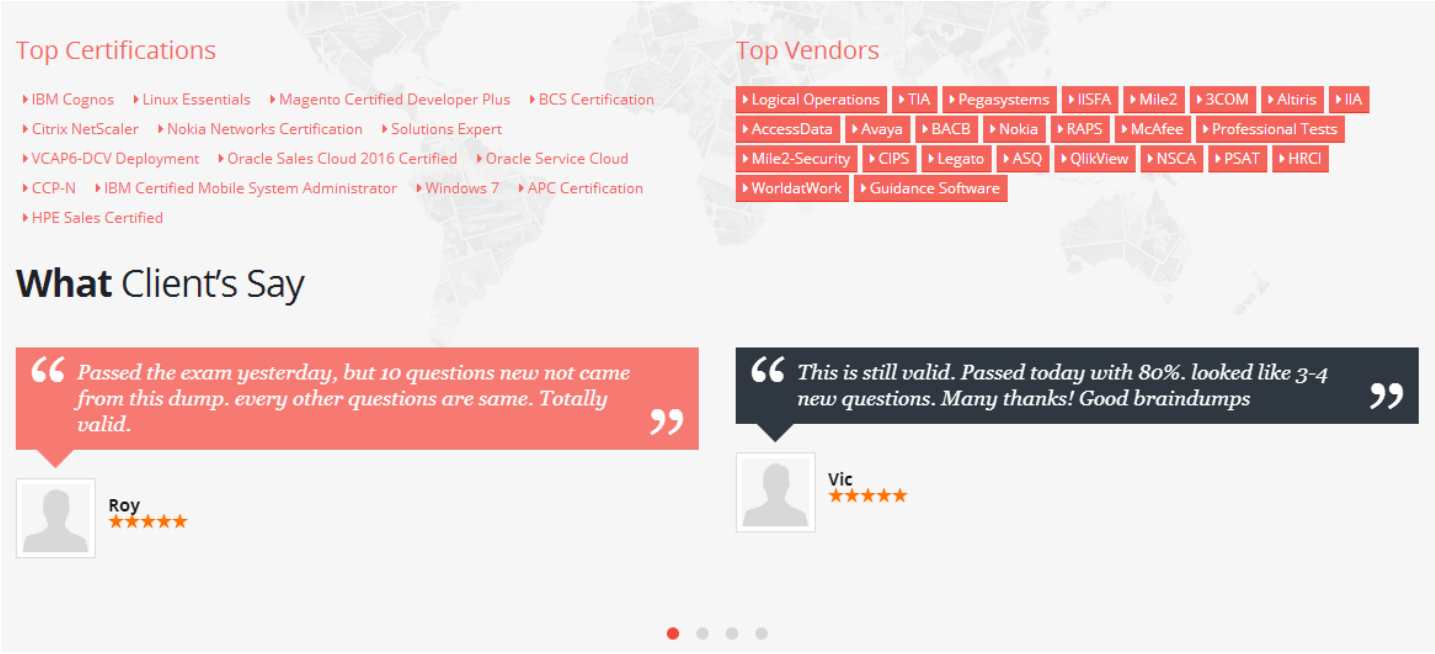
Lead2passExam



http://www.lead2passexam.com/

Available Exam Cram and Valid Dumps - Lead2Pass Exam

Exam : **AZ-600**

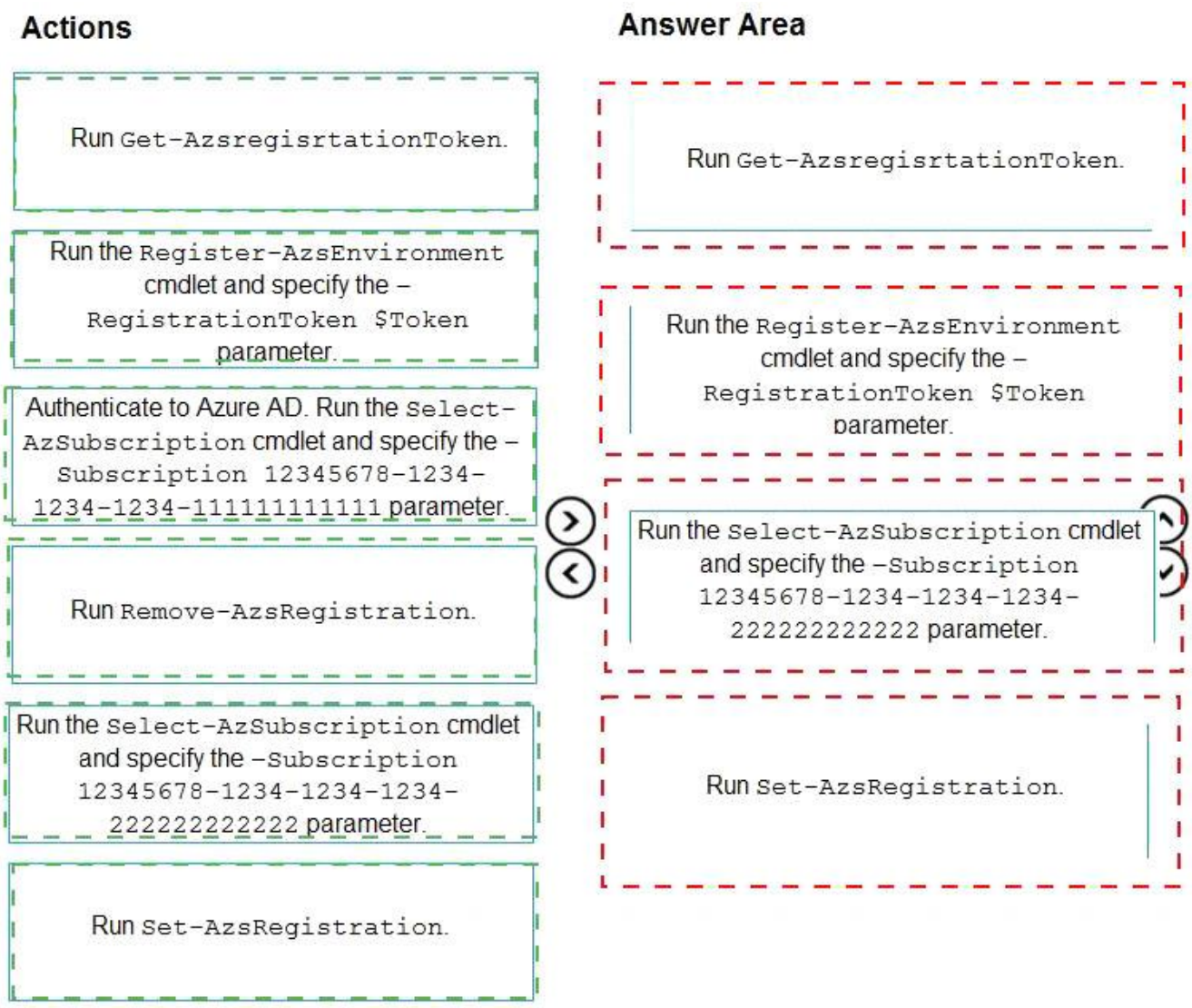
Title : Configuring and Operating a Hybrid Cloud with Microsoft Azure Stack Hub

