Lesson 3: Monitoring Servers

MOAC 70-411: Administering Windows Server 2012
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
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Task Scheduler</td>
<td>Manages tasks</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Multimedia Class Scheduler</td>
<td>Enables multimedia class scheduling</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>NetLogon</td>
<td>Manages user credentials</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Network Access Protection Agent</td>
<td>Manages network access</td>
<td>Running</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Network Connections</td>
<td>Manages network connections</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Network Connectivity Assistant</td>
<td>Manages network connectivity</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Network List Service</td>
<td>Manages network list</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Network Location Awareness</td>
<td>Manages network location</td>
<td>Running</td>
<td>Automatic</td>
<td>Network Service</td>
</tr>
<tr>
<td>Network Store Interface Service</td>
<td>Manages network storage</td>
<td>Running</td>
<td>Automatic</td>
<td>Local Service</td>
</tr>
<tr>
<td>Optimize Drives</td>
<td>Manages system optimization</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Performance Counter DLL Host</td>
<td>Manages performance counter DLL</td>
<td>Manual</td>
<td>Manual</td>
<td>Local Service</td>
</tr>
<tr>
<td>Power</td>
<td>Manages power policy</td>
<td>Running</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Power Service</td>
<td>Manages power service</td>
<td>Running</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Print Spooler</td>
<td>Manages print spooling</td>
<td>Running</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>Printer Extensions and Notifications</td>
<td>Manages printer extensions and notifications</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Problem Reports and Solutions Collector</td>
<td>Collects problem reports</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Remote Access Auto Connection Manager</td>
<td>Manages remote access</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Remote Access Connection Manager</td>
<td>Manages remote access</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Remote Desktop Configuration</td>
<td>Manages remote desktop</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Remote Desktop Services</td>
<td>Manages remote desktop services</td>
<td>Manual</td>
<td>Manual</td>
<td>Network Service</td>
</tr>
<tr>
<td>Remote Desktop Services User Mode</td>
<td>Manages remote desktop user mode</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC)</td>
<td>Manages remote procedure</td>
<td>Running</td>
<td>Automatic</td>
<td>Network Service</td>
</tr>
<tr>
<td>Remote Procedure Call (RPC) Locator</td>
<td>Manages remote procedure locator</td>
<td>Running</td>
<td>Automatic</td>
<td>Network Service</td>
</tr>
<tr>
<td>Remote Registry</td>
<td>Manages remote registry</td>
<td>Automatic</td>
<td>Manual</td>
<td>Local Service</td>
</tr>
<tr>
<td>Resultant Set of Policy Provider</td>
<td>Manages resultant set of policy provider</td>
<td>Manual</td>
<td>Manual</td>
<td>Local System</td>
</tr>
<tr>
<td>Routing and Remote Access</td>
<td>Manages routing and remote access</td>
<td>Manual</td>
<td>Automatic</td>
<td>Local System</td>
</tr>
<tr>
<td>RDP Endpoint Manager</td>
<td>Manages RDP endpoints</td>
<td>Running</td>
<td>Automatic</td>
<td>Network Service</td>
</tr>
</tbody>
</table>
The Services Console Properties Dialog Box

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

Viewing the Log On tab
Services Best Practices

• Use caution when changing the startup parameters for a service:
  o Includes the Startup type and Log on as settings.
  o Changes might prevent key services from running correctly.

• Do not change the Allow service to interact with desktop setting.
  o 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

Event Viewer
Understanding Logs and Events

- Custom Views
- Windows Logs
- Applications and Services Logs
Event Viewer MMC Snap-In

Viewing System logs

© 2013 John Wiley & Sons, Inc.
Event Viewer MMC Snap-In

Viewing an event:

Driver Send To Microsoft OneNote 2010Driver 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
Event ID: 1111
Level: Error
Task Category: None
Logged: 8/1/2012 6:20:30 PM
Keywords: Classic
User: N/A
Computer: WIN2012SRV.contoso.com
OpCode: Info

More Information: Event Log Online Help

Copy

Close
Common Files Displayed in Event Viewer Logs

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>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).</td>
</tr>
<tr>
<td>Event ID</td>
<td>A number identifying the particular event type.</td>
</tr>
</tbody>
</table>
| 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

The Filter Current Log dialog box
Create a Basic Task

Attaching a Task to an event
Create a Basic Task

Choosing an action

- Start a program
- Send an e-mail (deprecated)
- Display a message (deprecated)
Create a Basic Task

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

Creating a subscription
Create an Event Subscription

Subscription Properties

Subscription name: [field]
Description: [field]
Destination log: [field]

Subscription type and source computers:
- Collector initiated [Select Computers...]
- Source computer initiated [Select Computer Groups...]

