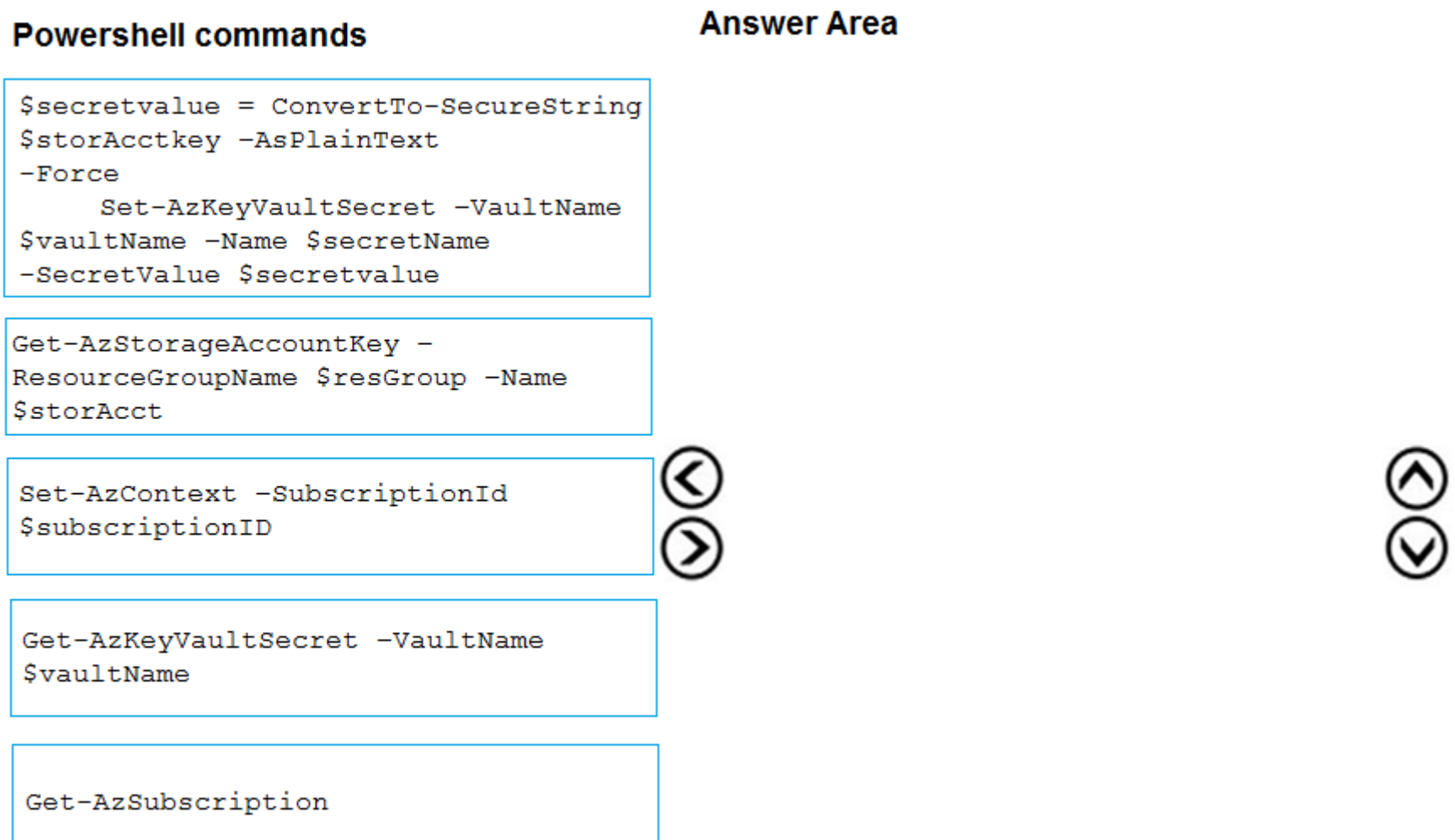
DRAG DROP -
You are developing an application. You have an Azure user account that has access to two subscriptions.
You need to retrieve a storage account key secret from Azure Key Vault.
In which order should you arrange the PowerShell commands to develop the solution? To answer, move all commands from the list of commands to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:

Powershell commands

```
$secretvalue = ConvertTo-SecureString
$storAcctkey -AsPlainText
-Force
     Set-AzKeyVaultSecret -VaultName
$vaultName -Name $secretName
-SecretValue $secretvalue
```

```
Get-AzStorageAccountKey -
ResourceGroupName $resGroup -Name
$storAcct
```

```
Set-AzContext -SubscriptionId
$subscriptionID
```

```
Get-AzKeyVaultSecret -VaultName
$vaultName
```

```
Get-AzSubscription
```

