Lesson 3: Monitoring Servers

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

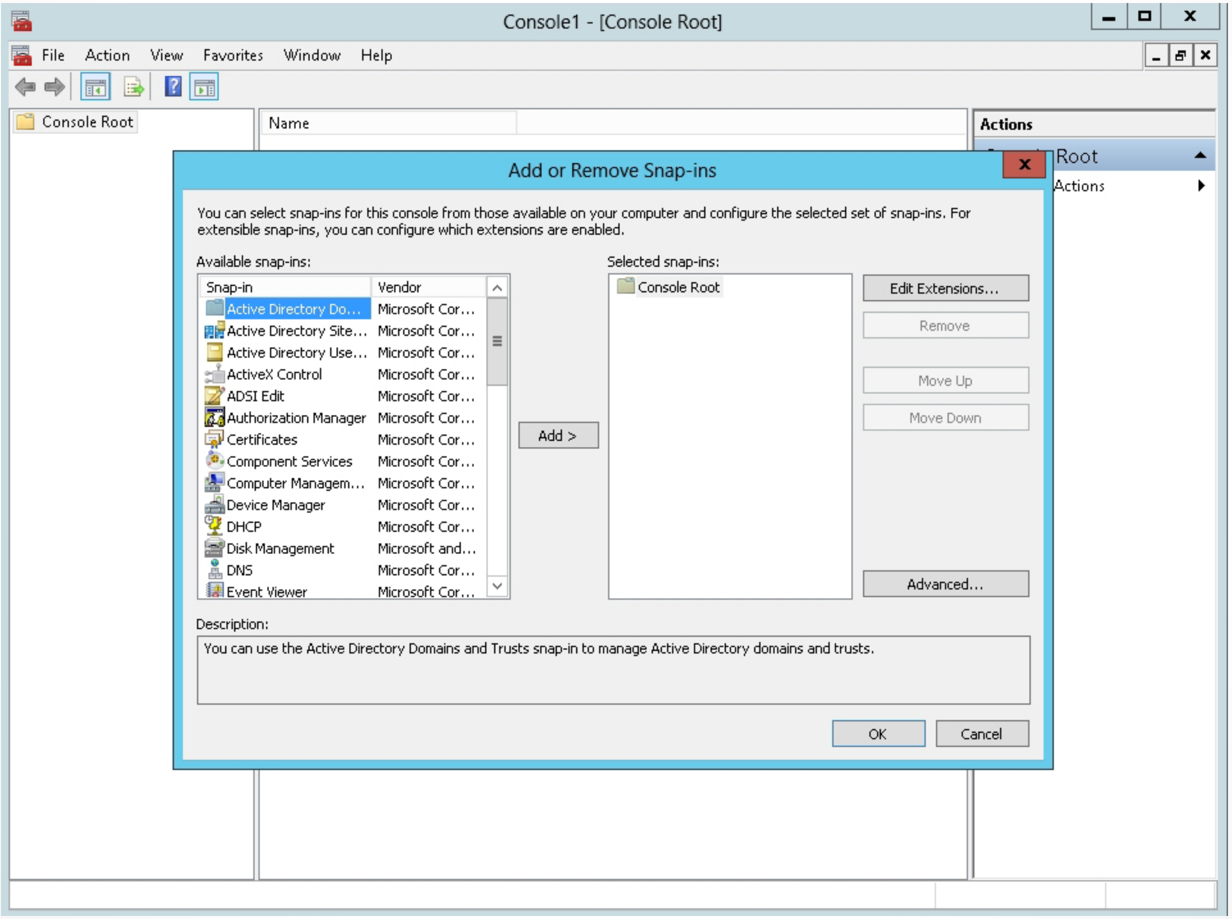
Overview

- Exam Objective 1.3: Monitor Servers
- Introducing the Microsoft Management Console (MMC)
- Using Event Viewer
- Using Reliability Monitor
- Managing Performance
- Monitoring the Network
- Monitoring Virtual Machines (VMs)

Introducing the Microsoft Management Console (MMC)

Lesson 3: Monitoring Servers

Microsoft Management Console (MMC)



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
DHCP	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...
Event Viewer	Microsoft Cor...

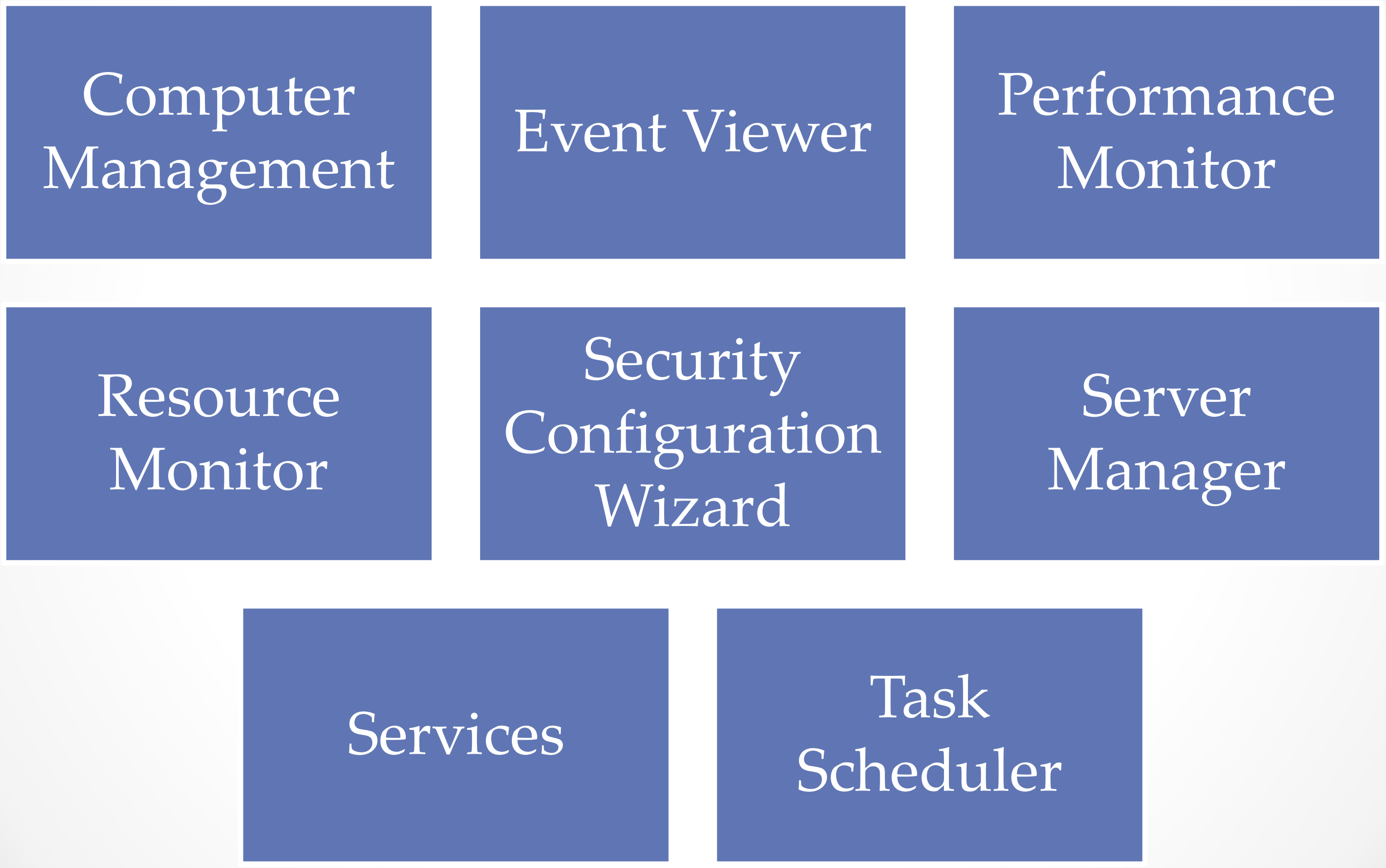
Selected snap-ins:

Console Root

Description:

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

Commonly Used Administrative Tools

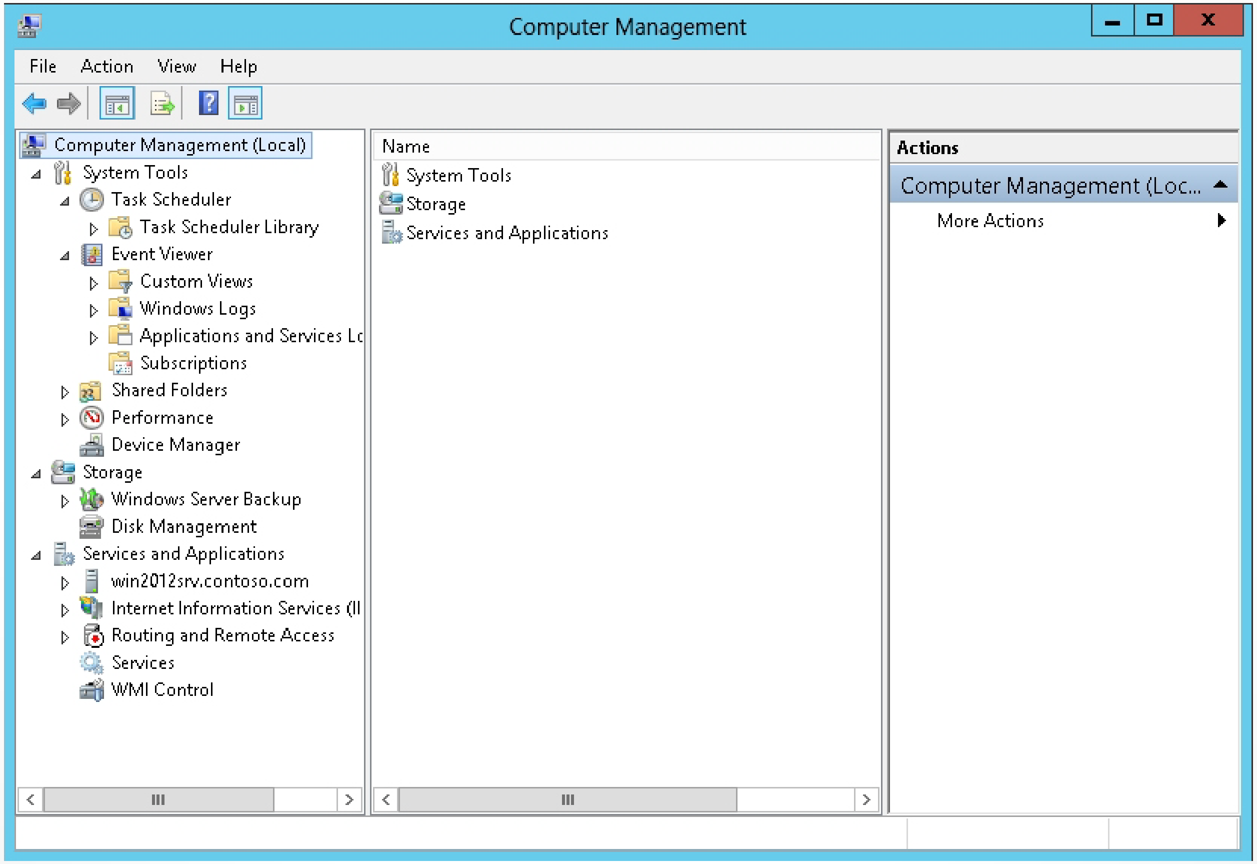


- Computer Management
- Event Viewer
- Performance Monitor
- Resource Monitor
- Security Configuration Wizard
- Server Manager
- Services
- Task Scheduler

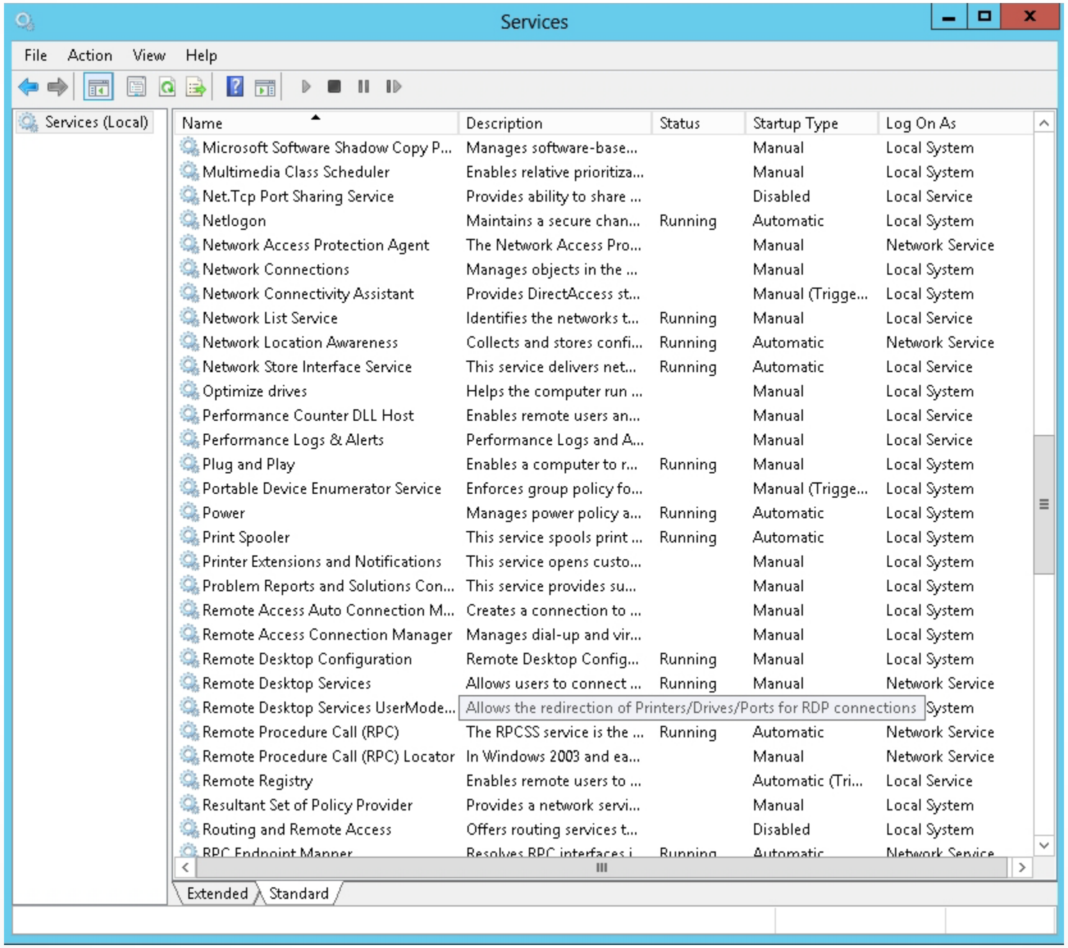
Using Server Manager

- Add roles and features.
- View events.
- Perform server configuration tasks.
- Add remote servers to a pool of servers that Server Manager can be used to manage.
- Install or uninstall roles, role services, and features on the local server or remote servers.
- View and make changes to server roles and features that are installed on local or remote servers.
- Perform management tasks.
- Scan roles for compliance with best practices.
- Run role-management tools.
- Determine server status, identify critical events, and analyze and troubleshoot configuration issues or failures.
- Restart servers.