Vendor : Microsoft

Version : DEMO

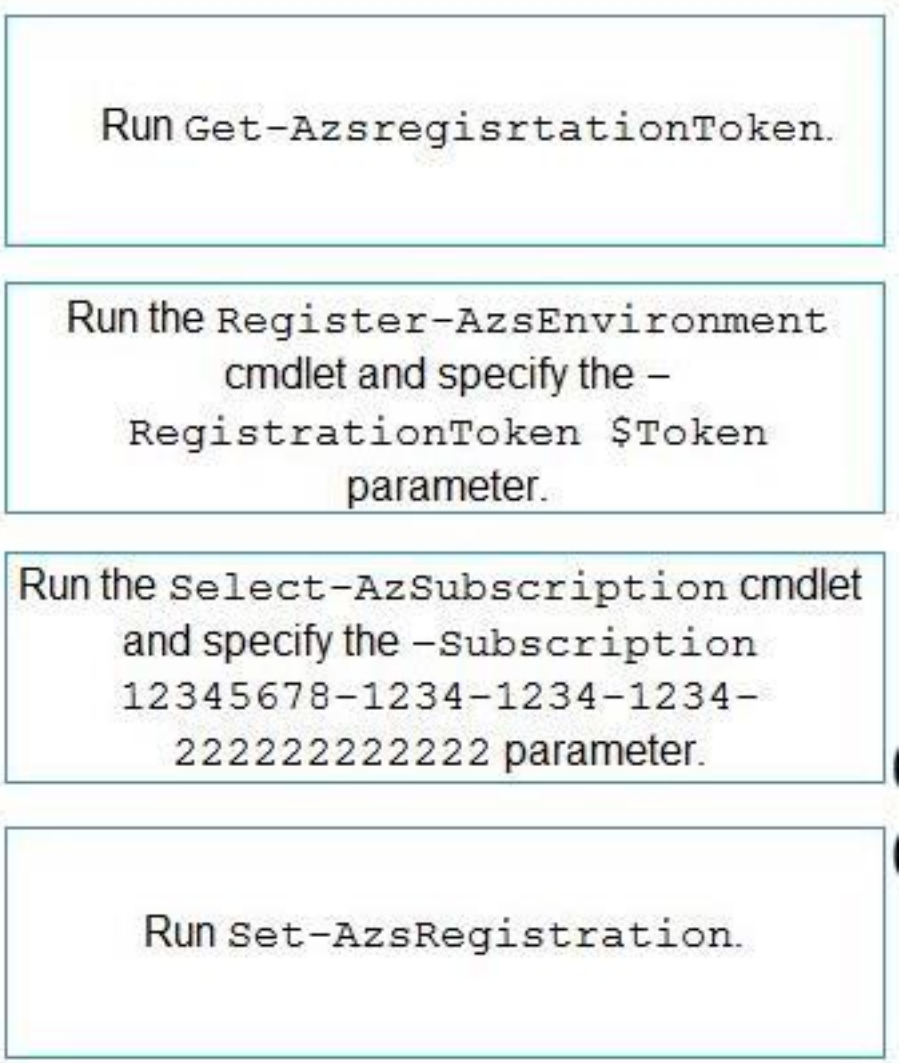
NO.1 You need to update the Azure Stack Hub integrated system registration to support the planned changes.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:



Explanation

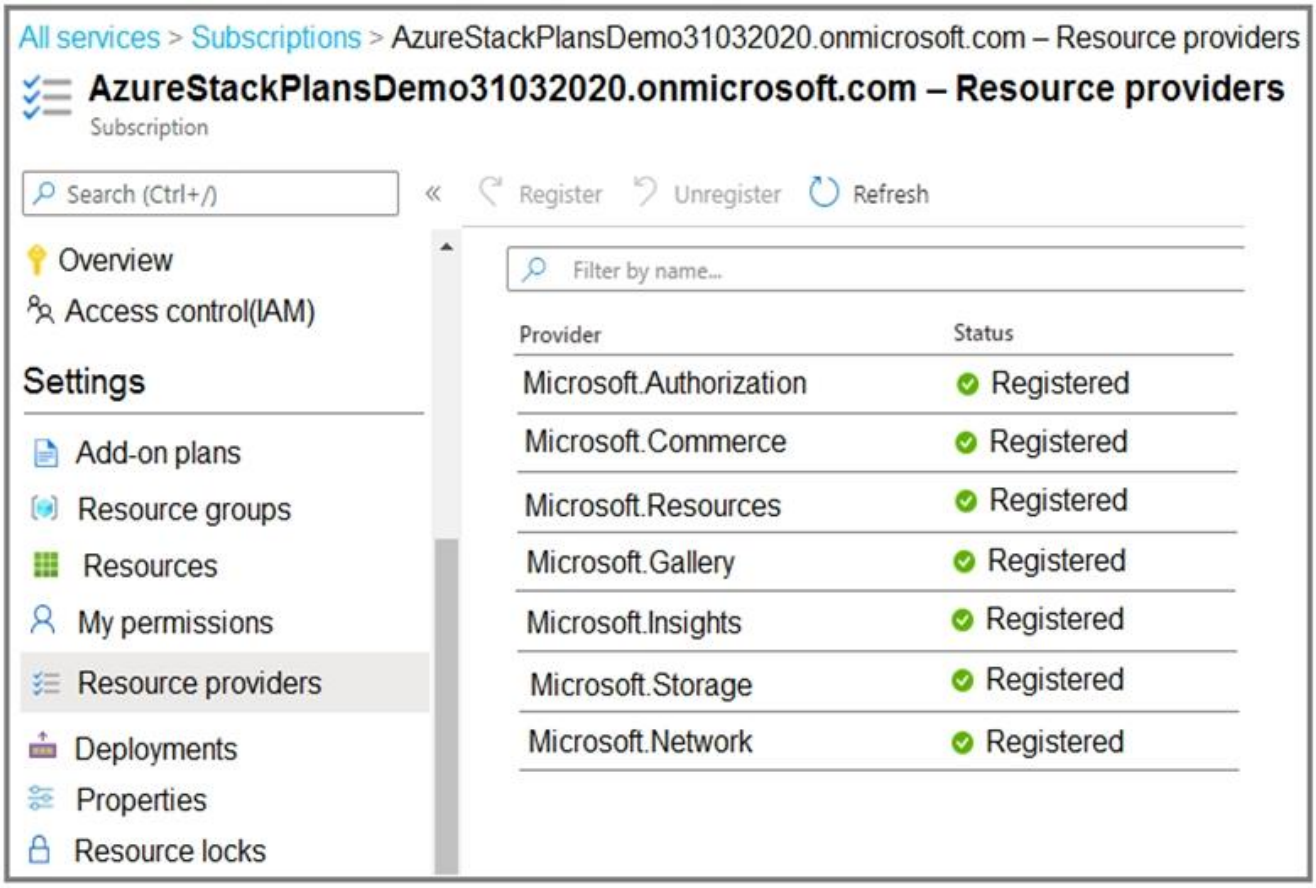
Graphical user interface, text, application Description automatically generated