Answer Area

```
Get-AzSubscription
```

```
Set-AzContext -SubscriptionId
$subscriptionID
```

```
Get-AzStorageAccountKey -
ResourceGroupName $resGroup -Name
$storAcct
```

```
$secretvalue = ConvertTo-SecureString
$storAcctkey -AsPlainText
-Force
     Set-AzKeyVaultSecret -VaultName
$vaultName -Name $secretName
-SecretValue $secretvalue
```

```
Get-AzKeyVaultSecret -VaultName
$vaultName
```

Step 1: Get-AzSubscription -
If you have multiple subscriptions, you might have to specify the one that was used to create your key vault. Enter the following to see the subscriptions for your account:

Get-AzSubscription -
Step 2: Set-AzContext -SubscriptionId
To specify the subscription that's associated with the key vault you'll be logging, enter:
Set-AzContext -SubscriptionId <subscriptionID>

Step 3: Get-AzStorageAccountKey -
You must get that storage account key.
Step 4: $secretvalue = ConvertTo-SecureString <storageAccountKey> -AsPlainText -Force
Set-AzKeyVaultSecret -VaultName <vaultName> -Name <secretName> -SecretValue $secretvalue
After retrieving your secret (in this case, your storage account key), you must convert that key to a secure string, and then create a secret with that value in your key vault.

Step 5: Get-AzKeyVaultSecret -
Next, get the URI for the secret you created. You'll need this URI in a later step to call the key vault and retrieve your secret.
Run the following PowerShell command and make note of the ID value, which is the secret's URI:
Get-AzKeyVaultSecret ع€"VaultName <vaultName>
Reference:
https://docs.microsoft.com/bs-latn-ba/Azure/key-vault/key-vault-key-rotation-log-monitoring

Question #18 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You develop Azure solutions.
You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager.
You need to obtain an Azure Resource Manager access token.
Solution: Use an X.509 certificate to authenticate the VM with Azure Resource Manager.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-arm

Question #19 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You develop Azure solutions.
You must grant a virtual machine (VM) access to specific resource groups in Azure Resource Manager.
You need to obtain an Azure Resource Manager access token.
Solution: Use the Reader role-based access control (RBAC) role to authenticate the VM with Azure Resource Manager.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Instead run the Invoke-RestMethod cmdlet to make a request to the local managed identity for Azure resources endpoint.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-arm

HOTSPOT -
You are building a website that is used to review restaurants. The website will use an Azure CDN to improve performance and add functionality to requests.
You build and deploy a mobile app for Apple iPhones. Whenever a user accesses the website from an iPhone, the user must be redirected to the app store.
You need to implement an Azure CDN rule that ensures that iPhone users are redirected to the app store.
How should you complete the Azure Resource Manager template? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

```
"conditions": [ {
    "name": "IsDevice",
    "parameters": {
      "@odata.type": "#Microsoft.Azure.Cdn.Models.[ ▼ ]",
      "operator": "Equal",
      "matchValues": [ "[ ▼ ]" ]
} },
  {
    "name": "RequestHeader",
    "parameters": {
      "@odata.type": "#Microsoft.Azure.Cdn.Models.[ ▼ ]",
      "operator": "Contains",
      "selector": "[ ▼ ]",
      "matchValues": [ "[ ▼ ]" ]
  } }
]
```

DeliveryRuleIsDeviceConditionParameters
DeliveryRuleCookiesConditionParameters
DeliveryRulePostArgsConditionParameters
DeliveryRuleRequestHeaderConditionParameters

