Vendor: Microsoft

Exam Code: MD-101

Exam Name: Managing Modern Desktops

Version: DEMO

QUESTION 1
Case Study 1 - Litware inc

General Overview
Litware, Inc. is an international manufacturing company that has 3,000 employees. The company has sales, marketing, research, human resources (HR), development, and IT departments. Litware has two main offices in New York and Los Angeles. Litware has five branch offices in Asia.

Existing Environment
Current Business Model
The Los Angeles office has 500 developers. The developers work flexible hours ranging from 11 AM to 10 PM.
Litware has a Microsoft Endpoint Configuration Manager deployment.
During discovery, the company discovers a process where users are emailing bank account information of its customers to internal and external recipients.

Current Environment
The network contains an Active Directory domain that is synced to Microsoft Azure Active Directory (Azure AD). The functional level of the forest and the domain is Windows Server 2012 R2. All domain controllers run Windows Server 2012 R2.
Litware has the computers shown in the following table.

Department	Windows version	Management platform	Domain-joined
Marketing	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Research	10	Endpoint Configuration Manager	Hybrid Azure-AD joined
HR	8.1	Endpoint Configuration Manager	Hybrid Azure-AD joined
Developers	10	Microsoft Intune	Azure AD-joined
Sales	10	Microsoft Intune	Azure AD-joined

The development department uses projects in Azure DevOps to build applications. Most of the employees in the sales department are contractors. Each contractor is assigned a computer that runs Windows 10. At the end of each contract, the computer is assigned to different contractor. Currently, the computers are re-provisioned manually by the IT department.

Problem Statements
Litware identifies the following issues on the network:
- Employees in the Los Angeles office report slow Internet performance when updates are downloading. The employees also report that the updates frequently consume considerable resources when they are installed. The Update settings are configured as shown in the Updates exhibit. (Click the Updates button.)
- Management suspects that the source code for the proprietary applications in Azure DevOps in being shared externally.
- Re-provisioning the sales department computers is too time consuming.

You need to capture the required information for the sales department computers to meet the technical requirements.
Which Windows PowerShell command should you run first?

 A.   Install-Module WindowsAutoPilotIntune

B. Install-Script Get-WindowsAutoPilotInfo
C. Import-AutoPilotCSV
D. Get-WindowsAutoPilotInfo

Answer: A
Explanation:
Re-provision the sales department computers by using Windows AutoPilot.
Windows Autopilot Deployment for existing devices, install required modules:
- Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
- Install-Module AzureAD -Force
- Install-Module WindowsAutopilotIntune -Force
- Install-Module Microsoft.Graph.Intune -Force
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

QUESTION 2
Case Study 2 - Contoso Ltd

Overview
Contoso, Ltd, is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop computers	Mobile devices
Montreal	2,500	2,800	300	3,100
Seattle	1,000	1,100	200	1,500
New York	300	320	30	400

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.
Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.
The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.

Existing Environment
The network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.
The computers are managed by using Microsoft System Center Configuration Manager. The mobile devices are managed by using Microsoft Intune.
The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.
Each department has an organization unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.

Intune Configuration
The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	*None*	GroupB

You need to meet the technical requirements for the iOS devices.
Which object should you create in Intune?

A. A compliance policy
B. An app protection policy
C. A deployment profile
D. A device configuration profile

Answer: D
Explanation:
Scenario: Technical requirements include: Block iOS devices from sending diagnostic and usage telemetry data.
Intune includes device restriction policies that help administrators control Android, iOS, macOS, and Windows devices. These restrictions let you control a wide range of settings and features to protect your organization's resources. For example, administrators can:
Allow or block the device camera
Control access to Google Play, app stores, viewing documents, and gaming
Block built-in apps, or create a list of apps that allowed or prohibited
Allow or prevent backing up files to cloud and storage accounts
Set a minimum password length, and block simple passwords

Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-configure
https://docs.microsoft.com/en-us/mem/intune/configuration/device-restrictions-ios#settings-apply-to-all-enrollment-types-4

QUESTION 3
Case Study 3 - Contoso, Ltd

Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York.

Contoso has a Microsoft 365 E5 subscription.

Environment
Network Environment
The network contains an on-premises Active Directory domain named contoso.com. The domain contains the servers shown in the following table.

