - **A.** Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable.
   - **B.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable.
   - **C.** Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.
   - **D.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable.
4. You want to disable all success and failure auditing on all auditing subcategories under the Object Access category. Which of the following commands should you use to accomplish this goal?
   - **A.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Disable.
   - **B.** Auditpol.exe /get /Category:"Object Access" /success:Disable /Failure:Enable.
   - **C.** Auditpol.exe /set /Category:"Object Access" /success:Enable /Failure:Enable.
   - **D.** Auditpol.exe /set /subcategory:"File System" /success:Enable /failure:Enable.

Practice exercises

The goal of this section is to provide you with hands-on practice with the following:

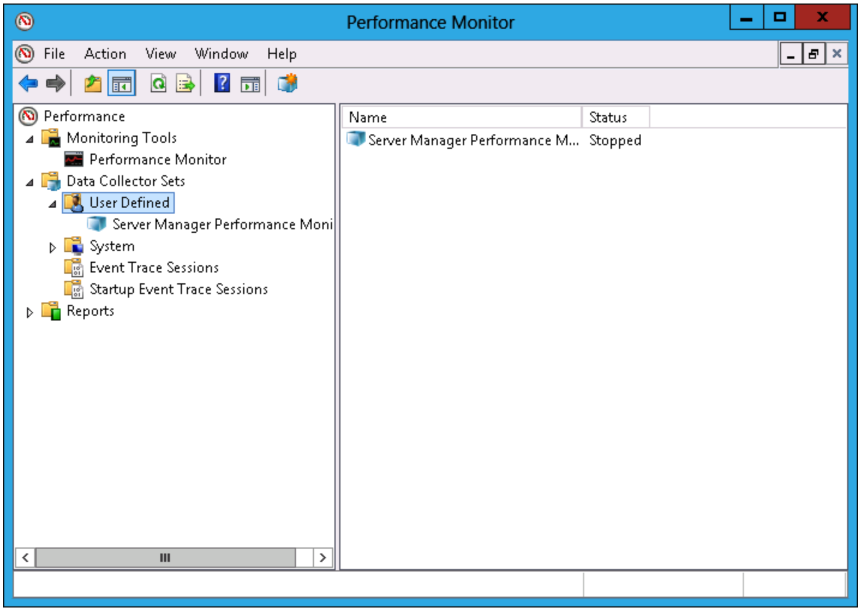
- Configure data collector sets
- Configure alerts
- Manage event subscriptions
- Perform network monitoring
- Configure removable device auditing
- Configure logon auditing
- Configure expression-based audit policies
- Enable folder auditing

To perform the exercises in this section, you need access to an evaluation version of Windows Server 2012. You should also have access to virtual machines SYD-DC, SYD-A, and SYD-B, the setup instructions for which are as described in the Appendix. You should ensure that you have a snapshot of these virtual machines that you can revert to at the end of the practice exercises.

EXERCISE 1 Configure data collector sets

In this exercise, you will configure data collector sets. To complete this exercise, perform the following steps:

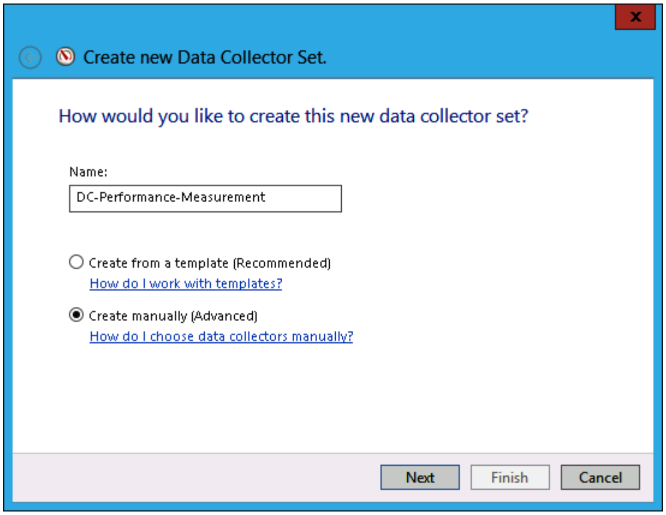
1. On DC, click Performance Monitor in the Tools menu of Server Manager.
2. In the Performance Monitor console, expand the Performance\Data Collector Sets\User Defined, as shown in Figure 10-25.



Name	Status
Server Manager Performance M...	Stopped

FIGURE 10-25 Accessing data collector sets

3. On the Action menu, click New and click Data Collector Set.
4. In the Create New Data Collector Set dialog box, enter the name **DC-Performance-Measurement** and click Create Manually (Advanced), as shown in Figure 10-26. Click Next.



How would you like to create this new data collector set?

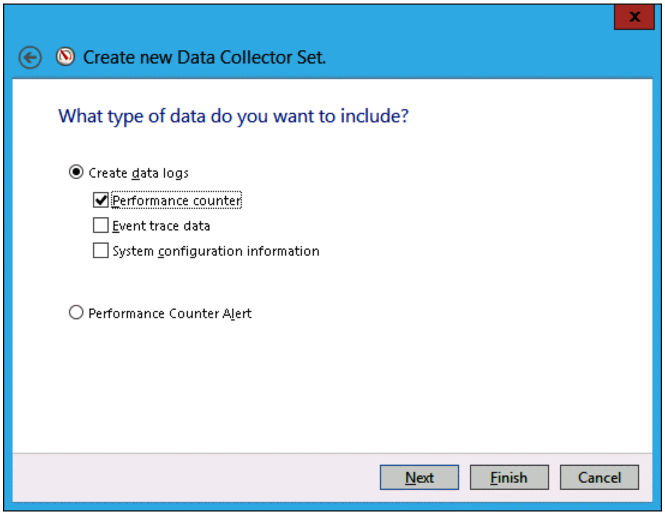
Name: DC-Performance-Measurement

○ Create from a template (Recommended)
How do I work with templates?

● Create manually (Advanced)
How do I choose data collectors manually?

FIGURE 10-26 Entering the data collector set name

5. On the What Type Of Date Do You Want To Include? page, click Performance Counter, as shown in Figure 10-27, and click Finish.



Create new Data Collector Set.

What type of data do you want to include?

● Create data logs

☑ Performance counter

□ Event trace data

□ System configuration information

○ Performance Counter Alert

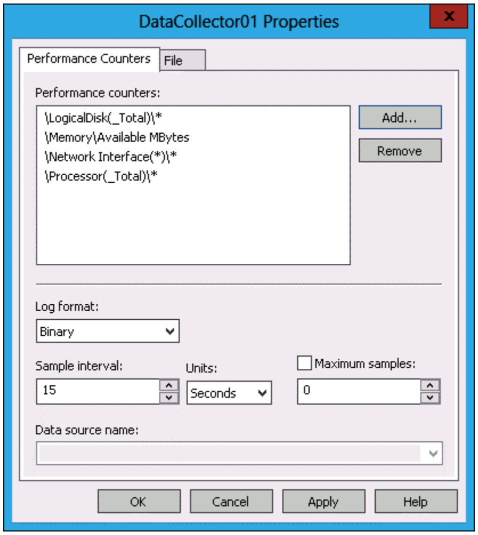
FIGURE 10-27 Selecting Performance Counter

6. In the Performance Monitor console, click DC-Performance-Measurement.

7. In the details pane, click DataCollector01.

8. On the Action menu, click Properties.

9. In the DataCollector01 Properties dialog box, shown in Figure 10-28, click Add.



DataCollector01 Properties

Performance counters:

```
\LogicalDisk(_Total)\*
\Memory\Available MBytes
\Network Interface(*)\*
\Processor(_Total)\*
```

Log format: Binary

Sample interval: 15

Units: Seconds

□ Maximum samples: 0

Data source name:

FIGURE 10-28 Performance counters

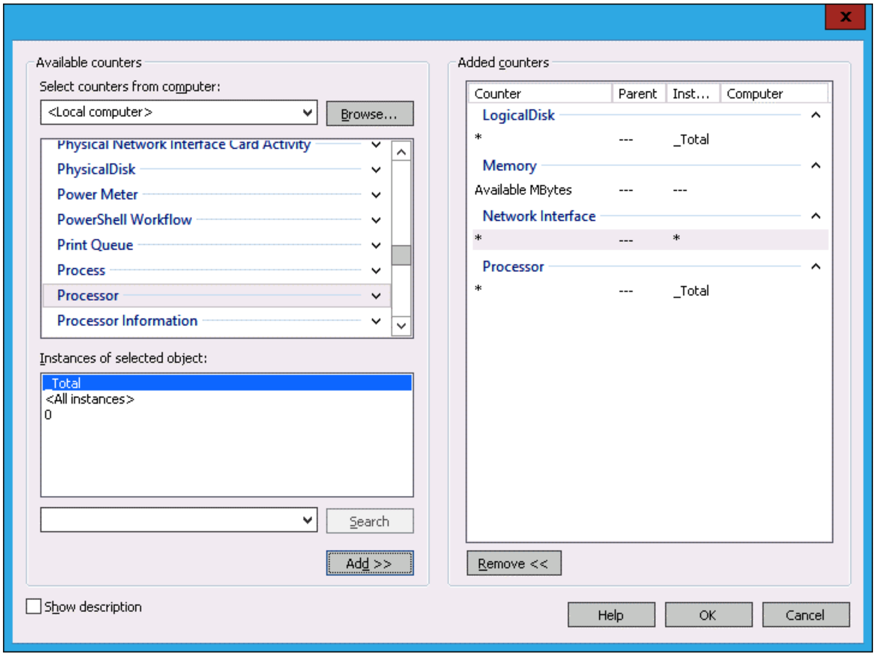
10. In the Available Counters dialog box, click Logical Disk and click Add.

11. Click Memory, click the arrow, click Available Mbytes, and click Add.

12. Click Network Interface and click Add.

13. Click Processor and click Add.

14. Verify that the list of added counters matches Figure 10-29 and click OK.



Available counters

Select counters from computer: <Local computer>

Physical Network Interface Card Activity
PhysicalDisk
Power Meter
PowerShell Workflow
Print Queue
Process
Processor
Processor Information

Instances of selected object:
_Total
<All instances>
0

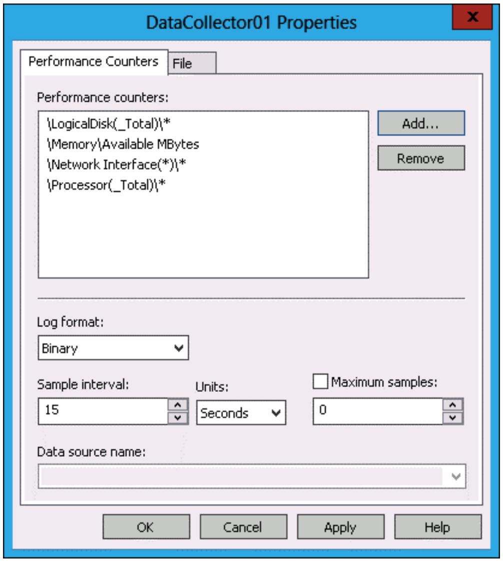
Added counters

Counter	Parent	Inst...	Computer
LogicalDisk			
*	---	_Total	
Memory			
Available MBytes	---	---	
Network Interface			
*	---	*	
Processor			
*	---	_Total	

☐ Show description

FIGURE 10-29 Matching added counters

15. In the DataCollector01 Properties dialog box, set the Sample Interval to 15 seconds (see Figure 10-30) and click OK.


DataCollector01 Properties

Performance Counters | File

Performance counters:

```
\LogicalDisk(_Total)\*
\Memory\Available MBytes
\Network Interface(*)\*
\Processor(_Total)\*
```

Log format: Binary

Sample interval: 15

Units: Seconds

□ Maximum samples: 0

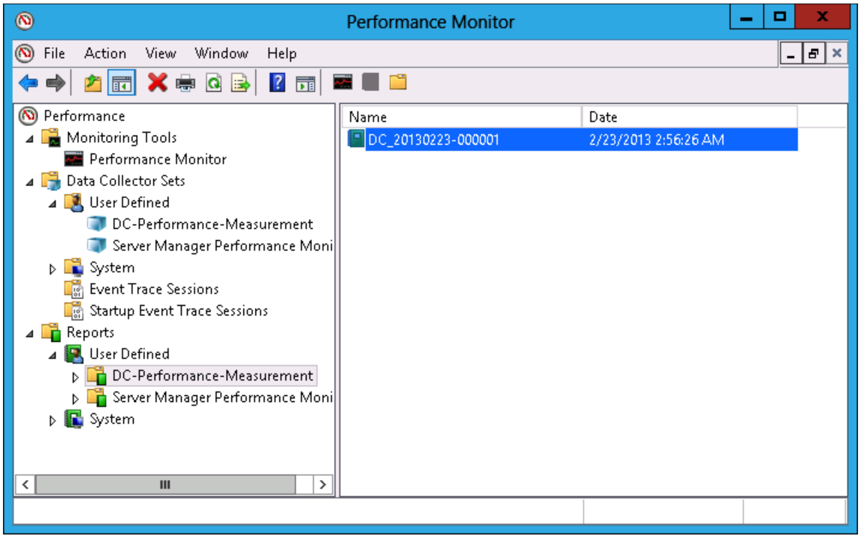
Data source name:

FIGURE 10-30 Setting the interval

EXERCISE 2 Collect data

In this exercise, you will collect data from the data collector set. To complete this exercise, perform the following steps:

1. In Performance Monitor, click Data Collector Sets\User Defined\DC-Performance-Measurement.
2. On the Action menu, click Start.
3. After 2 minutes, on the Action menu, click Stop.
4. Expand Reports, expand User Defined, and click DC-Performance-Measurement.
5. Click the report listed in the details pane, as shown in Figure 10-31.



