

**LESSON 6.3**

98-365 Windows Server Administration Fundamentals

# Understand Updates

## Lesson Overview

In this lesson, you will learn about:

- Update management
- Microsoft® Baseline Security Analyzer (MBSA)
- Windows Server® Update Services

## LESSON 6.3

### 98-365 Windows Server Administration Fundamentals

# Anticipatory Set

What is the Windows® Server Update Service?

## Update Management

- The process of controlling the deployment and maintenance of interim software releases into production environments
- Poor update management can result in:
  - Downtime
  - Remediation time
  - Questionable data integrity
  - Lost credibility
  - Negative public relations
  - Legal defenses
  - Stolen intellectual property



## Update Management

- Microsoft process for updating software after release
  - Microsoft makes available periodic updates.
  - Every Microsoft product group includes a sustaining engineering team which develops updates to resolve problems.
- The process is as follows:
  1. Microsoft is made aware of a security vulnerability.
  2. Issue is evaluated and verified by the Microsoft Security Response Center.
  3. The product groups sustaining team creates and tests update.
  4. Microsoft distributes the software update through the Microsoft Download Center and other services:
    - Automatic Updates and User Initiated Updates

## LESSON 6.3

### 98-365 Windows Server Administration Fundamentals

## Update Management (continued)

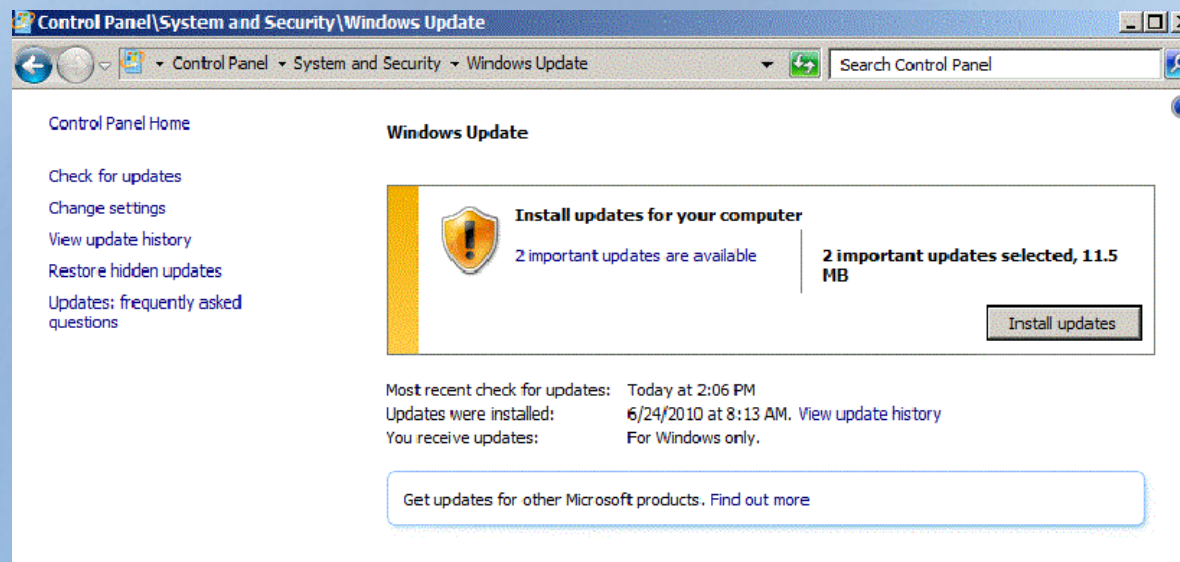
Term	Definition
Security patch	A broadly released fix for a specific product, addressing a security vulnerability
Critical update	A broadly released fix for a specific problem, addressing a critical, non-security-related bug
Update	A broadly released fix for a specific problem, addressing a non-critical, non-security-related bug
Hotfix	A single package composed of one or more files used to address a problem in a product.
Service pack	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.

## LESSON 6.3

### 98-365 Windows Server Administration Fundamentals

# Update Management

- Windows updates—additions to software that can help prevent or fix problems, improve how your computer works, or enhance your computing experience
- Windows updates can be managed through **Control Panel→System and Security→Windows Update**.