Name	Operating system	Role
DC1	Windows Server 2019	Domain controller
Server1	Windows Server 2016	Member server
Server2	Windows Server 2019	Member server

Contoso has a hybrid Azure Active Directory (Azure AD) tenant named contoso.com.

Contoso has a Microsoft Store for Business instance.

Users and Groups
The contoso.com tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Store for Business role	Member of
User1	Cloud device administrator	Basic Purchaser	GroupA
User2	Azure AD joined device local administrator	Device Guard signer	GroupB
User3	Global reader	Purchaser	GroupA, GroupB
User4	Global administrator	None	Group1

All users are assigned a Microsoft Office 365 license and an Enterprise Mobility + Security E3 license.

Enterprise State Roaming is enabled for Group1 and GroupA.

Group1 and Group2 have a Membership type of Assigned.

Devices
Contoso has the Windows 10 devices shown in the following table.

Name	Type	Member of	Scope (Tags)
Device1	Corporate-owned	Group1	Default
Device2	Corporate-owned	Group1, Group2	Tag2
Device3	Personally-owned	Group1	Tag1
Device4	Personally-owned	Group2	Tag2
Device5	Corporate-owned	Group3	Default

The Windows 10 devices are joined to Azure AD and enrolled in Microsoft Intune.

Which user can enroll Device6 in Intune?

 A. User4 and User2 only
 B. User4 and User1 only
 C. User4, User1, and User2 only
 D. User1, User2, User3, and User4

Answer: D
Explanation:
All users can ad devices to AAD, but to enroll to intune device most be added to group 1
And only a admin or a user with the roll for it can do that.

QUESTION 4
You have a Microsoft 365 E5 subscription that contains 100 iOS devices enrolled in Microsoft Intune.

You need to deploy a custom line-of-business (LOB) app to the devices by using Intune.
Which extension should you select for the app package file?

A. .intunemac
B. .apk
C. .ipa
D. .appx

Answer: C
Explanation:
iOS/iPadOS LOB apps: Select Line-of-business app as the app type, select the App package file, and then enter an iOS/iPadOS installation file with the extension .ipa.
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/apps-add

QUESTION 5
You have the devices shown in the following table.

Name	Operating system	Domain member
Device1	Windows 8.1 Enterprise	Yes
Device2	Windows 10 Pro	No
Device3	Windows 10 Enterprise	Yes
Device4	Mac OS X	No

You plan to implement Microsoft Defender for Endpoint.

You need to identify which devices can be onboarded to Microsoft Defender for Endpoint.

What should you identify?

A. Device3 only
B. Device1, Device2, and Device3 only
C. Device1, Device2, Device3, and Device4
D. Device2 and Device3 only
E. Device2, Device3, and Device4 only

Answer: B
Explanation:
All the operating systems are supported.
Note: You can onboard the following operating systems:
▪ Windows 8.1
▪ Windows 10, version 1607 or later
▪ Windows 11
▪ Windows Server 2012 R2
▪ Windows Server 2016
▪ Windows Server Semi-Annual Channel (SAC), version 1803 or later
▪ Windows Server 2019

▪ Windows Server 2022

Reference:
https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection#bkmk_os

QUESTION 6
You are responsible for your company's Microsoft 365 environment, with co-management enabled.

All company computers have been deployed via Microsoft Deployment Toolkit (MDT), and have Windows 10 installed.

You have been tasked devising a strategy for deploying Microsoft Office 365 ProPlus to new computers. You have to make sure that most recent version is installed at all times, while also reducing the effort required to meet the prerequisites.

Which of the following actions should you take?

 A. You should make use of Windows Deployment Services (WDS).
 B. You should make use of the Microsoft Deployment Toolkit
 C. You should make use of the Office Deployment Tool (ODT).
 D. You should make use of a Windows Configuration Designer provisioning package

Answer: C
Explanation:
The Office Deployment Tool (ODT) is a command-line tool that you can use to download and deploy Microsoft 365 Apps to your client computers. The ODT gives you more control over an Office installation: you can define which products and languages are installed, how those products should be updated, and whether or not to display the install experience to your users.
https://docs.microsoft.com/en-us/deployoffice/plan-office-365-proplus

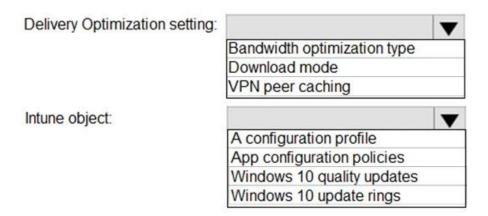**QUESTION 7**
Hotspot Question

You have 100 Windows 10 devices enrolled in Microsoft Intune.

