70-680 Q&As

Windows 7 Configuring

Pass Microsoft 70-680 Exam with 100% Guarantee

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

https://www.pass4itsure.com/70-680.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a computer that runs windows 7.

You have a third-party application.

You need to ensure that only a specific version of the application runs on the computer. You have the application vendor\\'s digital signature.

What should you do?

A. From Application Control Policies, configure a path rule.

B. From Application Control Policies, configure a publisher rule.

C. From Software Restriction policies, configure a path rule.

D. From Software Restriction policies, configure a certificate rule.

Correct Answer: B

AppLocker Application Control Policies

AppLocker is a feature new to Windows 7 that is available only in the Enterprise and Ultimate editions of the product. AppLocker policies are conceptually similar to Software Restriction Policies, though AppLocker policies have several

advantages, such as the ability to be applied to specific user or group accounts and the ability to apply to all future versions of a product. As you learned earlier in this chapter, hash rules apply only to a specific version of an application and

must be recalculated whenever you apply software updates to that application. AppLocker policies are located in the Computer Configuration\Windows Settings\ Security Settings \Application Control Policies node of a standard Windows 7 or

Windows Server 2008 R2 GPO. AppLocker relies upon the Application Identity Service being active. When you install Windows 7, the startup type of this service is set to Manual. When testing AppLocker, you should keep the startup type as

Manual in se you configure rules incorrectly. In that event, you can just reboot the computer and the AppLocker rules will no longer be in effect. Only when you are sure that your policies are applied correctly should you set the startup type of

the Application Identity Service to Automatic. You should take great care in testing AppLocker rules because it is possible to lock down a computer running Windows 7 to such an extent that the computer becomes unusable. AppLocker

policies are sometimes called application control policies.

AppLocker Application Control Policies - Publisher Rules Publisher rules in AppLocker work on the basis of the code-signing certificate used by the file\\'s publisher.

Unlike a Software Restriction Policy certificate rule, it is not necessary to obtain a certificate to use a publisher rule because the details of the digital signature are extracted from a reference application file. If a file has no digital signature, you

cannot restrict or allow it using AppLocker publisher rules. Publisher rules allow you more flexibility than hash rules because you can specify not only a specific version of a file but also all future versions of that file. This means that you do not

have to re-create publisher rules each time you apply a software update because the existing rule remains valid. You can also allow only a specific version of a file by setting the Exactly option.

AppLocker Application Control Policies - Path Rules

AppLocker path rules work in a similar way to Software Restriction Policy path rules. Path rules let you specify a folder, in which case the path rule applies to the entire contents of the folder, including subfolders, and the path to a specific file.

The advantage of path rules is that they are easy to create. The disadvantage of path rules is that they are the least secure form of AppLocker rules. An attacker can subvert a path rule if they copy an executable file into a folder covered by a

path rule or overwrite a file that is specified by a path rule. Path rules are only as effective as the file and folder permissions applied on the computer.

Software Restriction Policies

Software Restriction Policies is a technology available to clients running Windows 7 that is available in Windows XP, Windows Vista, Windows Server 2003, and Windows Server 2008. You manage Software Restriction Policies through Group

Policy. You can find Software Restriction Policies in the Computer Configuration \Windows Settings\Security Settings\Software Restriction Policies node of a group policy. When you use Software Restriction Policies, you use the Unrestricted

setting to allow an application to execute and the Disallowed setting to block an application from executing. You can achieve many of the same application restriction objectives with Software Restriction Policies that you can with AppLocker

policies. The advantage of Software Restriction Policies over AppLocker policies is that Software Restriction Policies can apply to computers running Windows XP and Windows Vista, as well as to computers running Windows 7 editions that

do not support AppLocker. The disadvantage of Software Restriction Policies is that all rules must be created manually because there are no built-in wizards to simplify the process of rule creation.

Software Restriction Policies - Path Rules

Path rules, allow you to specify a file, folder, or registry key as the target of a Software Restriction Policy. The more specific a path rule is, the higher its precedence. For example, if you have a path rule that sets the file C: \Program files

\Application\App.exe to Unrestricted and one that sets the folder C:\Program files\Application to Disallowed, the more specific rule takes precedence and the application can execute. Wildcards can be used in path rules, so it is possible to

have a path rule that specifies C:\Program files\Application*.exe. Wildcard rules are less specific than rules that use a file\\'s full path. The drawback of path rules is that they rely on files and folders remaining in place. For example, if you

created a path rule to block the application C:\Apps\Filesharing.exe, an attacker could execute the same application by moving it to another directory or renaming it something other than Filesharing.exe.

Path rules work only when the file and folder permissions of the underlying operating system do not allow files to be moved and renamed.