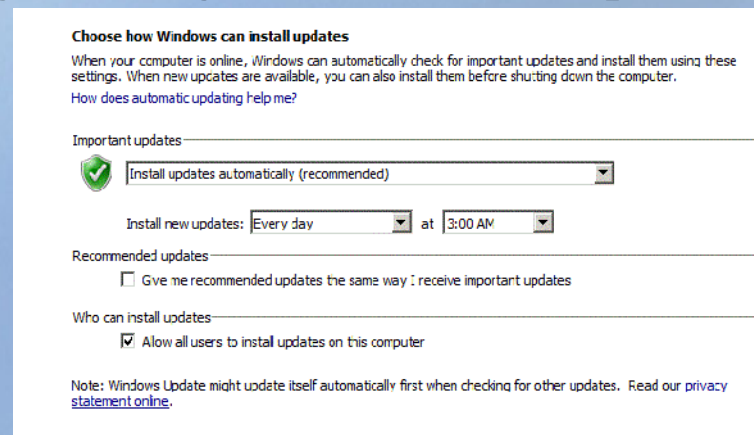


## LESSON 6.3

### 98-365 Windows Server Administration Fundamentals

# Update Management (continued)


- Within Windows updates, an administrator can:
  - Check for updates—check online for available updates
  - Change settings—change how and when updates are installed



**Choose how Windows can install updates**

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.  
[How does automatic updating help me?](#)

**Important updates**



Install new updates:  at

**Recommended updates**

☐ Give me recommended updates the same way I receive important updates

**Who can install updates**

☒ Allow all users to install updates on this computer

Note: Windows Update might update itself automatically first when checking for other updates. Read our [privacy statement online](#).

- View update history—see what updates have already been installed and can be uninstalled
- Restore hidden updates—allows you to restore hidden updates to manage



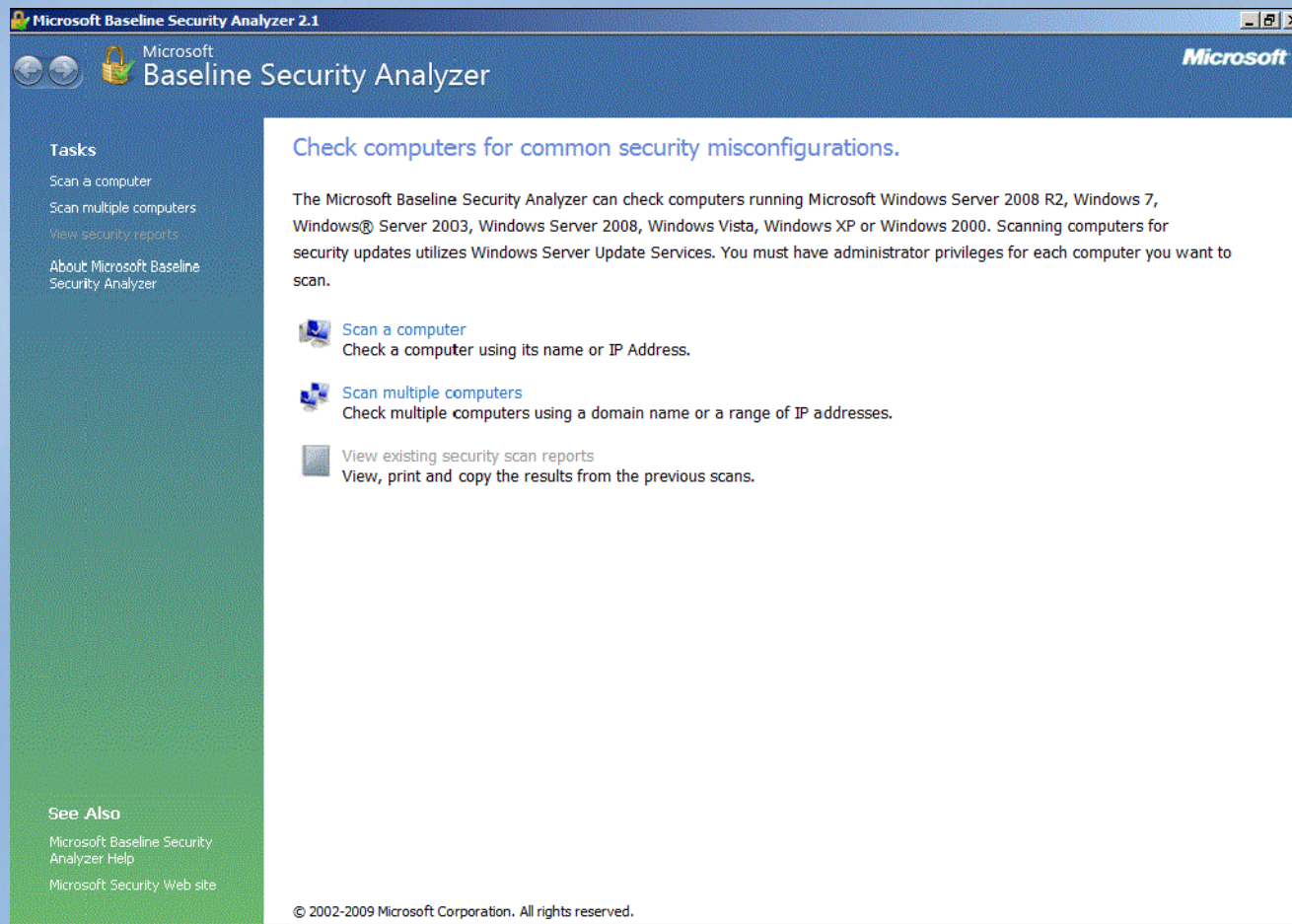
## Microsoft Baseline Security Analyzer (MBSA)

