



98-367

MTA Windows Server

A Success Guide to Prepare-  
Microsoft Security Fundamentals

[edusum.com](http://edusum.com)

## Table of Contents

|   |          |
|---|----------|
| <b>Introduction to 98-367 Exam on Microsoft Security Fundamentals .....</b> | <b>2</b> |
| <b>Microsoft 98-367 Certification Details: .....</b>                        | <b>2</b> |
| <b>Microsoft 98-367 Exam Syllabus: .....</b>                                | <b>3</b> |
| <b>98-367 Sample Questions: .....</b>                                       | <b>5</b> |
| <b>Answers to 98-367 Exam Questions: .....</b>                              | <b>6</b> |

# Introduction to 98-367 Exam on Microsoft Security Fundamentals

Use this quick start guide to collect all the information about Microsoft Security Fundamentals (98-367) Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the 98-367 Microsoft Security Fundamentals exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual Microsoft MTA Windows Server certification exam.

The Microsoft Security Fundamentals certification is mainly targeted to those candidates who want to build their career in Windows Server domain. The Microsoft Technology Associate (MTA) - Windows Server 2016 exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of Microsoft MTA Windows Server.

## Microsoft 98-367 Certification Details:

|                     |   |
|---------------------|---|
| Exam Name           | Microsoft Technology Associate (MTA) - Windows Server 2016  |
| Exam Code           | 98-367  |
| Exam Price          | \$127 (USD)   |
| Duration            | 50 min  |
| Number of Questions | 30-50   |
| Passing Score       | 700 / 1000  |
| Books / Training    | <a href="#">40032A: Networking and Security Fundamentals: Training two-pack for MTA Exams 98-366 and 98-367</a><br><a href="#">40367A: Security Fundamentals: MTA Exam 98-367</a> |
| Schedule Exam       | <a href="#">Pearson VUE</a>   |
| Sample Questions    | <a href="#">Microsoft Security Fundamentals Sample Questions</a>  |
| Practice Exam       | <a href="#">Microsoft 98-367 Certification Practice Exam</a>  |

## Microsoft 98-367 Exam Syllabus:

| Topic                                | Details   | Weights |
|--------------------------------------|---|---------|
| Understand security layers           | <p>Understand core security principles</p> <ul style="list-style-type: none"> <li>- Confidentiality; integrity; availability; how threat and risk impact principles; principle of least privilege; social engineering; attack surface analysis; threat modelling</li> </ul> <p>Understand physical security</p> <ul style="list-style-type: none"> <li>- Site security; computer security; removable devices and drives; access control; mobile device security; keyloggers</li> </ul> <p>Understand Internet security</p> <ul style="list-style-type: none"> <li>- Browser security settings; secure websites</li> </ul> <p>Understand wireless security</p> <ul style="list-style-type: none"> <li>- Advantages and disadvantages of specific security types; keys; service set identifiers (SSIDs); MAC filters</li> </ul>   | 25-30%  |
| Understand operating system security | <p>Understand user authentication</p> <ul style="list-style-type: none"> <li>- Multifactor authentication; physical and virtual smart cards; Remote Authentication Dial-In User Service (RADIUS); biometrics; use Run As to perform administrative tasks</li> </ul> <p>Understand permissions</p> <ul style="list-style-type: none"> <li>- File system permissions; share permissions; registry; Active Directory; enable or disable inheritance; behavior when moving or copying files within the same disk or on another disk; multiple groups with different permissions; basic permissions and advanced permissions; take ownership; delegation; inheritance</li> </ul> <p>Understand password policies</p> <ul style="list-style-type: none"> <li>- Password complexity; account lockout; password length; password history; time between password changes; enforce by using Group Policies; common attack methods; password reset procedures; protect domain user account passwords</li> </ul> <p>Understand audit policies</p> <ul style="list-style-type: none"> <li>- Types of auditing; what can be audited; enable auditing; what to audit for specific purposes; where to save audit information; how to secure audit information</li> </ul> <p>Understand encryption</p> <ul style="list-style-type: none"> <li>- Encrypting file system (EFS); how EFS-encrypted folders impact moving/copying files; BitLocker (To Go); TPM; software-based encryption; MAIL encryption and</li> </ul> | 35-40%  |