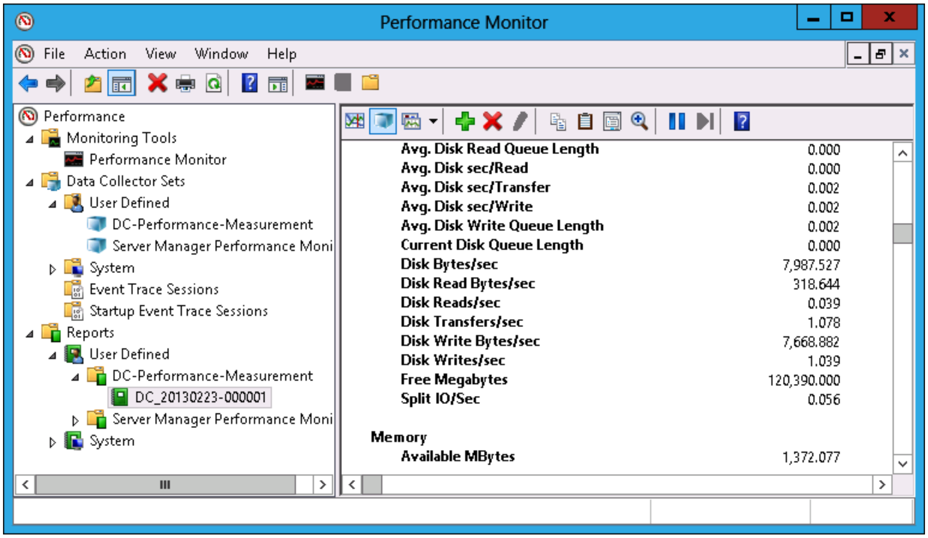
Name	Date
DC_20130223-000001	2/23/2013 2:56:26 AM

FIGURE 10-31 Selecting a report

6. Click View Data In Performance Monitor.

7. Click Change Graph Type and click Report.

8. View the report, as shown in Figure 10-32.



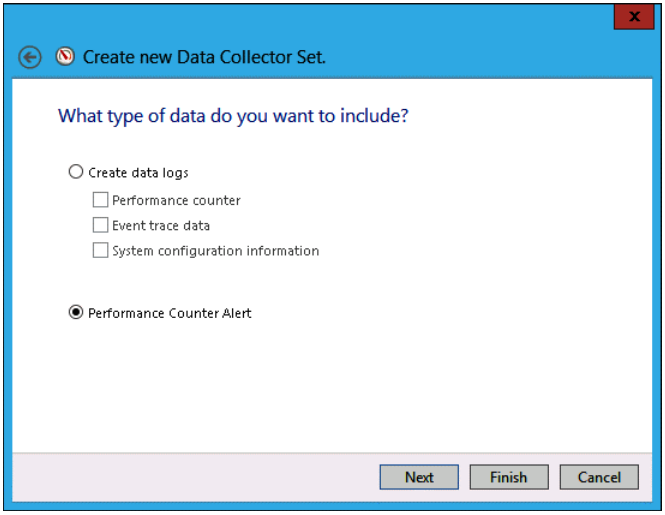
```
    Avg. Disk Read Queue Length                         0.000
    Avg. Disk sec/Read                                  0.000
    Avg. Disk sec/Transfer                              0.002
    Avg. Disk sec/Write                                 0.002
    Avg. Disk Write Queue Length                        0.002
    Current Disk Queue Length                           0.000
    Disk Bytes/sec                                  7,987.527
    Disk Read Bytes/sec                               318.644
    Disk Reads/sec                                      0.039
    Disk Transfers/sec                                  1.078
    Disk Write Bytes/sec                            7,668.882
    Disk Writes/sec                                     1.039
    Free Megabytes                                120,390.000
    Split IO/Sec                                        0.056

Memory
    Available MBytes                                1,372.077
```

FIGURE 10-32 Viewing the report

EXERCISE 3 Configure alerts

In this exercise, you will configure a free disk space alert. To complete this exercise, perform the following steps:

1. In Performance Monitor, click User Defined under Data Collector Sets.
2. On the Action menu, click New and click Data Collector Set.
3. On the Create New Data Collector Set page, type **Disk Space Alert**, click Create Manually (Advanced), and click Next.
4. On the Create New Data Collector Set page, click Performance Counter Alert, as shown in Figure 10-33, and click Next.


Create new Data Collector Set.

What type of data do you want to include?

○ Create data logs

☐ Performance counter

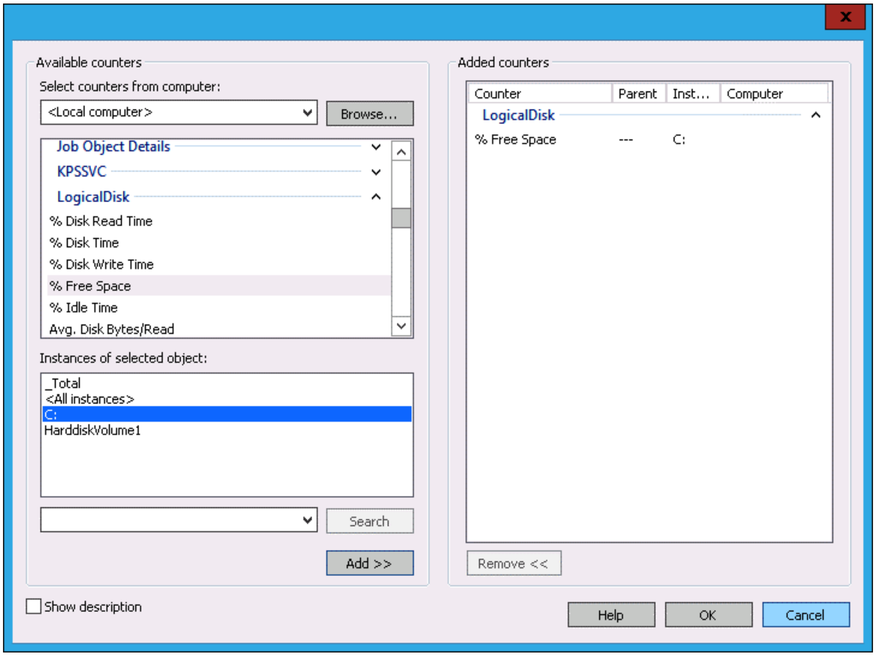
☐ Event trace data

☐ System configuration information

● Performance Counter Alert

FIGURE 10-33 Choosing Performance Counter Alert

5. On the Which Performance Counters Would You Like To Monitor? page, click Add.
6. In the Available Counters dialog box, click LogicalDisk, click %Free Space, click C:, and click Add, as shown in Figure 10-34. Click OK.



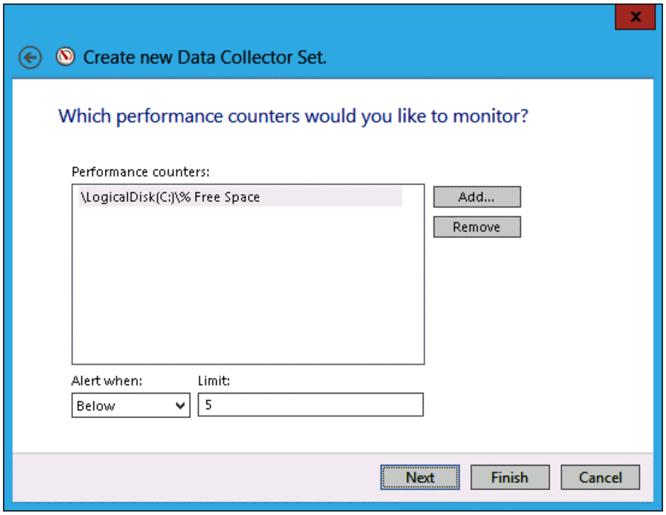
Select counters from computer: <Local computer>

Counter	Parent	Inst...	Computer
LogicalDisk			
% Free Space	---	C:	

FIGURE 10-34 Selecting LogicalDisk

7. Set the Alert When drop-down menu to Below.

8. Set the Limit value to 5, as shown in Figure 10-35, and click Next.



Which performance counters would you like to monitor?

Performance counters: \LogicalDisk(C:)\% Free Space

Alert when: Below

Limit: 5

FIGURE 10-35 Setting the limit value

9. Click Finish.

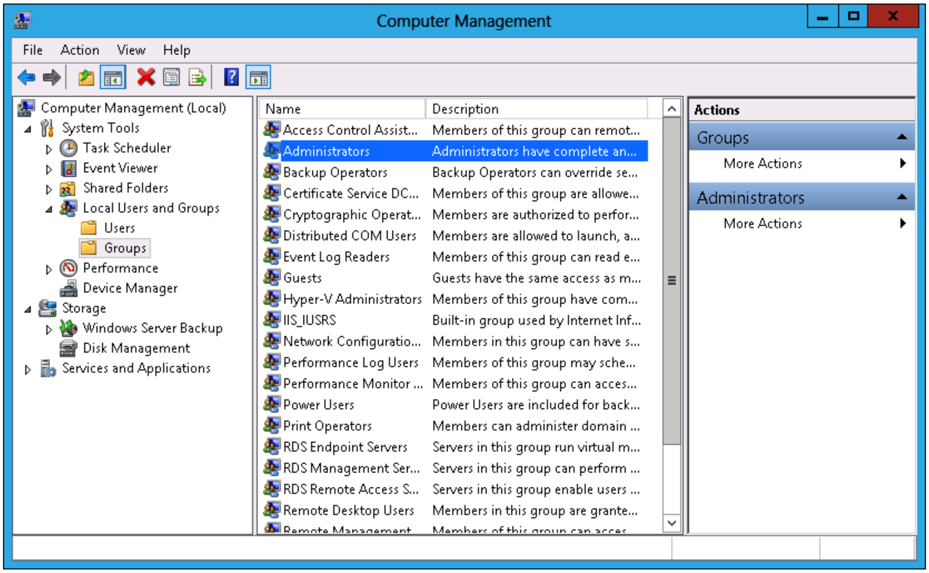
EXERCISE 4 Prepare computers for event subscriptions

In this exercise, you will configure computers to support event log subscriptions. To complete this exercise, perform the following steps:

1. On DC, click Windows PowerShell on the task bar.
2. Enter the following command and press Enter:

   ```
   Wecutil qc
   ```

3. When prompted, press Y and press Enter.
4. Close the Windows PowerShell prompt.
5. Sign on to SYD-A as Contoso\Administrator.
6. In the Tools menu on Server Manager, click Computer Management.
7. In the Computer Management console, expand Local Users And Groups, click Groups, and then click Administrators, as shown in Figure 10-36.

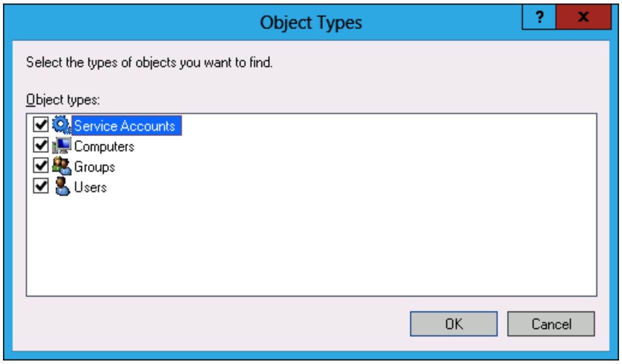


Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DC...	Members of this group are allowe...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Print Operators	Members can administer domain ...
RDS Endpoint Servers	Servers in this group run virtual m...
RDS Management Ser...	Servers in this group can perform ...
RDS Remote Access S...	Servers in this group enable users ...
Remote Desktop Users	Members in this group are grante...
Remote Management	Members of this group can acces

FIGURE 10-36 Accessing Administrators

8. On the Actions pane, click More Actions and click Properties under Administrator.
9. In the Administrators Properties dialog box, click Add.
10. In the Select Users, Computers, Service Accounts, Or Groups dialog box, click Object Types.

