70-692^Q&As

Upgrading Your Windows XP Skills to MCSA Windows 8

Pass Microsoft 70-692 Exam with 100% Guarantee

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

https://www.passapply.com/70-692.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

You manage computers that run Windows 8.1.

You plan to install a desktop app named MarketingApp on one of the client computers.

You need to display a progress bar to the user while installing the app.

Which command should you run?

A. msiexec /i marketingapp.msi /qn

B. msiexec /x marketingapp.msi /qb

C. msiexec /x marketingapp.msi /qn

D. msiexec /i marketingapp.msi /qb

Correct Answer: B

QUESTION 2

You have a client computer that runs Windows 8 Pro. The computer contains a storage pool. You need to remove a disk named Disk 2 from the storage pool.
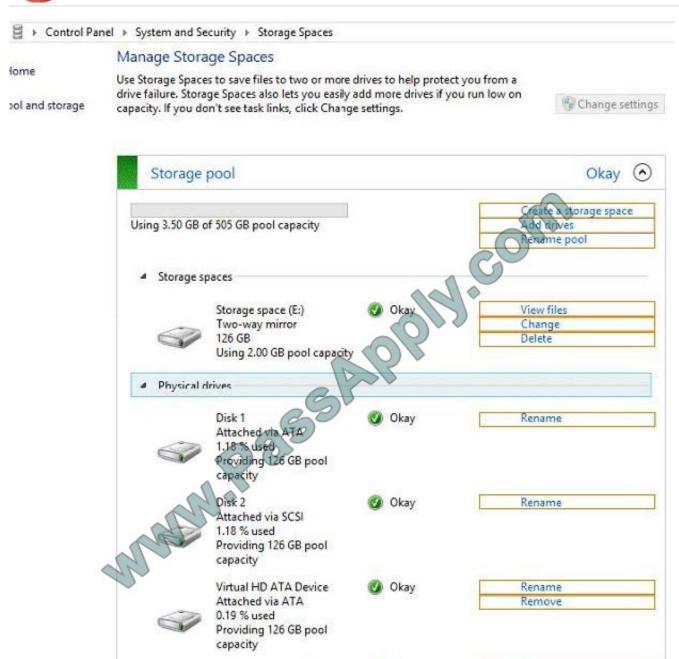
What should you configure first? (To answer, select the appropriate option in the answer area.)

Hot Area:

Control Panel ▸ System and Security ▸ Storage Spaces

Manage Storage Spaces

Home

ool and storage

Use Storage Spaces to save files to two or more drives to help protect you from a drive failure. Storage Spaces also lets you easily add more drives if you run low on capacity. If you don't see task links, click Change settings.

Change settings

Storage pool   Okay ⌃

Using 3.50 GB of 505 GB pool capacity

Create a storage space
Add drives
Rename pool

◢ Storage spaces

Storage space (E:)
Two-way mirror
126 GB
Using 2.00 GB pool capacity

✓ Okay

View files
Change
Delete

◢ Physical drives

Disk 1
Attached via ATA
1.18 % used
Providing 126 GB pool capacity

✓ Okay

Rename

Disk 2
Attached via SCSI
1.18 % used
Providing 126 GB pool capacity

✓ Okay

Rename

Virtual HD ATA Device
Attached via ATA
0.19 % used
Providing 126 GB pool capacity

✓ Okay

Rename
Remove

Microsoft Virtual Disk
Attached via SCSI
0.19 % used
Providing 126 GB pool capacity

✓ Okay

Rename
Remove

Correct Answer:

Control Panel ▸ System and Security ▸ Storage Spaces

Manage Storage Spaces

Home

Use Storage Spaces to save files to two or more drives to help protect you from a
drive failure. Storage Spaces also lets you easily add more drives if you run low on
capacity. If you don't see task links, click Change settings.