Events to collect: [filter not configured] [Select Events...]
User account (the selected account must have read access to the source log):
- Machine Account [Advanced...]
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

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

Ending a task
Using Task Manager

Viewing CPU usage
Using Task Manager

Viewing Memory usage
Using Task Manager

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

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

Viewing Performance Monitor
Using Performance Monitor

Adding counters to Performance Monitor
Using Performance Monitor

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

Creating a new Data Collector Set
Create a Data Collector Set

Starting the Data Collector Set

Start the Data Collector Set.
Create a Performance Alert

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

OK  Cancel
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:
  o Ping the loopback address (127.0.0.1).
  o Ping a local IP address.
  o Ping a remote gateway.
  o 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

Using the Microsoft Network Monitor
Capture Packets with Network Monitor

Configuring capture settings

Capture Settings: Capture1

Current capture filter:
- Apply
- Remove
- History
- Load Filter
- Save Filter
- Clear Text

Select network adapters to capture:
- Ethernet
  - Description: Qualcomm Atheros AR8152 PCI-E Fast
- isatap: {D620AEO3-720B-4584-B74F-853E26FA8FD1}
  - Description: Microsoft ISATAP Adapter #2
- Local Area Connection# 11
  - Description: Teredo Tunneling Pseudo-Interface
- NDISWANBH
  - Description: WAN Miniport
- Reusable ISATAP Interface {66D41785-9934-4ECF-AF02-AFFF6113F17}
  - Description: Microsoft ISATAP Adapter

Global Options...
Capture Packets with Network Monitor

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

- To change the interval to one minute:
  
  ```powershell
  Set-vmhost -computername <HostName> -ResourceMeteringSaveInterval 00:01:00
  ```

- To get all VMs metering data for a host:
  
  ```powershell
  Get-VM -ComputerName <HostName> | Measure-VM
  ```
## Resource Metering

### Enabling Resource Metering

```powershell
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

<table>
<thead>
<tr>
<th>VMName</th>
<th>AvgCPU(MHz)</th>
<th>AvgRAM(M)</th>
<th>MaxRAM(M)</th>
<th>MinRAM(M)</th>
<th>TotalDisk(M)</th>
<th>NetworkInbound(M)</th>
<th>NetworkOutbound(M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestMachine</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

PS C:\Users\Administrator.WIN2012SRV.000> Get-vm -computername win2012srv | Measure-vm

<table>
<thead>
<tr>
<th>VMName</th>
<th>AvgCPU(MHz)</th>
<th>AvgRAM(M)</th>
<th>MaxRAM(M)</th>
<th>MinRAM(M)</th>
<th>TotalDisk(M)</th>
<th>NetworkInbound(M)</th>
<th>NetworkOutbound(M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestMachine</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

PS C:\Users\Administrator.WIN2012SRV.000> Get-vm -computername win2012srv | Measure-vm

<table>
<thead>
<tr>
<th>VMName</th>
<th>AvgCPU(MHz)</th>
<th>AvgRAM(M)</th>
<th>MaxRAM(M)</th>
<th>MinRAM(M)</th>
<th>TotalDisk(M)</th>
<th>NetworkInbound(M)</th>
<th>NetworkOutbound(M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestMachine</td>
<td>8</td>
<td>38</td>
<td>1024</td>
<td>1024</td>
<td>40960</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

PS C:\Users\Administrator.WIN2012SRV.000> Get-vm -computername win2012srv | Measure-vm

<table>
<thead>
<tr>
<th>VMName</th>
<th>AvgCPU(MHz)</th>
<th>AvgRAM(M)</th>
<th>MaxRAM(M)</th>
<th>MinRAM(M)</th>
<th>TotalDisk(M)</th>
<th>NetworkInbound(M)</th>
<th>NetworkOutbound(M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestMachine</td>
<td>8</td>
<td>55</td>
<td>1024</td>
<td>1024</td>
<td>40960</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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:
  o 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.