Step 1: Run Get-AzsRegistrationToken
Change the Azure Stack Hub integrated system registration to use an Azure subscription named Subscription3 that has a GUID of 12345678-1234-1234-1234-222222222222.
Get-AzsRegistrationToken
Get-AzsRegistrationToken generates a registration token from the input parameters.
To register the Azure Stack Hub resource provider with Azure, start PowerShell ISE as an administrator and use PowerShell cmdlets with the EnvironmentName parameter set to the appropriate Azure subscription type.
Step 2: Run the Register-AszEnvironment cmdlet and specify the -RegistrationToken $Token parameter.
Step 3: Run the Select-AzSubscription cmdlet and specify the -Subscription 12345678-1234-1234-1234-222222222222 parameter.
To change the azure subscription using PowerShell, we can use the Select-AZSubscription command. When you use this command, you can use either the subscription ID, Subscription Name, or the Tenant ID.
Step 4: Run Set-AszRegistration.
Before proceeding, in the same PowerShell session, verify again that you're signed in to the correct Azure PowerShell context.
This context is the Azure account that was used to register the Azure Stack Hub resource provider. In

the same PowerShell session, run the Set-AzsRegistration cmdlet:
$CloudAdminCred = Get-Credential -UserName <Privileged endpoint credentials> -Message "Enter the cloud domain credentials to access the privileged endpoint."
$RegistrationName = "<unique-registration-name>"
Set-AzsRegistration `
-PrivilegedEndpointCredential $CloudAdminCred `
-PrivilegedEndpoint <PrivilegedEndPoint computer name> `
-AgreementNumber <EA agreement number> `
-BillingModel Capacity `
-RegistrationName $RegistrationName
Reference:
https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-registration
https://learn.microsoft.com/en-us/azure-stack/mdc/operator/registration-tzl

NO.2 You open the Resource providers blade for a user subscription as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Users of the user subscription can deploy **[answer choice]** successfully.

- an App Service plan
- an event hub
- a key vault
- a virtual network

You must make the **[answer choice]** resource provider available before users of the user subscription can create virtual machines.

- Microsoft.Compute
- Microsoft.KeyVault
- Microsoft.Subscription
- Microsoft.VirtualMachineImages

Answer:

Users of the user subscription can deploy **[answer choice]** successfully.

- an App Service plan
- an event hub
- a key vault
- a virtual network

You must make the **[answer choice]** resource provider available before users of the user subscription can create virtual machines.

- Microsoft.Compute
- Microsoft.KeyVault
- Microsoft.Subscription
- Microsoft.VirtualMachineImages

Explanation
Graphical user interface, text, application, email Description automatically generated

Users of the user subscription can deploy **[answer choice]** successfully.

- an App Service plan
- an event hub
- a key vault
- a virtual network

You must make the **[answer choice]** resource provider available before users of the user subscription can create virtual machines.

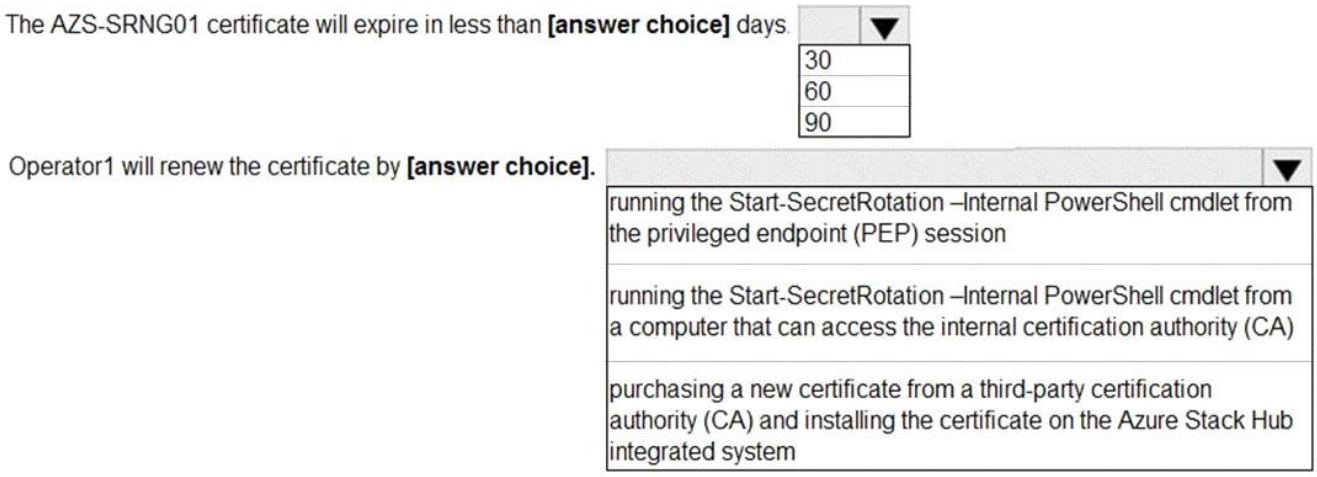
- Microsoft.Compute
- Microsoft.KeyVault
- Microsoft.Subscription
- Microsoft.VirtualMachineImages