11. In the Object Types dialog box, enable the Computers check box, as shown in Figure 10-37, and click OK.



Select the types of objects you want to find.

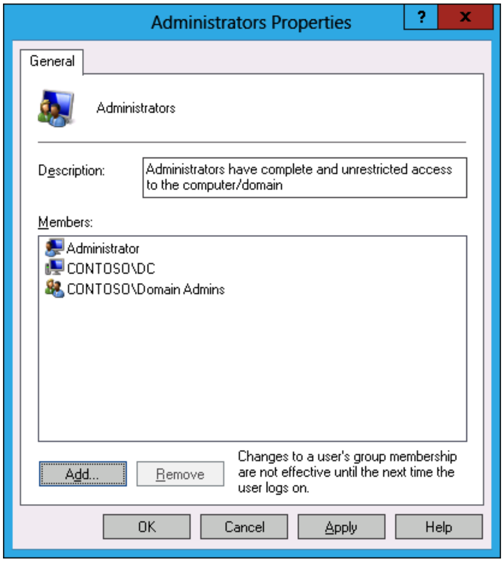
Object types:

- ☑ Service Accounts
- ☑ Computers
- ☑ Groups
- ☑ Users

FIGURE 10-37 Selecting Computers

12. In the Select Users, Computers, Service Accounts, Or Groups dialog box, type **DC**, click Check Names, and click OK.

13. Verify that the Administrators Properties dialog box matches Figure 10-38 and click OK.



Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

- Administrator
- CONTOSO\DC
- CONTOSO\Domain Admins

Changes to a user's group membership are not effective until the next time the user logs on.

FIGURE 10-38 Administrators Properties dialog box

14. Restart SYD-A.

EXERCISE 5 Configure event subscriptions

In this exercise, you will configure event subscriptions. To complete this exercise, perform the following steps:

1. In the Server Manager console on DC, open the Tools menu and click Event Viewer.
2. In Event Viewer, click the Subscriptions node, as shown in Figure 10-39.

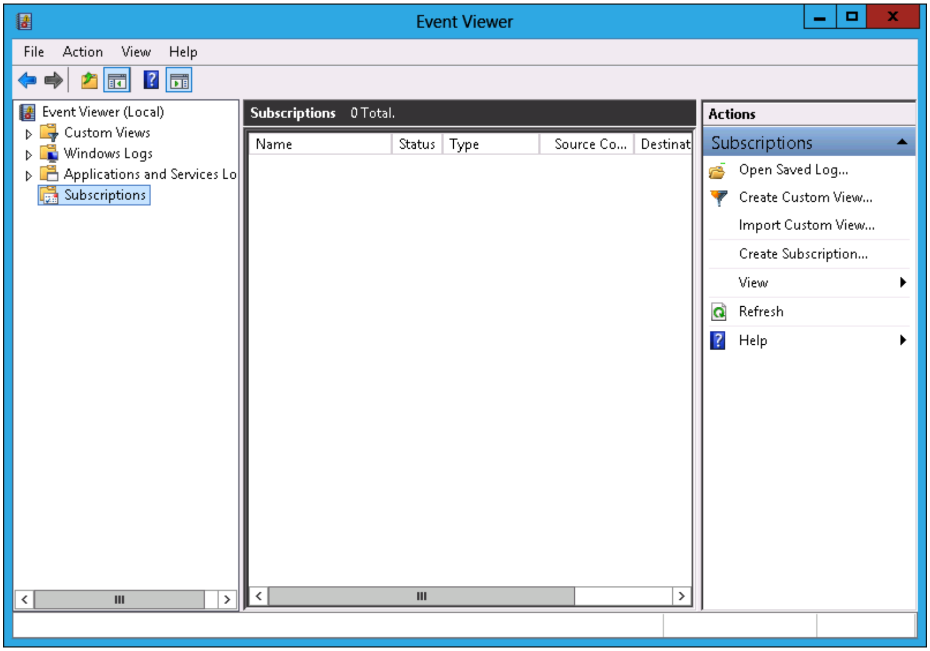
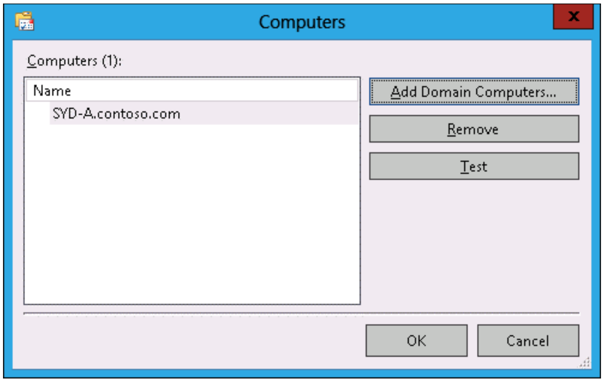


FIGURE 10-39 Clicking the Subscriptions node

3. On the Actions pane, click Create Subscription.
4. In the Subscription Properties dialog box, enter the name as **Subscription-Alpha**, click Collector Initiated, and click Select Computers.
5. In the Computers dialog box, click Add Domain Computers.
6. In the Select Computer dialog box, type SYD-A, click Check Names, and click OK.
7. Verify that the Computers dialog box matches Figure 10-40 and click Test.



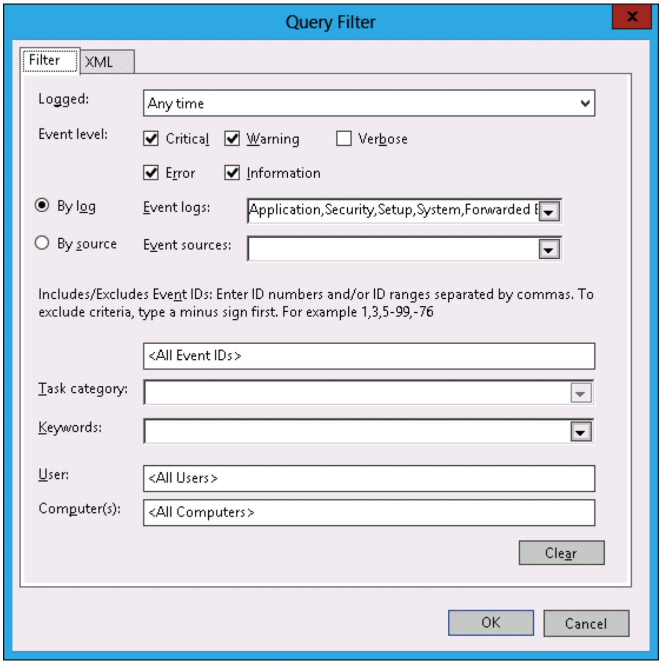
Computers

Computers (1):

Name
SYD-A.contoso.com

FIGURE 10-40 Computers dialog box

8. In the Event Viewer dialog box, click OK.
9. In the Computers dialog box, click OK.
10. Click Select Events.
11. In the Query Filter dialog box, select Critical, Error, Warning, and Information.
12. Click the Event Logs drop-down menu and click Windows Logs.
13. Verify that the Query Filter appears the same as Figure 10-41 and click OK.



Query Filter

Filter | XML

Logged: Any time

Event level: ☑ Critical ☑ Warning □ Verbose

☑ Error ☑ Information

● By log Event logs: Application,Security,Setup,System,Forwarded E

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

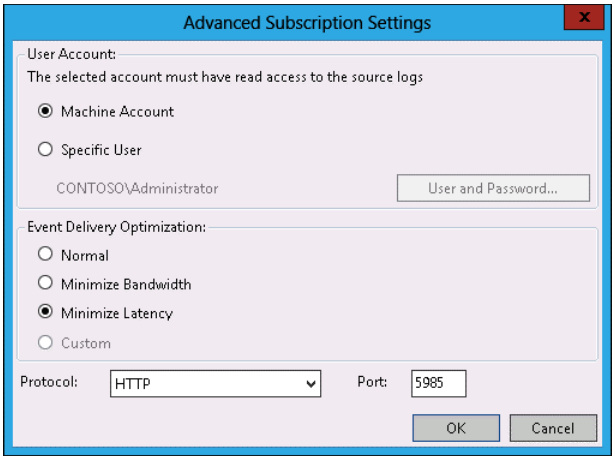
User: <All Users>

Computer(s): <All Computers>

FIGURE 10-41 The Query Filter dialog box

14. In the Subscription Properties dialog box, click Advanced.

15. In the Advanced Subscription Settings dialog box, click Minimize Latency, as shown in Figure 10-42, and click OK.



Advanced Subscription Settings

User Account:

The selected account must have read access to the source logs

● Machine Account

○ Specific User

CONTOSO\Administrator

Event Delivery Optimization:

○ Normal

○ Minimize Bandwidth

● Minimize Latency

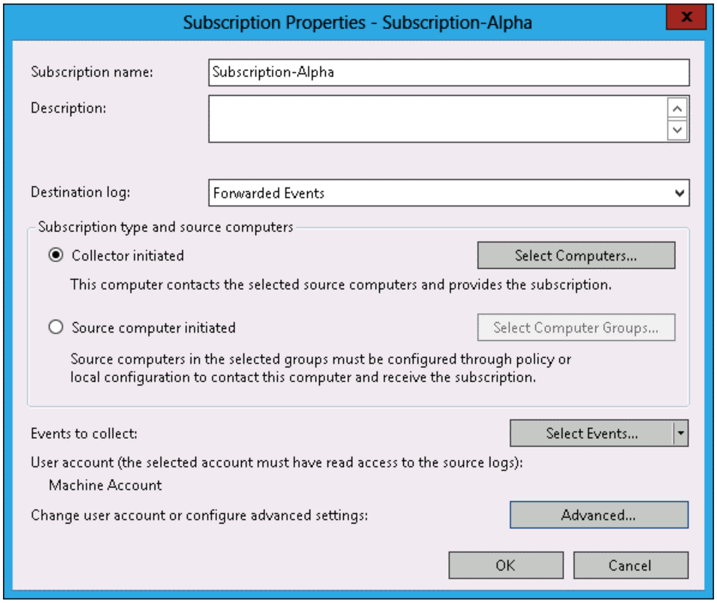
○ Custom

Protocol: HTTP

Port: 5985

FIGURE 10-42 Advanced Subscription Settings dialog box

16. Verify that the Subscription Properties – Subscription-Alpha dialog box matches Figure 10-43 and then click OK.



Subscription Properties - Subscription-Alpha

Subscription name: Subscription-Alpha

Description:

Destination log: Forwarded Events

Subscription type and source computers

● Collector initiated

This computer contacts the selected source computers and provides the subscription.

○ Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

User account (the selected account must have read access to the source logs):

Machine Account

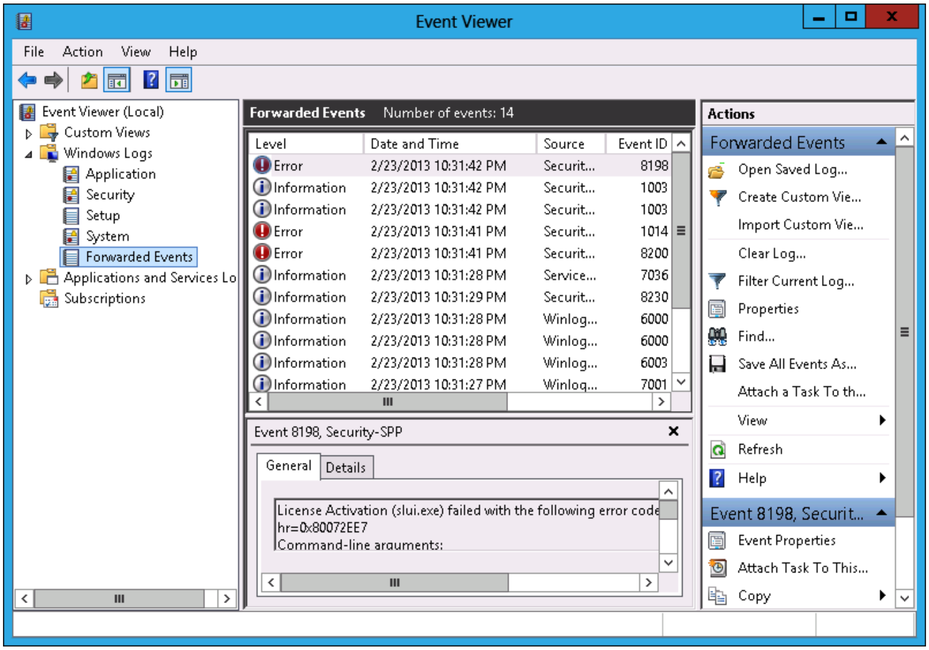
Change user account or configure advanced settings:

FIGURE 10-43 Subscription Properties dialog box

17. Restart server SYD-A.

18. Expand the Windows Logs node and click Forwarded Events.

19. Verify the presence of items in the event log, as shown in Figure 10-44.



Level	Date and Time	Source	Event ID
Error	2/23/2013 10:31:42 PM	Securit...	8198
Information	2/23/2013 10:31:42 PM	Securit...	1003
Information	2/23/2013 10:31:42 PM	Securit...	1003
Error	2/23/2013 10:31:41 PM	Securit...	1014
Error	2/23/2013 10:31:41 PM	Securit...	8200
Information	2/23/2013 10:31:28 PM	Service...	7036
Information	2/23/2013 10:31:29 PM	Securit...	8230
Information	2/23/2013 10:31:28 PM	Winlog...	6000
Information	2/23/2013 10:31:28 PM	Winlog...	6000
Information	2/23/2013 10:31:28 PM	Winlog...	6003
Information	2/23/2013 10:31:27 PM	Winlog...	7001

License Activation (slui.exe) failed with the following error code
hr=0x80072EE7
Command-line arguments:

FIGURE 10-44 Event log

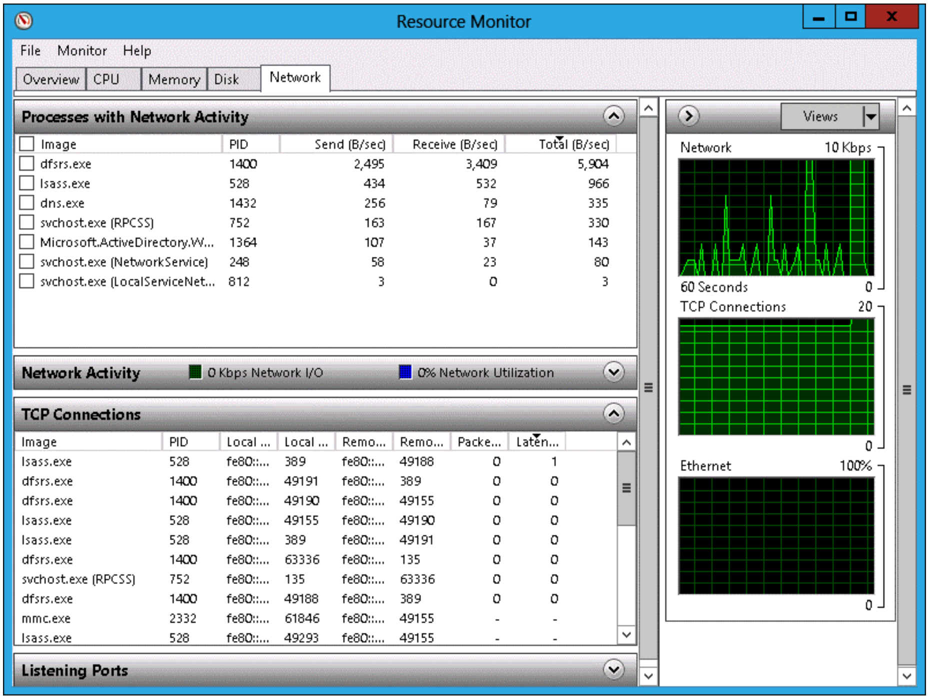
20. Close Event Viewer.

EXERCISE 6 Configure network monitoring

In this exercise, you will monitor the processes and services that use network interfaces. To complete this exercise, perform the following steps:

1. On the Tools menu of the Server Manager console on DC, click Resource Monitor.

2. On the Network tab, click the arrow next to TCP Connections, as shown in Figure 10-45.



Processes with Network Activity

Image	PID	Send (B/sec)	Receive (B/sec)	Total (B/sec)
□ dfsrs.exe	1400	2,495	3,409	5,904
□ lsass.exe	528	434	532	966
□ dns.exe	1432	256	79	335
□ svchost.exe (RPCSS)	752	163	167	330
□ Microsoft.ActiveDirectory.W...	1364	107	37	143
□ svchost.exe (NetworkService)	248	58	23	80
□ svchost.exe (LocalServiceNet...	812	3	0	3

Network Activity 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

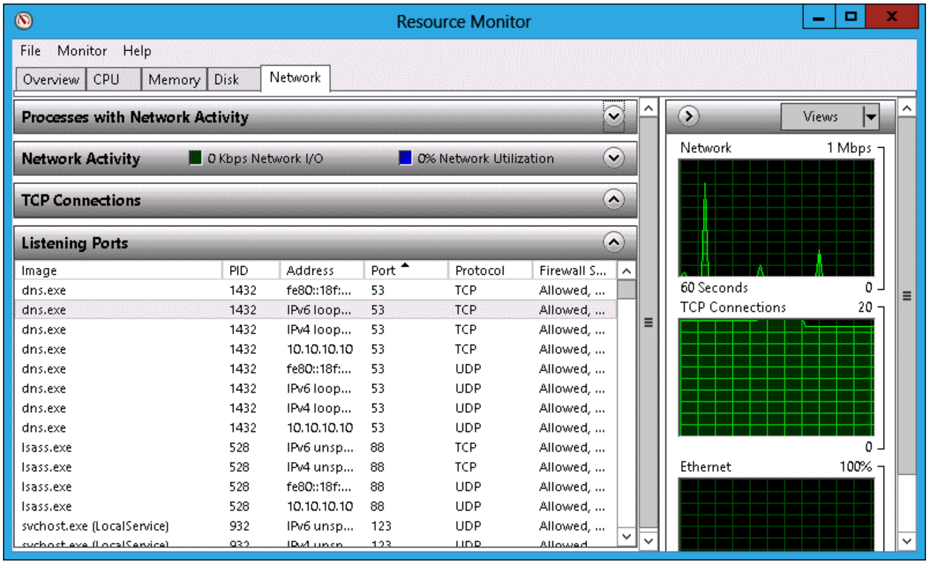
TCP Connections

Image	PID	Local ...	Local ...	Remo...	Remo...	Packe...	Laten...
lsass.exe	528	fe80::...	389	fe80::...	49188	0	1
dfsrs.exe	1400	fe80::...	49191	fe80::...	389	0	0
dfsrs.exe	1400	fe80::...	49190	fe80::...	49155	0	0
lsass.exe	528	fe80::...	49155	fe80::...	49190	0	0
lsass.exe	528	fe80::...	389	fe80::...	49191	0	0
dfsrs.exe	1400	fe80::...	63336	fe80::...	135	0	0
svchost.exe (RPCSS)	752	fe80::...	135	fe80::...	63336	0	0
dfsrs.exe	1400	fe80::...	49188	fe80::...	389	0	0
mmc.exe	2332	fe80::...	61846	fe80::...	49155	-	-
lsass.exe	528	fe80::...	49293	fe80::...	49155	-	-

Listening Ports

FIGURE 10-45 Network tab of the Resource Monitor

3. Click the arrow next to Listening Ports to list the ports on which different services are listening (see Figure 10-46).



Processes with Network Activity

Network Activity 🟩 0 Kbps Network I/O 🟦 0% Network Utilization

TCP Connections

Listening Ports

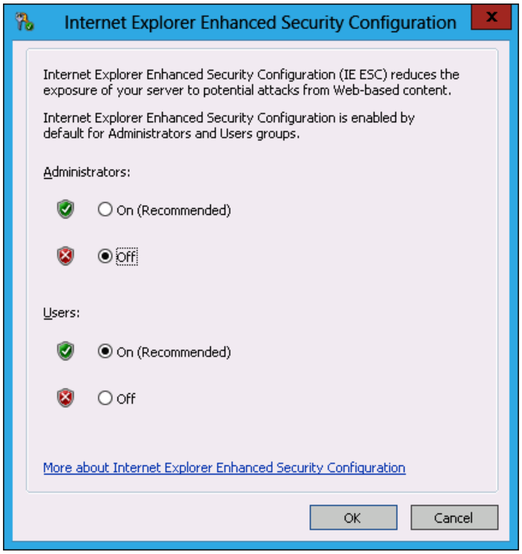
Image	PID	Address	Port	Protocol	Firewall S...
dns.exe	1432	fe80::18f:...	53	TCP	Allowed, ...
dns.exe	1432	IPv6 loop...	53	TCP	Allowed, ...
dns.exe	1432	IPv4 loop...	53	TCP	Allowed, ...
dns.exe	1432	10.10.10.10	53	TCP	Allowed, ...
dns.exe	1432	fe80::18f:...	53	UDP	Allowed, ...
dns.exe	1432	IPv6 loop...	53	UDP	Allowed, ...
dns.exe	1432	IPv4 loop...	53	UDP	Allowed, ...
dns.exe	1432	10.10.10.10	53	UDP	Allowed, ...
lsass.exe	528	IPv6 unsp...	88	TCP	Allowed, ...
lsass.exe	528	IPv4 unsp...	88	TCP	Allowed, ...
lsass.exe	528	fe80::18f:...	88	UDP	Allowed, ...
lsass.exe	528	10.10.10.10	88	UDP	Allowed, ...
svchost.exe (LocalService)	932	IPv6 unsp...	123	UDP	Allowed, ...
svchost.exe (LocalService)	932	IPv4 unsp...	123	UDP	Allowed, ...

FIGURE 10-46 Listing the different ports.

EXERCISE 7 Using Message Analyzer

In this exercise, you use Message Analyzer to perform network monitoring. This exercise requires that you have downloaded Message Analyzer from the Microsoft website and installed it on SYD-A, but have not run the program yet. To complete this exercise, perform the following steps:

1. In Server Manager on SYD-A, click Local Server and then select IE Enhanced Security Configuration.
2. In the Internet Explorer Enhanced Security Configuration dialog box, set the Administrators setting to Off, as shown in Figure 10-47, and click OK.



Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

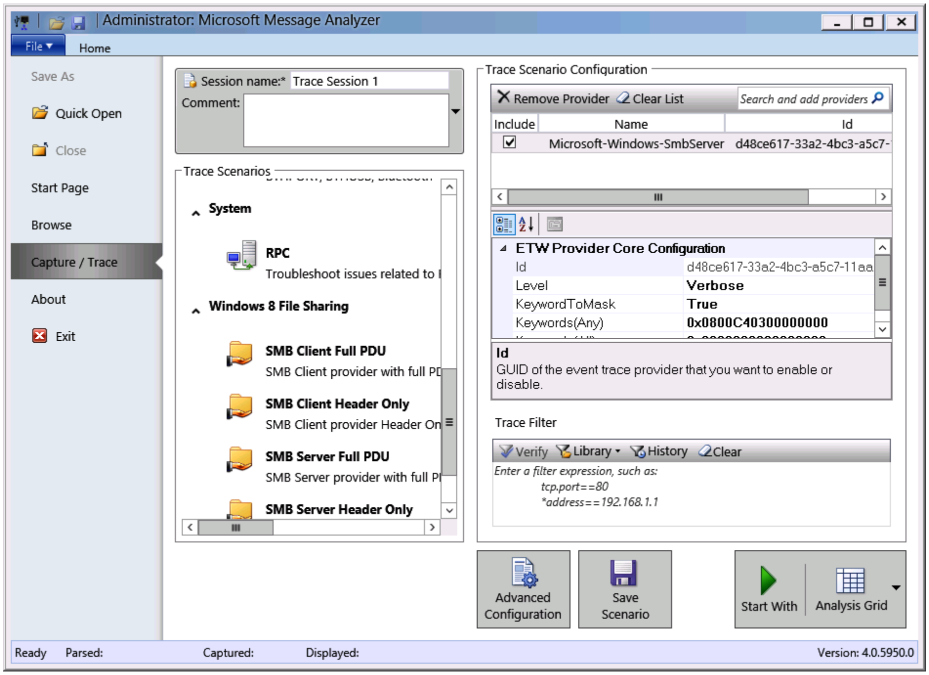
● On (Recommended)

○ Off

More about Internet Explorer Enhanced Security Configuration

FIGURE 10-47 Internet Explorer security

3. In the Search charm on SYD-A, type **Microsoft Message Analyzer**.
4. Click Microsoft Message Analyzer in the results list.
5. On the File menu, click SMB Server Full PDU on the Capture/Trace option, as shown in Figure 10-48, and click Start With.