| Topic                        | Details   | Weights |
|------------------------------|---|---------|
|                              | <p>signing and other uses; virtual private network (VPN); public key/private key; encryption algorithms; certificate properties; certificate services; PKI/certificate services infrastructure; token devices; lock down devices to run only trusted applications</p> <p>Understand malware</p> <ul style="list-style-type: none"> <li>- Buffer overflow; viruses, polymorphic viruses; worms; Trojan horses; spyware; ransomware; adware; rootkits; backdoors; zero day attacks</li> </ul>   |         |
| Understand network security  | <p>Understand dedicated firewalls</p> <ul style="list-style-type: none"> <li>- Types of hardware firewalls and their characteristics; when to use a hardware firewall instead of a software firewall; stateful versus stateless firewall inspection; Security Compliance Manager; security baselines</li> </ul> <p>Understand network isolation</p> <ul style="list-style-type: none"> <li>- Routing; honeypot; perimeter networks; network address translation (NAT); VPN; IPsec; server and domain isolation</li> </ul> <p>Understand protocol security</p> <ul style="list-style-type: none"> <li>- Protocol spoofing; IPsec; tunneling; DNSsec; network sniffing; denial-of-service (DoS) attacks; common attack methods</li> </ul>   | 20–25%  |
| Understand security software | <p>Understand client protection</p> <ul style="list-style-type: none"> <li>- Antivirus; protect against unwanted software installations; User Account Control (UAC); keep client operating system and software updated; encrypt offline folders, software restriction policies; principle of least privilege</li> </ul> <p>Understand email protection</p> <ul style="list-style-type: none"> <li>- Antispam, antivirus, spoofing, phishing, and pharming; client versus server protection; Sender Policy Framework (SPF) records; PTR records</li> </ul> <p>Understand server protection</p> <ul style="list-style-type: none"> <li>- Separation of services; hardening; keep server updated; secure dynamic Domain Name System (DNS) updates; disable unsecure authentication protocols; Read-Only Domain Controllers (RODC)</li> </ul> | 15–20%  |

---

## 98-367 Sample Questions:

**01. To implement multifactor authentication you should use:**

- a) encryption.
- b) a smart card and a PIN.
- c) a username and password.
- d) a biometric input device.

**02. Creating MD5 hash for files is an example of ensuring what?**

- a) Confidentiality
- b) Availability
- c) Least privilege
- d) Integrity

**03. You need to ensure that all security updates have been applied to one of your servers. What should you use?**

- a) Microsoft Baseline Security Analyzer
- b) ScanState.exe
- c) A RADIUS server
- d) Windows Deployment Services

**04. Which type of security service is concerned with preventing or detecting any tampering with data?**

- a) Authentication
- b) Availability
- c) Integrity
- d) Confidentiality

**05. What does implementing Windows Server Update Services (WSUS) allow a company to manage?**

- a) Shared private encryption key updates
- b) Updates to Group Policy Objects
- c) Active Directory server replication
- d) Windows updates for workstations and servers

**06. How does the sender policy framework (SPF) aim to reduce spoofed email?**

- a) It provides a list of IP address ranges for particular domains so senders can be verified.
- b) It includes an XML policy file with each email that confirms the validity of the message.
- c) It lists servers that may legitimately forward mail for a particular domain.
- d) It provides an encryption key so that authenticity of an email message can be validated

**07. Windows Firewall is a:**

- a) stateless software firewall.
- b) stateful software firewall.
- c) means of physically protecting a Windows server.
- d) hardware firewall.

**08. You have a training room with 10 computers. You need to be able to control what software can be run by specific users logging on to the computers. What should you use?**

(Choose two.)

- a) SmartScreen Filtering
- b) Network Access Protection
- c) Software restriction policies
- d) AppLocker
- e) A firewall filter

**09. A mail system administrator scans for viruses in incoming emails to increase the speed of mail processing. Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed" if the underlined text makes the statement correct.**

- a) Decrease the chances of a virus getting to a client machine
- b) Verify that the senders of the messages are legitimate
- c) Ensure that all links in the messages are trustworthy
- d) No change is needed.

**10. Which type of firewall allows for inspection of all characteristics of a packet?**

- a) NAT
- b) Stateful
- c) Stateless
- d) Windows Defender

### Answers to 98-367 Exam Questions:

|                           |                           |                              |                           |                           |
|---------------------------|---------------------------|------------------------------|---------------------------|---------------------------|
| Question: 01<br>Answer: b | Question: 02<br>Answer: d | Question: 03<br>Answer: a    | Question: 04<br>Answer: c | Question: 05<br>Answer: d |
| Question: 06<br>Answer: a | Question: 07<br>Answer: b | Question: 08<br>Answer: c, d | Question: 09<br>Answer: a | Question: 10<br>Answer: b |

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on [feedback@edusum.com](mailto:feedback@edusum.com)