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers

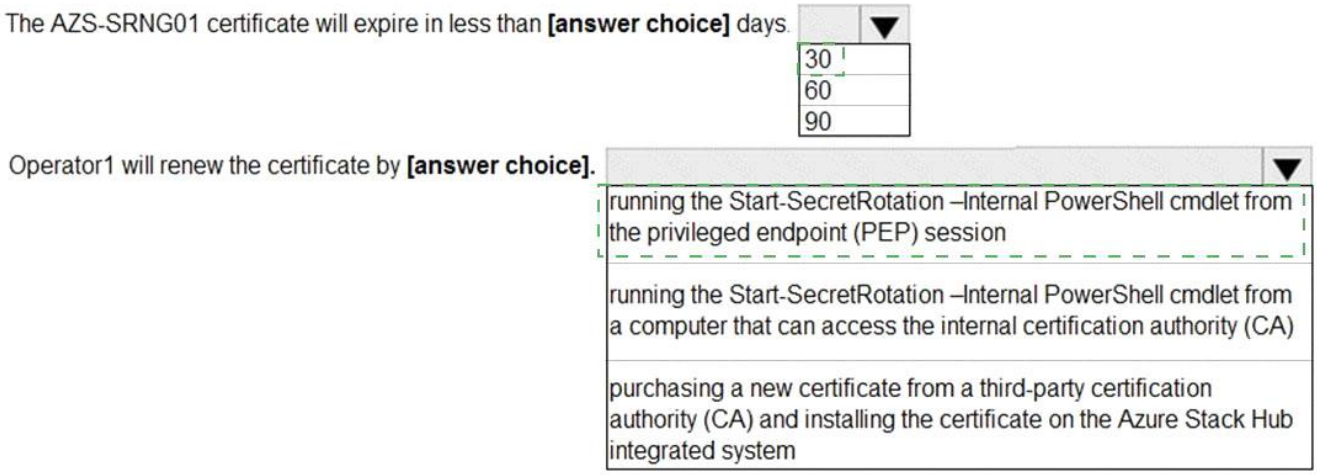
NO.3 You have an Azure Stack Hub integrated system that uses an Active Directory (Azure AD) tenant named contoso.com.
An Azure Stack Hub operator named Operator1 receives the alert shown in the following exhibit.

Name	Severity	Component	State	Created time	Last Modified Time
Pending internal certificate expiration	Warning	AZS-SRNG01	Active	2 days ago	6 hours ago

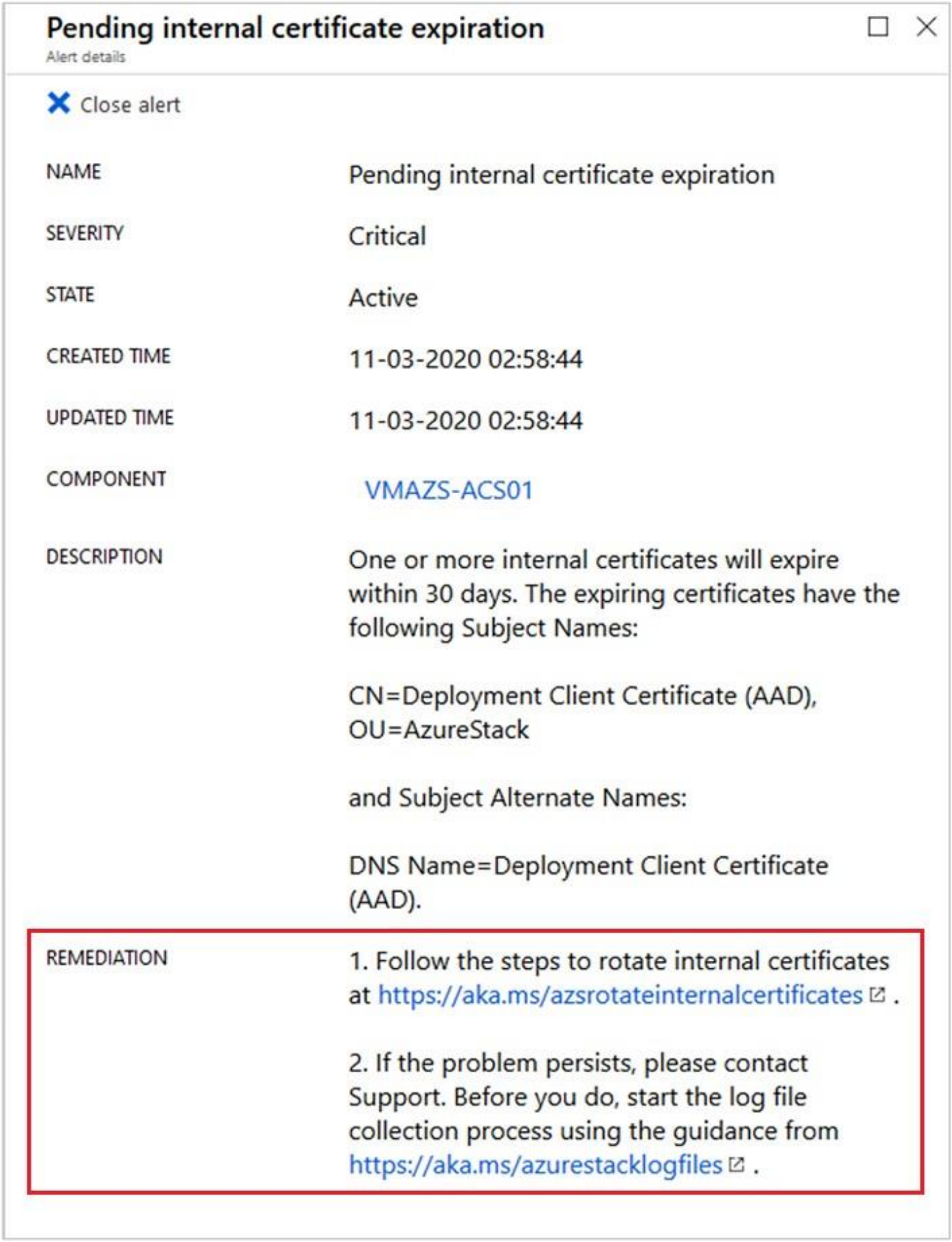
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