Session name:* Trace Session 1

Comment:

System

RPC
Troubleshoot issues related to I

Windows 8 File Sharing

SMB Client Full PDU
SMB Client provider with full PD

SMB Client Header Only
SMB Client provider Header On

SMB Server Full PDU
SMB Server provider with full PI

SMB Server Header Only

Include	Name	Id
☑	Microsoft-Windows-SmbServer	d48ce617-33a2-4bc3-a5c7-

ETW Provider Core Configuration

Id	d48ce617-33a2-4bc3-a5c7-11aa
Level	Verbose
KeywordToMask	True
Keywords(Any)	0x0800C40300000000

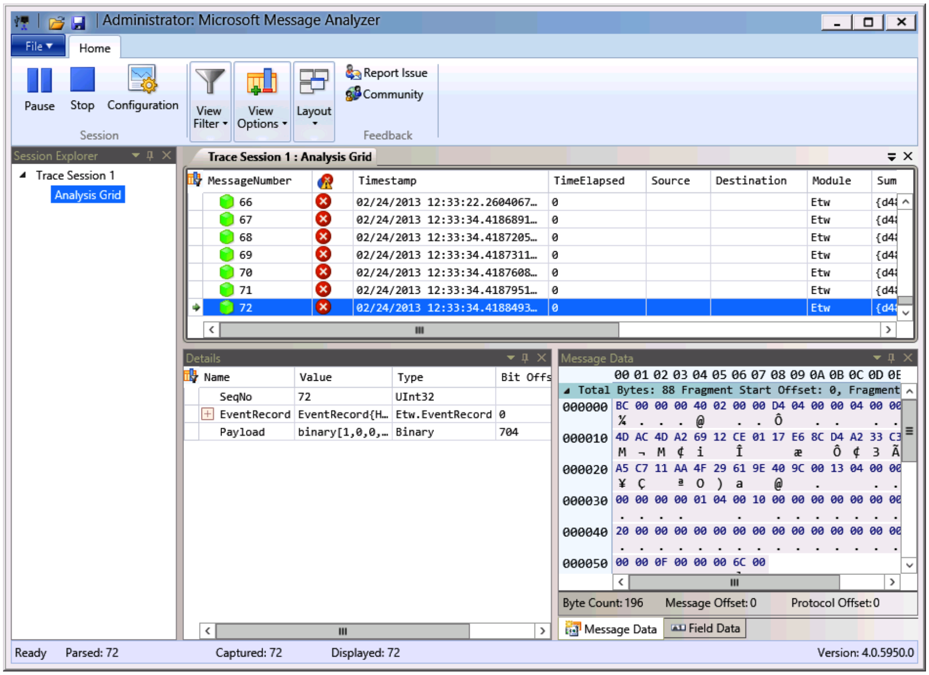
Id
GUID of the event trace provider that you want to enable or disable.

Enter a filter expression, such as:
tcp.port==80
**address==192.168.1.1*

Ready Parsed: Captured: Displayed: Version: 4.0.5950.0

FIGURE 10-48 SMB Server Full PDU

6. On the taskbar, click File Explorer.
7. In File Explorer, click Computer and then double-click Local Disk (C:).
8. On the title bar, click New Folder. Name the new folder **TEST**.
9. Right-click the TEST folder, click Share With, and click Specific People.
10. In the File Sharing dialog box, click Share and then click Done.
11. In Microsoft Message Analyzer, verify that messages have been recorded and click the final message, as shown in Figure 10-49.



MessageNumber		Timestamp	TimeElapsed	Source	Destination	Module	Sum
66	☒	02/24/2013 12:33:22.2604067…	0			Etw	{d4
67	☒	02/24/2013 12:33:34.4186891…	0			Etw	{d4
68	☒	02/24/2013 12:33:34.4187205…	0			Etw	{d4
69	☒	02/24/2013 12:33:34.4187311…	0			Etw	{d4
70	☒	02/24/2013 12:33:34.4187608…	0			Etw	{d4
71	☒	02/24/2013 12:33:34.4187951…	0			Etw	{d4
72	☒	02/24/2013 12:33:34.4188493…	0			Etw	{d4

Name	Value	Type	Bit Offs
SeqNo	72	UInt32	
EventRecord	EventRecord{H…	Etw.EventRecord	0
Payload	binary[1,0,0,…	Binary	704

```
       00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E
◢ Total Bytes: 88 Fragment Start Offset: 0, Fragment
000000 BC 00 00 00 40 02 00 00 D4 04 00 00 04 00 00
       ¼  .  .  .  @     .  .  Ô     .  .     .  .
000010 4D AC 4D A2 69 12 CE 01 17 E6 8C D4 A2 33 C3
       M  ¬  M  ¢  i     Î        æ     Ô  ¢  3  Ã
000020 A5 C7 11 AA 4F 29 61 9E 40 9C 00 13 04 00 00
       ¥  Ç     ª  O  )  a     @     .        .  .
000030 00 00 00 00 01 04 00 10 00 00 00 00 00 00 00
       .  .  .  .        .     .  .  .  .  .  .  .
000040 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00
       .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
000050 00 00 0F 00 00 00 6C 00
```

Byte Count: 196 Message Offset: 0 Protocol Offset: 0

Ready Parsed: 72 Captured: 72 Displayed: 72 Version: 4.0.5950.0

FIGURE 10-49 Verifying that messages have been recorded

12. Use File Explorer to navigate to C:\TEST.

13. Create a text file in C:\TEST named **secretfile.txt**. The content of the file should be the words “secret secret”.

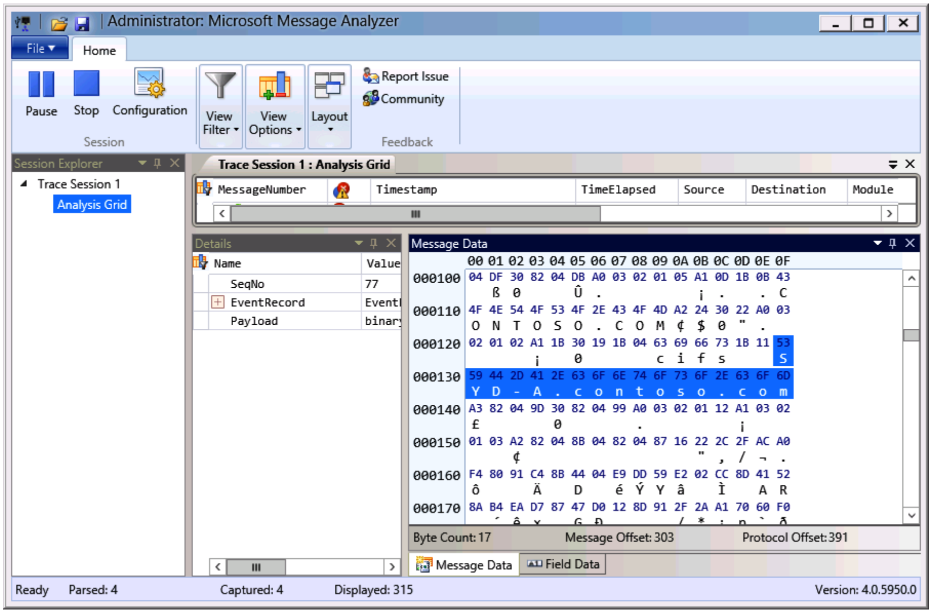
14. Switch to DC.

15. On DC, in the Search charm, type **\\SYD-A\TEST\secretfile.txt** and click secretfile.txt in the Results pane.

16. Switch to SYD-A.

17. Verify that additional traffic has been recorded.

18. Examine the message data for network addresses, such as server SYD-A.contoso.com (see Figure 10-50).



MessageNumber		Timestamp	TimeElapsed	Source	Destination	Module

Name	Value
SeqNo	77
EventRecord	Event
Payload	binary

```
       00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
000100 04 DF 30 82 04 DB A0 03 02 01 05 A1 0D 1B 0B 43
          ß  0        Û  .              ¡  .     .  C
000110 4F 4E 54 4F 53 4F 2E 43 4F 4D A2 24 30 22 A0 03
       O  N  T  O  S  O  .  C  O  M  ¢  $  0  "  .
000120 02 01 02 A1 1B 30 19 1B 04 63 69 66 73 1B 11 53
                ¡     0           c  i  f  s        S
000130 59 44 2D 41 2E 63 6F 6E 74 6F 73 6F 2E 63 6F 6D
       Y  D  -  A  .  c  o  n  t  o  s  o  .  c  o  m
000140 A3 82 04 9D 30 82 04 99 A0 03 02 01 12 A1 03 02
       £           0           .              ¡
000150 01 03 A2 82 04 8B 04 82 04 87 16 22 2C 2F AC A0
             ¢                          "  ,  /  ¬  .
000160 F4 80 91 C4 8B 44 04 E9 DD 59 E2 02 CC 8D 41 52
       ô        Ä     D     é  Ý  Y  â     Ì     A  R
000170 8A B4 EA D7 87 47 D0 12 8D 91 2F 2A A1 70 60 F0
          ´  ê  ×     G  Ð           /  *  :  p  `  ð
```

Byte Count: 17 Message Offset: 303 Protocol Offset: 391

Ready Parsed: 4 Captured: 4 Displayed: 315 Version: 4.0.5950.0

FIGURE 10-50 Examining message data

19. Close Microsoft Message Analyzer.

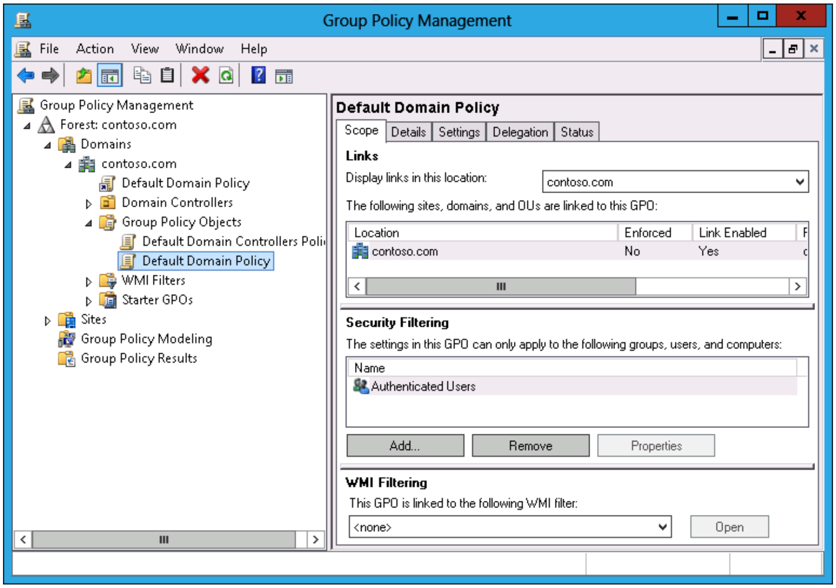
20. When prompted to save the captured trace, click No.

EXERCISE 8 Configure removable device auditing

In this exercise, you will configure a GPO so that removable device usage is audited. To complete this exercise, perform the following steps:

1. On DC, click Group Policy Management in the Tools menu of Server Manager.

2. **Expand Forest:** contoso.com\Domains\contoso.com\Group Policy Objects and click Default Domain Policy, as shown in Figure 10-51.



