



70-243^{Q&As}

Administering and Deploying System Center 2012 Configuration Manager

Pass Microsoft 70-243 Exam with 100% Guarantee

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

<https://www.geekcert.com/70-243.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

DRAG DROP

Your network contains a System Center 2012 R2 Configuration Manager Service Pack 1 (SP1) environment. Three users named User1, User2, and User3 will perform the following tasks:

- User1 will review software metering data and inventory reports.
- User2 will deploy applications and create alerts.
- User3 will create configuration items.

You need to identify which security role must be assigned to which user.

What should you identify?

To answer, drag the appropriate security role to the correct user in the answer area. Each security role may be used once, more than once, or not at all. Additionally, you may need to drag the split bar between panes or scroll to view content.

Select and Place:

Security Role

Application Deployment Manager

Asset Manager

Compliance Settings Manager

Answer Area

User1

Security role

User2

Security role

User3

Security role

Correct Answer:

Security Role

Answer Area

User1

Asset Manager

User2

Application Deployment Manager

User3

Compliance Settings Manager

*

Box 1: Asset Manager



Grants permissions to manage the Asset Intelligence Synchronization Point, Asset Intelligence reporting classes, software inventory, hardware inventory, and metering rules.

*

Box 2: Application Deployment Manager

Grants permissions to deploy applications. Administrative users who are associated with this role can view a list of applications, and they can manage deployments for applications, alerts, templates and packages, and programs.

Administrative users who are associated

with this role can also view collections and their members, status messages, queries, and conditional delivery rules.

*

Box 3: Compliance Settings Manager

Grants permissions to define and monitor Compliance Settings. Administrative users associated with this role can create, modify, and delete configuration items and baselines.

They can also deploy configuration baselines to collections, and initiate compliance evaluation, and initiate remediation for non-compliant computers.

References: <https://blogs.technet.microsoft.com/hhoy/2012/03/06/role-basedadministration-in-system-center-2012-configuration-manager/>

QUESTION 2

HOTSPOT

You have a System Center 2012 R2 Configuration Manager Service Pack 1 (SP1) deployment.

You have two domain users named User1 and User2.

The users will perform the following administrative tasks:

User1 will create device collections.

User2 will create task sequences.

You need to identify to which security role each user must be added. The solution must use the principle of least privilege.

Which security roles should you identify? To answer, select the appropriate options in the answer area.

Hot Area:



Answer Area

Option

User1:

Application Author

Asset Manager

Company Resource Access Manager

Operations Administrator

User2:

Application Deployment Manager

Company Resource Access Manager

Operating System Deployment Manager

Infrastructure Administrator

Correct Answer:



Answer Area

Option

User1:

Application Author

Asset Manager

Company Resource Access Manager

Operations Administrator

User2:

Application Deployment Manager

Company Resource Access Manager

Operating System Deployment Manager

Infrastructure Administrator

Box 1: Asset Manager.

Grants permissions to manage the Asset Intelligence Synchronization Point, Asset Intelligence reporting classes, software inventory, hardware inventory, and metering rules.

This role also has the permission to create device collections. Operations Manager can also create task sequences but Asset Manager has least privilege.

Box 2: Operating System Deployment Manager

Grants permissions to create operating system images and deploy them to computers.

Administrative users who are associated with this role can manage operating system installation packages and images, task sequences, drivers, boot images, and state migration settings.

QUESTION 3

DRAG DROP

You have a System Center 2012 R2 Configuration Manager Service Pack 1 (SP1) deployment.

You need to implement anti-virus protection for all Configuration Manager clients. The solution must ensure that servers have different anti-virus settings than client computers.

In which order should you perform the required actions? To answer drag the appropriate actions to the correct locations.



Each action may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll

to view content.

Select and Place:

Actions

- Create a Configuration Manager Application.
- Create two deployments.
- Deploy the Endpoint Protection point site system role.
- Deploy the System Health Validator point site system role.
- Modify the Client Settings from the Administration workspace.

Answer Area

- First Action: Action
- Second Action: Action
- Third Action: Create two custom antimalware policies
- Fourth Action: Action

Correct Answer:

Actions

- Create a Configuration Manager Application.
-
-
- Deploy the System Health Validator point site system role.
-

Answer Area

- First Action: Deploy the Endpoint Protection point site system role.
- Second Action: Modify the Client Settings from the Administration workspace.
- Third Action: Create two custom antimalware policies
- Fourth Action: Create two deployments.