Answer:



Explanation
Box 1: 30 days
We cannot tell for sure without the exhibit. It would likely be either 30 or 90 days.
The Azure Stack Hub root certificate is provisioned during deployment with an expiration of five years.
Starting with 2108, internal secret rotation also rotates the root certificate. The standard secret expiration alert identifies the expiry of the root certificate and generates alerts at both 90 (warning) and 30 (critical) days.
Note: Manual remediation
If the Repair option is not supported, be sure to follow the complete set of remediation instructions provided in the alert. As an example, the internal certificate expiration remediation steps will guide you through the process of secret rotation:
Graphical user interface, text, application Description automatically generated



Box 2: running the Start-SecreatRotation -Internal PowerShell cmdlet from the priveged endpoint (PEP) session Start-SecretRotation cmdlet rotates the infrastructure secrets of an Azure Stack Hub

system. This cmdlet can only be executed against the Azure Stack Hub privileged endpoint, by using an Invoke-Command script block passing the PEP session in the -Session parameter. By default, it rotates only the certificates of all external network infrastructure endpoints.
Reference:
https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets
https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-monitor-health

NO.4 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 plan to install an update to an Azure Stack Hub integrated system.
You need to verify whether the integrated system is healthy, and whether you can apply the update.
You must achieve the goal as quickly as possible.
Solution: From the administrator management endpoint, you run
Test-AzureStack -Group "UpdateReadiness".
Does this meet the goal?

A. No

B. Yes

Answer: A
Reference:
https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-diagnostic-test?view=azs-2008

NO.5 You have an Azure Stack Hub integrated system that was recently moved to a new datacenter and powered on.
You need to verify whether the infrastructure components are fully operational.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Run the Get-AzureStackStampInformation cmdlet

B. Run the Test-AzureStack cmdlet

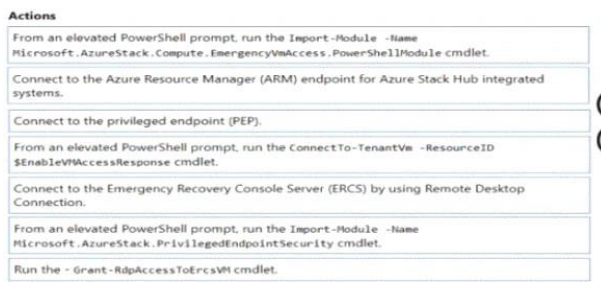
C. Run the Start-AzureStack cmdlet

D. Connect to the administrator portal

E. Connect to the privileged endpoint (PEP)

Answer: B,C,E
Reference:
https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-diagnostic-test?view=azs-2008

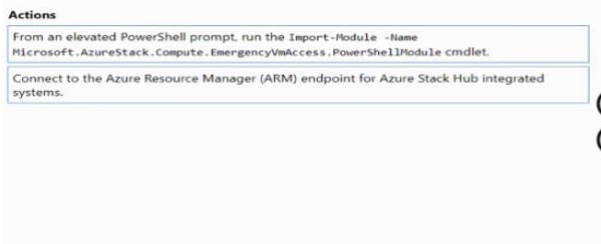
NO.6 You have an Azure Stack Hub integrated system that contains a user named User1.
User1 creates a new virtual machine named VM01.
You need to grant User1 console access to VM01.
Which five actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation

Graphical user interface, application Description automatically generated



NO.7 You have an Azure Stack Hub integrated system that is not yet in production and has no workloads running.

You configure the Infrastructure Backup Service, and you complete a backup.

You need to recommend a method to verify the restore process once the integrated system is in production.

What should you recommend?

A. Install the Azure Stack Development Kit (ASDK) and select the infrastructure backup data as the configuration during the installation.

B. Instruct the IT team to redeploy the integrated system in restore mode by using the backup data.

C. From the administrator portal, restore the domain controller backup to the default provider subscription and ensure that the domain controller starts successfully.

D. Run Get-FileIntegrity against the infrastructure backup data files stored in the file share.

Answer: A

Reference:

https://docs.microsoft.com/en-us/azure-stack/asdk/asdk-validate-backup?view=azs-2102

NO.8 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 have an Azure Stack Hub integrated system.

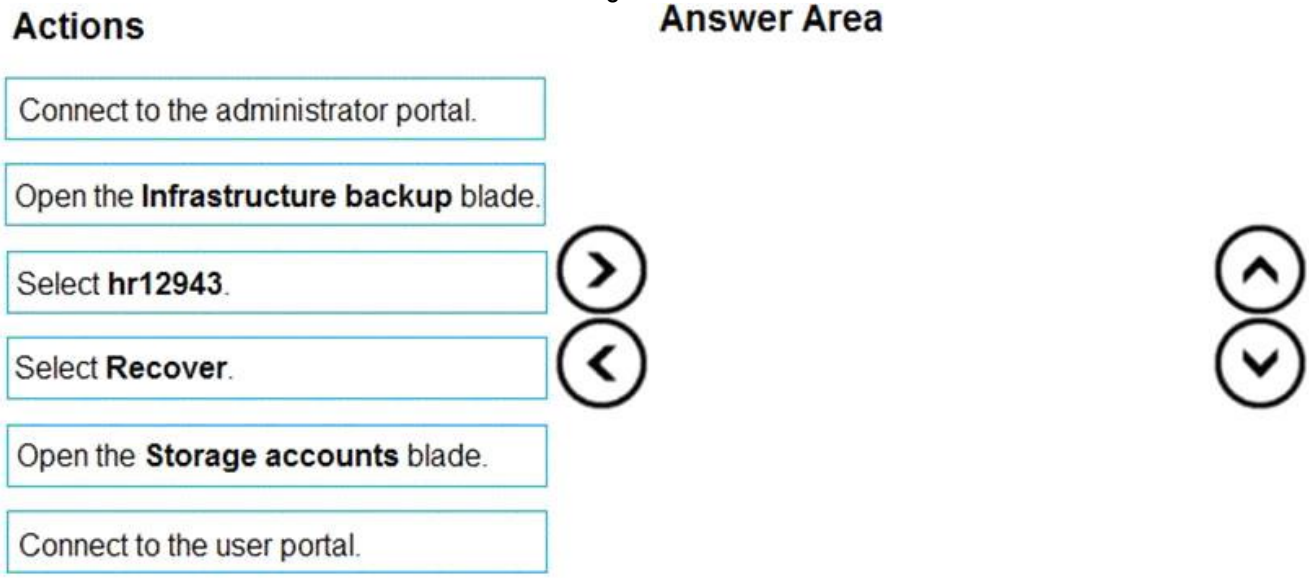
The security department at your company wants a list of all the users who can manage the integrated system from the privileged endpoint (PEP).
You need to create the list.
Solution: From the Azure portal, you open the Azure Active Directory blade and view the users who are assigned the Global administrator role.
Does this meet the goal?