- Group Policy Management
  - Forest: contoso.com
    - Domains
      - contoso.com
        - Default Domain Policy
        - Domain Controllers
        - Group Policy Objects
          - Default Domain Controllers Poli
          - Default Domain Policy
        - WMI Filters
        - Starter GPOs
    - Sites
    - Group Policy Modeling
    - Group Policy Results

Default Domain Policy

Links

Display links in this location: contoso.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	F
contoso.com	No	Yes	c

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

WMI Filtering

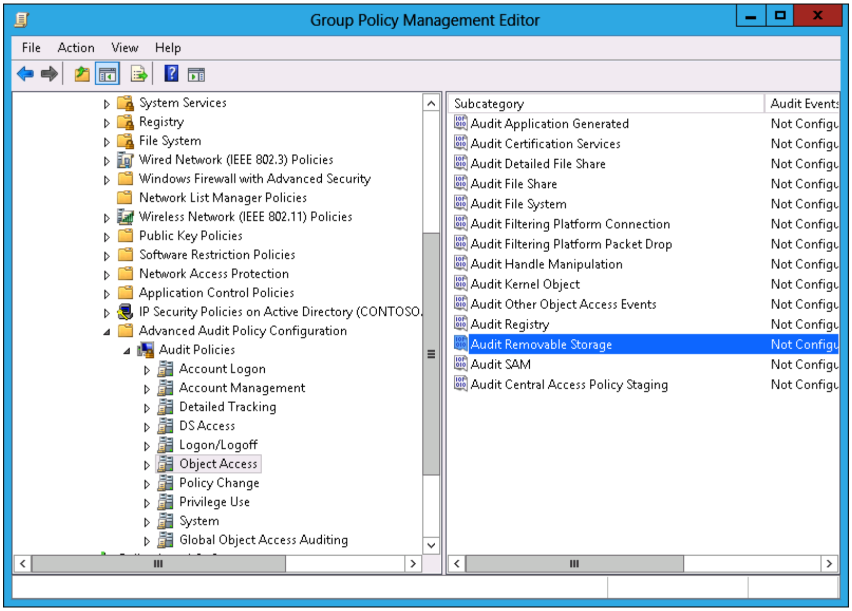
This GPO is linked to the following WMI filter:

<none>

FIGURE 10-51 Clicking Default Domain Policy

3. On the Action menu, click Edit.

4. In the GPME, navigate to the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access node and click Audit Removable Storage, as shown in Figure 10-52.



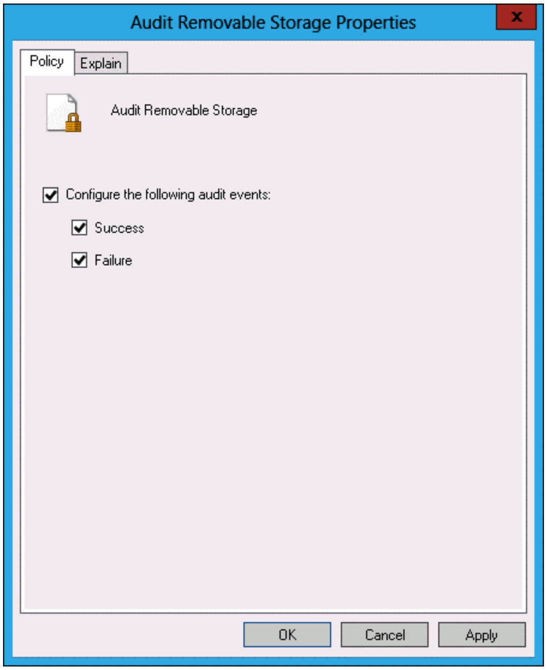
- System Services
- Registry
- File System
- Wired Network (IEEE 802.3) Policies
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
- Software Restriction Policies
- Network Access Protection
- Application Control Policies
- IP Security Policies on Active Directory (CONTOSO.
- Advanced Audit Policy Configuration
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing

Subcategory	Audit Events
Audit Application Generated	Not Configu
Audit Certification Services	Not Configu
Audit Detailed File Share	Not Configu
Audit File Share	Not Configu
Audit File System	Not Configu
Audit Filtering Platform Connection	Not Configu
Audit Filtering Platform Packet Drop	Not Configu
Audit Handle Manipulation	Not Configu
Audit Kernel Object	Not Configu
Audit Other Object Access Events	Not Configu
Audit Registry	Not Configu
Audit Removable Storage	Not Configu
Audit SAM	Not Configu
Audit Central Access Policy Staging	Not Configu

FIGURE 10-52 Clicking Audit Removable Storage

5. Double-click Audit Removable Storage.

6. In the Audit Removable Storage Properties dialog box, select Configure The Following Audit Events, Success, and Failure; then click OK (see Figure 10-53).



Audit Removable Storage

☑ Configure the following audit events:

☑ Success

☑ Failure

FIGURE 10-53 Auditing properties

7. Close the GPME.

8. On the taskbar, click Windows PowerShell.

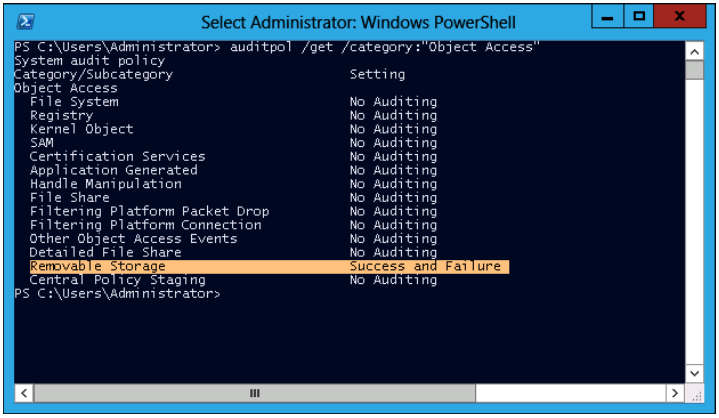
9. In the Windows PowerShell window, type the following command and press Enter:

```
Gpupdate /force
```

10. In the Windows PowerShell window, type the following command and press Enter:

```
Auditpol /get /category:"Object Access"
```

11. Verify that Removable Storage is configured for Success And Failure auditing, as shown in Figure 10-54.



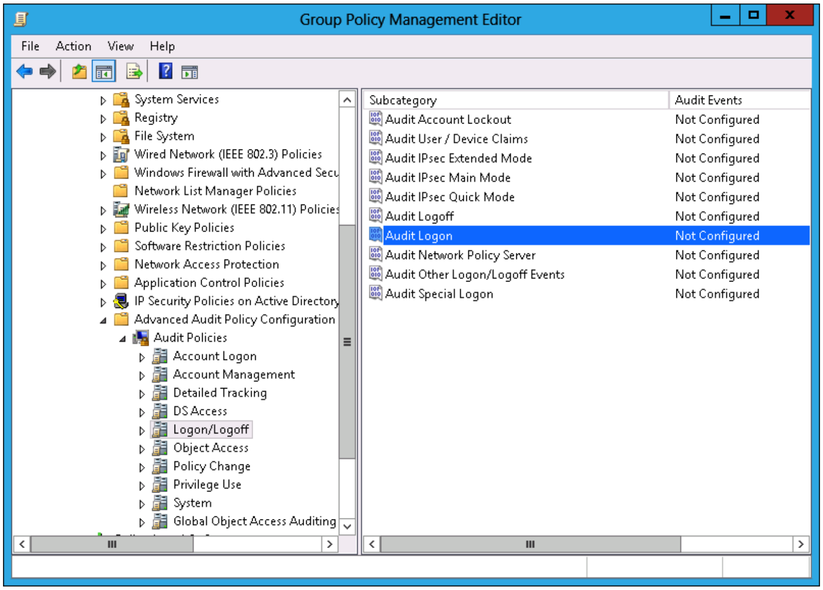
```
PS C:\Users\Administrator> auditpol /get /category:"Object Access"
System audit policy
Category/Subcategory                      Setting
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
  File Share                              No Auditing
  Filtering Platform Packet Drop          No Auditing
  Filtering Platform Connection           No Auditing
  Other Object Access Events              No Auditing
  Detailed File Share                     No Auditing
  Removable Storage                       Success and Failure
  Central Policy Staging                  No Auditing
PS C:\Users\Administrator>
```

FIGURE 10-54 Configuring Removable Storage

EXERCISE 9 Configure logon auditing

In this exercise, you will configure logon auditing. To complete this exercise, perform the following steps:

1. In the Group Policy Management Console (GPMC) on DC, right-click the Default Domain Policy and click Edit.
2. In the GPME, navigate to the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff and click Audit Logon, as shown in Figure 10-55.

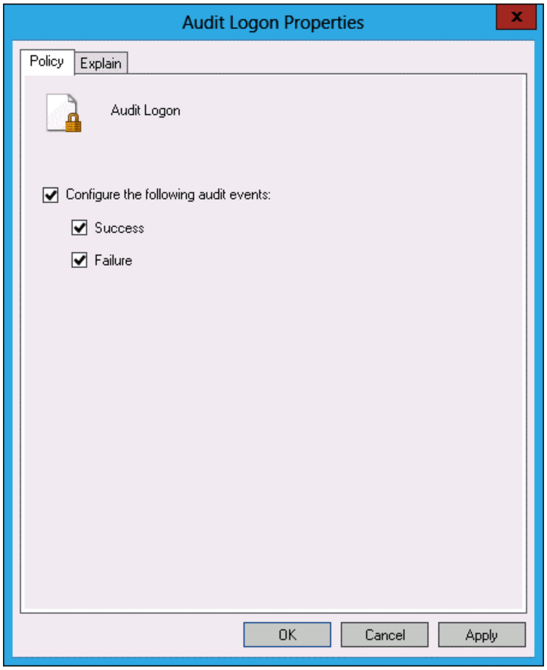

Group Policy Management Editor
File
Action
View
Help
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Not Configured
Audit Logon	Not Configured
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

FIGURE 10-55 Selecting Audit Logon

3. On the Action menu, click Properties.

4. In the Audit Logon Properties dialog box, select Configure The Following Audit Events, Success, and Failure (see Figure 10-56). Click OK.



☑ Configure the following audit events:

☑ Success

☑ Failure

FIGURE 10-56 Setting audit properties

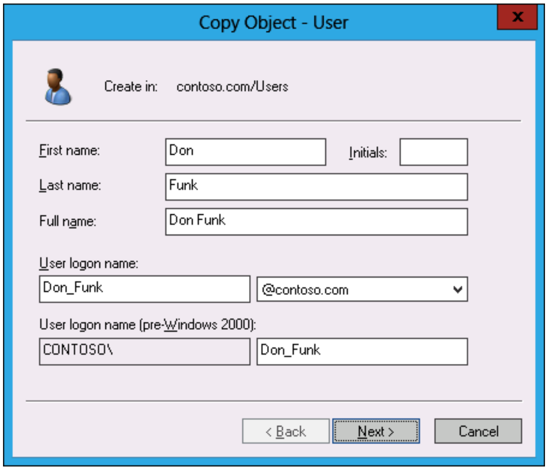
5. Close the GPME.

6. In the Tools menu of the Server Manager console, click Active Directory Users And Computers.

7. In Active Directory Users And Computers, select Users and then click Administrator.

8. On the Action menu, click Copy.

9. In the Copy Object – User dialog box, configure the following information, as shown in Figure 10-57, and click Next.
   - First Name: Don
   - Last Name: Funk
   - User Logon Name: Don_Funk



Copy Object - User

Create in: contoso.com/Users

First name: Don

Initials:

Last name: Funk

Full name: Don Funk

User logon name:

Don_Funk @contoso.com

User logon name (pre-Windows 2000):

CONTOSO\ Don_Funk

FIGURE 10-57 Setting copy object data

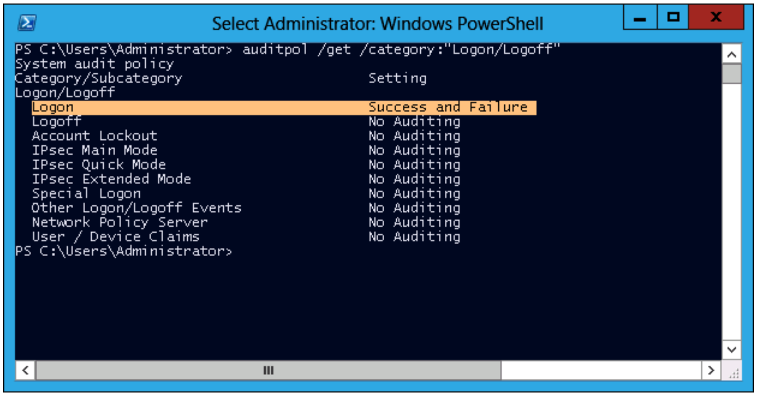
10. Enter **Pa$$w0rd** in the Password and Confirm Password text boxes, click Next, and click Finish.
11. Close Active Directory Users And Computers.
12. In Windows PowerShell, enter the following command and press Enter:

```
Gpupdate /force
```

13. In Windows PowerShell, enter the following command and press Enter:

```
Auditpol /get /category:"Logon/Logoff"
```

14. Verify that Logon is configured for Success And Failure auditing, as shown in Figure 10-58.



Select Administrator: Windows PowerShell

```
PS C:\Users\Administrator> auditpol /get /category:"Logon/Logoff"
System audit policy
Category/Subcategory                      Setting
Logon/Logoff
  Logon                                   Success and Failure
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
PS C:\Users\Administrator>
```