Step 1: EndPoint Protection

When System Center 2012 Endpoint Protection is used with Microsoft System Center 2012 Configuration Manager, it provides a comprehensive enterprise management solution that lets you do the following:

*

Centrally deploy and configure the EndpointProtection client.

*

Configure default and custom antimalware policies that apply to groups of computers.

Etc

Step 2:



Client settings for devices include Endpoint Protection.

All client settings in System Center 2012 Configuration Manager are managed in the Configuration Manager console from the Client Settings node in the Administration workspace. A set of default settings is supplied with Configuration

Manager. When you modify the default client settings, these settings are applied to all clients in the hierarchy. You can also configure custom client settings, which override the default client settings when you assign these to collections.

QUESTION 4

HOTSPOT

You have a System Center 2012 R2 Configuration Manager Service Pack 1 (SP1) deployment.

You are creating a custom security role named Role1.

You need to ensure that users to whom Role1 is assigned can create and deploy configuration baselines.

Which two permissions should you modify for Role1? To answer, select the appropriate permissions in the answer area.

Hot Area:



Copy Security Role

Specify details for the customized copy of the selected security role.

Name:

Description:

Based on:

Customize the permissions for this copy of the security role.

Permissions:

▶ Boundaries	Read
▶ Boundary Group	Read
▶ Certificate Profile	Read, Run Report
▶ Client Agent Setting	Read
▶ Cloud Subscription	Read
▶ Collection	Read, View Collected File, Read Resource, Audit S
▶ Communications Provisioning Profile	Read, Run Report
▶ Computer Association	Read, Run Report
▶ Configuration Item	Read, Run Report
▶ Configuration Policy	Read
▶ Deployment Templates	Read
▶ Device Drivers	Read, Run Report
▶ Distribution Point	Read
▶ Distribution Point Group	Read
▶ Driver Package	Read
▶ Firewall Settings	Read, Run Report

OK Cancel

Correct Answer:



Copy Security Role

Specify details for the customized copy of the selected security role.

Name:

Description:

Based on:

Customize the permissions for this copy of the security role.

Permissions:

Permission	Level
Boundaries	Read
Boundary Group	Read
Certificate Profile	Read, Run Report
Client Agent Setting	Read
Cloud Subscription	Read
Collection	Read, View Collected File, Read Resource, Audit S
Communications Provisioning Profile	Read, Run Report
Computer Association	Read, Run Report
Configuration Item	Read, Run Report
Configuration Policy	Read
Deployment Templates	Read
Device Drivers	Read, Run Report
Distribution Point	Read
Distribution Point Group	Read
Driver Package	Read
Firewall Settings	Read, Run Report

OK Cancel

QUESTION 5

HOTSPOT

You have a System Center 2012 R2 Configuration Manager Service Pack 1 (SP1) deployment.

You use Configuration Manager to deploy Windows 8.1 to client computers.

You need to encrypt the contents of the operating system volume during the operating system deployment and to store recovery keys in Active Directory. The solution must minimize the amount of time required to deploy the operating system.

Which task sequence steps should you use to perform each task? To answer, select the appropriate options in the answer area.

Hot Area:



Answer Area

Encrypt the drive:

▼

Enable BitLocker

Pre-provision BitLocker

Store the recovery key:

▼

Enable BitLocker

Capture the Windows settings

Pre-provision BitLocker

Correct Answer:

Answer Area

Encrypt the drive:

▼

Enable BitLocker

Pre-provision BitLocker

Store the recovery key:

▼

Enable BitLocker

Capture the Windows settings

Pre-provision BitLocker

*

Pre-provision BitLocker

This step enables BitLocker on a drive while in Windows PE. Only the used drive space is encrypted. Because you partitioned and formatted the hard drive in the previous step, there is no data, and encryption completes very quickly.

*

Enable BitLocker

This step enables BitLocker encryption on the hard drive and sets key protectors. Because the hard drive was pre-provisioned with BitLocker, this step completes very quickly.

Windows 7/8/10 requires that you add a key protector.

Note: The Pre-provision BitLocker task sequence step in Microsoft System Center 2012 Configuration Manager allows you to enable BitLocker from the Windows Preinstallation Environment (Windows PE) prior to operating system

deployment. Only the used drive space is encrypted, and therefore, encryption times are much faster.



VCE & PDF

GeekCert.com

<https://www.geekcert.com/70-243.html>

2024 Latest geekcert 70-243 PDF and VCE dumps Download

References: <https://technet.microsoft.com/en-us/library/dn456883.aspx>

[70-243 PDF Dumps](#)

[70-243 VCE Dumps](#)

[70-243 Braindumps](#)