You need to configure the devices to retrieve Windows updates from the internet and from other computers on a local network.

Which Delivery Optimization setting should you configure, and which type of Intune object should you create? To answer, select the appropriate options in the answer area.
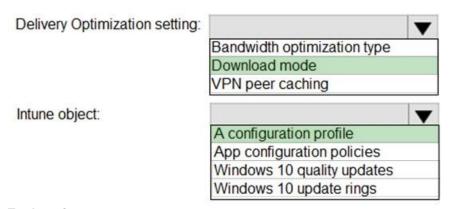
NOTE: Each correct selection is worth one point.

Answer Area

Delivery Optimization setting:
| Bandwidth optimization type |
| Download mode |
| VPN peer caching |

Intune object:
| A configuration profile |
| App configuration policies |
| Windows 10 quality updates |
| Windows 10 update rings |

Answer:

Answer Area

Delivery Optimization setting:
| Bandwidth optimization type |
| Download mode |
| VPN peer caching |

Intune object:
| A configuration profile |
| App configuration policies |
| Windows 10 quality updates |
| Windows 10 update rings |

Explanation:
Box 1: Download mode
Download mode specifies the download method that Delivery Optimization uses to download content.

Box 2: A configuration profile
Delivery Optimization settings are configured as part of the device configuration profile.

Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-settings
https://docs.microsoft.com/en-us/mem/intune/configuration/delivery-optimization-windows

QUESTION 8
Your company has an Active Directory domain, named weylandindustries.com, and a Microsoft Office 365 subscription. The domain is also synced to Microsoft Azure Active Directory (Azure AD).

All company computers are domain-joined, and are running the most recent Microsoft OneDrive sync client.

You are currently configuring OneDrive group policy settings.

Which of the following is the setting that will minimize the disk space consumed by a user profile, when enabled?

A. OneDrive Files On-Demand
B. Silently move known folders to OneDrive
C. Prompt users to move Windows known folders to OneDrive
D. Silently configure OneDrive using the primary Windows account

Answer: A
Explanation:
OneDrive Files On-Demand enables users to view, search for, and interact with files stored in OneDrive from within File Explorer without downloading them and taking up space on the local hard drive.
References:
https://docs.microsoft.com/en-us/onedrive/plan-onedrive-enterprise

QUESTION 9
You company has a Microsoft Azure Active Directory (Azure AD) tenant that includes Microsoft Intune. All of the Windows 10 devices are enrolled in Intune.

You are preparing to configure a Windows Information Protection (WIP) policy:

You need to make sure that the policy is configured to allow for the logging of unacceptable data sharing, but not blocking the action.

Which of the following is the WIP protection mode that you should use?

A. Block
B. Silent
C. Off
D. Allow Overrides

Answer: B
Explanation:
Silent: WIP runs silently, logging inappropriate data sharing, without blocking anything that would have been prompted for employee interaction while in Allow
Override mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.
Reference:
https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune

QUESTION 10
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's environment includes a Microsoft 365 subscription.

Users in the company's sales division have personal iOS or Android devices that are enrolled in Microsoft Intune. New users are added to the sales division on a monthly basis.

After a mobile application is created for users in the sales division, you are instructed to make sure that the application can only be downloaded by the sales division users.

Solution: You start by adding the application to Intune.

Does the solution meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Before you can configure, assign, protect, or monitor apps, you must add them to Microsoft Intune.
Reference:
https://docs.microsoft.com/en-us/intune/apps-add

QUESTION 11
You need to consider the underlined segment to establish whether it is accurate.

To enable sideloading in Windows 10, you should navigate to the For developers setting via Update & Security in the Settings app.

Select "No adjustment required" if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required.
B. Widows Insider
C. Delivery Optimization
D. Activation

Answer: A
Explanation:
How to allow Windows 10 to sideload apps on your computer
1. Open Settings.
2. Click on Update & security.
3. Click on For developers.
4. Under "Use developer features," select the Sideload apps option.
Reference:
https://www.windowscentral.com/how-enable-windows-10-sideload-apps-outside-store
https://docs.microsoft.com/en-us/windows/application-management/sideload-apps-in-windows-10

QUESTION 12
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a number of Windows 10 Microsoft Azure Active Directory (Azure AD) joined workstations. These workstations have been enrolled in Microsoft Intune.