- A tool designed for the IT professional that helps determine their security state in accordance with Microsoft security recommendations and offers remediation guidance. You can use MBSA to detect common security misconfigurations and missing security updates on your computer systems.
- The MBSA can check computers running:
  - Windows Server 2008<sup>®</sup> R2, Windows Server 2008
  - Windows 7<sup>®</sup>
  - Windows Server 2003<sup>®</sup>
  - Windows Vista<sup>®</sup>
  - Windows XP<sup>®</sup>
  - Windows 2000<sup>®</sup>

## LESSON 6.3

# 98-365 Windows Server Administration Fundamentals

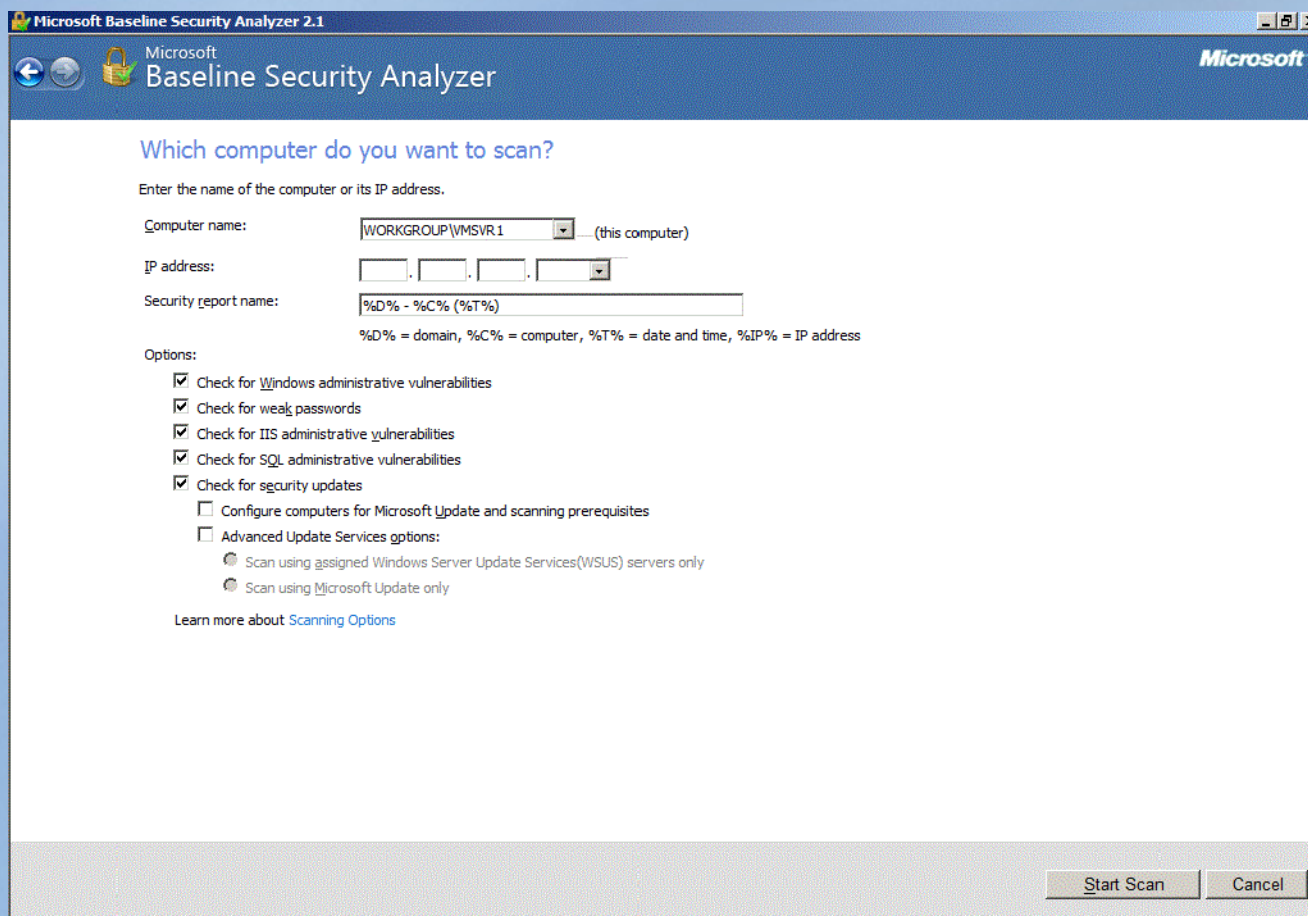
## MBSA (continued)