ool and storage

Change settings

| Storage pool | Okay ⌃ |

Using 3.50 GB of 505 GB pool capacity

Create a storage space
Add drives
Rename pool

⊿ Storage spaces

Storage space (E:)
Two-way mirror
126 GB
Using 2.00 GB pool capacity

✔ Okay

View files
Change
Delete

⊿ Physical drives

Disk 1
Attached via ATA
1.18 % used
Providing 126 GB pool
capacity

✔ Okay

Rename

Disk 2
Attached via SCSI
1.18 % used
Providing 126 GB pool
capacity

✔ Okay

Rename

Virtual HD ATA Device
Attached via ATA
0.19 % used
Providing 126 GB pool
capacity

✔ Okay

Rename
Remove

Microsoft Virtual Disk
Attached via SCSI
0.19 % used
Providing 126 GB pool
capacity

✔ Okay

Rename
Remove

QUESTION 3

Your company has a main office and a branch office. Each office contains several servers that run Windows Server
2012.

You need to configure BranchCache for the client computers in the branch office. The solution must ensure that all of

the cached content is in a central location.

What should you run on each client computer?

A. The Enable-BCHostedServer cmdlet

B. The Enable-BCLocal cmdlet

C. The Enable-BCDistributed cmdlet

D. The Enable-BCHostedClient cmdlet

Correct Answer: C

QUESTION 4

A company has Windows 8.1 client computers. The company develops a Windows Store app but does not publish it to the Windows Store.

You need to sideload the Windows Store app on all client computers.

Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Run the get-appxpackage Windows PowerShell cmdlet.

B. Run the add-appxpackage Windows PowerShell cmdlet.

C. Enable the Allow all trusted applications to install Group Policy setting.

D. Enable the Allow installation of desktop items Group Policy setting.

E. Run the msiexec command.

Correct Answer: BC

http://technet.microsoft.com/en-us/library/hh856048.aspx Add-AppxPackage

The Add-AppxPackage cmdlet adds a signed app package (.appx) to a user account. Use the DependencyPath parameter to add all other packages that are required for the installation of the app package.

You can use the Register parameter to install from a folder of unpackaged files during development of Windows?Store apps.

To update an already installed package, the new package must have the same package family name.

http://technet.microsoft.com/en-US/windows/jj874388.aspx Try It Out: Sideload Windows Store Apps

By now, you are familiar with Windows Store apps. There are some pretty cool ones available in the store, and publishers are adding more every week. A great thing about Windows Store apps is they are super simple to install (and uninstall).

But what about line of business (LOB) apps? You probably do not want to publish them through the Windows Store since that would make them publically available. Instead, you can sideload LOB apps. Sideloading simply means installing a

Windows Store app without publishing it in and downloading it from the store. You install it directly.

Verify the Requirements

There are a small number of requirements computers must meet to sideload Windows Store apps on them. We will start with computers running Windows 8 Enterprise:

The computer running Windows 8 Enterprise must be joined to the domain. You must enable the "Allow all trusted apps to install" Group Policy setting. The app must be signed by a \ certificate that is chained to a trusted root certificate.

Further Information:

http://technet.microsoft.com/en-us/library/hh856044.aspx Get-AppxPackage

The Get-AppxPackage cmdlet gets a list of the app packages (.appx) that are installed in a user profile.

To get the list of packages for a user profile other than the profile for the current user, you must run this command by using administrator permissions. http:// www.advancedinstaller.com/user-guide/msiexec.html Msiexec.exe Command Line

The Windows Installer technology uses Msiexec.exe for installing MSI and MSP packages.

QUESTION 5

A company has an Active Directory Domain Services (AD DS) domain with Windows 8.1 client computers.

You need to minimize the amount of Trusted Platform Module (TPM) authorization information that is stored in the registry.

What should you do?

A. Create a Group Policy object (GPO) that sets the Configure the level of TPM owner authorization information available to operating system policy setting to None.

B. Create a Group Policy object (GPO) that enables the Turn on TPM Local Encryption policy setting.

C. Create a Group Policy object (GPO) that disables the Configure the level of TPM owner authorization information available to operating system policy setting.