A. Yes

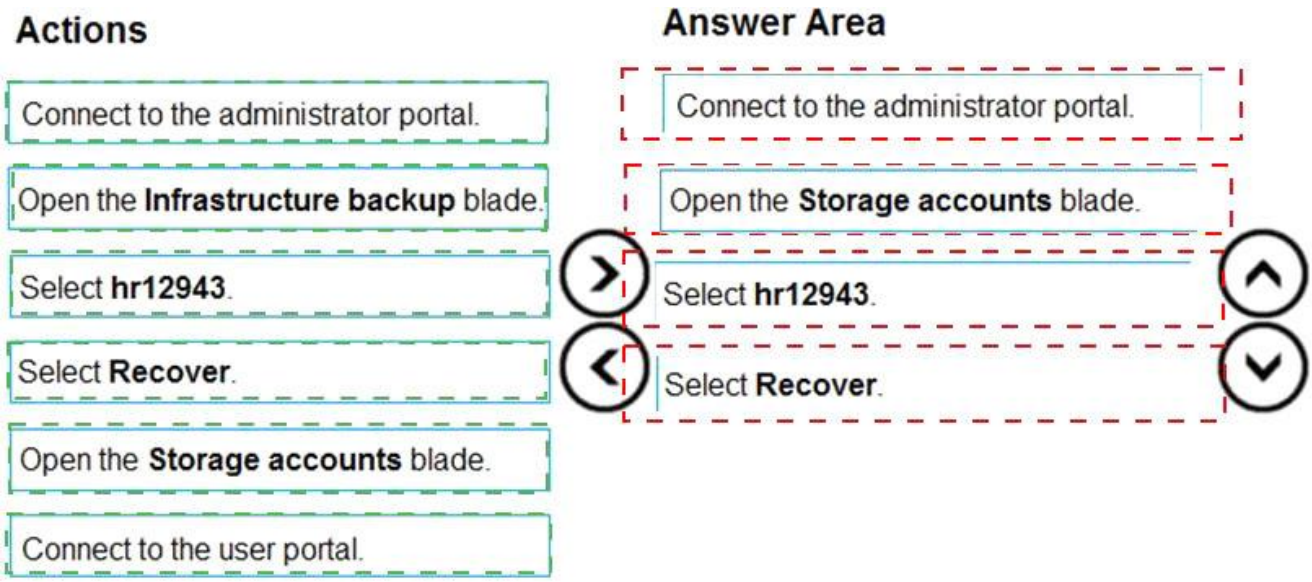
B. No

Answer: B
Reference:
https://docs.microsoft.com/en-us/azure-stack/reference/pep-2002/get-cloudadminuserlist

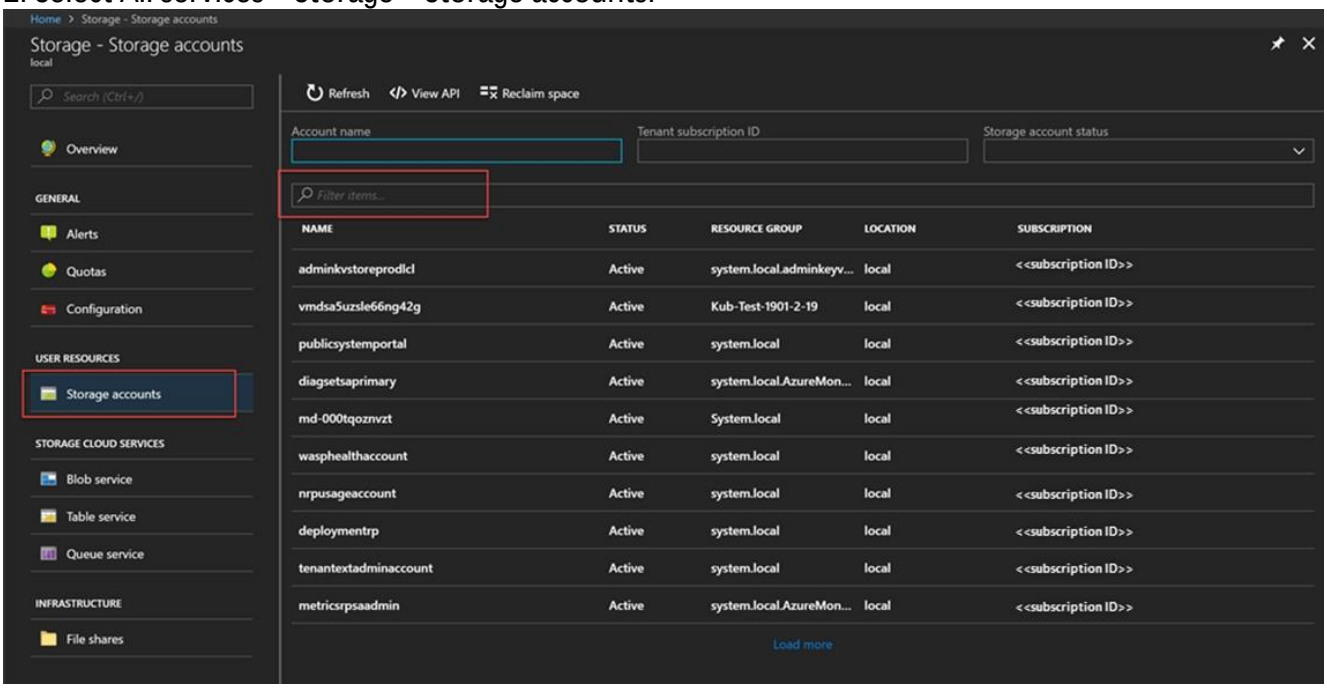
NO.9 You have an Azure Stack Hub integrated system.
The retention period for storage accounts is set to 7 days.
A user reports that a storage account named hr12943 was deleted accidentally two days ago.
You need to restore hr12943.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