Using Computer Management

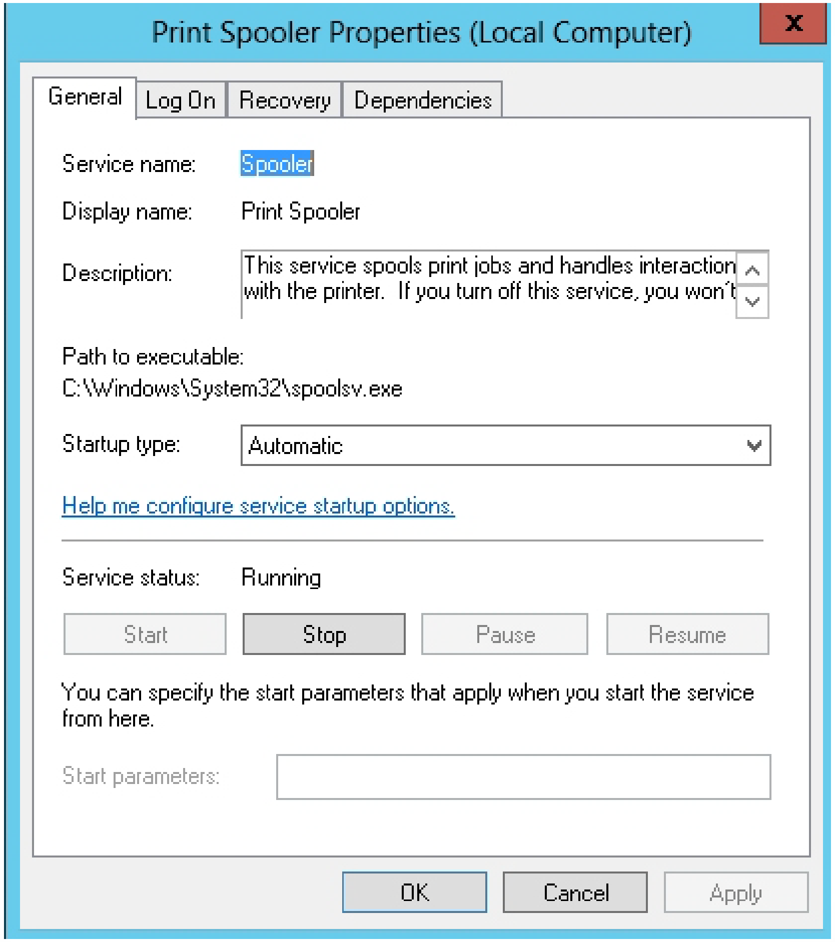


Using the Services Console



Name	Description	Status	Startup Type	Log On As
Microsoft Software Shadow Copy P...	Manages software-base...		Manual	Local System
Multimedia Class Scheduler	Enables relative prioritiza...		Manual	Local System
Net.Tcp Port Sharing Service	Provides ability to share ...		Disabled	Local Service
Netlogon	Maintains a secure chan...	Running	Automatic	Local System
Network Access Protection Agent	The Network Access Pro...		Manual	Network Service
Network Connections	Manages objects in the ...		Manual	Local System
Network Connectivity Assistant	Provides DirectAccess st...		Manual (Trigge...	Local System
Network List Service	Identifies the networks t...	Running	Manual	Local Service
Network Location Awareness	Collects and stores confi...	Running	Automatic	Network Service
Network Store Interface Service	This service delivers net...	Running	Automatic	Local Service
Optimize drives	Helps the computer run ...		Manual	Local System
Performance Counter DLL Host	Enables remote users an...		Manual	Local Service
Performance Logs & Alerts	Performance Logs and A...		Manual	Local Service
Plug and Play	Enables a computer to r...	Running	Manual	Local System
Portable Device Enumerator Service	Enforces group policy fo...		Manual (Trigge...	Local System
Power	Manages power policy a...	Running	Automatic	Local System
Print Spooler	This service spools print ...	Running	Automatic	Local System
Printer Extensions and Notifications	This service opens custo...		Manual	Local System
Problem Reports and Solutions Con...	This service provides su...		Manual	Local System
Remote Access Auto Connection M...	Creates a connection to ...		Manual	Local System
Remote Access Connection Manager	Manages dial-up and vir...		Manual	Local System
Remote Desktop Configuration	Remote Desktop Config...	Running	Manual	Local System
Remote Desktop Services	Allows users to connect ...	Running	Manual	Network Service
Remote Desktop Services UserMode...	Allows the redirection of Printers/Drives/Ports for RDP connections			System
Remote Procedure Call (RPC)	The RPCSS service is the ...	Running	Automatic	Network Service
Remote Procedure Call (RPC) Locator	In Windows 2003 and ea...		Manual	Network Service
Remote Registry	Enables remote users to ...		Automatic (Tri...	Local Service
Resultant Set of Policy Provider	Provides a network servi...		Manual	Local System
Routing and Remote Access	Offers routing services t...		Disabled	Local System
RPC Endpoint Mapper	Resolves RPC interfaces i...	Running	Automatic	Network Service

The Services Console Properties Dialog Box



Service name: Spooler

Display name: Print Spooler

Description: This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't

Path to executable:
C:\Windows\System32\spoolsv.exe

Startup type: Automatic

Help me configure service startup options.

Service status: Running

You can specify the start parameters that apply when you start the service from here.

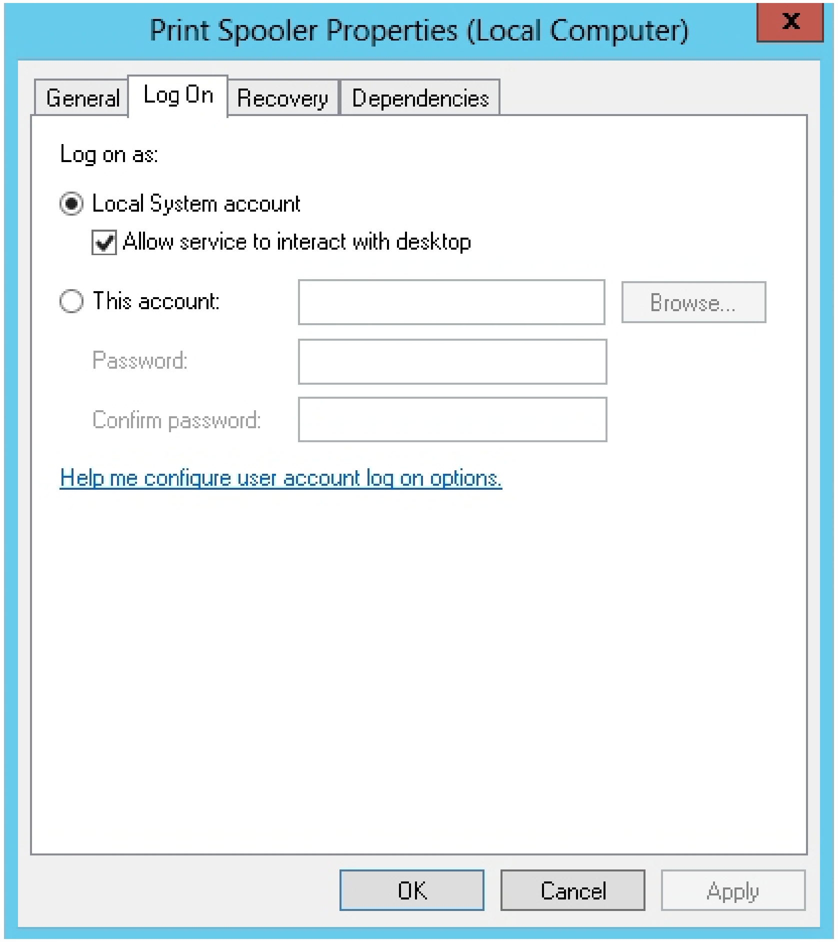
Start parameters:

Configuring a service

Windows Built-In Accounts

- **Local System**: Highly privileged account that can access most resources on the local computer.
- **NT Authority\LocalService**: Has the same privileges of the local Users group on the computer. When it accesses Network resources, it uses no credentials and a null session.
- **NT Authority\NetworkService**: Has the same level of access as the Users group on the local computer. When it accesses network resources, it does so under the context of the local computer account.

The Services Console Properties Dialog Box



Print Spooler Properties (Local Computer)

Log on as:

● Local System account

☑ Allow service to interact with desktop

○ This account:

Password:

Confirm password:

Viewing the Log On tab

Services Best Practices

- Use caution when changing the startup parameters for a service:
  - Includes the *Startup type* and *Log on as* settings.
  - Changes might prevent key services from running correctly.
- Do not change the *Allow service to interact with desktop* setting.
  - Allows service to access any information displayed on the interactive user's desktop.
- Use the account with minimum rights and permissions for the service to operate.
- Use different service accounts for different services.

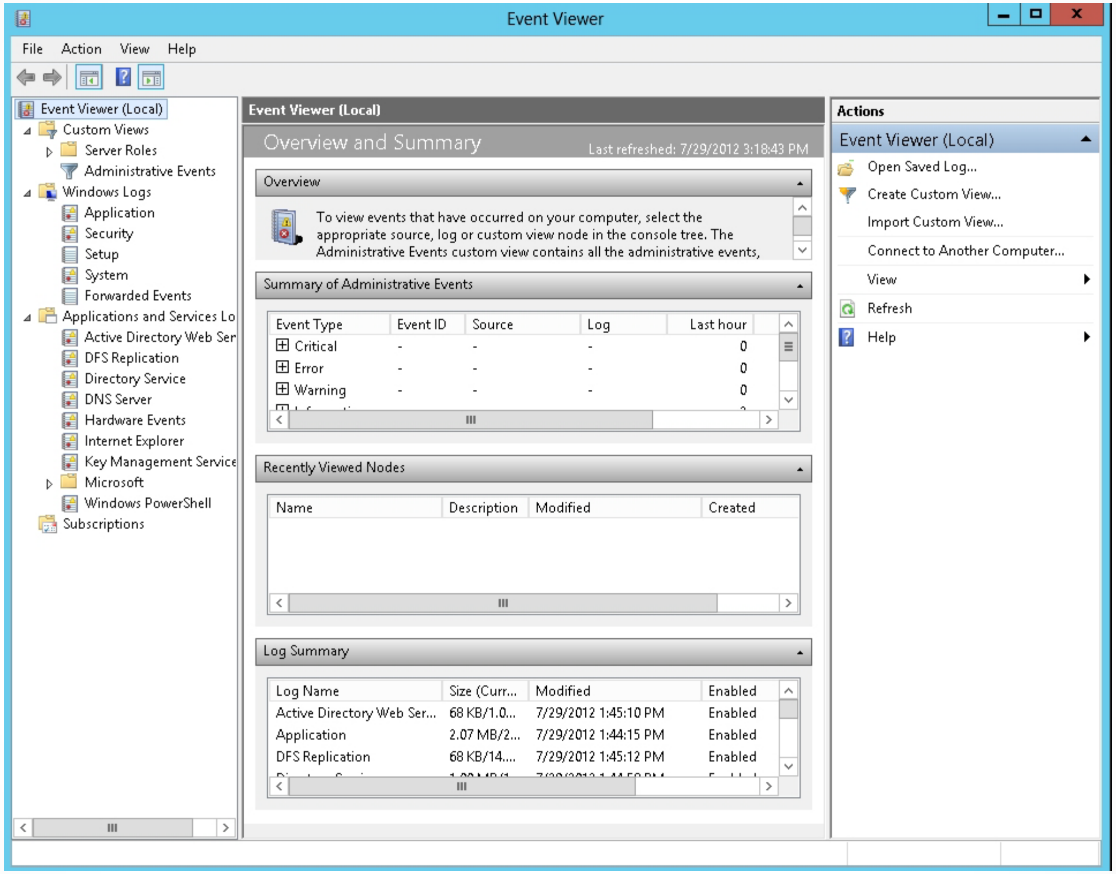
Using Event Viewer

Lesson 3: Monitoring Servers

Event Viewer

- View events from multiple event logs.
- Save useful event filters as custom views that can be reused.
- Schedule a task to run in response to an event.
- Create and manage event subscriptions.

Event Viewer MMC Snap-In



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

Event Type	Event ID	Source	Log	Last hour
⊞ Critical	-	-	-	0
⊞ Error	-	-	-	0
⊞ Warning	-	-	-	0

Name	Description	Modified	Created

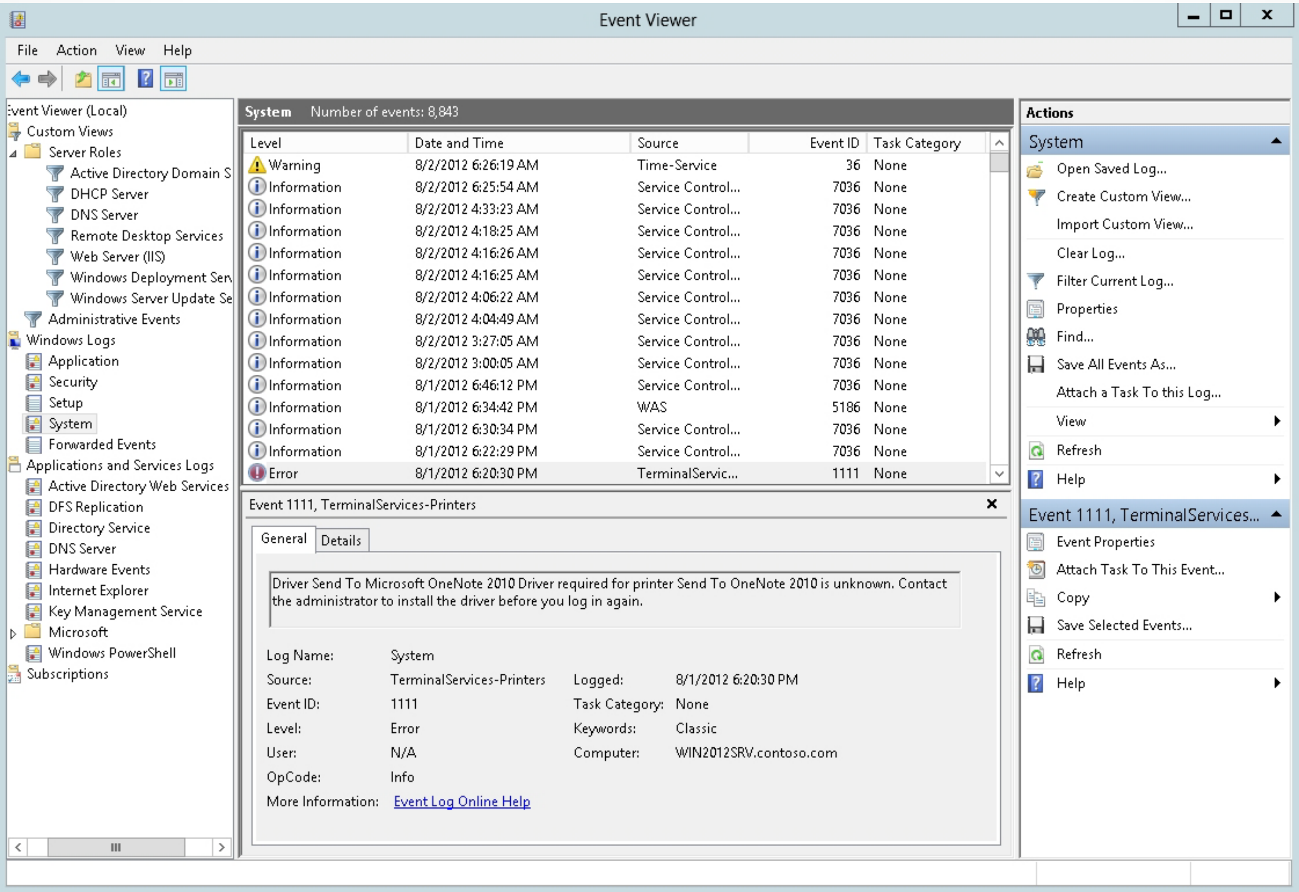
Log Name	Size (Curr...	Modified	Enabled
Active Directory Web Ser...	68 KB/1.0...	7/29/2012 1:45:10 PM	Enabled
Application	2.07 MB/2...	7/29/2012 1:44:15 PM	Enabled
DFS Replication	68 KB/14....	7/29/2012 1:45:12 PM	Enabled

Event Viewer

Understanding Logs and Events

- Custom Views
- Windows Logs
- Applications and Services Logs

Event Viewer MMC Snap-In



System Number of events: 8,843

Level	Date and Time	Source	Event ID	Task Category
Warning	8/2/2012 6:26:19 AM	Time-Service	36	None
Information	8/2/2012 6:25:54 AM	Service Control...	7036	None
Information	8/2/2012 4:33:23 AM	Service Control...	7036	None
Information	8/2/2012 4:18:25 AM	Service Control...	7036	None
Information	8/2/2012 4:16:26 AM	Service Control...	7036	None
Information	8/2/2012 4:16:25 AM	Service Control...	7036	None
Information	8/2/2012 4:06:22 AM	Service Control...	7036	None
Information	8/2/2012 4:04:49 AM	Service Control...	7036	None
Information	8/2/2012 3:27:05 AM	Service Control...	7036	None
Information	8/2/2012 3:00:05 AM	Service Control...	7036	None
Information	8/1/2012 6:46:12 PM	Service Control...	7036	None
Information	8/1/2012 6:34:42 PM	WAS	5186	None
Information	8/1/2012 6:30:34 PM	Service Control...	7036	None
Information	8/1/2012 6:22:29 PM	Service Control...	7036	None
Error	8/1/2012 6:20:30 PM	TerminalServic...	1111	None

Event 1111, TerminalServices-Printers

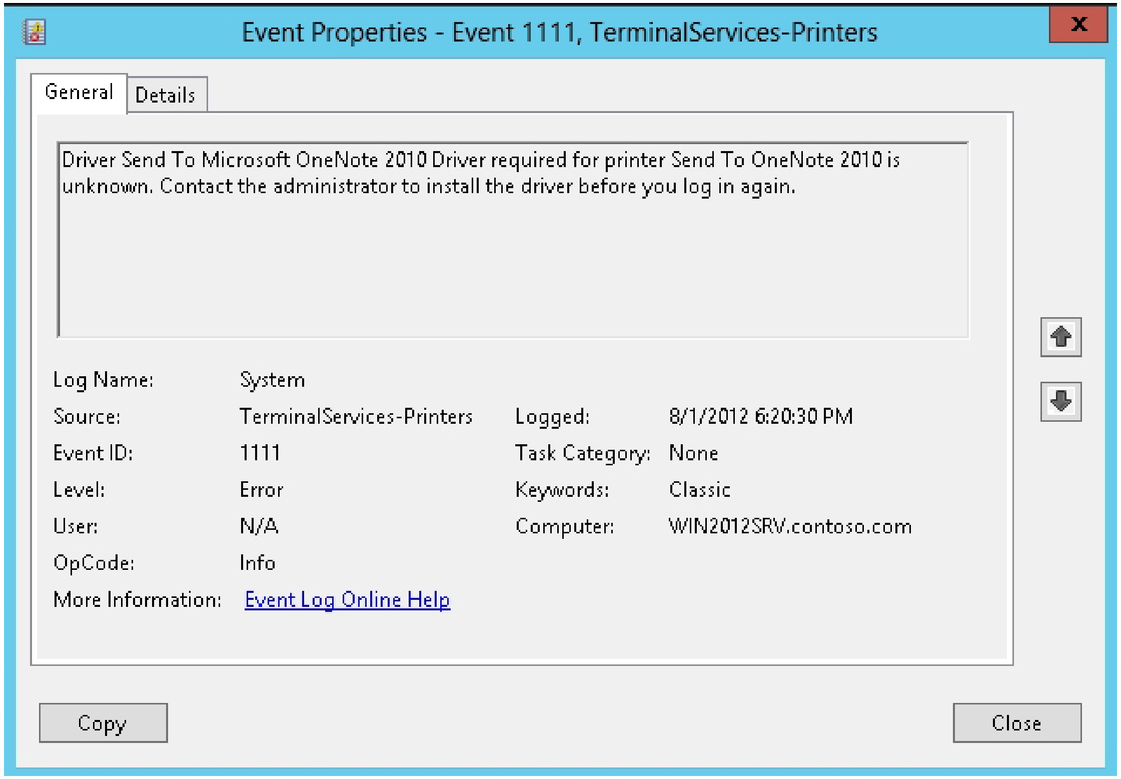
General Details

Driver Send To Microsoft OneNote 2010 Driver required for printer Send To OneNote 2010 is unknown. Contact the administrator to install the driver before you log in again.

