REVIEW LESSON

MTA Course: 98-365 Windows Server® Administration Fundamentals
Lesson name: Understanding Server Maintenance 6.3
Topic: Understand Updates
(One 50-minute class period)
File name: WinServerFund_RL_6.3

Lesson Objective

6.3: Understand updates. *This objective may include but is not limited to:* software; driver; operating systems; applications; Windows® Update; Windows Server Update Services (WSUS).

Preparation Details

Prerequisite student experiences and knowledge

This MTA Certification Exam Review lesson is written for students who have learned about Windows Server Administration fundamentals. Students who do not have the prerequisite knowledge and experiences cited in the objective will find additional learning opportunities using resources such as those listed in the Microsoft® resources and Web links at the end of this review lesson.

Students should have successfully configured Windows Software Update Services.

Instructor preparation activities

- Make copies of Student Activity WinServerFund_SA_6.3
- If available, have one virtual machine:
  - Windows Server 2008® R2 configured as an Active Directory® Domain Controller

Resources, software, and additional files needed for this lesson

- WinServerFund_PPT_6.3

- WinServerFund_SA_6.3
- Microsoft Baseline Security Analyzer *http://www.microsoft.com/downloads/details.aspx?FamilyID=b1e76bbe-71df-41e8-8b52-c871d012ba78&displaylang=en*

Teaching Guide

Essential Vocabulary

critical update—a broadly released fix for a specific problem, addressing a critical, non-security–related bug.

hotfix—a single package composed of one or more files used to address a problem in a product. Hotfixes address a specific customer situation, are available only through a support relationship with Microsoft, and may not be distributed outside the customer organization without written legal consent from Microsoft. The terms QFE (quick-fix engineering update), patch, and update have been used in the past as synonyms for hotfix.

Microsoft Baseline Security Analyzer (MBSA)—a tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. MBSA is used to detect common security misconfigurations and missing security updates on your computer systems.

service packs—a cumulative set of hotfixes, security patches, critical updates, and updates since the release of the product, including many resolved problems that have not been made available through any other software updates. Service packs may also contain a limited number of customer-requested design changes or features. Service packs are broadly distributed and tested by Microsoft more than any other software updates.

security patch—a broadly released fix for a specific product, addressing a security vulnerability. A security patch is often described as having a particular level of severity.

software notifications—messages that will periodically inform the user about new programs that can enhance your experiences with the computer and the Internet.

update—a broadly released fix for a specific problem, addressing a non-critical, non-security–related bug.

update management—the process of controlling the deployment and maintenance of interim software releases into production environments. It helps you to maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of your production environment.

virus—an intrusive program that infects computer files by inserting copies of self-replicating code, and deletes critical files, makes system modifications, or performs some other action to cause harm to data on the computer or to the computer itself. A virus attaches itself to a host program.

Windows Server Update Services (WSUS)—enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

worm—a self-replicating program, often malicious like a virus, that can spread from computer to computer without infecting files first by exploiting security vulnerabilities.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Student prompt (see PowerPoint® slide 3): On a sheet of paper, describe the role of Windows Server Update Services.
2. Give students a few minutes to respond, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their responses.

Lesson activity (40 minutes)

1. Teacher Instruction (20 minutes)
    - Use the included PowerPoint presentation to review updates.
    - At the end of the presentation, ask the students to answer the Review Questions. Small-group discussions or a "think-pair-share" approach may be beneficial.
        - Show the question and give the students 1 minute to process the question and come up with answers.
        - Then give the students 2 minutes to discuss answers with a partner.
        - Finally, have each pair of students share their answers with the whole group.
        - Repeat for each additional review question.
2. Guided Practice (20 minutes; please see the "Additional notes to the instructor" section regarding this assignment)
    - Students complete WinServerFund_SA_6.3, downloading and installing Microsoft Baseline Security Analyzer and adding Windows Server Update Services as a role.
    - If time allows, you may review all or part of the worksheet.

Assessment/lesson reflection (10 minutes)

1. At the bottom of WinServerFund_SA_6.3, ask students to describe why having good update management practices is important. Students should be prepared to share their answers.

Microsoft resources and Web links

- **Microsoft TechNet: Update Management Process**
  http://technet.microsoft.com/en-us/library/cc700845.aspx
- **Microsoft TechNet: Windows Server Update Service**
  http://technet.microsoft.com/en-us/wsus/default.aspx

Suggested best practices

- Dialogue with the students about the importance of patch management. Provide examples of when you should immediately apply an update and when not to. It is also important to stress that service pack updates are not always supported by third-party software developers at release time.

Additional notes to the instructor

- The worksheet asks students to download and install the Microsoft Baseline Security Analyzer. The worksheet specifies that they are working on Windows Server 2008 R2, which will require a 64-bit version of the tool.
- The students are asked to add the Windows Server Update Service as a role and then modify the server's local group policy so it will retrieve updates from itself. The installation process is somewhat time-consuming, therefore, the group policy portion may be finished outside of class.