You have been tasked with making sure that the workstations are only able to run applications that you have explicitly permitted.

Solution: You make use of Windows Defender Application Guard.

Does the solution meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Windows Defender Application Control is designed to protect PCs against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.
Windows Defender Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Application Control does not have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy on PCs in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-based protection of Application Control policies deployed through Configuration Manager can be enabled through Group Policy on capable hardware.

QUESTION 13
Your company plans to deploy tablets to 50 meeting rooms.

The tablets run Windows 10 and are managed by using Microsoft Intune. The tablets have an application named App1.

You need to configure the tablets so that any user can use App1 without having to sign in. Users must be prevented from using other applications on the tablets.

Which device configuration profile type should you use?

A. Kiosk
B. Endpoint protection
C. Identity protection
D. Device restrictions

Answer: A
Explanation:
A single-app kiosk uses the Assigned Access feature to run a single app above the lock screen. When the kiosk account signs in, the app is launched automatically. The person using the kiosk cannot do anything on the device outside of the kiosk app.
Reference:
https://docs.microsoft.com/en-us/windows/configuration/kiosk-single-app

QUESTION 14
Your company has a Microsoft 365 subscription.

You have enrolled all the company computers in Microsoft Intune.

You have been tasked with making sure that devices with a high Windows Defender Advanced Threat Protection (Windows Defender ATP) risk score are locked.

Which of the following actions should you take?

A. You should create a device configuration profile.
B. You should create a device compliance policy.
C. You should create a Windows AutoPilot deployment profile.
D. You should create a conditional access policy.

Answer: B
Explanation:
By default, each compliance policy includes the action for noncompliance of Mark device noncompliant with a schedule of zero days (0). The result of this default is when Intune detects a device isn't compliant, Intune immediately marks the device as noncompliant. After a device is marked as noncompliance, Azure Active Directory (AD) Conditional Access can block the device. https://docs.microsoft.com/en-us/mem/intune/protect/actions-for-noncompliance

QUESTION 15
You need to consider the underlined segment to establish whether it is accurate.

Your company has Microsoft Azure Active Directory (Azure AD) joined Windows 10 Pro computers that have been enrolled in Microsoft Intune.

You have been tasked with making sure that the computers are upgraded to Windows 10 Enterprise.

You start by configuring a device enrollment policy in Intune.

Select "No adjustment required" if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

What should you configure in Intune?

A. No adjustment required
B. an app protection policy
C. a Windows AutoPilot deployment profile
D. A device configuration profile

Answer: D
Explanation:
Do you have a bunch of Windows 10 Pro devices and would like upgrade them to Windows 10 Enterprise Microsoft 365 (specifically Microsoft Intune) can help you!
First, create a Microsoft Intune configuration policy. In the Azure Portal navigate to Microsoft Intune -> Device Configuration -> Profiles. Click Create Profile
Reference:
https://blogs.technet.microsoft.com/skypehybridguy/2018/09/21/intune-upgrade-windows-from-pro-to-enterprise-automatically/

QUESTION 16
Your company has a Microsoft 365 subscription.

You have enrolled all the company computers in Microsoft Intune.

You have been tasked with making sure that Microsoft Exchange Online is only accessible from known locations.

Which of the following actions should you take?

A. You should create a device configuration profile.
B. You should create a device compliance policy.
C. You should create a Windows AutoPilot deployment profile.
D. You should create a conditional access policy.

Answer: D
Explanation:
Within a Conditional Access policy, an administrator can make use of signals from conditions like risk, device platform, or location to enhance their policy decisions.
Locations -
When configuring location as a condition, organizations can choose to include or exclude locations. These named locations may include the public IPv4 network information, country or region, or even unknown areas that don't map to specific countries or regions. Only IP ranges can be marked as a trusted location.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions

QUESTION 17
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company Windows 10 computers that are enrolled in Microsoft Intune. You make use of Intune to manage the servicing channel settings of all company computers.

You receive an enquiry regarding the servicing status of a specific computer.

You need to review the necessary policy report.

Solution: You navigate to the audit logs via Software updates.