Software Restriction Policies - Certificate Rules

Certificate rules use a code-signed software publisher\\'s certificate to identify applications signed by that publisher. Certificate rules allow multiple applications to be the target of a single rule that is as secure as a hash rule. It is not necessary

to modify a certificate rule in the event that a software update is released by the vendor because the updated application will still be signed using the vendor\\'s signing certificate. To configure a certificate rule, you need to obtain a certificate

from the vendor. Certificate rules impose a performance burden on computers on which they are applied because the certificate\\'s validity must be checked before the application can execute. Another disadvantage of certificate rules is that

they apply to all applications from a vendor. If you want to allow only 1 application from a vendor to execute but the vendor has 20 applications available, you are better off using a different type of Software Restriction Policy because otherwise

users can execute any of those other 20 applications.

QUESTION 2

Which of the following is used to control when the security pop-up notifications are used?

A. Security Control Manager

B. User Account Control

C. User Access Control Panel

D. Notification Control Settings Manager

Correct Answer: B

QUESTION 3

You have a computer that runs Windows 7.

You enable Advanced Audit Policy Configuration in the Local Computer Policy and discover that the policy is not applied.

You need to ensure that Advanced Audit Policy Configuration is applied on the computer.

What should you do?

A. Restart the computer.

B. Run Gpupdate /force.

C. Enable the Security Settings policy option.

D. Run Secedit /refreshpolicy machine_policy.

Correct Answer: B

QUESTION 4

A company has Windows 7 Enterprise computers that use BitLocker drive encryption on operating system drives.

You need to configure multi-factor authentication before client computers are booted into Windows.

On each client computer, what should you do?

A. Require the use of a startup key.

B. Implement fingerprint authentication.

C. Implement a Dynamic Password Policy.

D. Implement a Dynamic Access Control policy.

E. Configure a TPM PIN.

Correct Answer: E

BitLocker supports multifactor authentication for operating system drives. If you enable BitLocker on a computer that has a TPM version 1.2, you can use additional forms of authentication with the TPM protection. BitLocker offers the option to lock the normal boot process until the user supplies a personal identification number (PIN) or inserts a USB device (such as a flash drive) that contains a BitLocker startup key, or both the PIN and the USB device can be required. These additional security measures provide multifactor authentication and help ensure that the computer will not start or resume from hibernation until the correct authentication method is presented.

QUESTION 5

You have a standalone computer that runs Windows 7. Multiple users share the computer. You need to ensure that you can read the content of all encrypted files on the computer.

What should you do?

A. Run the Certificates Enrollment wizard and then run Certutil.exe -importpfx.

B. Run the Certificates Enrollment wizard and then run Certutil.exe -installcert.

C. Run Cipher.exe /r and then add a data recovery agent from the local security policy.

D. Run Cipher.exe /rekey and then import a security template from the local security policy.

Correct Answer: C

Cipher Displays or alters the encryption of folders and files on NTFS volumes. Used without parameters, cipher displays the encryption state of the current folder and any files it contains. Administrators can use Cipher.exe to encrypt and decrypt data on drives that use the NTFS file system and to view the encryption status of files and folders from a command prompt. The updated version adds another security option. This new option is the ability to overwrite data that you have deleted so that it cannot be recovered and accessed.

When you delete files or folders, the data is not initially removed from the hard disk. Instead, the space on the disk that was occupied by the deleted data is "deallocated." After it is deallocated, the space is available for use when new data is written to the disk. Until the space is overwritten, it is possible to recover the deleted data by using a low-level disk

editor or data-recovery software.

If you create files in plain text and then encrypt them, Encrypting File System (EFS) makes a backup copy of the file so that, if an error occurs during the encryption process, the data is not lost. After the encryption is complete, the backup copy is deleted. As with other deleted files, the data is not completely removed until it has been overwritten. The new version of the Cipher utility is designed to prevent unauthorized recovery of such data.

/K Creates a new certificate and key for use with EFS. If this option is chosen, all the other options will be ignored. By default, /k creates a certificate and key that conform to current group plicy. If ECC is specified, a self-signed certificate will be created with the supplied key size.

/R Generates an EFS recovery key and certificate, then writes them to a .PFX file (containing certificate and private key) and a .CER file (containing only the certificate). An administrator may add the contents of the .CER to the EFS recovery policy to create the recovery for users, and import the .PFX to recover individual files. If SMARTCARD is specified, then writes the recovery key and certificate to a smart card. A .CER file is generated (containing only the certificate). No .PFX file is genereated. By default, /R creates an 2048-bit RSA recovery key and certificate. If EECC is specified, it must be followed by a key size of 356, 384, or 521.