Log Name: System
Source: TerminalServices-Printers
Logged: 8/1/2012 6:20:30 PM
Event ID: 1111
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: WIN2012SRV.contoso.com
OpCode: Info
More Information: Event Log Online Help

Viewing System logs

Event Viewer MMC Snap-In

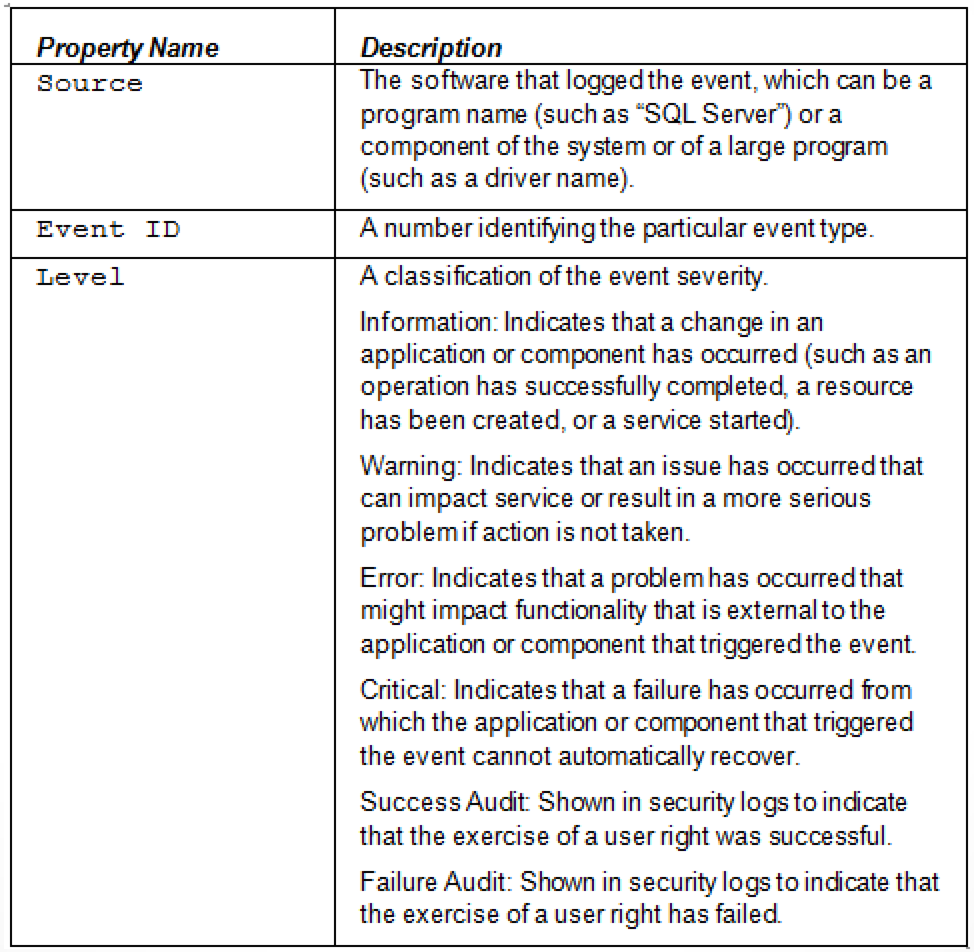


Driver Send To Microsoft OneNote 2010 Driver required for printer Send To OneNote 2010 is unknown. Contact the administrator to install the driver before you log in again.

Log Name:	System		
Source:	TerminalServices-Printers	Logged:	8/1/2012 6:20:30 PM
Event ID:	1111	Task Category:	None
Level:	Error	Keywords:	Classic
User:	N/A	Computer:	WIN2012SRV.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		

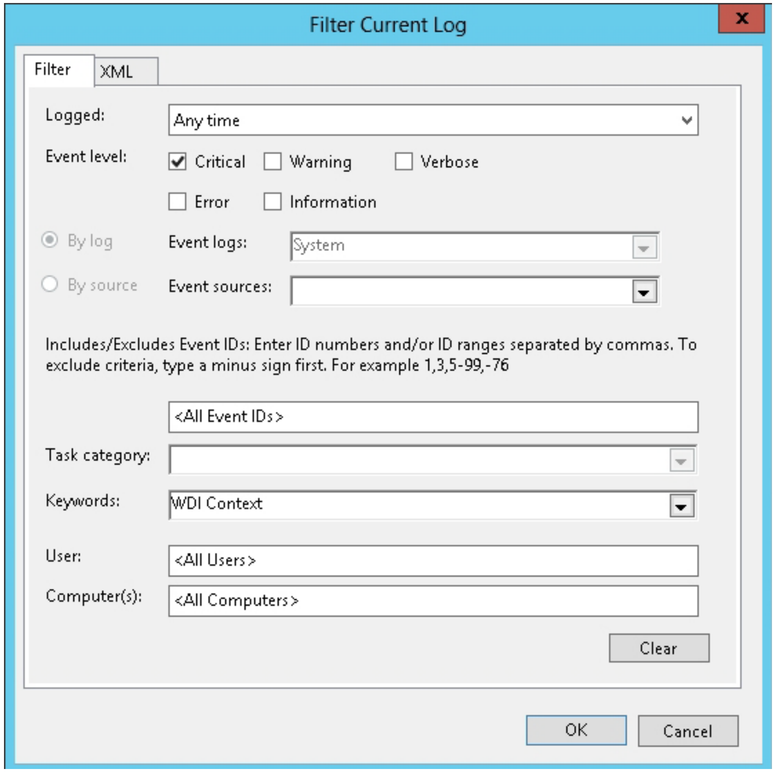
Viewing an event

Common Files Displayed in Event Viewer Logs



Property Name	***Description***
`Source`	The software that logged the event, which can be a program name (such as "SQL Server") or a component of the system or of a large program (such as a driver name).
`Event ID`	A number identifying the particular event type.
`Level`	A classification of the event severity. Information: Indicates that a change in an application or component has occurred (such as an operation has successfully completed, a resource has been created, or a service started). Warning: Indicates that an issue has occurred that can impact service or result in a more serious problem if action is not taken. Error: Indicates that a problem has occurred that might impact functionality that is external to the application or component that triggered the event. Critical: Indicates that a failure has occurred from which the application or component that triggered the event cannot automatically recover. Success Audit: Shown in security logs to indicate that the exercise of a user right was successful. Failure Audit: Shown in security logs to indicate that the exercise of a user right has failed.

Filtering Events



Logged: Any time

Event level: ☑ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

● By log Event logs: System

○ 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:

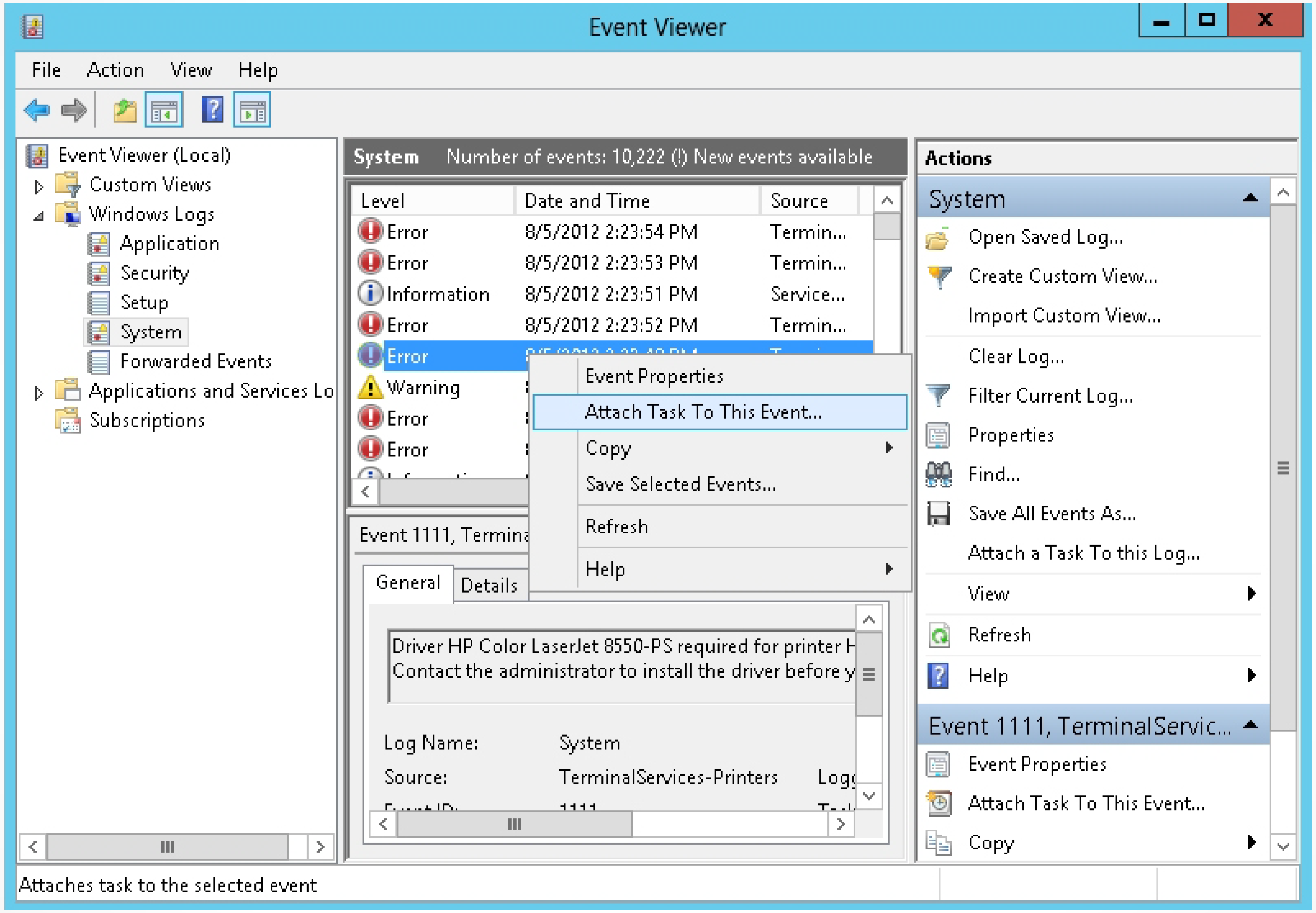
Keywords: WDI Context

User: <All Users>

Computer(s): <All Computers>

The Filter Current Log dialog box

Create a Basic Task



Level	Date and Time	Source
Error	8/5/2012 2:23:54 PM	Termin...
Error	8/5/2012 2:23:53 PM	Termin...
Information	8/5/2012 2:23:51 PM	Service...
Error	8/5/2012 2:23:52 PM	Termin...
Error		
Warning		
Error		
Error		

Driver HP Color LaserJet 8550-PS required for printer H
Contact the administrator to install the driver before y

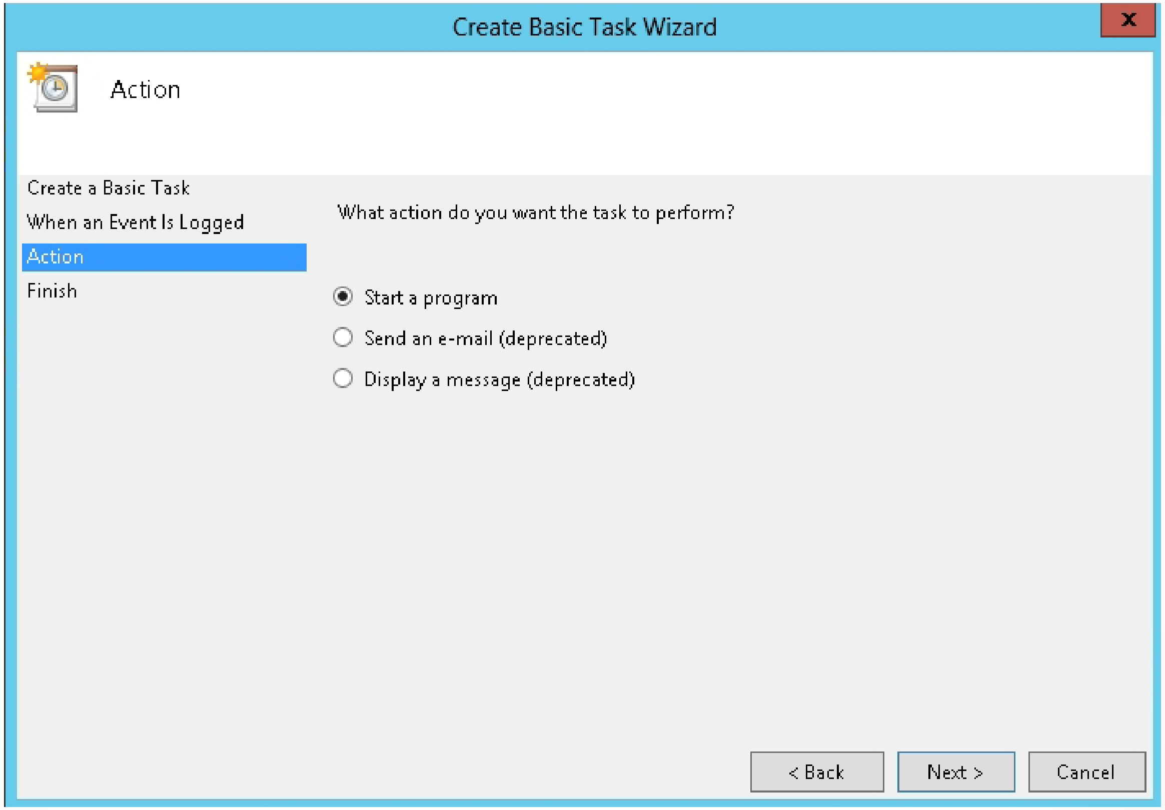
Log Name: System

Source: TerminalServices-Printers Log

Attaches task to the selected event

Attaching a Task to an event

Create a Basic Task



What action do you want the task to perform?