## LESSON 6.3

### 98-365 Windows Server Administration Fundamentals

# MBSA (continued)



The screenshot shows the Microsoft Baseline Security Analyzer 2.1 window. The title bar reads "Microsoft Baseline Security Analyzer 2.1". The main window has a blue header with the Microsoft logo and the text "Microsoft Baseline Security Analyzer". The main content area is white and contains the following elements:

- Which computer do you want to scan?**
- Enter the name of the computer or its IP address.**
- Computer name:** A dropdown menu showing "WORKGROUP\VMSSVR1" with a "(this computer)" link to its right.
- IP address:** Four input boxes for IP address segments, with a dropdown arrow on the right.
- Security report name:** A text box containing "%D% - %C% (%T%)". Below this, a legend states: "%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address".
- Options:**
  - ☒ Check for Windows administrative vulnerabilities
  - ☒ Check for weak passwords
  - ☒ Check for IIS administrative vulnerabilities
  - ☒ Check for SQL administrative vulnerabilities
  - ☒ Check for security updates
  - ☐ Configure computers for Microsoft Update and scanning prerequisites
  - ☐ Advanced Update Services options:
    - ☒ Scan using assigned Windows Server Update Services(WSUS) servers only
    - ☐ Scan using Microsoft Update only
- [Learn more about Scanning Options](#)

At the bottom right, there are two buttons: "Start Scan" and "Cancel".



## LESSON 6.3

# 98-365 Windows Server Administration Fundamentals

## MBSA (continued)

The screenshot shows the Microsoft Baseline Security Analyzer 2.1 interface. The title bar reads "Microsoft Baseline Security Analyzer 2.1". The main window displays a report for "WORKGROUP - VMSVR1" dated "2010-07-14 09:26:39". A red warning icon indicates a "Severe Risk (One or more critical checks failed.)".

**Report Details for WORKGROUP - VMSVR1 (2010-07-14 09:26:39)**

**Security assessment:**  
Severe Risk (One or more critical checks failed.)

**Computer name:** WORKGROUP\VMSVR1  
**IP address:** 192.168.0.101  
**Security report name:** WORKGROUP - VMSVR1 (7-14-2010 9-26 AM)  
**Scan date:** 7/14/2010 9:26 AM  
**Scanned with MBSA version:** 2.1.2112.0  
**Catalog synchronization date:** 7/14/2010 9:26 AM  
**Security update catalog:** Microsoft Update

Sort Order:

**Security Update Scan Results**

Score	Issue	Result
✓	SQL Server Security Updates	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>
✓	Windows Security Updates	No security updates are missing. <a href="#">What was scanned</a> <a href="#">Result details</a>

**Windows Scan Results**

**Administrative Vulnerabilities**

Score	Issue	Result
⚠	Password Expiration	Some user accounts (1 of 4) have non-expiring passwords. <a href="#">What was scanned</a> <a href="#">Result details</a> <a href="#">How to correct this</a>
i	Incomplete	No incomplete software update installations were found.