FIGURE 10-58 Logon for Success And Failure auditing

15. Switch to SYD-A.

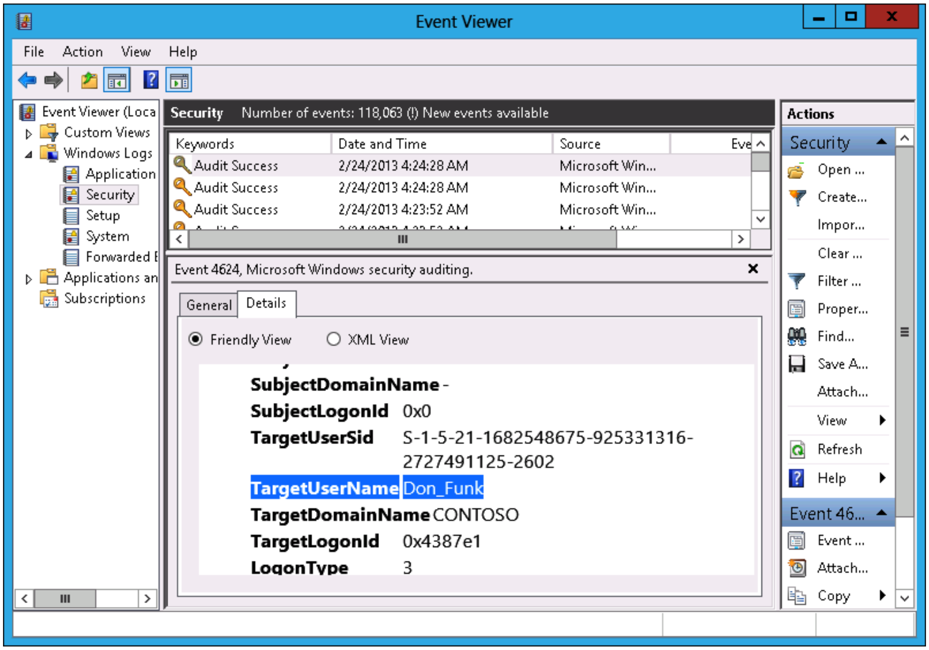
16. Sign out and sign on as contoso\don_funk with the password **Pa$$w0rd**.

17. Switch to DC.

18. On the Tools menu of the Server Manager console, click Event Viewer.

19. Expand Windows Logs\Security Logs and click the most recent event with Event ID 4624.

20. Click the Details pane and verify that the TargetUserName Don_Funk is listed, as shown in Figure 10-59. You may need to scroll through several events to find this TargetUserName.



Security Number of events: 118,063 (!) New events available

Keywords	Date and Time	Source	Eve
Audit Success	2/24/2013 4:24:28 AM	Microsoft Win...	
Audit Success	2/24/2013 4:24:28 AM	Microsoft Win...	
Audit Success	2/24/2013 4:23:52 AM	Microsoft Win...	

Event 4624, Microsoft Windows security auditing.

General | Details

● Friendly View ○ XML View

SubjectDomainName -
SubjectLogonId 0x0
TargetUserSid S-1-5-21-1682548675-925331316-2727491125-2602
TargetUserName Don_Funk
TargetDomainName CONTOSO
TargetLogonId 0x4387e1
LogonType 3

FIGURE 10-59 TargetUserName Don_Funk

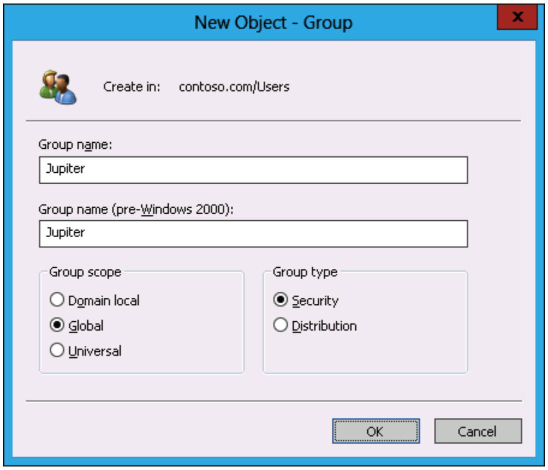
EXERCISE 10 Configure expression-based audit policies

In this exercise, you will configure expression-based audit policies in Group Policy. To complete this exercise, perform the following steps:

1. On DC, open Active Directory Users And Computers from the Tools menu of the Server Manager console.

2. Right-click the Users container, click New, and click Group.

3. In the New Object – Group dialog box, enter the name **Jupiter**, as shown in Figure 10-60, and click OK.


New Object - Group

Create in: contoso.com/Users

Group name:
Jupiter

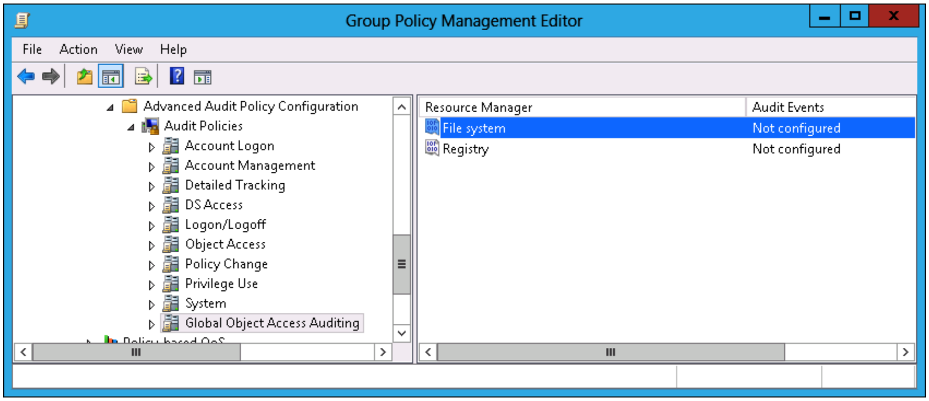
Group name (pre-Windows 2000):
Jupiter

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

FIGURE 10-60 Entering the group name

4. Right-click the Users container, click New, and click Group.
5. In the New Object – Group dialog box, enter the name **Saturn** and click OK.
6. Right-click the Users container, click New, and click Group.
7. In the New Object – Group dialog box, enter the name **Neptune** and click OK.
8. Right-click the Users container, click New, and click Group.
9. In the New Object – Group dialog box, enter the name **Mars** and click OK.
10. Close Active Directory Users And Computers.
11. In the GPMC, right-click Default Domain Policy and click Edit.
12. In the GPME, navigate to the Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Global Object Access Auditing and click File System, as shown in Figure 10-61.



- Advanced Audit Policy Configuration
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing
- Policy-based QoS

Resource Manager	Audit Events
File system	Not configured
Registry	Not configured

FIGURE 10-61 Selecting File System

13. On the Action menu, click Properties.

14. In the File System Properties dialog box, click Define This Policy Setting and click Configure.

15. In the Advanced Security Settings for Global File SACL dialog box, click Add.

16. In the Auditing Entry For Global File SACL dialog box, click Select A Principal Link.

17. In the Select User, Computer, Service Account, Or Group dialog box, type **Jupiter**, click Check Names, and click OK.

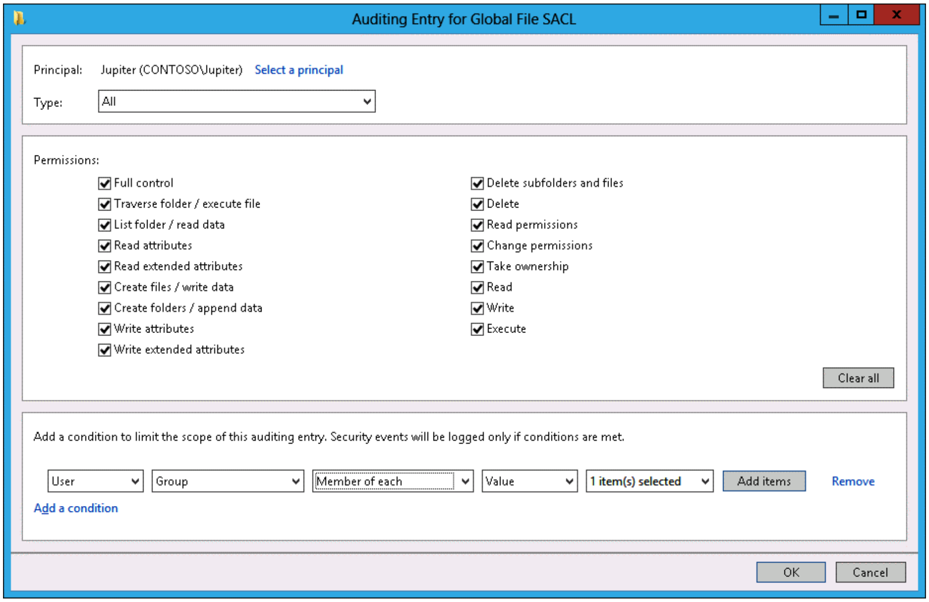
18. In the Type drop-down menu, click All.

19. Click the Add A Condition link.

20. Click the Add Items button.

21. In the Select User, Computer, Service Account, Or Group dialog box, type **Saturn**, click Check Names, and click OK.

22. Verify that the Auditing Entry For Global File SACL dialog box matches Figure 10-62 and click OK.



Principal: Jupiter (CONTOSO\Jupiter)

Type: All

Permissions:

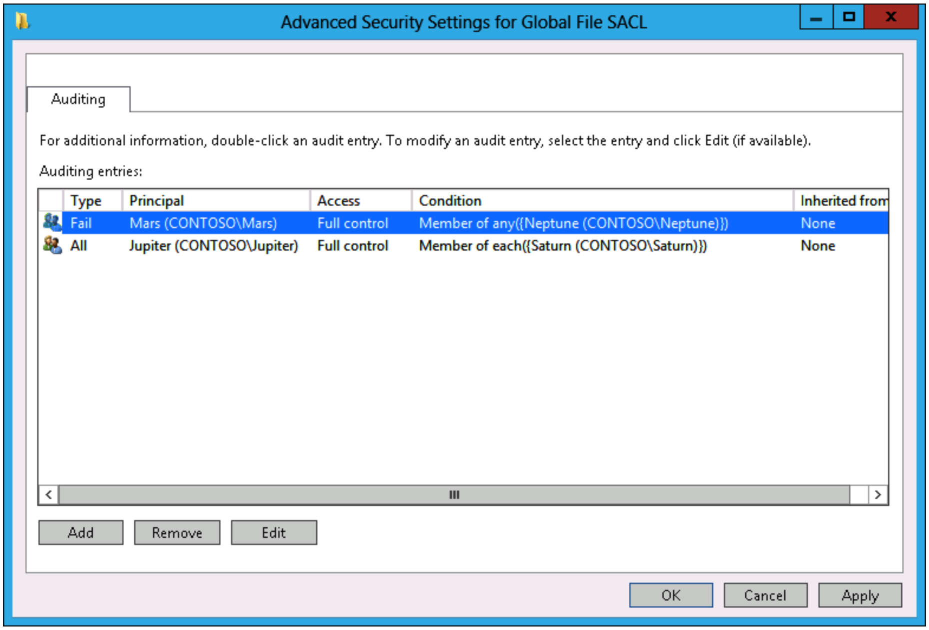
☑ Full control
☑ Traverse folder / execute file
☑ List folder / read data
☑ Read attributes
☑ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☑ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☑ Read permissions
☑ Change permissions
☑ Take ownership
☑ Read
☑ Write
☑ Execute

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

User | Group | Member of each | Value | 1 item(s) selected

FIGURE 10-62 Auditing the Entry For Global File SACL dialog box

23. In the Advanced Security Settings For Global File SACL dialog box, click Add.
24. In the Auditing Entry For Global File SACL dialog box, click Select A Principal link.
25. In the Select User, Computer, Service Account, Or Group dialog box, type **Mars**, click Check Names, and click OK.
26. Set the Type drop-down menu to Fail.
27. Click the Add A Condition link.
28. Click the Member Of Each drop down menu and select Not Member Of Any.
29. Click the Add Items button.
30. In the Select User, Computer, Service Account, Or Group dialog box, type **Neptune**, click Check Names, and click OK twice.
31. Verify that the Advanced Security Settings For Global File SACL dialog box matches Figure 10-63 and click OK.