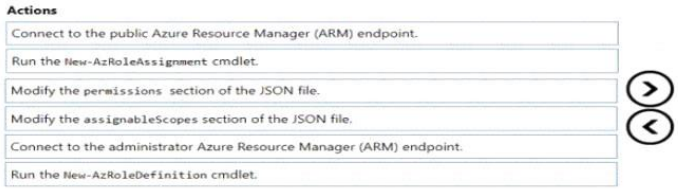
Explanation
Step 1: Connect to the administrator portal
Find a storage account
The list of storage accounts in the region can be viewed in Azure Stack Hub by following these steps:
1. Sign in to the administrator portal https://adminportal.local.azurestack.external.
2. Select All services > Storage > Storage accounts.



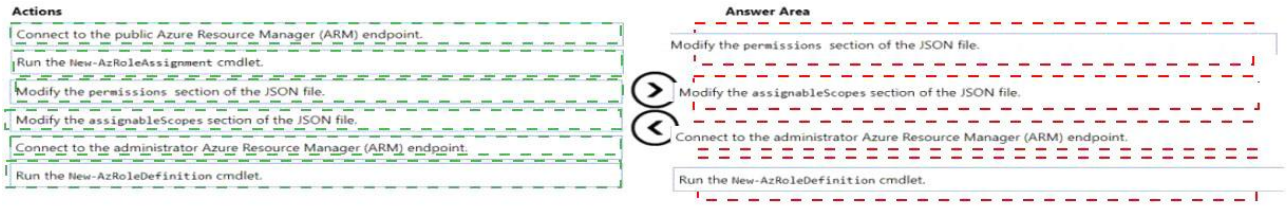
By default, the first 10 accounts are displayed. You can choose to fetch more by clicking the Load more link at the bottom of the list.
Step 2: Open the Storage accounts blade.
Step 3: Select hr12943.
Once you've located the accounts you're interested in viewing, you can select the particular account to view certain details. A new pane opens with the account details. These details include the kind of account, creation time, location, and so on.
Step 4: Select Recover.
Recover a deleted account

You may be in a situation where you need to recover a deleted account.
In Azure Stack Hub, there's a simple way to do that:
Browse to the storage accounts list. For more information, see Find a storage account at the top of this article.
Locate that particular account in the list. You may need to filter.
Check the state of the account. It should say Deleted.
Select the account, which opens the account details pane. (Step 3 above) On top of this pane, locate the Recover button and select it. (Step 4) Select Yes to confirm.
Reference:
https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-manage-storage-accounts

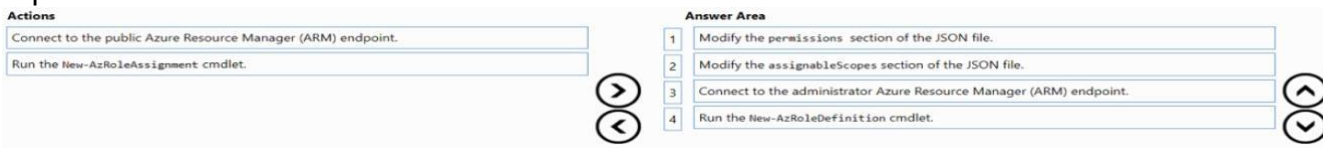
NO.10 You have an Azure Stack Hub integrated system that contains a user named User1.
You have a JSON file that contains the definition of the Reader role.
You need to create a custom role to enable User1 to manage updates for the integrated system.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation



Step 1: Modify the permissions section of the JSON file
Step 2: Modify the assignableScopes section of the JSON file.
Replace <SubscriptionID> with your Azure subscription ID.
Sample JSON file:
{
"Name": "Azure Stack Hub registration role",
"Id": null,
"IsCustom": true,
"Description": "Allows access to register Azure Stack Hub",
"Actions": [
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.AzureStack/registrations/*",

"Microsoft.AzureStack/register/action",
"Microsoft.Authorization/roleAssignments/read",
"Microsoft.Authorization/roleAssignments/write",
"Microsoft.Authorization/roleAssignments/delete",
"Microsoft.Authorization/permissions/read",
"Microsoft.Authorization/locks/read",
"Microsoft.Authorization/locks/write"
],
"NotActions": [
],
"AssignableScopes": [
"/subscriptions/<SubscriptionID>"
]
}
Step 3: Connect to the administrator Azure Resource Manager (ARM) endpoint.
In PowerShell, connect to Azure to use Azure Resource Manager. When prompted, authenticate using an account with sufficient permissions such as Owner or User Access Administrator.
Connect-AzAccount
Step 4: Run the New-AzRoleDefinition cmdlet.
To create the custom role, use New-AzRoleDefinition specifying the JSON template file.
New-AzRoleDefinition -InputFile "C:\CustomRoles\registrationrole.json
Reference: https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-registration-role

NO.11 You have an Azure Stack Hub integrated system that is disconnected from the internet. The integrated system has an Azure App Service resource provider.
You generate a new certificate.
You need to rotate the certificate of the App Service identity application to use the new certificate.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From the administrator portal, get the value of the AzureStack-AppService object ID.