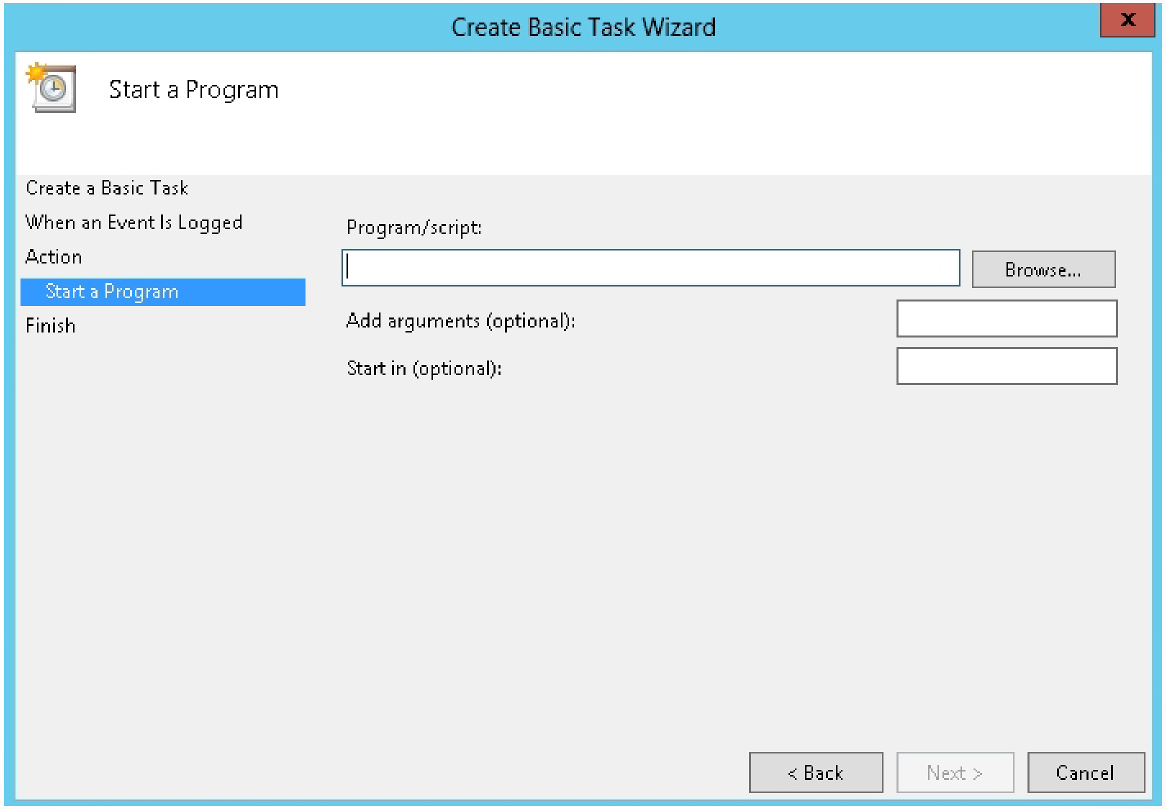
● Start a program

○ Send an e-mail (deprecated)

○ Display a message (deprecated)

Choosing an action

Create a Basic Task



Create Basic Task Wizard

Start a Program

Program/script:

Add arguments (optional):

Start in (optional):

Configuring the Start a Program page

Configuring Event Subscriptions

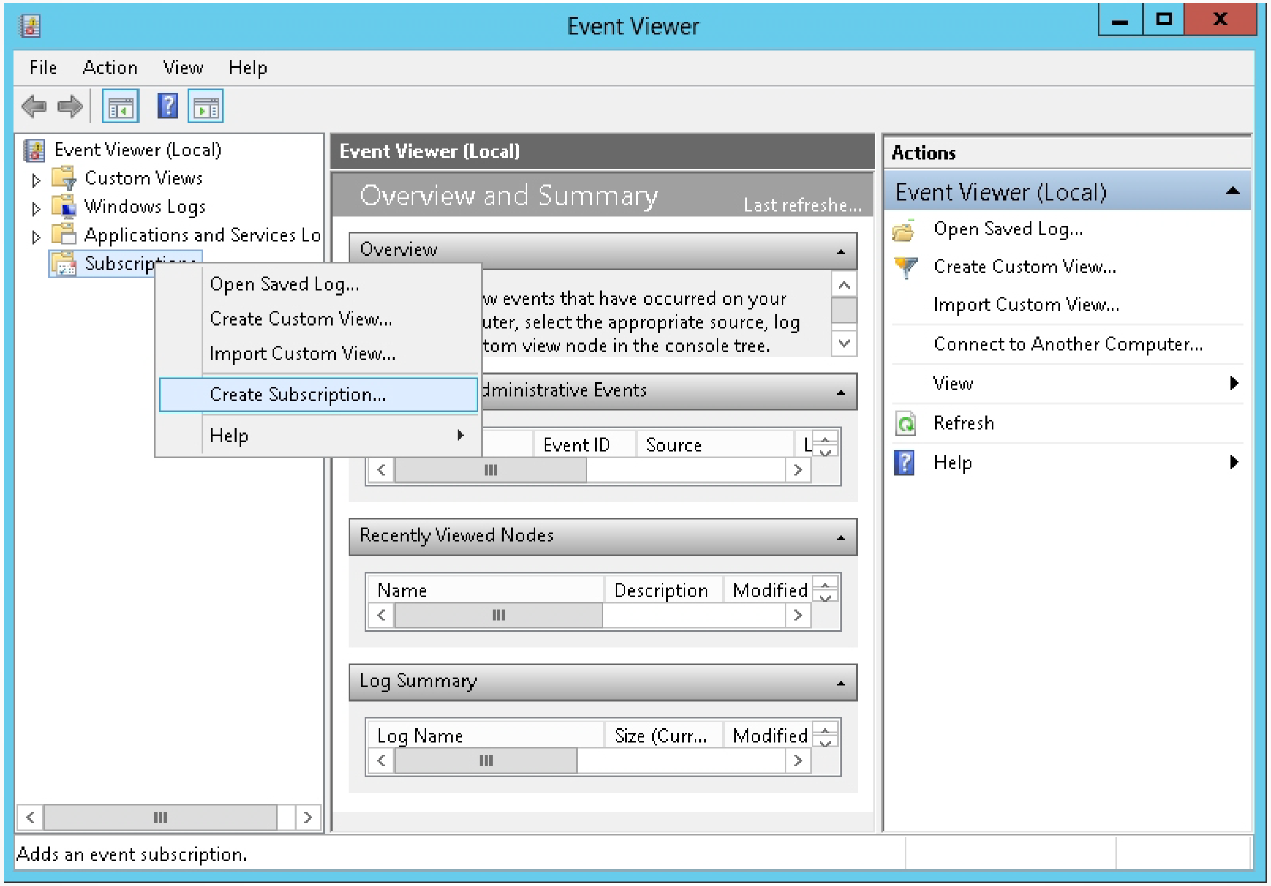
Event Viewer can collect copies of events from multiple remote computers and store them locally.

An **event subscription** specifies which events to collect.

To configure event subscriptions:

1. Configure the forwarding computer.
2. Configure the collecting computer.
3. Create an event subscription.

Create an Event Subscription

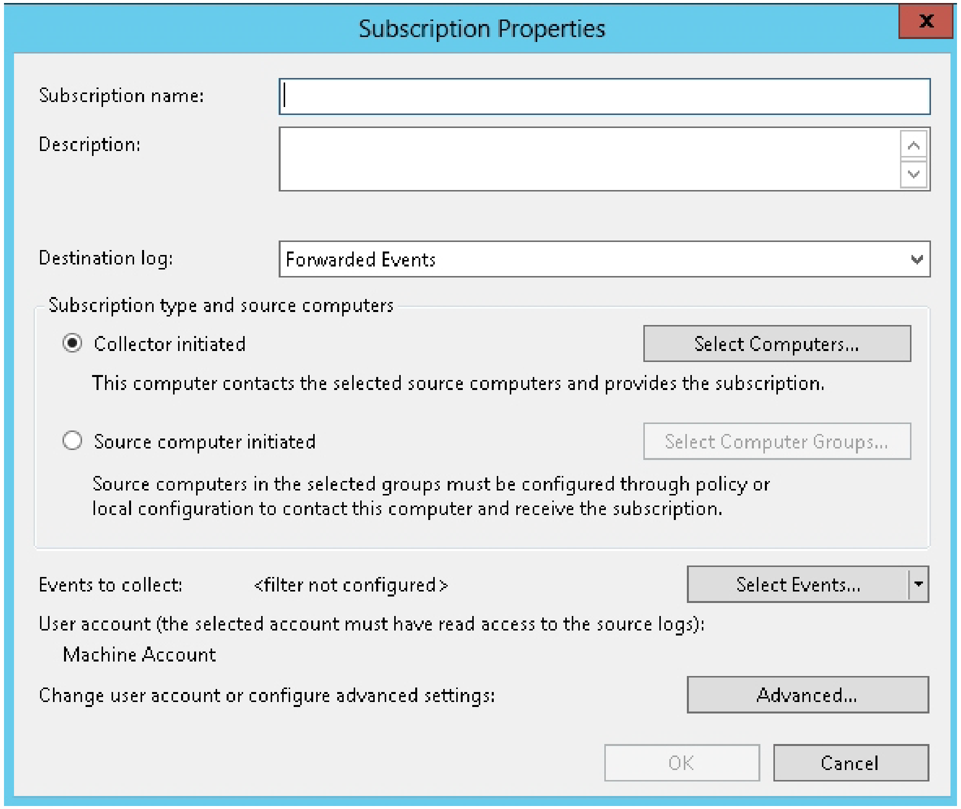


w events that have occurred on your
uter, select the appropriate source, log
tom view node in the console tree.

Adds an event subscription.

Creating a subscription

Create an Event Subscription



Subscription Properties

Subscription name:

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: <filter not configured>

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

Machine Account

Change user account or configure advanced settings:

Configuring subscription properties

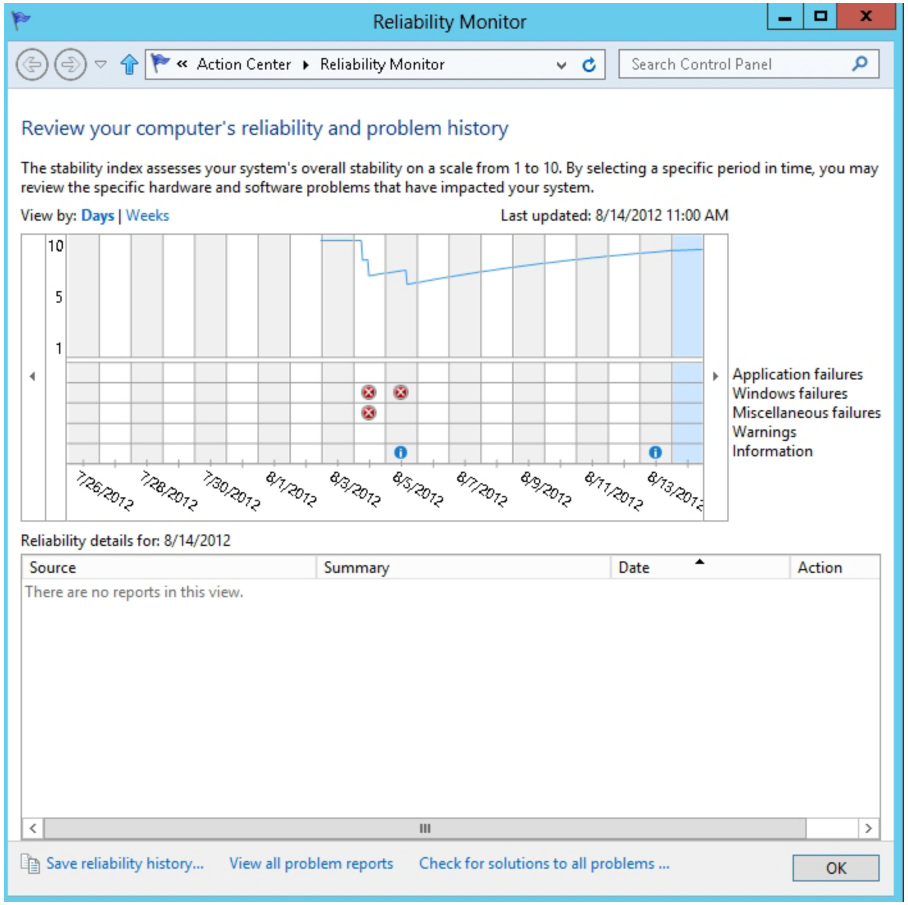
Using Reliability Monitor

Lesson 3: Monitoring Servers

Reliability Monitor

- Provides a stability index that ranges from 1 (the least stable) to 10 (the most stable).
- Index helps you evaluate the reliability of your computer.
- In Reliability Monitor, view:
  - Event details
  - Stability index over a specific period of time
  - Reports of problems that have occurred on your computer

Reliability Monitor



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

View by: **Days** | Weeks

Last updated: 8/14/2012 11:00 AM

Reliability details for: 8/14/2012

Source	Summary	Date	Action

There are no reports in this view.

Viewing the Reliability Monitor information

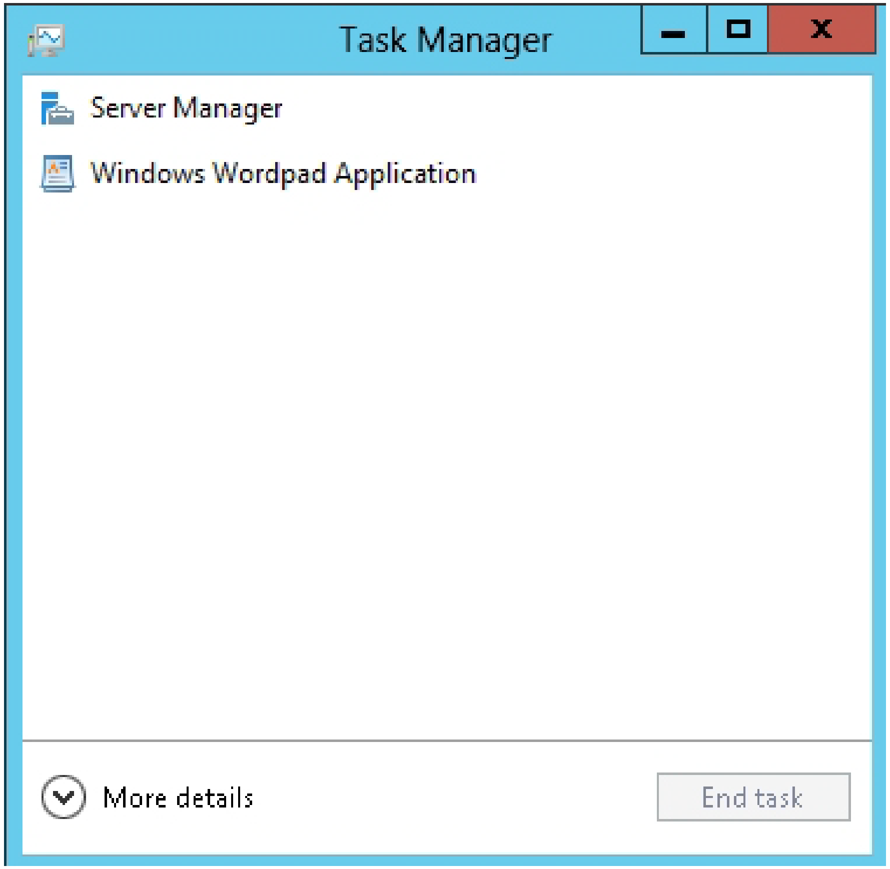
Managing Performance

Lesson 3: Monitoring Servers

Using Task Manager

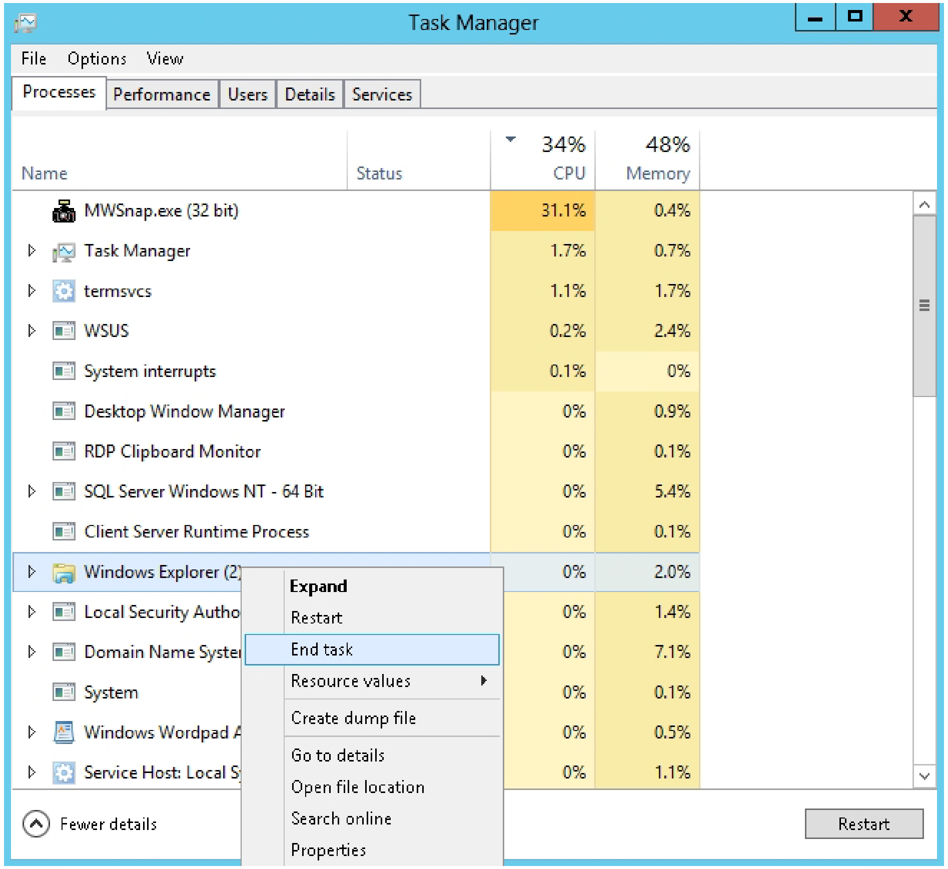
- Shows which programs are using the most system resources on your computer.
- Displays status of running programs and programs that have stopped responding.