iOS
Mobile
iPhone
Desktop

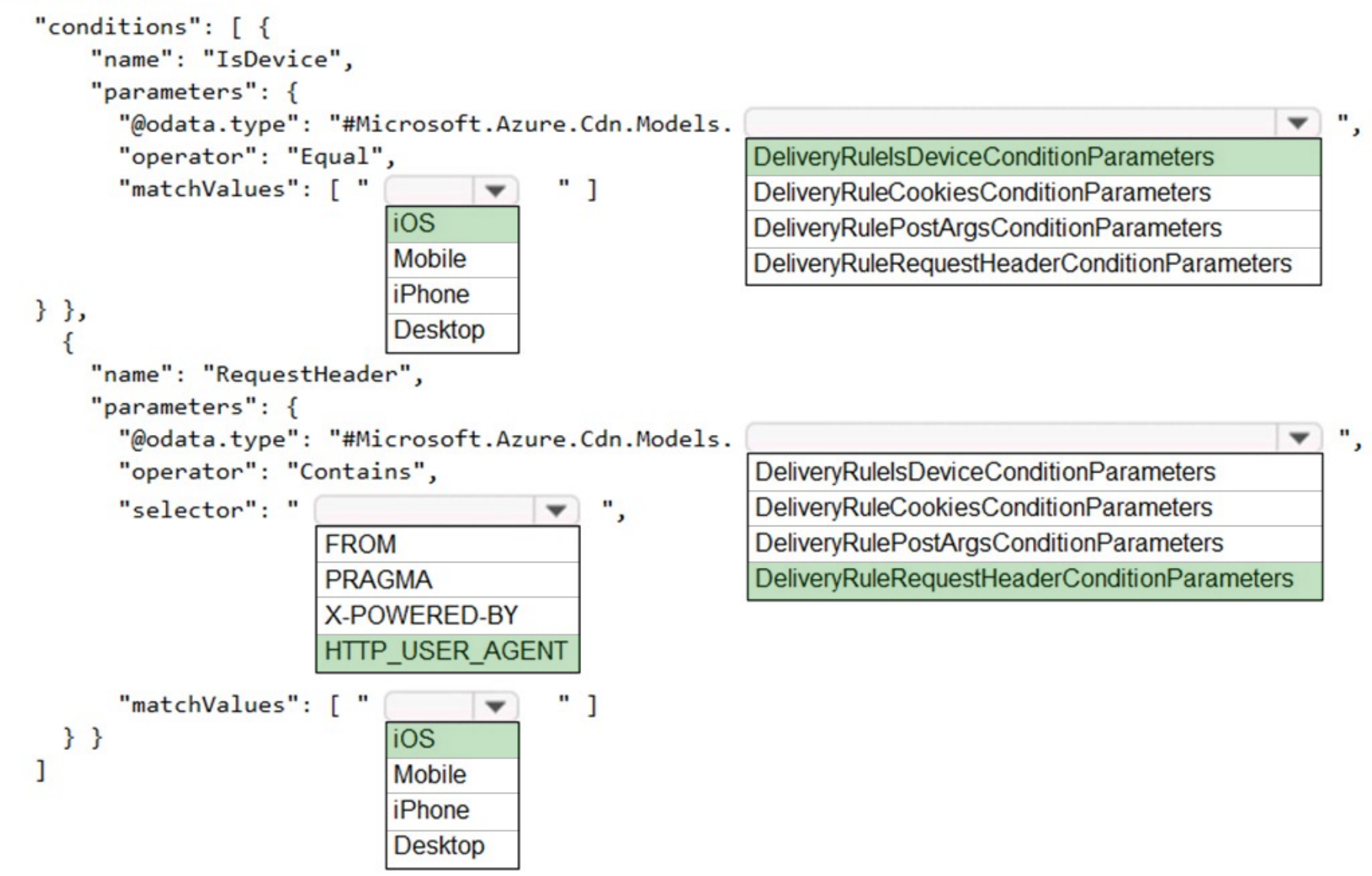
DeliveryRuleIsDeviceConditionParameters
DeliveryRuleCookiesConditionParameters
DeliveryRulePostArgsConditionParameters
DeliveryRuleRequestHeaderConditionParameters

FROM
PRAGMA
X-POWERED-BY
HTTP_USER_AGENT

iOS
Mobile
iPhone
Desktop

Correct Answer:

Answer Area



Box 1: iOS -

Azure AD Conditional Access supports the following device platforms:

☞ Android

☞ iOS

☞ Windows Phone

☞ Windows

macOS

▪

Box 2: DeliveryRuleIsDeviceConditionParameters

The DeliveryRuleIsDeviceCondition defines the IsDevice condition for the delivery rule. parameters defines the parameters for the condition.

Box 3: HTTP_USER_AGENT -

Incorrect Answers:

☞ The Pragma HTTP/1.0 general header is an implementation-specific header that may have various effects along the request-response chain. It is used for backwards compatibility with HTTP/1.0 caches.

☞ "X-Powered-By" is a common non-standard HTTP response header (most headers prefixed with an 'X-' are non-standard).

Box 4: DeliveryRuleRequestHeaderConditionParameters

DeliveryRuleRequestHeaderCondition defines the RequestHeader condition for the delivery rule. parameters defines the parameters for the condition.

Box 5: iOS -

The Require approved client app requirement only supports the iOS and Android for device platform condition.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-grant

Question #21 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are developing a website that will run as an Azure Web App. Users will authenticate by using their Azure Active Directory (Azure AD) credentials.
You plan to assign users one of the following permission levels for the website: admin, normal, and reader. A user's Azure AD group membership must be used to determine the permission level.
You need to configure authorization.
Solution:
☞ Configure and use Integrated Windows Authentication in the website.
☞ In the website, query Microsoft Graph API to load the group to which the user is a member.
Does the solution meet the goal?

A. Yes

B. No

Correct Answer: *B*
Microsoft Graph is a RESTful web API that enables you to access Microsoft Cloud service resources.
Instead in the Azure AD applicationג€™s manifest, set value of the groupMembershipClaims option to All. In the website, use the value of the groups claim from the
JWT for the user to determine permissions.
Reference:
https://blogs.msdn.microsoft.com/waws/2017/03/13/azure-app-service-authentication-aad-groups/

Previous Questions Next Questions