B. From a privileged endpoint (PEP) session, run the New-Object cmdlet. and then run the import-PfxCertificace cmdlet

C. From the administrator portal, get the value of the default provider subscription object ID.

D. From a privileged endpoint (PEP) session, run the Export-Cercificace cmdlet. and then run the Import-Certificace cmdlet

E. From a privileged endpoint (PEP) session, run the New-Objecc cmdlet, and then run the Sec-GraphApplicacion cmdlet

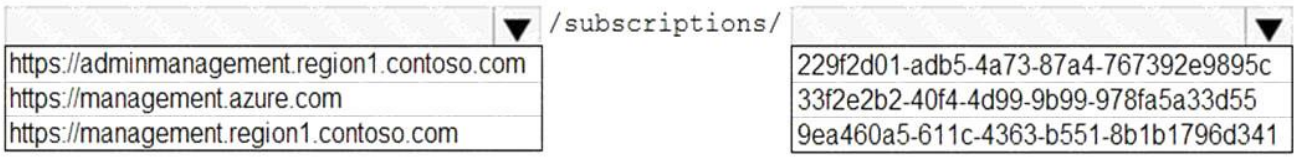
Answer: A,E
Explanation
Your choice of either Azure AD or AD FS is determined by the mode in which you deploy Azure Stack Hub:
When you deploy it in a connected mode, you can use either Azure AD or AD FS.
When you deploy it in a disconnected mode, without a connection to the internet, only AD FS is supported.
E:

Rotate certificate for AD FS identity application
The identity application is created by the operator before deployment of Azure App Service on Azure Stack Hub. If the application's object ID is unknown, follow these steps to discover it:
Go to the Azure Stack Hub administrator portal.
Go to Subscriptions and select Default Provider Subscription.
Select Access Control (IAM) and select the AzureStack-AppService-<guid> application.
Take a note of the Object ID, this value is the ID of the Service Principal that must be updated in AD FS.
D: To rotate the certificate for the application in AD FS, you need to have access to the privileged endpoint (PEP). Then you update the certificate credential using PowerShell.
Sign in to PowerShell interactively, using credentials that have access to the VM running the Privileged Endpoint
$Creds = Get-Credential
Create a new Certificate object from the identity application certificate exported as .cer file
$Cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("<CertificateFileLocation>")
Create a new PSSession to the PrivelegedEndpoint VM
$Session = New-PSSession -ComputerName "<PepVm>" -ConfigurationName PrivilegedEndpoint -Credential $Creds -SessionOption (New-PSSessionOption -Culture en-US -UICulture en-US)
Use the privileged endpoint to update the certificate thumbprint, used by the service principal associated with the App Service identity application
$SpObject = Invoke-Command -Session $Session -ScriptBlock {Set-GraphApplication -ApplicationIdentifier "<ApplicationObjectId>" -ClientCertificates $using:Cert}
$Session | Remove-PSSession
Output the updated service principal details
$SpObject
Reference:
https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-identity-overview
https://learn.microsoft.com/en-us/azure-stack/operator/app-service-rotate-certificates

NO.12 You have an Azure Stack Hub integrated system that is enabled for multi-tenancy and contains a tenant. The integrated system is configured as shown in the following table.

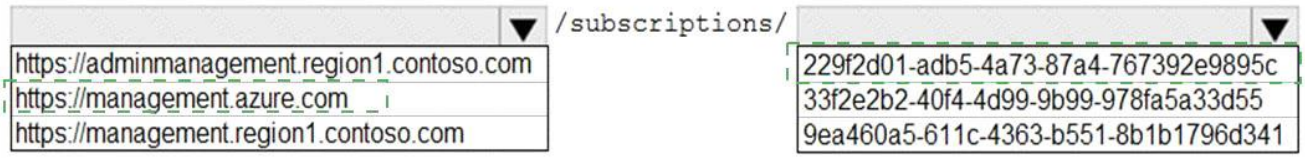
Attribute	Value
Region name	region1
FQDN	contoso.com
Default provider subscription identifier	9ea460a5-611c-4363-b551-8b1b1796d341
Tenant subscription identifier	33f2e2b2-40f4-4d99-9b99-978fa5a33d55
Consumption subscription identifier	229f2d01-adb5-4a73-87a4-767392e9895c

You need to configure the URI that will be used by the tenant to query the subscription usage.
How should you complete the URI? To answer, select the appropriate options in the answer area.



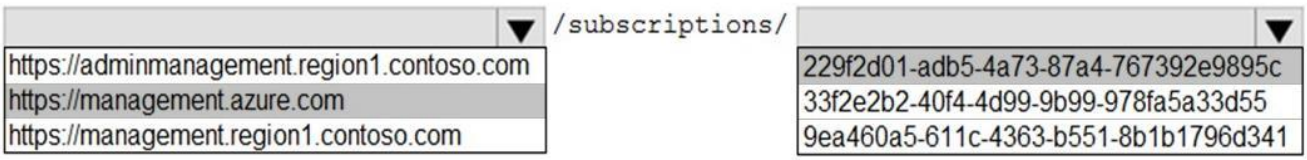

```
/providers/Microsoft.Commerce/usageAggregates?reportedStartTime={reportedStartTime}
&reportedEndTime=
={reportedEndTime}&aggregationGranularity=Daily&api-version=2015-06-01-
preview&continuationToken={token-value}
```

Answer:




```
/providers/Microsoft.Commerce/usageAggregates?reportedStartTime={reportedStartTime}
&reportedEndTime=
={reportedEndTime}&aggregationGranularity=Daily&api-version=2015-06-01-
preview&continuationToken={token-value}
```

Explanation




```
/providers/Microsoft.Commerce/usageAggregates?reportedStartTime={reportedStartTime}
&reportedEndTime=
={reportedEndTime}&aggregationGranularity=Daily&api-version=2015-06-01-
preview&continuationToken={token-value}
```

Box 1: https://management.contoso.com
Do not include the region1 in the URI.
Use management not adminmanagentment (see below).
Note: Tenant resource usage API reference
A tenant can use the tenant APIs to view the tenant's own resource usage data. These APIs are consistent with the Azure usage APIs.
You can use the Windows PowerShell cmdlet Get-UsageAggregates to get usage data, just like in Azure.
API call
Request
The request gets consumption details for the requested subscriptions and for the requested time frame. There is no request body.
Method Request URI
GET
https://{armendpoint}/subscriptions/{subId}/providers/Microsoft.Commerce/usageAggregates?reportedStartTim Parameters
* Armendpoint
Azure Resource Manager endpoint of your Azure Stack Hub environment. The Azure Stack Hub convention is that the name of Azure Resource Manager endpoint is in the format

https://management.{domain-name}. For example, for the development kit, the domain name is local.azurestack.external, then the Resource Manager endpoint is https://management.local.azurestack.external.
Box 2: 22f2d01-...
Use the tenant subscription identifier.
Parameters continued
* subId
Subscription ID of the user who is making the call. You can use this API only to query for a single subscription's usage. Providers can use the provider resource usage API to query usage for all tenants.
Reference:
https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-tenant-resource-usage-api