Using Task Manager



Task Manager displays running applications

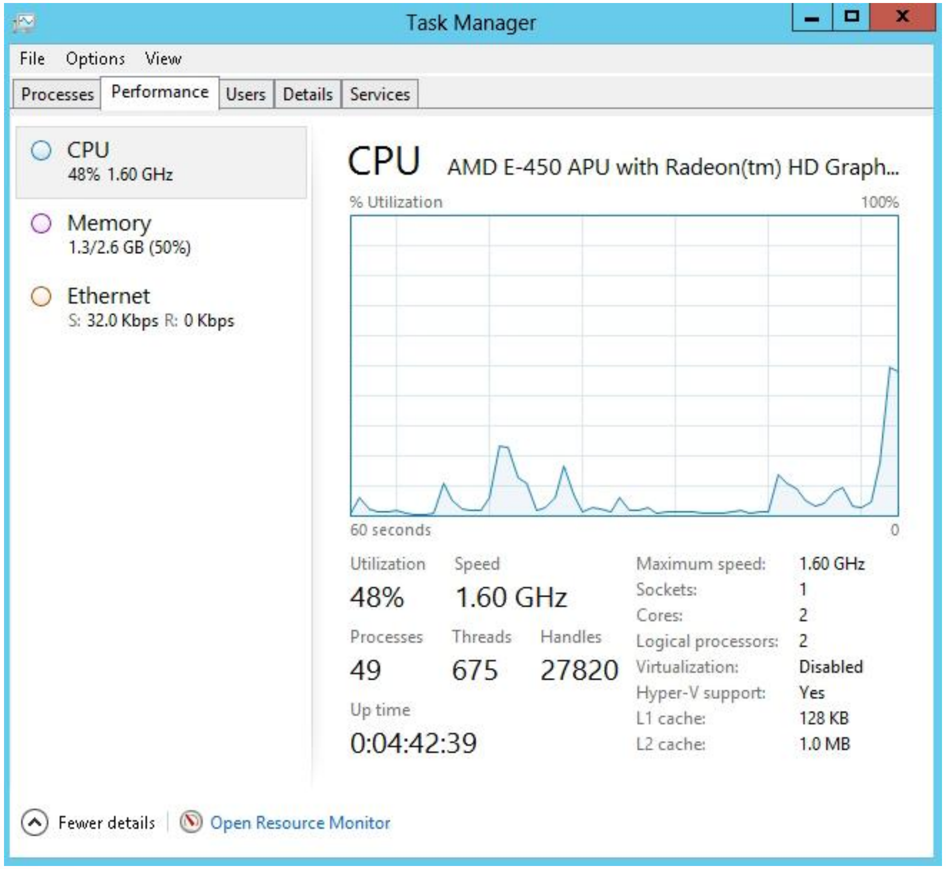
Using Task Manager



Name	Status	34% CPU	48% Memory
MWSnap.exe (32 bit)		31.1%	0.4%
Task Manager		1.7%	0.7%
termsvcs		1.1%	1.7%
WSUS		0.2%	2.4%
System interrupts		0.1%	0%
Desktop Window Manager		0%	0.9%
RDP Clipboard Monitor		0%	0.1%
SQL Server Windows NT - 64 Bit		0%	5.4%
Client Server Runtime Process		0%	0.1%
Windows Explorer (2)		0%	2.0%
Local Security Autho		0%	1.4%
Domain Name Syste		0%	7.1%
System		0%	0.1%
Windows Wordpad A		0%	0.5%
Service Host: Local S		0%	1.1%

Ending a task

Using Task Manager



CPU
48% 1.60 GHz

Memory
1.3/2.6 GB (50%)

Ethernet
S: 32.0 Kbps R: 0 Kbps

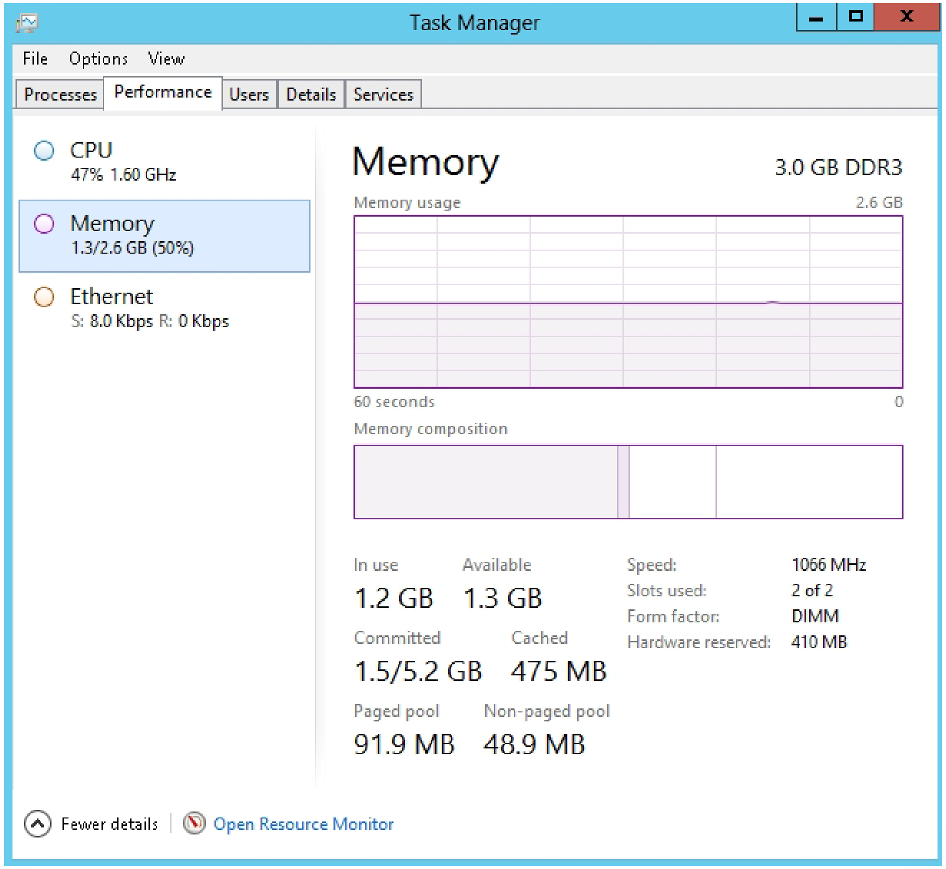
CPU AMD E-450 APU with Radeon(tm) HD Graph...

Utilization 48%
Speed 1.60 GHz
Processes 49
Threads 675
Handles 27820
Up time 0:04:42:39

Maximum speed:	1.60 GHz
Sockets:	1
Cores:	2
Logical processors:	2
Virtualization:	Disabled
Hyper-V support:	Yes
L1 cache:	128 KB
L2 cache:	1.0 MB

Viewing CPU usage

Using Task Manager



CPU
47% 1.60 GHz

Memory
1.3/2.6 GB (50%)

Ethernet
S: 8.0 Kbps R: 0 Kbps

Memory 3.0 GB DDR3

In use 1.2 GB

Available 1.3 GB

Committed 1.5/5.2 GB

Cached 475 MB

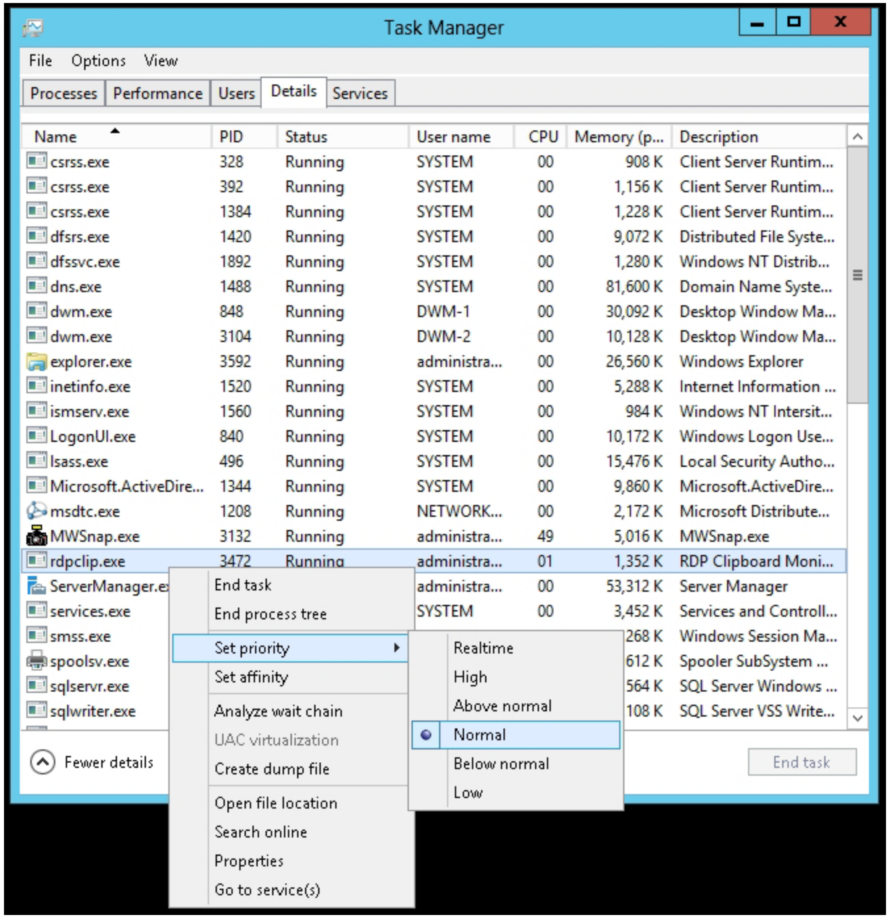
Paged pool 91.9 MB

Non-paged pool 48.9 MB

Speed: 1066 MHz
Slots used: 2 of 2
Form factor: DIMM
Hardware reserved: 410 MB

Viewing Memory usage

Using Task Manager



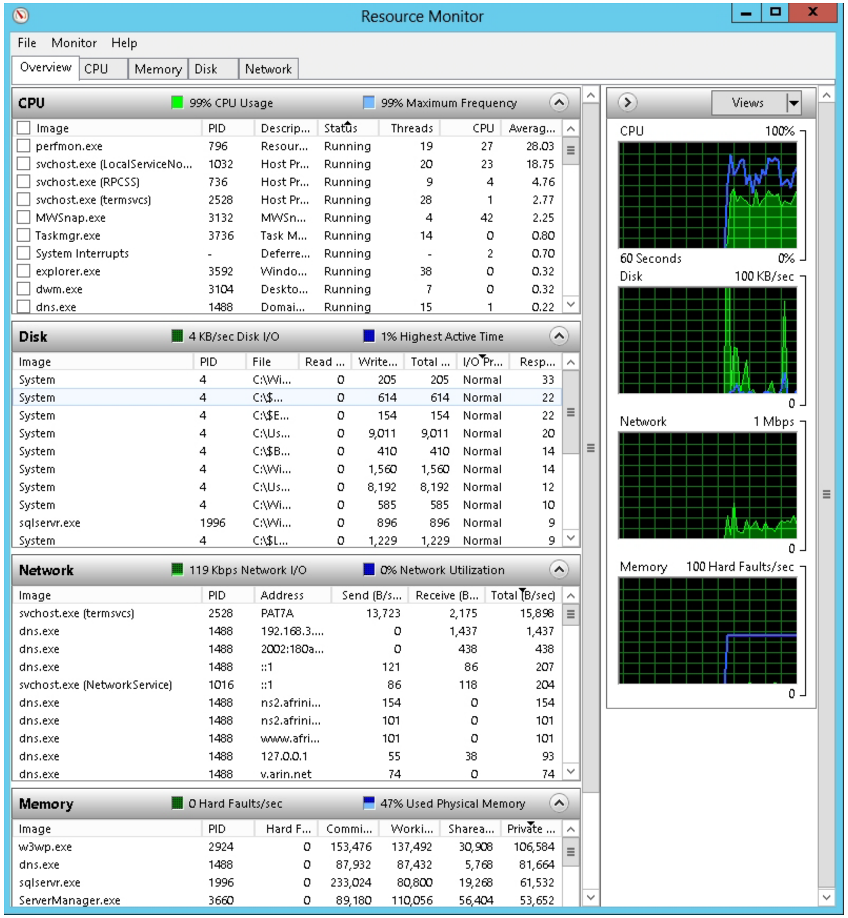
Name	PID	Status	User name	CPU	Memory (p...	Description
csrss.exe	328	Running	SYSTEM	00	908 K	Client Server Runtim...
csrss.exe	392	Running	SYSTEM	00	1,156 K	Client Server Runtim...
csrss.exe	1384	Running	SYSTEM	00	1,228 K	Client Server Runtim...
dfsrs.exe	1420	Running	SYSTEM	00	9,072 K	Distributed File Syste...
dfssvc.exe	1892	Running	SYSTEM	00	1,280 K	Windows NT Distrib...
dns.exe	1488	Running	SYSTEM	00	81,600 K	Domain Name Syste...
dwm.exe	848	Running	DWM-1	00	30,092 K	Desktop Window Ma...
dwm.exe	3104	Running	DWM-2	00	10,128 K	Desktop Window Ma...
explorer.exe	3592	Running	administra...	00	26,560 K	Windows Explorer
inetinfo.exe	1520	Running	SYSTEM	00	5,288 K	Internet Information ...
ismserv.exe	1560	Running	SYSTEM	00	984 K	Windows NT Intersit...
LogonUI.exe	840	Running	SYSTEM	00	10,172 K	Windows Logon Use...
lsass.exe	496	Running	SYSTEM	00	15,476 K	Local Security Autho...
Microsoft.ActiveDire...	1344	Running	SYSTEM	00	9,860 K	Microsoft.ActiveDire...
msdtc.exe	1208	Running	NETWORK...	00	2,172 K	Microsoft Distribute...
MWSnap.exe	3132	Running	administra...	49	5,016 K	MWSnap.exe
rdpclip.exe	3472	Running	administra...	01	1,352 K	RDP Clipboard Moni...
ServerManager.ex			administra...	00	53,312 K	Server Manager
services.exe			SYSTEM	00	3,452 K	Services and Controll...
smss.exe					268 K	Windows Session Ma...
spoolsv.exe					612 K	Spooler SubSystem ...
sqlservr.exe					564 K	SQL Server Windows ...
sqlwriter.exe					108 K	SQL Server VSS Write...

Setting a priority level

Using Resource Monitor

- Monitors resource usage in real time.
- Shows how system resources are used by processes and services.
- Helps analyze unresponsive processes.
- Identifies which applications are using files.
- Controls processes and services.

Using Resource Monitor



CPU 🟩 99% CPU Usage 🟦 99% Maximum Frequency

□ Image	PID	Descrip...	Status	Threads	CPU	Averag...
□ perfmon.exe	796	Resour...	Running	19	27	28.03
□ svchost.exe (LocalServiceNo...	1032	Host Pr...	Running	20	23	18.75
□ svchost.exe (RPCSS)	736	Host Pr...	Running	9	4	4.76
□ svchost.exe (termsvcs)	2528	Host Pr...	Running	28	1	2.77
□ MWSnap.exe	3132	MWSn...	Running	4	42	2.25
□ Taskmgr.exe	3736	Task M...	Running	14	0	0.80
□ System Interrupts	-	Deferre...	Running	-	2	0.70
□ explorer.exe	3592	Windo...	Running	38	0	0.32
□ dwm.exe	3104	Deskto...	Running	7	0	0.32
□ dns.exe	1488	Domai...	Running	15	1	0.22

Disk 🟩 4 KB/sec Disk I/O 🟦 1% Highest Active Time

Image	PID	File	Read ...	Write...	Total ...	I/O Pr...	Resp...
System	4	C:\Wi...	0	205	205	Normal	33
System	4	C:\$...	0	614	614	Normal	22
System	4	C:\$E...	0	154	154	Normal	22
System	4	C:\Us...	0	9,011	9,011	Normal	20
System	4	C:\$B...	0	410	410	Normal	14
System	4	C:\Wi...	0	1,560	1,560	Normal	14
System	4	C:\Us...	0	8,192	8,192	Normal	12
System	4	C:\Wi...	0	585	585	Normal	10
sqlservr.exe	1996	C:\Wi...	0	896	896	Normal	9
System	4	C:\$L...	0	1,229	1,229	Normal	9

Network 🟩 119 Kbps Network I/O 🟦 0% Network Utilization

Image	PID	Address	Send (B/s...	Receive (B...	Total (B/sec)
svchost.exe (termsvcs)	2528	PAT7A	13,723	2,175	15,898
dns.exe	1488	192.168.3....	0	1,437	1,437
dns.exe	1488	2002:180a...	0	438	438
dns.exe	1488	::1	121	86	207
svchost.exe (NetworkService)	1016	::1	86	118	204
dns.exe	1488	ns2.afrini...	154	0	154
dns.exe	1488	ns2.afrini...	101	0	101
dns.exe	1488	www.afri...	101	0	101
dns.exe	1488	127.0.0.1	55	38	93
dns.exe	1488	v.arin.net	74	0	74