Print this report    Copy to clipboard    Previous security report    Next security report    OK



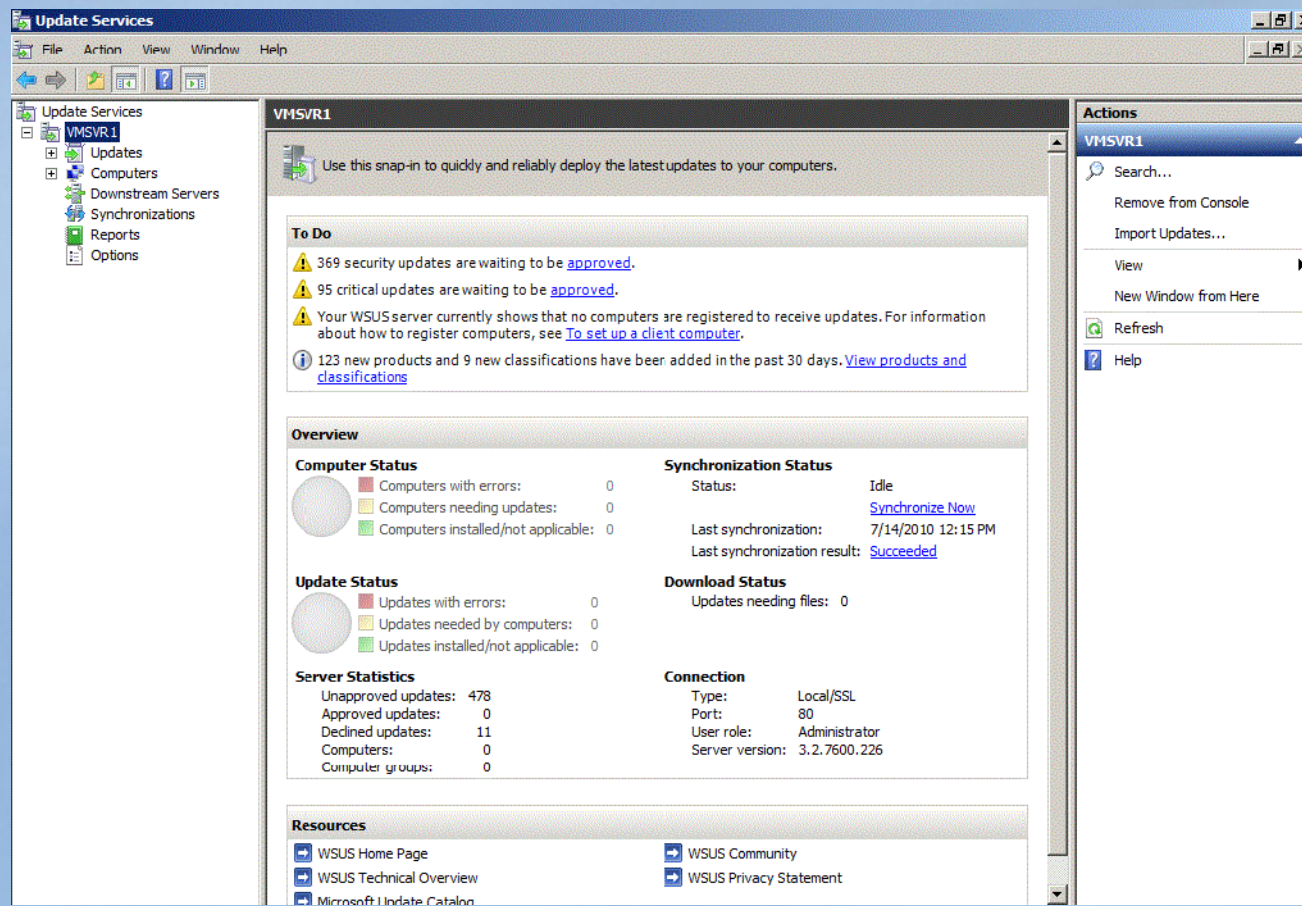
## **Windows Server Update Service (WSUS)**

- 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.
- Must be added as a Role for Windows Server 2008 R2
  - Requires Internet Information Services to be added as a Role Service

## LESSON 6.3

# 98-365 Windows Server Administration Fundamentals

## WSUS (continued)



## Lesson Review

- What Role service is required to install the Windows Software Update Services?
- What versions of Windows will Microsoft Baseline Security Analyzer work with?
- What is the difference between a service pack and security update?