

## MD-100<sup>Q&As</sup>

Windows Client

**Pass Microsoft MD-100 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/md-100.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft  
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Your network contains an Active Directory domain. All users have been issued with computers that run Windows 8.1.

A user named Mia Hamm has a computer named Computer1. You upgrade Computer1 to Windows 10 by performing a clean installation of Windows 10 without formatting the drives.

You need to migrate the settings for Mia Hamm from Windows 8.1 to Windows 10.

Which two actions should you perform?

NOTE: Each correct selection is worth one point.

- A. Run scanstate.exe and specify the C:\Users folder
- B. Run loadstate.exe and specify the C:\Windows.old folder
- C. Run usmultils.exe and specify the C:\Users folder
- D. Run scanstate.exe and specify the C:\Windows.old folder
- E. Run loadstate.exe and specify the C:\Users folder
- F. Run usmultils.exe and specify the C:\Windows.old folder

Correct Answer: DE

D: As we have performed a clean installation of Windows 10 without formatting the drives, User1\'s Windows 8.1 user profile will be located in the \Windows.old folder. Therefore, we need to run scanstate.exe on the \Windows.old folder.

E: User1\'s Windows 10 profile will be in the C:\Users folder so we need to run loadstate.exe to apply the changes in the C:\Users folder.

Reference: <https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-how-it-works>

<https://docs.microsoft.com/en-us/windows/deployment/usmt/usmt-common-migration-scenarios#bkmk-fourpcrefresh>

---

**QUESTION 2****HOTSPOT**

Your network contains an Active Directory domain. The domain contains a computer named Computer1 that runs Windows 10.

The domain contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2

Computer1 contains the shared folders shown in the following table.

Name	Path	Access-based enumeration
Share1\$	D:\Folder1	Disabled
Share2	D:\Folder2	Enabled

The shared folders have the permissions shown in the following table.

Name	Security permission	Sharing permission
Share1\$	Group1: Read Group2: Full control	Everyone: Read Group2: Full control
Share2	Group2: Full control	Everyone: Read Group2: Full control

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Statements	Yes	No
When User1 connects to \\Computer1, Share1\$ is visible.	<input type="radio"/>	<input type="radio"/>
When User2 connects to \\Computer1\Share1\$, the contents of D:\Folder1 are accessible.	<input type="radio"/>	<input type="radio"/>
When User1 connects to \\Computer1\Share2, the contents of D:\Folder2 are accessible.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

**Answer Area**

Statements	Yes	No
When User1 connects to \\Computer1, Share1\$ is visible.	<input type="radio"/>	<input checked="" type="radio"/>
When User2 connects to \\Computer1\Share1\$, the contents of D:\Folder1 are accessible.	<input checked="" type="radio"/>	<input type="radio"/>
When User1 connects to \\Computer1\Share2, the contents of D:\Folder2 are accessible.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No

Share1\$ is a hidden share (dollar sign appended) so the share will never be visible.

Box 2: Yes

User2 is in Group1 and Group2. Both groups have access to Share1\$. Therefore, the contents of the shared folder will

be visible.

Box 3: No

User1 is in Group1. Group1 does not have the necessary security permission to access Share2. You need both security permissions (NTFS permissions) AND share permissions to view the contents of a shared folder. User1 has the necessary share permissions (Everyone: Read), but not the security permission.

---

### QUESTION 3

You have a computer named Computer1. Computer1 runs Windows 10 Pro.

Computer1 is experiencing connectivity issues.

You need to view the IP addresses of any remote computer that Computer1 has an active TCP connection to.

Should you do?

- A. In Windows Administrative Tools, open Performance Monitor
- B. In the Control Panel, open Network and Internet Then select Network and Sharing Center
- C. In Windows Administrative Tools, open Resource Monitor
- D. In the Setting app. open Update and Security Then open Windows Security and select Firewall and Network protection

Correct Answer: C

---

### QUESTION 4

You need to sign in as LocalAdmin on Computer11. What should you do first?

- A. From the LAPS UI tool, view the administrator account password for the computer object of Computer11.
- B. From Local Security Policy, edit the policy password settings on Computer11.
- C. From the LAPS UI tool, reset the administrator account password for the computer object of Computer11.
- D. From Microsoft Intune, edit the policy password settings on Computer11.

Correct Answer: A

References: <https://technet.microsoft.com/en-us/mt227395.aspx>

---

### QUESTION 5

You need to ensure that all the current and future users in the Active Directory domain can establish Remote Desktop connections to Client1. The solution must use the principle of least privilege.

To complete this task, sign in to the required computer or computers.

Correct Answer: See explanation below.

Step 1. Add Remote Desktop Users to the Remote Desktop Users Group.

1.

Open Server Manager.

2.

From Tools menu, select Active Directory Users and Computers

3.

Double click at your domain on the left and then select Builtin.

4.

Open Remote Desktop Users on the right pane.

5.

At Members tab, click Add.

6.

Type the AD users that you want to give Remote access to the RDS Server and click OK.

7.

After selecting the remote desktop users, click OK again to close the window.

Step 2. Allow the log on through remote desktop Services.

1. Open Group Policy Editor. To do that:

a.

Simultaneously press the Windows + R keys to open run command box.

b.

Type gpedit.msc and press Enter.

2.

In Group Policy Editor navigate to: Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment.

3.

At the right Pane: double click at Allow log on through Remote Desktop Services.

4.

Click Add User or Group.

5.

Type remote and then click Check Names.

6.

Select the Remote Desktop Users and click OK.

7.

Click OK at '\\Select users, computers...\\' window.

8.

Finally click OK again and close Group Policy Editor.

Reference: <https://www.wintips.org/fix-to-sign-in-remotely-you-need-the-right-to-sign-in-through-remote-desktop-services-server-2016/>

[MD-100 PDF Dumps](#)

[MD-100 VCE Dumps](#)

[MD-100 Practice Test](#)