Memory 🟩 0 Hard Faults/sec 🟦 47% Used Physical Memory

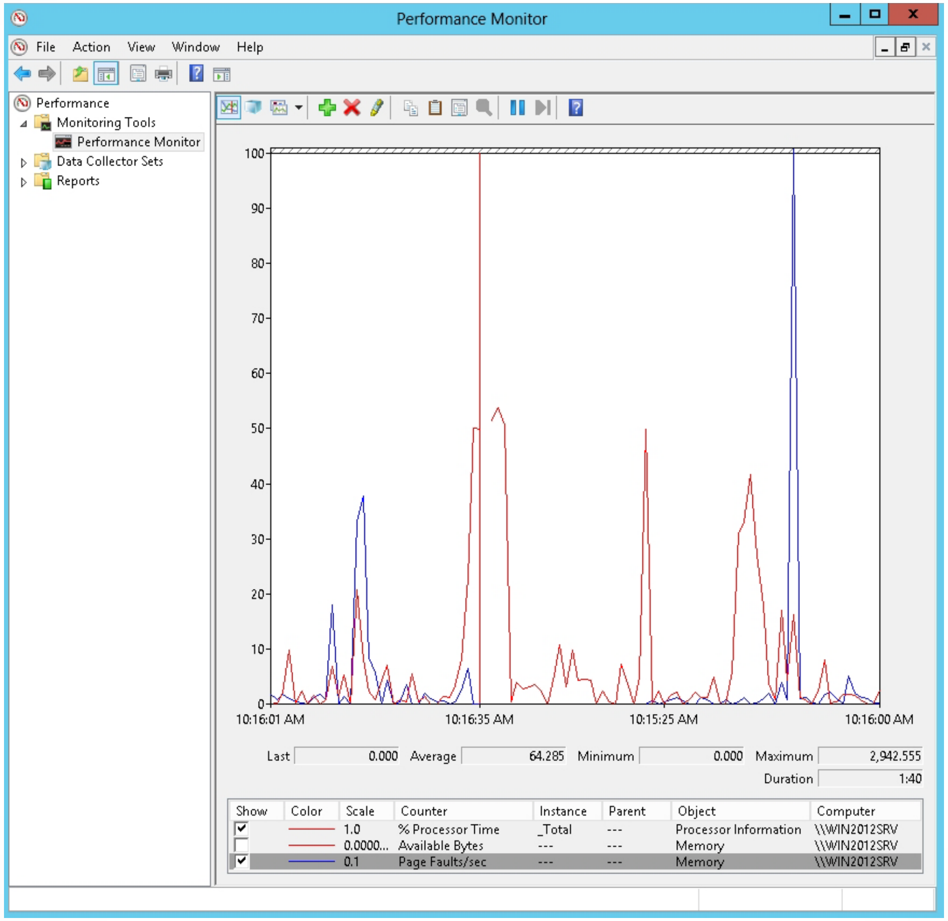
Image	PID	Hard F...	Commi...	Worki...	Sharea...	Private ...
w3wp.exe	2924	0	153,476	137,492	30,908	106,584
dns.exe	1488	0	87,932	87,432	5,768	81,664
sqlservr.exe	1996	0	233,024	80,800	19,268	61,532
ServerManager.exe	3660	0	89,180	110,056	56,404	53,652

Viewing Resource Monitor

Using Performance Monitor

- An MMC snap-in that provides tools for analyzing system performance.
- Monitors application and hardware performance in real time.
- Generates reports.
- Displays past performance data in a variety of ways.
- Lets you specify:
  - Data you want to collect in logs
  - Thresholds for alerts and automatic actions

Using Performance Monitor



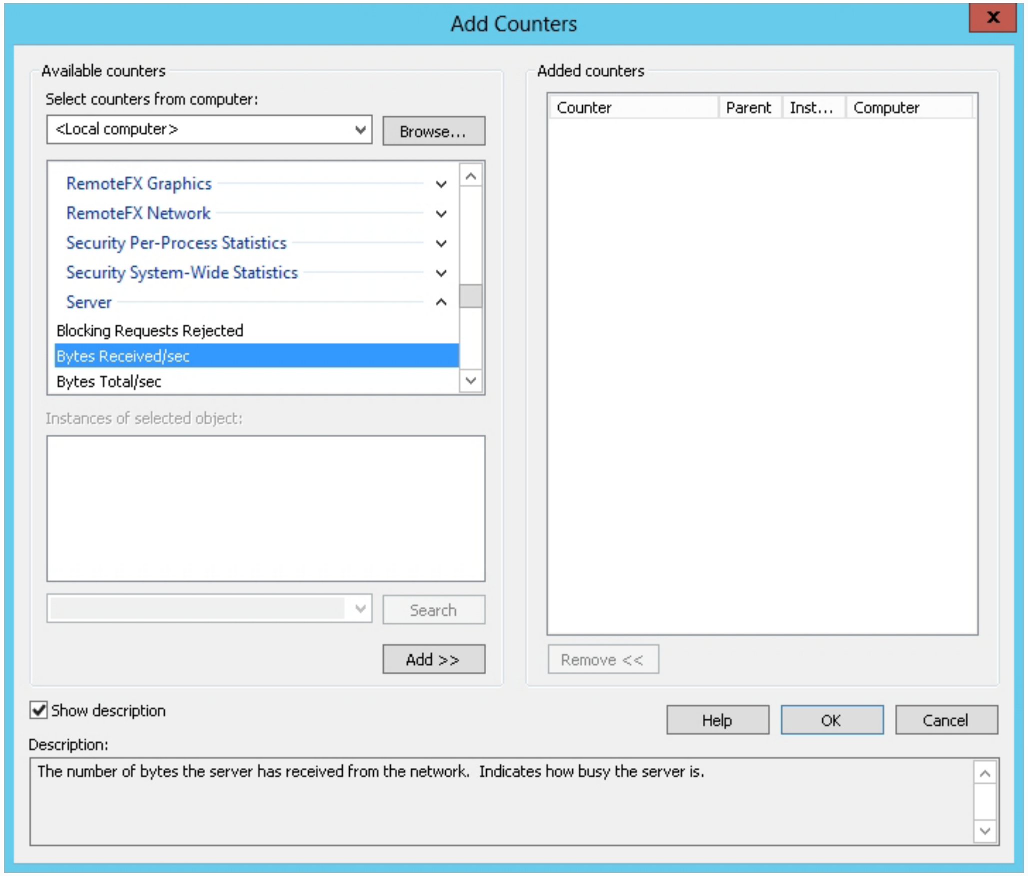
Last 0.000 Average 64.285 Minimum 0.000 Maximum 2,942.555

Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	1.0	% Processor Time	_Total	---	Processor Information	\\WIN2012SRV
□	🟥	0.0000...	Available Bytes	---	---	Memory	\\WIN2012SRV
☑	🟦	0.1	Page Faults/sec	---	---	Memory	\\WIN2012SRV

Viewing Performance Monitor

Using Performance Monitor



Select counters from computer: <Local computer>

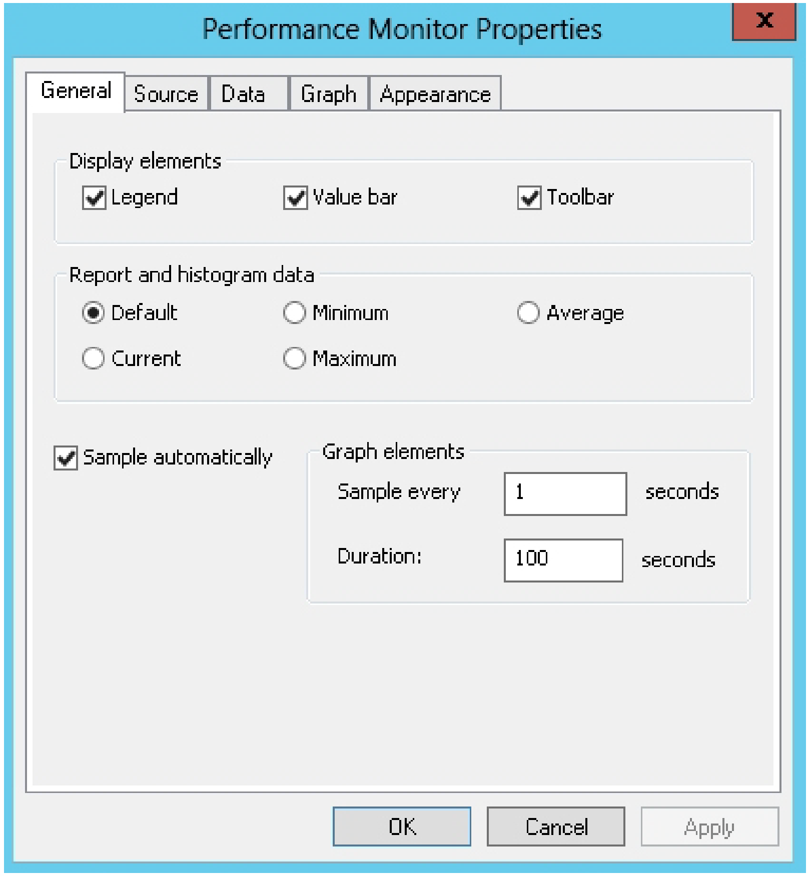
RemoteFX Graphics
RemoteFX Network
Security Per-Process Statistics
Security System-Wide Statistics
Server
Blocking Requests Rejected
Bytes Received/sec
Bytes Total/sec

☑ Show description

Description:
The number of bytes the server has received from the network. Indicates how busy the server is.

Adding counters to Performance Monitor

Using Performance Monitor



Display elements

☑ Legend ☑ Value bar ☑ Toolbar

Report and histogram data

● Default ○ Minimum ○ Average

○ Current ○ Maximum

☑ Sample automatically

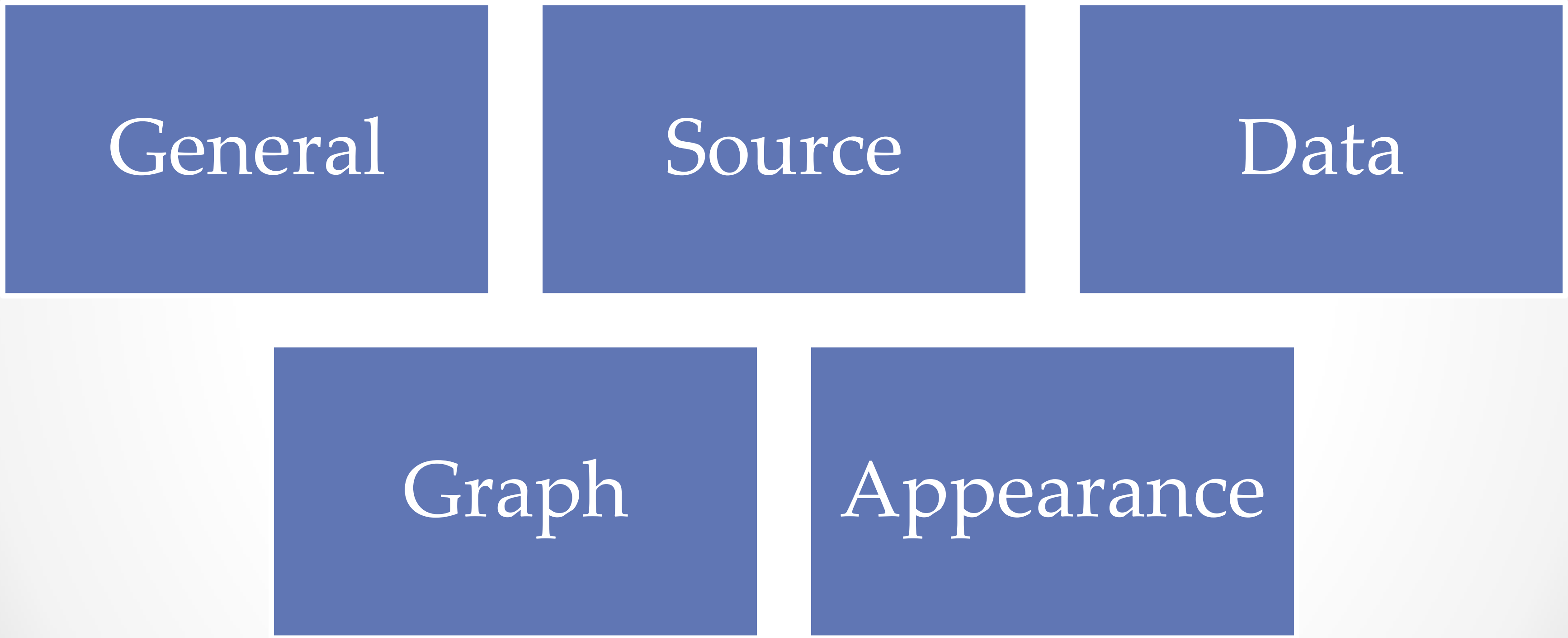
Graph elements

Sample every 1 seconds

Duration: 100 seconds

Configuring Performance Monitor properties

Performance Monitor Tabs



General

Source

Data

Graph

Appearance

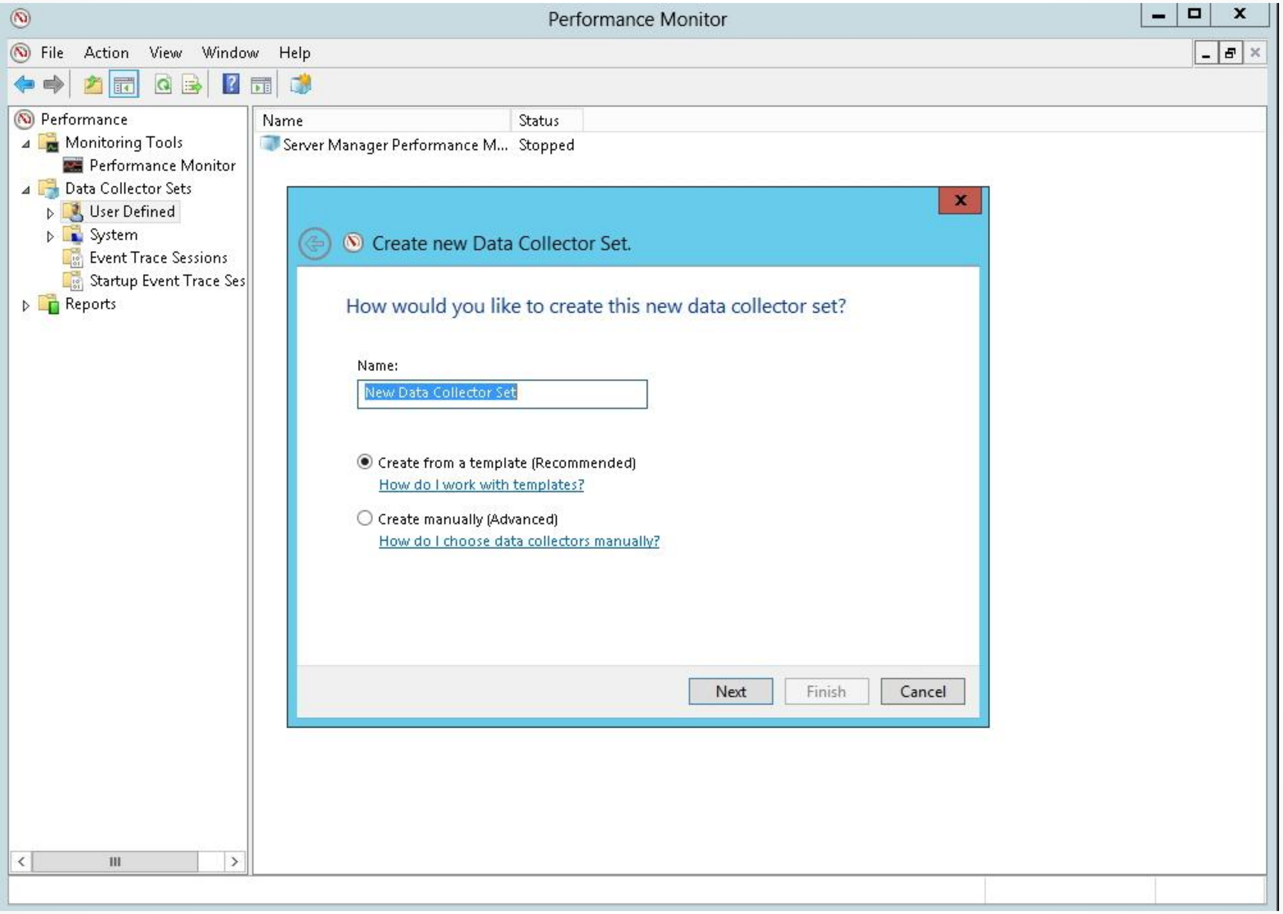
Using Common Performance Counters

- Processor:%Processor Time
- pages/sec
- Paging File:%Usage
- Physical Disk:%Disk Time
- Physical Disk:%Avg. Disk Queue Length

Configuring Data Collector Sets (DCS)

- Windows Performance Monitor uses performance counters, event trace data, and configuration information, which can be combined into Data Collector Sets:
  - **Performance counters**: Current value requested at specified time intervals by Windows Performance Monitor.
  - **Event trace data**: Collected from trace providers, which are components of the operating system or of individual applications that report actions or events.
  - **Configuration information**: Collected from key values in the Windows registry.

Create a Data Collector Set



Create new Data Collector Set.