Does the solution meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Intune offers integrated report views for the Windows update ring policies you deploy. These views display details about the update ring deployment and status:
Sign in to Microsoft Endpoint Manager admin center.
Select Devices > Monitor. Then under Software updates select Per update ring deployment state and choose the deployment ring to review.
https://docs.microsoft.com/en-us/intune/windows-update-compliance-reports

QUESTION 18
Your network contains an Active Directory domain. The domain contains 5,000 computers that

run Windows 10.
All users use Roaming User Profiles.
Some users report that it takes a long time to sign in to the computers.
You discover that the users have user profiles that are larger than 1 GB.
You need to reduce the amount of time it takes for the users to sign in.
What should you configure?

A. Folder Redirection by using a Group Policy Object (GPO)
B. Sync your settings in the Settings app
C. Delivery Optimization in the Settings app
D. Microsoft User Experience Virtualization (UE-V) by using PowerShell

Answer: A
Explanation:
Folder Redirection and Offline Files are used together to redirect the path of local folders (such as the Documents folder) to a network location, while caching the contents locally for increased speed and availability. Roaming User Profiles is used to redirect a user profile to a network location.
Reference:
https://docs.microsoft.com/en-us/windows-server/storage/folder-redirection/folder-redirection-rup-overview

QUESTION 19
Drag and Drop Question

You have a Microsoft Deployment Toolkit (MDT) deployment share named DS1.
You import a Windows 10 image to DS1.
You have an executable installer for an application named App1.

You need to ensure that App1 will be installed for all the task sequences that deploy the image.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions   **Answer Area**

Modify a Windows 10 operating system setting.

Add App1 to DS1.

Modify a selection profile.

Identify the GUID of App1.

Modify CustomSettings.ini.

Answer:

Explanation:
Step 1: Add App1 to DS1
Add an application in the MDT console.

Step 2: Identify the GUID of App1.

Step 3: Modify the CustomSettings.ini
It is possible in the CustomSettings.ini file, to check the default program to add the following line:
ApplicationsXXX ={GUID-APPLICATION}
or to force the installation of the application box checked and grayed out:
MandatoryApplicationsXXX ={GUID-APPLICATION}

Reference:
https://rdr-it.com/en/mdt-installation-of-applications-when-deploying-windows/

QUESTION 20
Your network contains an Active Directory domain named contoso.com. The domain contains
computers that run Windows 10 and are joined to the domain.
The domain is synced to Microsoft Azure Active Directory (Azure AD).

You create an Azure Log Analytics workspace and deploy the Update Compliance solution.

You need to enroll the computers in the Update Compliance solution.

Which Group Policy setting should you configure?

 A.   Specify intranet Microsoft update service location
 B.   Allow Telemetry
 C.   Configure the Commercial ID
 D.   Connected User Experiences and Telemetry

Answer: C
Explanation::
Microsoft uses a unique commercial ID to map information from user computers to your Azure
workspace.
Copy your commercial ID key from any of the Windows Analytics solutions you have added to
your Windows Portal, and then deploy it to user computers.

Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started

QUESTION 21
You have a Microsoft 365 tenant that contains the devices shown in the following table.

Name	Member of
Device1	Group1
Device2	Group1
Device3	Group1

The devices are managed by using Microsoft Intune.

You create a compliance policy named Policy1 and assign Policy1 to Group1. Policy1 is configured to mark a device as Compliant only if the device security settings match the settings specified in the policy.

You discover that devices that are not members of Group1 are shown as Compliant.

You need to ensure that only devices that are assigned a compliance policy can be shown as Compliant. All other devices must be shown as Not compliant.

What should you do?

 A. From Endpoint security, configure the Conditional access settings.
 B. From Device compliance, configure the Compliance policy settings.
 C. From Policy1, modify the actions for noncompliance.
 D. From Tenant administration, modify the Diagnostic settings.

Answer: B
Explanation:
There are two parts to compliance policies in Intune:
Compliance policy settings - Tenant-wide settings that are like a built-in compliance policy that every device receives. Compliance policy settings set a baseline for how compliance policy works in your Intune environment, including whether devices that haven't received any device compliance policies are compliant or noncompliant.
Device compliance policy - Platform-specific rules you configure and deploy to groups of users or devices. These rules define requirements for devices, like minimum operating systems or the use of disk encryption. Devices must meet these rules to be considered compliant.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: ASTR14