D. Enable Platform Configuration Register indices (PCRs) 0, 2, 4, and 11 for the Configure TPM validation profile for native UEFI firmware configuration policy setting.

Correct Answer: A

Explanation: http://technet.microsoft.com/en-us/library/ jj679889.aspx#BKMK_tpmgp_oauthos Configure the level of TPM owner authorization information available to the operating system

This policy setting configures how much of the TPM owner authorization information is stored in the registry of the local computer. Depending on the amount of TPM owner authorization information that is stored locally, the Windows operating

system and TPM- based applications can perform certain actions in the TPM that require TPM owner authorization without requiring the user to enter the TPM owner password.

There are three TPM owner authentication settings that are managed by the Windows operating system.

You can choose a value of Full, Delegate, or None. Full - This setting stores the full TPM owner authorization, the TPM administrative delegation blob, and the TPM user delegation blob in the local registry. With this setting, you can use the

TPM without requiring remote or external storage of the TPM owner authorization value. This setting is appropriate for scenarios that do not require you to reset the TPM anti-hammering logic or change the TPM owner authorization value.

Some TPM- based applications may require that this setting is changed before features that depend on the TPM anti-hammering logic can be used. Delegated - This setting stores only the TPM administrative delegation blob and the TPM

user delegation blob in the local registry. This setting is appropriate for use with TPM-based applications that depend on the TPM antihammering logic. When you use this setting, we recommend using external or remote storage for the full

TPM owner authorization value--for example, backing up the value in Active Directory Domain Services (AD DS).

None - This setting provides compatibility with previous operating systems and applications. You can also use it for scenarios when TPM owner authorization cannot be stored locally. Using this setting might cause issues with some TPM-

based applications.

Further Information:

http://technet.microsoft.com/en-us/library/cc770660.aspx Active Directory Domain Services (AD DS) can be used to store Trusted Platform Module (TPM) recovery information.

There is only one TPM owner password per computer; therefore, the hash of the TPM owner password is stored as an attribute of the computer object in AD DS. The attribute has the common name (CN) of ms-TPM-OwnerInformation. http://

www.group-policy.com/ref/policy/2859/Configure_TPM_platform_validation_profile Configure TPM platform validation profile

This policy setting allows you to configure how the computer\\'s Trusted Platform Module (TPM) security hardware secures the BitLocker encryption key. This policy setting does not apply if the computer does not have a compatible TPM or if

BitLocker has already been turned on with TPM protection.

If you enable this policy setting before turning on BitLocker, you can configure the boot components that the TPM will validate before unlocking access to the BitLocker-encrypted operating system drive. If any of these components change while BitLocker protection is in effect, the TPM will not release the encryption key to unlock the drive and the computer will instead display the BitLocker Recovery console and require that either the recovery password or recovery key be provided to unlock the drive.

If you disable or do not configure this policy setting, the TPM uses the default platform validation profile or the platform validation profile specified by the setup script. A platform validation profile consists of a set of Platform Configuration Register (PCR) indices ranging from 0 to 23, The default platform validation profile secures the encryption key against changes to the Core Root of Trust of Measurement (CRTM), BIOS, and Platform Extensions (PCR 0), the Option ROM Code (PCR 2), the Master Boot Record (MBR) Code (PCR 4), the NTFS Boot Sector (PCR 8), the NTFS Boot Block (PCR 9), the Boot Manager (PCR 10), and the BitLocker Access Control (PCR 11). The descriptions of PCR settings for computers that use an Extensible Firmware Interface (EFI) are different than the PCR settings described for computers that use a standard BIOS. The BitLocker Drive Encryption Deployment Guide on Microsoft TechNet contains a complete list of PCR settings for both EFI and standard BIOS. Warning: Changing from the default platform validation profile affects the security and manageability of your computer. BitLocker\\'s sensitivity to platform modifications (malicious or authorized) is increased or decreased depending upon inclusion or exclusion (respectively) of the PCRs.