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

Name: New Data Collector Set

● Create from a template (Recommended)

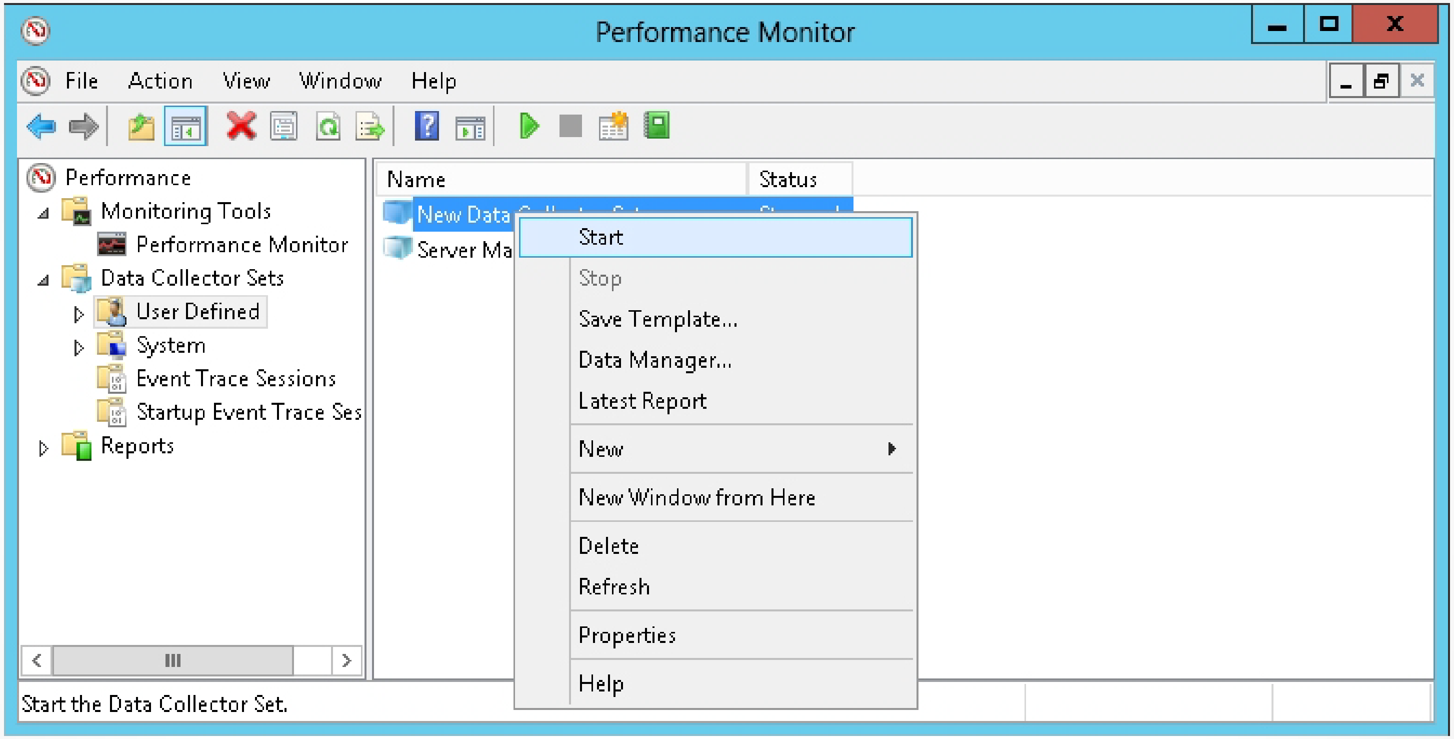
How do I work with templates?

○ Create manually (Advanced)

How do I choose data collectors manually?

Creating a new Data Collector Set

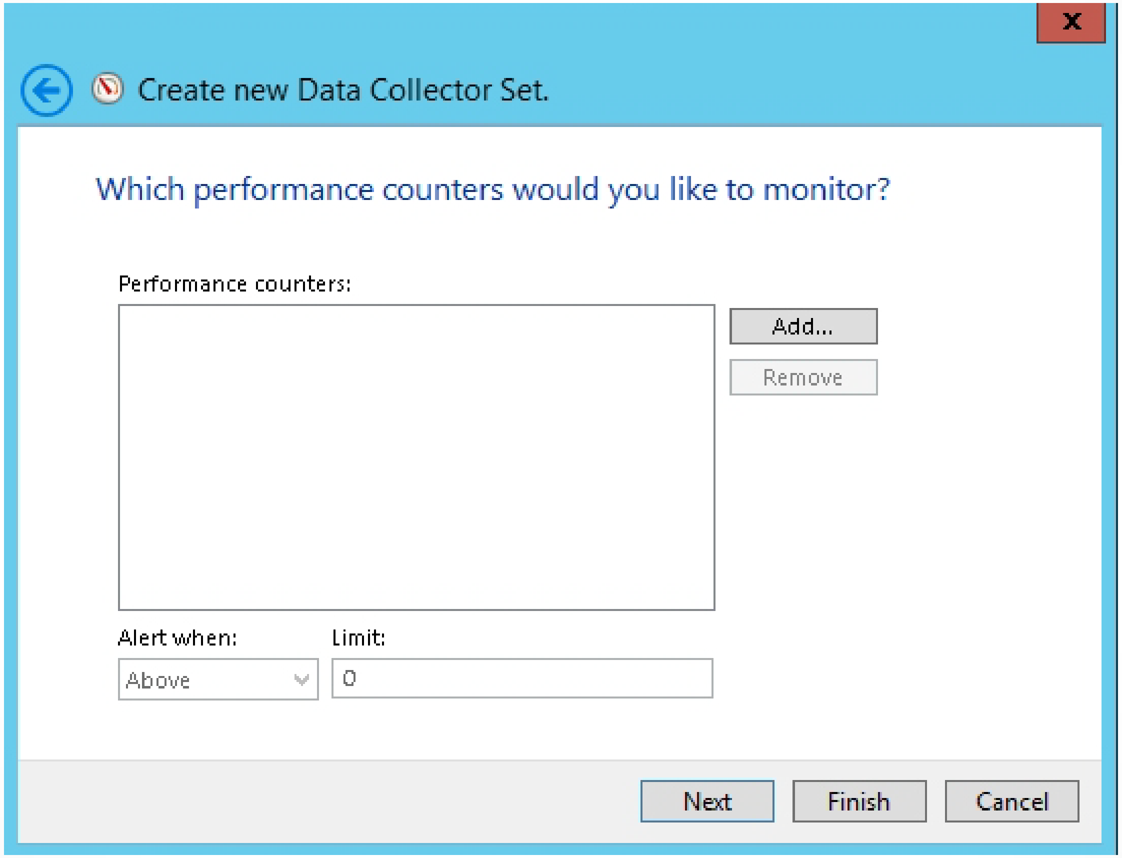
Create a Data Collector Set



Start the Data Collector Set.

Starting the Data Collector Set

Create a Performance Alert



Create new Data Collector Set.

Which performance counters would you like to monitor?

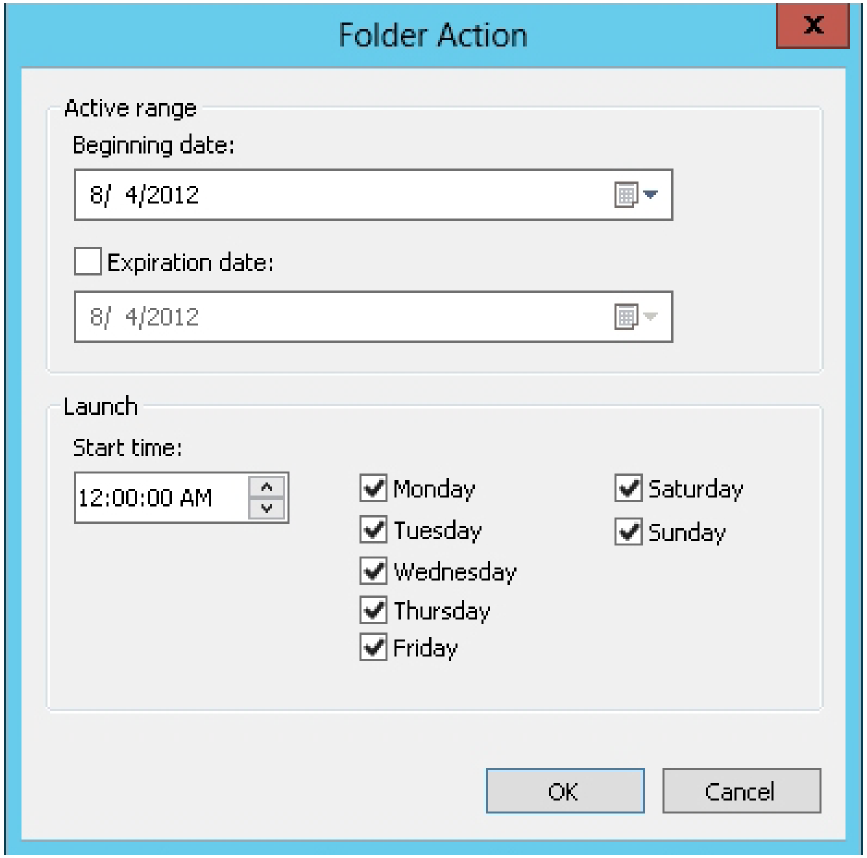
Performance counters:

Alert when: Above

Limit: 0

Choosing performance counters

Create a Performance Alert



Folder Action

Active range

Beginning date: 8/ 4/2012

□ Expiration date: 8/ 4/2012

Launch

Start time: 12:00:00 AM

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Configuring a schedule

Monitoring the Network

Lesson 3: Monitoring Servers

Troubleshooting Network Issues

- Make sure you are connected.
- Make sure the network interface is enabled.
- Check local IP configuration using `ipconfig`.
- Use the `ping` command to determine what you can reach and what you cannot reach:
  - Ping the loopback address (127.0.0.1).
  - Ping a local IP address.
  - Ping a remote gateway.
  - Ping a remote computer.
- Identify each hop (router) between two systems using the `tracert` command.
- Verify DNS configuration using the `nslookup` command (discussed in Lessons 8 and 9).

Using the `netstat` Command

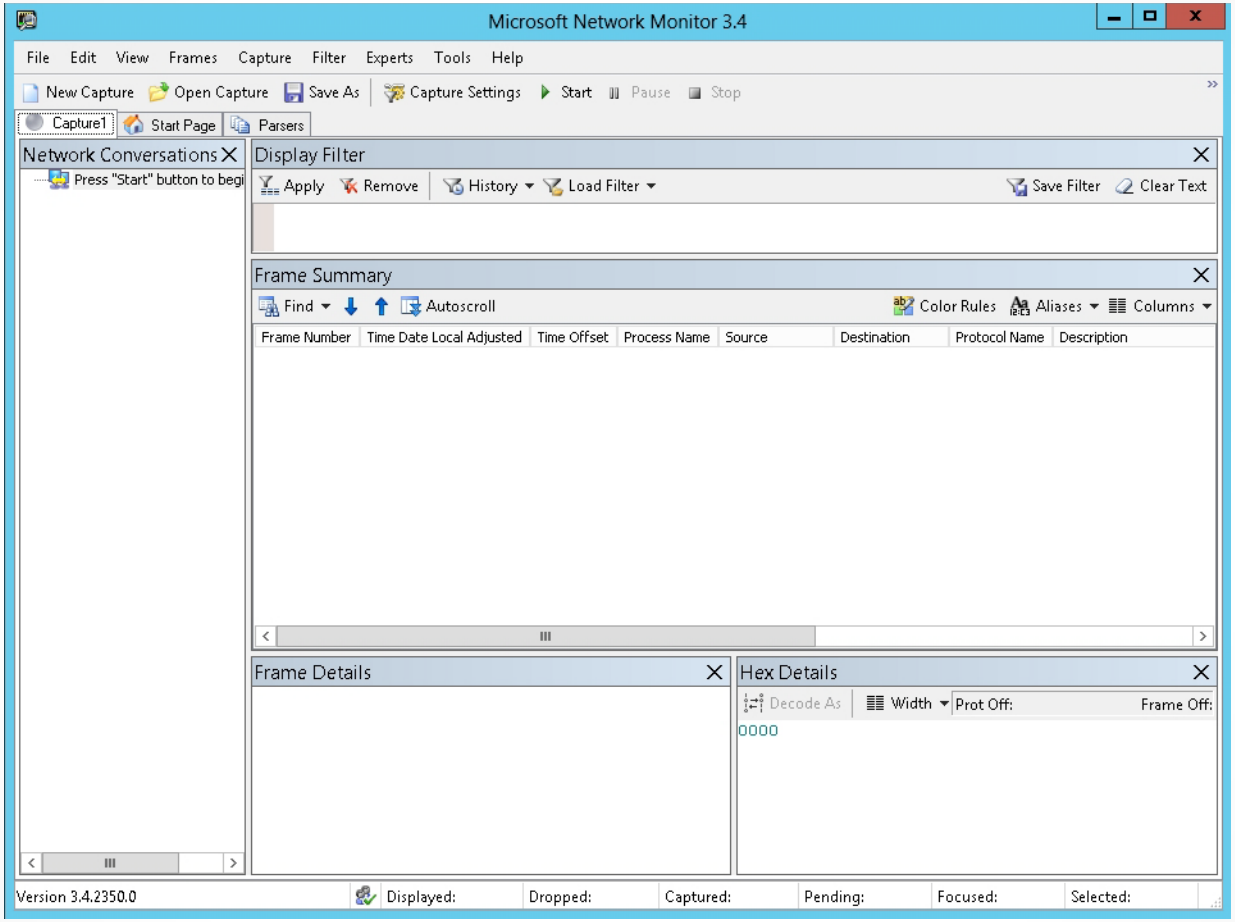
`netstat` shows all the outbound TCP/IP connections. Options include:

- `netstat -a` displays all connections
- `netstat -r` displays the route table plus active connections
- `netstat -e` displays Ethernet statistics
- `netstat -s` displays per-protocol statistics

Using Protocol Analyzers

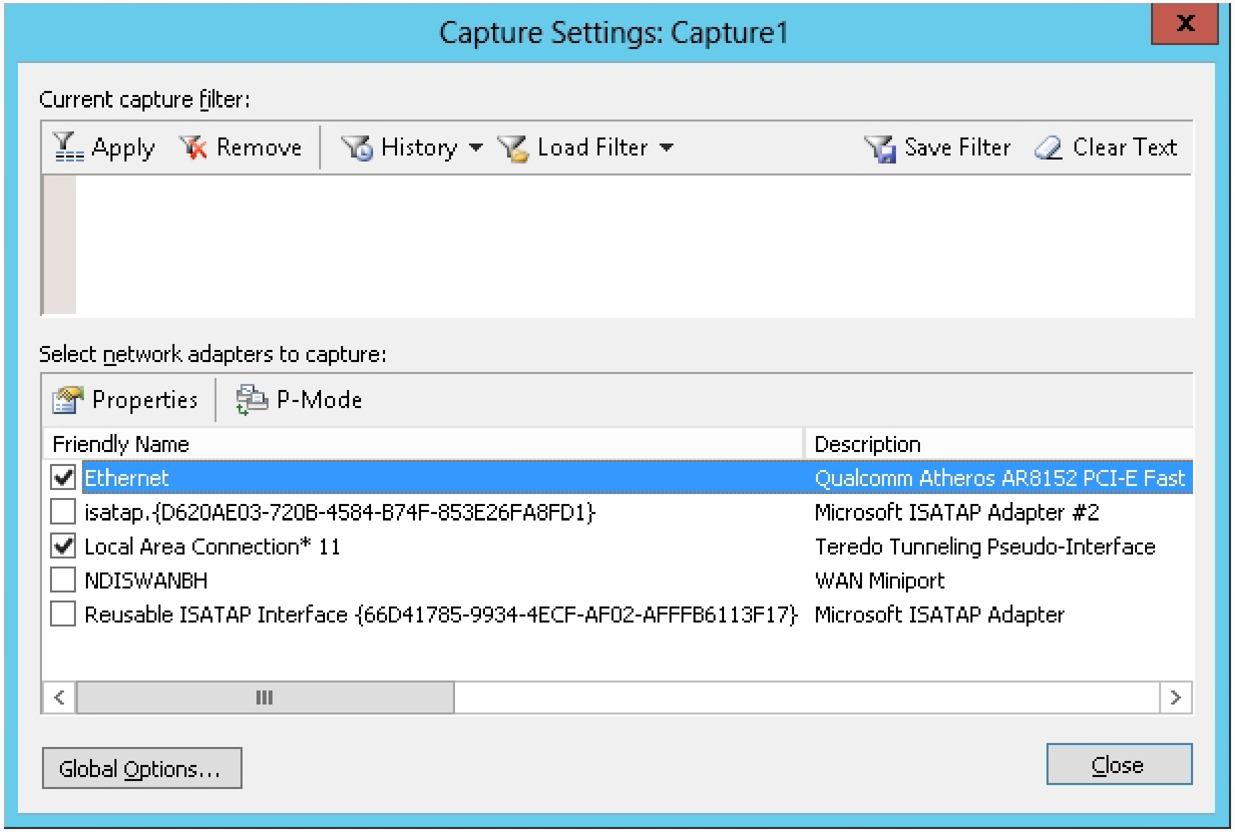
- Allows you to view actual packets on a network
- Examples: Wireshark and Microsoft Network Monitor

Capture Packets with Network Monitor


Microsoft Network Monitor 3.4
File Edit View Frames Capture Filter Experts Tools Help
New Capture Open Capture Save As Capture Settings Start Pause Stop
Capture1 Start Page Parsers
Network Conversations
Press "Start" button to begi
Display Filter
Apply Remove History Load Filter Save Filter Clear Text
Frame Summary
Find Autoscroll Color Rules Aliases Columns
Frame Number Time Date Local Adjusted Time Offset Process Name Source Destination Protocol Name Description
Frame Details
Hex Details
Decode As Width Prot Off: Frame Off:
0000
Version 3.4.2350.0 Displayed: Dropped: Captured: Pending: Focused: Selected:

Using the Microsoft Network Monitor

Capture Packets with Network Monitor



Capture Settings: Capture1

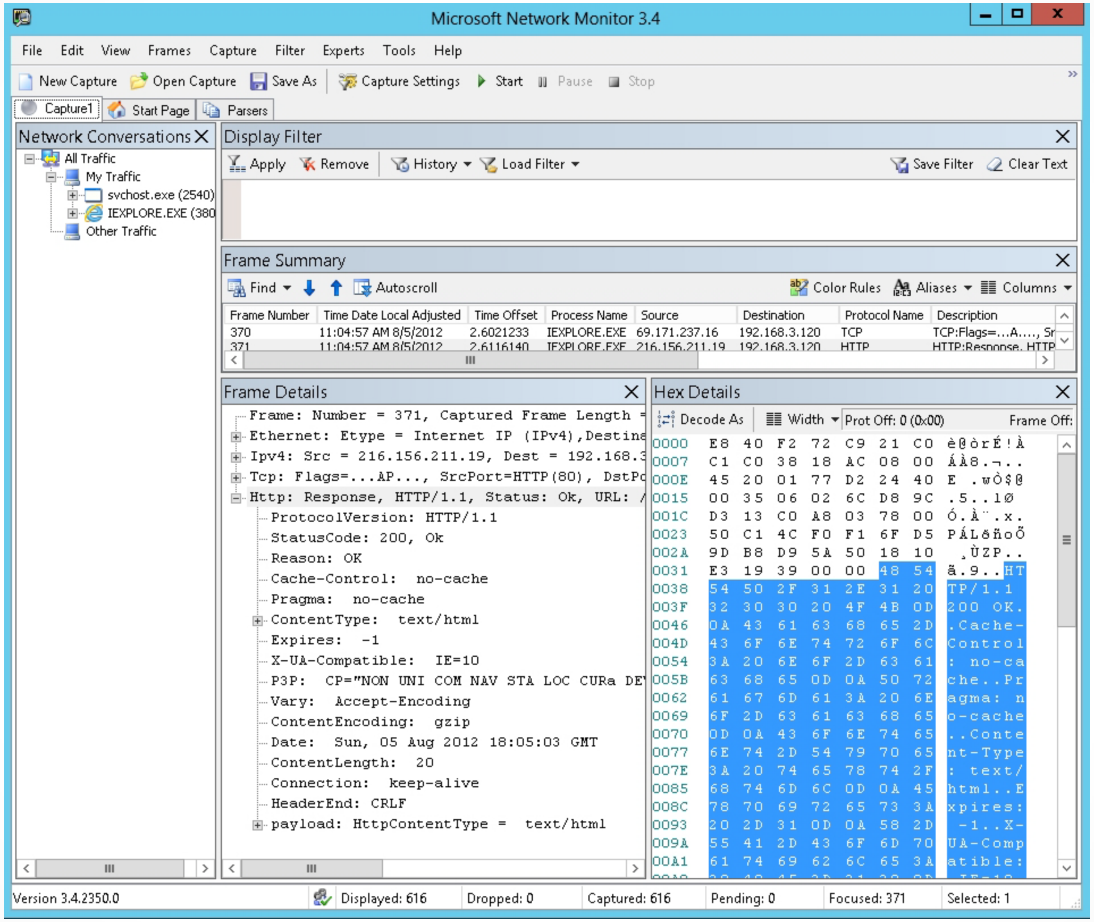
Current capture filter:

Select network adapters to capture:

	Friendly Name	Description
☑	Ethernet	Qualcomm Atheros AR8152 PCI-E Fast
□	isatap.{D620AE03-720B-4584-B74F-853E26FA8FD1}	Microsoft ISATAP Adapter #2
☑	Local Area Connection* 11	Teredo Tunneling Pseudo-Interface
□	NDISWANBH	WAN Miniport
□	Reusable ISATAP Interface {66D41785-9934-4ECF-AF02-AFFFB6113F17}	Microsoft ISATAP Adapter

Configuring capture settings

Capture Packets with Network Monitor



Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
370	11:04:57 AM 8/5/2012	2.6021233	IEXPLORE.EXE	69.171.237.16	192.168.3.120	TCP	TCP:Flags=...A...., Sr
371	11:04:57 AM 8/5/2012	2.6116140	IEXPLORE.EXE	216.156.211.19	192.168.3.120	HTTP	HTTP:Response, HTTP

```
Frame: Number = 371, Captured Frame Length =
Ethernet: Etype = Internet IP (IPv4),Destina
Ipv4: Src = 216.156.211.19, Dest = 192.168.3
Tcp: Flags=...AP..., SrcPort=HTTP(80), DstPo
Http: Response, HTTP/1.1, Status: Ok, URL: /
  ProtocolVersion: HTTP/1.1
  StatusCode: 200, Ok
  Reason: OK
  Cache-Control:  no-cache
  Pragma:  no-cache
  ContentType:  text/html
  Expires:  -1
  X-UA-Compatible:  IE=10
  P3P:  CP="NON UNI COM NAV STA LOC CURa DE
  Vary:  Accept-Encoding
  ContentEncoding:  gzip
  Date:  Sun, 05 Aug 2012 18:05:03 GMT
  ContentLength:  20
  Connection:  keep-alive
  HeaderEnd: CRLF
  payload: HttpContentType =  text/html
```

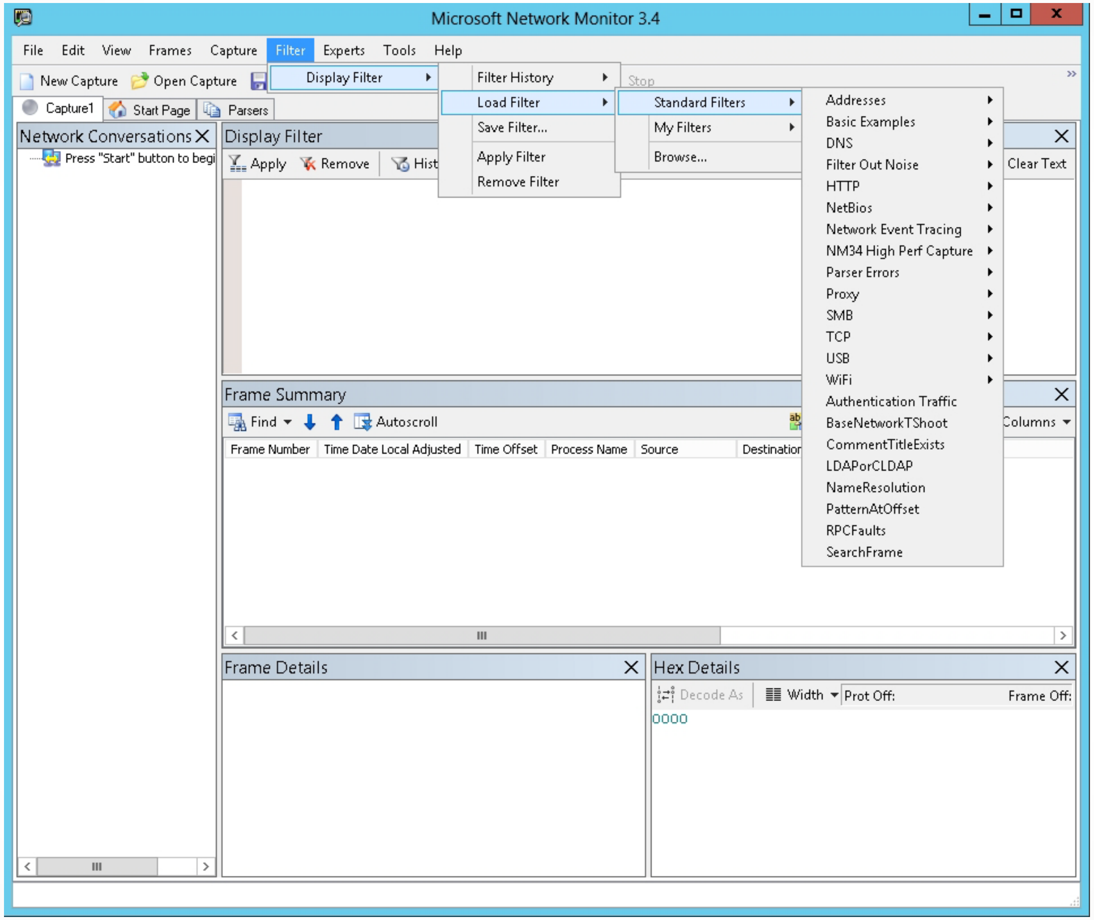
Prot Off: 0 (0x00)   Frame Off:

```
0000  E8 40 F2 72 C9 21 C0  è@òrÉ!À
0007  C1 C0 38 18 AC 08 00  ÁÀ8.¬..
000E  45 20 01 77 D2 24 40  E .wÒ$@
0015  00 35 06 02 6C D8 9C  .5..lØ
001C  D3 13 C0 A8 03 78 00  Ó.À¨.x.
0023  50 C1 4C F0 F1 6F D5  PÁLðñoÕ
002A  9D B8 D9 5A 50 18 10   ¸ÙZP..
0031  E3 19 39 00 00 48 54  ã.9..HT
0038  54 50 2F 31 2E 31 20  TP/1.1
003F  32 30 30 20 4F 4B 0D  200 OK.
0046  0A 43 61 63 68 65 2D  .Cache-
004D  43 6F 6E 74 72 6F 6C  Control
0054  3A 20 6E 6F 2D 63 61  : no-ca
005B  63 68 65 0D 0A 50 72  che..Pr
0062  61 67 6D 61 3A 20 6E  agma: n
0069  6F 2D 63 61 63 68 65  o-cache
0070  0D 0A 43 6F 6E 74 65  ..Conte
0077  6E 74 2D 54 79 70 65  nt-Type
007E  3A 20 74 65 78 74 2F  : text/
0085  68 74 6D 6C 0D 0A 45  html..E
008C  78 70 69 72 65 73 3A  xpires:
0093  20 2D 31 0D 0A 58 2D   -1..X-
009A  55 41 2D 43 6F 6D 70  UA-Comp
00A1  61 74 69 62 6C 65 3A  atible:
```

Version 3.4.2350.0 | Displayed: 616 | Dropped: 0 | Captured: 616 | Pending: 0 | Focused: 371 | Selected: 1

Viewing the frame details

Capture Packets with Network Monitor



Choosing a standard filter

Monitoring Virtual Machines (VMs)

Lesson 3: Monitoring Servers

Hyper-V Resource Metering

- ***Hyper-V Resource Metering*** is a tool that allows you to view the resource usage of a host and individual VMs.
- Some Hyper-V Resource metering cmdlets:
  - `Enable-VMResourceMetering` starts collecting data per virtual machine.
  - `Disable-VMResourceMetering` disables resource metering per virtual machine.
  - `Reset-VMResourceMetering` resets virtual machine resource-metering counters.
  - `Measure-VM` displays resource-metering statistics for a specific virtual machine.

Resource Metering with Windows PowerShell

- To enable Hyper-V resource metering on a Hyper-V host:

```
Get-VM -ComputerName <HostName> | Enable-
VMResourceMetering
```

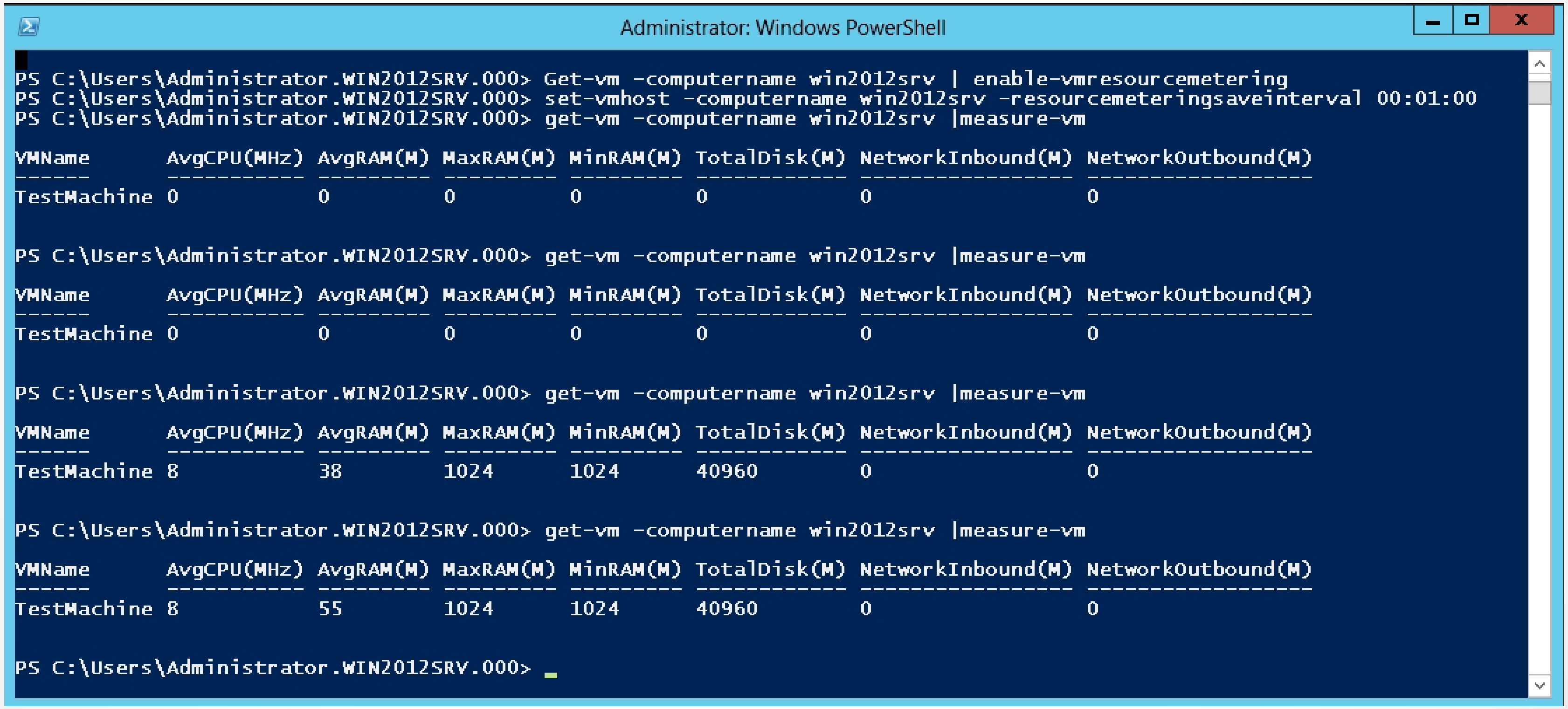
- To change the interval to one minute:

```
Set-vmhost -computername <HostName>
-ResourceMeteringSaveInterval 00:01:00
```

- To get all VMs metering data for a host:

```
Get-VM -ComputerName <HostName> |
Measure-VM
```

Resource Metering



```
PS C:\Users\Administrator.WIN2012SRV.000> Get-vm -computername win2012srv | enable-vmresourcemetering
PS C:\Users\Administrator.WIN2012SRV.000> set-vmhost -computername win2012srv -resourcemeteringsaveinterval 00:01:00
PS C:\Users\Administrator.WIN2012SRV.000> get-vm -computername win2012srv |measure-vm

VMName      AvgCPU(MHz) AvgRAM(M) MaxRAM(M) MinRAM(M) TotalDisk(M) NetworkInbound(M) NetworkOutbound(M)
------      ----------- --------- --------- --------- ------------ ----------------- ------------------
TestMachine 0           0         0         0         0            0                 0


PS C:\Users\Administrator.WIN2012SRV.000> get-vm -computername win2012srv |measure-vm

VMName      AvgCPU(MHz) AvgRAM(M) MaxRAM(M) MinRAM(M) TotalDisk(M) NetworkInbound(M) NetworkOutbound(M)
------      ----------- --------- --------- --------- ------------ ----------------- ------------------
TestMachine 0           0         0         0         0            0                 0


PS C:\Users\Administrator.WIN2012SRV.000> get-vm -computername win2012srv |measure-vm

VMName      AvgCPU(MHz) AvgRAM(M) MaxRAM(M) MinRAM(M) TotalDisk(M) NetworkInbound(M) NetworkOutbound(M)
------      ----------- --------- --------- --------- ------------ ----------------- ------------------
TestMachine 8           38        1024      1024      40960        0                 0


PS C:\Users\Administrator.WIN2012SRV.000> get-vm -computername win2012srv |measure-vm

VMName      AvgCPU(MHz) AvgRAM(M) MaxRAM(M) MinRAM(M) TotalDisk(M) NetworkInbound(M) NetworkOutbound(M)
------      ----------- --------- --------- --------- ------------ ----------------- ------------------
TestMachine 8           55        1024      1024      40960        0                 0


PS C:\Users\Administrator.WIN2012SRV.000> _
```

Enabling Resource Metering

Lesson Summary

- The Microsoft Management Console (MMC) is one of the primary administrative tools used to manage Windows and many network services provided by Windows.
- Administrative Tools is a folder in the Control Panel that contains tools for system administrators and advanced users.
- Server Manager is a management console in Windows Server 2012 that helps you manage local and remote Windows-based servers.
- The Event Viewer enables you to browse and manage event logs.
- Use Microsoft enhanced Event Viewer to capture events from multiple computers so that you can view the events using one console.
- The Reliability Monitor provides a stability index that ranges from 1 (the least stable) to 10 (the most stable). You can use the index to help evaluate the reliability of your computer.

Lesson Summary

- Performance is the overall effectiveness of how data moves through the system.
- Task Manager provides information about programs and processes running on your computer.
- Resource Monitor is a powerful tool for understanding how your system resources are used by processes and services.
- Performance Monitor provides tools for analyzing system performance:
  - Create Data Collector Sets (DCS) to organize a set of performance counters, event traces, and system configuration data into a single object that can be reused as needed.
- The `netstat` command displays TCP/IP connections.
- Hyper-V Resource Metering allows you to view the resource usage of a host and individual VMs.