Advanced Security Settings for Global File SACL

Auditing

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Condition	Inherited from
Fail	Mars (CONTOSO\Mars)	Full control	Member of any({Neptune (CONTOSO\Neptune)})	None
All	Jupiter (CONTOSO\Jupiter)	Full control	Member of each({Saturn (CONTOSO\Saturn)})	None

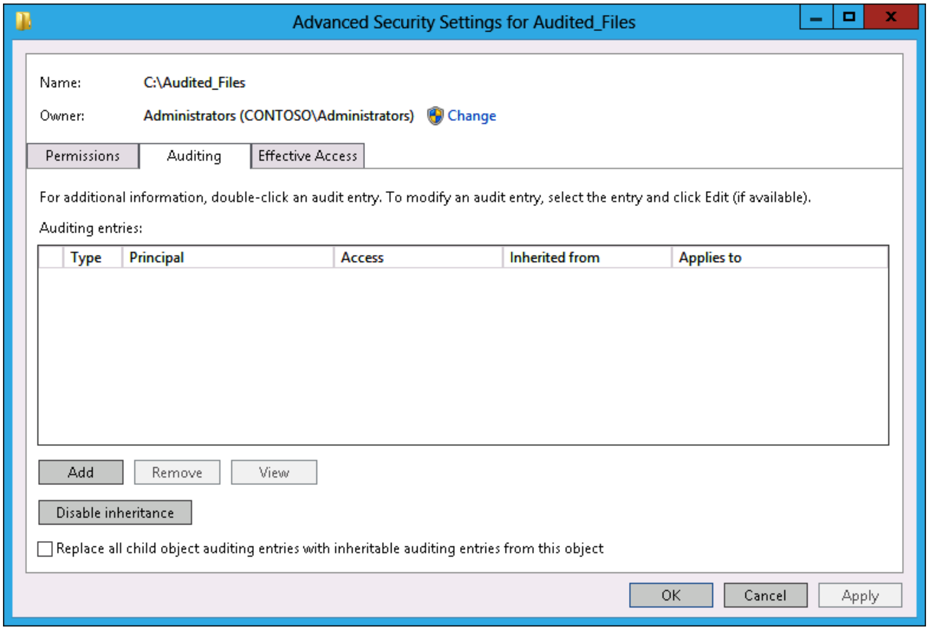
FIGURE 10-63 Advanced Security Settings For Global File SACL dialog box

32. Click OK to close the File System Properties dialog box and close the GPME.

EXERCISE 11 Configure folder auditing

In this exercise, you will configure expression-based audit policies at the folder level. To complete this exercise, perform the following steps:

1. Click File Explorer on the taskbar.
2. Click Computer and double-click Local Disk (C:).
3. On the title bar, click the New Folder icon.
4. Name the new folder **Audited_Files**.
5. Right-click the Audited_Files folder and click Properties.
6. On the Security tab, click Advanced.
7. On the Auditing tab of the Advanced Security Settings For Audited_Files dialog box, shown in Figure 10-64, click Add.


Advanced Security Settings for Audited_Files

Name: C:\Audited_Files

Owner: Administrators (CONTOSO\Administrators) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

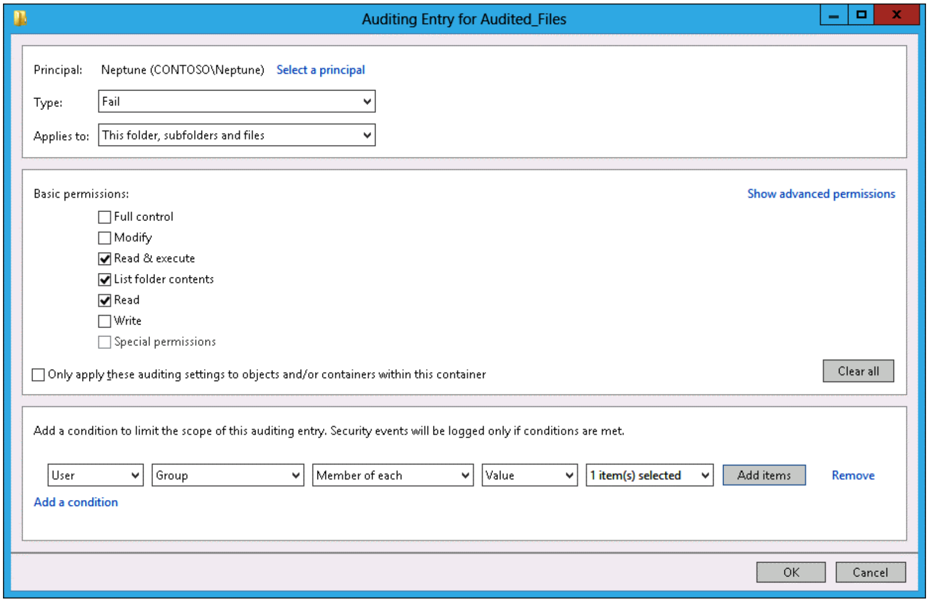
Auditing entries:

Type	Principal	Access	Inherited from	Applies to

□ Replace all child object auditing entries with inheritable auditing entries from this object

FIGURE 10-64 Auditing tab of the Advanced Security Settings For Audited_Files dialog box

8. In the Auditing Entry For Audited_Files dialog box, click Select A Principal link.
9. In the Select User, Computer, Service Account, Or Group dialog box, type **Neptune**, click Check Names, and click OK.
10. Change the type from Success to Fail.
11. Click the Add A Condition link.
12. Click the Add Items button.
13. In the Select User, Computer, Service Account, Or Group dialog box, type **Saturn**, click Check Names, and click OK.
14. Verify that the Auditing Entry For Audited Files dialog box matches Figure 10-65 and click OK.



Auditing Entry for Audited_Files

Principal: Neptune (CONTOSO\Neptune)

Type: Fail

Applies to: This folder, subfolders and files

Basic permissions:

☐ Full control
☐ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☐ Write
☐ Special permissions

☐ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

User | Group | Member of each | Value | 1 item(s) selected

FIGURE 10-65 Auditing Entry For Audited Files dialog box

15. Click OK twice to close all dialog boxes.

Suggested practice exercises

The following additional practice exercises are designed to give you more opportunities to practice what you've learned and to help you successfully master the lessons presented in this chapter.

- **Exercise 1** Use auditpol.exe to enable File System, Registry, and File Share Success And Failure auditing on SYD-A.
- **Exercise 2** Create a test share on DC and populate it with text files. Add user accounts to the Mars, Jupiter, Saturn, and Neptune groups. Sign on to SYD-A and access the files across the network using different accounts. Verify that the expression-based audit policies record auditing information appropriately.

Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct answer: C**
   - A. **Incorrect:** Resource Monitor enables you to view point in time resource utilization information. You can't use this tool to record resource utilization information for later review.
   - B. **Incorrect:** Task Manager does enable you to view resource utilization information, but you can't record that data for later review.
   - C. **Correct:** A data collector set can be used to capture performance counters and trace information related to resource utilization for later review.
   - D. **Incorrect:** Message Analyzer, the successor to Network Monitor, enables you to capture and analyze network traffic. Although it can capture and record network traffic, you can't use this tool to record processor and memory utilization information

2. **Correct answer: B**
   - A. **Incorrect:** Task Manager provides real-time information about network utilization, but doesn't provide information about port utilization and firewall configuration.
   - B. **Correct:** Resource Monitor provides information about services, the ports that they listen on, and firewall configuration.
   - C. **Incorrect:** Message Analyzer enables you to capture and analyze network traffic, but it can't be used to determine port utilization and associated firewall configuration.
   - D. **Incorrect:** A data collector set can record performance information and system trace information, but it can't be used to determine port utilization and associated firewall configuration.

3. **Correct answer: B**
   - A. **Incorrect:** A data collector set can be used to capture performance counters and trace information related to network traffic, but it can't be used to capture network traffic.
   - B. **Correct:** Message Analyzer, the successor to Network Monitor, enables you to capture and analyze network traffic.
   - C. **Incorrect:** Resource Monitor enables you to view point in time network utilization information. You can't use Resource Monitor to capture and analyze network traffic.
   - D. **Incorrect:** Task Manager does enable you to view network traffic, but doesn't enable you to capture and analyze that traffic.

4. **Correct answer: D**

   A. **Incorrect:** Members of the Backup Operators group are enabled to perform backups; they do not have access to the Security event log.

   B. **Incorrect:** The Power Users group is included for backward compatibility; members of this group do not have access to the Security event log.

   C. **Incorrect:** Although members of the Event Log Readers group have access to the other event logs, they don’t have access to the Security event log. Only members of the local Administrators group have access to the Security event log.

   D. **Correct:** When configuring event log subscriptions involving events in the Security event log, it is necessary to add the account of the collector computer to the local Administrators group on the source computer.

Lesson 2

1. **Correct answer: B**

   A. **Incorrect:** This command enables success and failure auditing for the File System subcategory.

   B. **Correct:** This command enables success and failure auditing for all subcategories under the Object Access category.

   C. **Incorrect:** This command disables success and failure auditing for all subcategories under the Object Access category.

   D. **Incorrect:** This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.

2. **Correct answer: A**

   A. **Correct:** This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.

   B. **Incorrect:** This command disables success and failure auditing for all subcategories under the Object Access category.

   C. **Incorrect:** This command enables success and failure auditing for all subcategories under the Object Access category.

   D. **Incorrect:** This command enables success and failure auditing for the File System subcategory.

3. **Correct answer: C**
    - **A. Incorrect:** This command enables success and failure auditing for all subcategories under the Object Access category.
    - **B. Incorrect:** This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.
    - **C. Correct:** This command enables success and failure auditing for the File System subcategory.
    - **D. Incorrect:** This command disables success and failure auditing for all subcategories under the Object Access category.
4. **Correct answer: A**
    - **A. Correct:** This command disables success and failure auditing for all subcategories under the Object Access category.
    - **B. Incorrect:** This command enables only failure auditing, not success auditing, for all subcategories under the Object Access category.
    - **C. Incorrect:** This command enables success and failure auditing for all subcategories under the Object Access category.
    - **D. Incorrect:** This command enables success and failure auditing for the File System subcategory.

Index

About the Author

ORIN THOMAS is an MVP, an MCT, and has a string of Microsoft MCSE and MCITP certifications. He has written more than 25 books for Microsoft Press and is a contributing editor at *Windows IT Pro* magazine. He has been working in IT since the early 1990s. He regularly speaks at events like TechED in Australia and around the world on Windows Server, Windows Client, System Center, and security topics. Orin founded and runs the Melbourne System Center Users Group. You can follow him on Twitter at *http://twitter.com/orinthomas*.

Training Guide: Administering Windows Server 2012 and Exam 70-411

The following is a list of 70-411 objectives and the mapping between those topics and the chapters in this book.

DEPLOY, MANAGE, AND MAINTAIN SERVERS	
Deploy and manage server images	Chapter 1, Lessons 1 and 2
Implement patch management	Chapter 1, Lesson 3
Monitor servers	Chapter 10, Lesson 1
CONFIGURE FILE AND PRINT SERVICES	
Configure Distributed File System (DFS)	Chapter 9, Lesson 2
Configure File Server Resource Manager (FSRM)	Chapter 9, Lesson 1
Configure file and disk encryption	Chapter 9, Lesson 3
Configure advanced audit policies	Chapter 10, Lesson 2
CONFIGURE NETWORK SERVICES AND ACCESS	
Configure DNS zones	Chapter 3, Lesson 2
Configure DNS records	Chapter 3, Lesson 3
Configure VPN and routing	Chapter 8, Lesson 2
Configure DirectAccess	Chapter 8, Lesson 3
CONFIGURE A NETWORK POLICY SERVER INFRASTRUCTURE	
Configure Network Policy Server (NPS)	Chapter 8, Lesson 1
Configure NPS policies	Chapter 7, Lesson 1
Configure Network Access Protection (NAP)	Chapter 7, Lessons 2 and 3
CONFIGURE AND MANAGE ACTIVE DIRECTORY	
Configure service authentication	Chapter 2, Lesson 3
Configure domain controllers	Chapter 4, Lesson 1
Maintain Active Directory	Chapter 4, Lessons 2 and 3
Configure account policies	Chapter 2, Lesson 2

CONFIGURE AND MANAGE GROUP POLICY	
Configure Group Policy processing	Chapter 5, Lesson 2
Configure Group Policy settings	Chapter 6, Lesson 1
Manage Group Policy objects (GPOs)	Chapter 5, Lesson 1
Configure Group Policy preferences	Chapter 6, Lesson 3

Exam Objectives The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at Microsoft's sole discretion. Please visit the Microsoft Learning website for the most current listing of exam objectives: *http://www.microsoft.com/learning/en/us/exam-70-411.aspx*.