Free Questions for AZ-800

Shared by Barker on 04-10-2024

Question 1

Question Type: MultipleChoice

SIMULATION

Task 4

You need to run a container that uses the mcrmicrosoft.com/windows/servercofe/iis image on SRV1. Port 80 on the container must be published to port 5001 on SRV1 and the container must run in the background

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To run a container on SRV1 using the mcrmicrosoft.com/windows/servercofe/iis image, publish port 80 on the container to port 5001 on SRV1, and ensure it runs in the background, you can follow these steps:

Step 1: Pull the IIS Image First, pull the correct IIS image from the Microsoft Container Registry:

```
docker pull mcr.microsoft.com/windows/servercore/iis
```

Step 2: Run the Container Next, run the container with the required port mapping and ensure it runs in the background using the -d flag:

```
docker run -d -p 5001:80 --name iis_container mcr.microsoft.com/windows/servercore/iis
```

This command will start a container named iis_container using the IIS image, map port 80 inside the container to port 5001 on SRV1, and run the container in detached mode.

Step 3: Verify the Container is Running To verify that the container is running and the port is published, use the following command:

```
docker ps
```

This will list all running containers and show the port mappings.

Step 4: Access the IIS Server You can now access the IIS server running in the container by navigating to http://<SRV1_IP>:5001 in a web browser, where <SRV1_IP> is the IP address of SRV1.

Note: Ensure that Docker is installed on SRV1 and that the port 5001 is open on the firewall to allow incoming connections1.

By following these steps, you should be able to run the IIS container on SRV1 with the specified port mapping and have it running in the background. Please replace mcrmicrosoft.com/windows/servercofe/iis with the correct image name mcr.microsoft.com/windows/servercore/iis as shown in the commands above.

Question 2

Question Type: **MultipleChoice**

SIMULATION

Task 3

You need to run a container that uses the mcr.microsoft.com/windows/servercore/iis image on SRV1. Pott 60 on the container must be published to port 5001 on SRV1 and the container must run in the background.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To run a container on SRV1 using the mcr.microsoft.com/windows/servercore/iis image, publish port 60 on the container to port 5001 on SRV1, and ensure it runs in the background, you can follow these steps:

Step 1: Pull the IIS Image First, pull the IIS image from the Microsoft Container Registry:

```
docker pull mcr.microsoft.com/windows/servercore/iis
```

Step 2: Run the Container Next, run the container with the required port mapping and ensure it runs in the background using the -d flag:

```
docker run -d -p 5001:60 --name iis_container mcr.microsoft.com/windows/servercore/iis
```

This command will start a container named iis_container using the IIS image, map port 60 inside the container to port 5001 on SRV1, and run the container in detached mode.

Step 3: Verify the Container is Running To verify that the container is running and the port is published, use the following command:

```
docker ps
```

This will list all running containers and show the port mappings.

Step 4: Access the IIS Server You can now access the IIS server running in the container by navigating to http://<SRV1_IP>:5001 in a web browser, where <SRV1_IP> is the IP address of SRV1.

Note: Ensure that Docker is installed on SRV1 and that the port 5001 is open on the firewall to allow incoming connections1.

By following these steps, you should be able to run the IIS container on SRV1 with the specified port mapping and have it running in the background.

Question 3

Question Type: **MultipleChoice**

SIMULATION

Task 2

You need to ensure that you can manage SRV1 remotely by using PowerShell

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To manage SRV1 remotely using PowerShell, you'll need to set up PowerShell Remoting. Here's a step-by-step guide:

Step 1: Enable PowerShell Remoting on SRV1 On SRV1, run the following command to enable PowerShell Remoting:

```
Enable-PSRemoting -Force
```

This command configures the computer to receive PowerShell remote commands that are sent by using the WS-Management technology.

Step 2: Configure the TrustedHosts List (If Needed) If you're managing SRV1 from a computer that is not part of the same domain, you'll need to add the managing computer's name to the TrustedHosts list on SRV1:

```
Set-Item wsman:\localhost\Client\TrustedHosts -Value 'ManagingComputerName' -Concatenate -Force
```

Replace "ManagingComputerName" with the name of your managing computer.

Step 3: Start a Remote Session From your managing computer, start a remote session with SRV1 using the Enter-PSSession cmdlet:

```
Enter-PSSession -ComputerName SRV1 -Credential (Get-Credential)
```

This command prompts you for credentials and then starts a remote session with SRV1.

Step 4: Run Remote Commands Once the remote session is established, you can run any PowerShell command as if you were directly on SRV1. For example:

```
Get-Service
```

This command gets the status of services on SRV1.

Step 5: Exit the Remote Session When you're finished, exit the remote session:

```
Exit-PSSession
```

Note: Ensure that both the managing computer and SRV1 are properly configured to communicate over the network, and that any firewalls allow for the necessary ports (default is 5985 for HTTP and 5986 for HTTPS) to be open for WS-Management traffic12.

By following these steps, you should be able to manage SRV1 remotely using PowerShell. Make sure you have the appropriate administrative privileges to perform these actions.

Question 4

Question Type: **MultipleChoice**

SIMULATION

Task 1

You need to create a group-managed service account (gMSA) named gMSA1 and make gMSA1 available on SRV1.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To create a group-managed service account (gMSA) named gMSA1 and make it available on SRV1, you can follow these steps:

Step 1: Create the Key Distribution Services Root Key First, you need to create the KDS Root Key, which is required for the gMSA to function. You can do this with the following PowerShell command:

```
Add-KdsRootKey --EffectiveTime ((get-date).addhours(-10))
```

Note: The -EffectiveTime parameter is set to 10 hours in the past to ensure immediate effect.

Step 2: Create the gMSA Next, use the New-ADServiceAccount cmdlet to create the gMSA:

```
New-ADServiceAccount -Name gMSA1 -DNSHostName gmsa1.domain.com -PrincipalsAllowedToRetrieveManagedPassword SRV1$
```

Replace domain.com with your actual domain name.

Step 3: Install the gMSA on SRV1 Now, you need to install the gMSA on the server SRV1. Run the following command on SRV1:

```
Install-ADServiceAccount -Identity gMSA1
```

Step 4: Test the gMSA To ensure that the gMSA is installed correctly and ready for use, perform a test using:

```
Test-ADServiceAccount -Identity gMSA1
```

If the test returns True, the gMSA is correctly installed and ready for use on SRV1.

Step 5: Configure the Service to Use the gMSA Finally, configure the service that requires the gMSA to use gMSA1 by setting the service's logon account to domain\gMSA1$ and leave the password field blank.

This will create and make the gMSA gMSA1 available on SRV1. Ensure that you have the necessary permissions and that SRV1 is properly joined to the domain before proceeding with these steps123.

Question 5

Question Type: MultipleChoice

SIMULATION

Task 12

You need to create a Group Policy Object (GPO) named GPO1 that only applies to a group named MemberServers.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To create a GPO named GPO1 that only applies to a group named MemberServers, you can follow these steps:

On a domain controller or a computer that has the Remote Server Administration Tools (RSAT) installed, openGroup Policy Managementfrom theAdministrative Toolsmenu or by typinggpmc.mscin the Run box.

In the left pane, expand your domain and right-click onGroup Policy Objects. SelectNewto create a new GPO.

In theNew GPOdialog box, enterGPO1as theNameof the new GPO and clickOK. You can also optionally select a source GPO to copy the settings from.

Right-click on the new GPO and selectEditto open theGroup Policy Management Editor. Here, you can configure the settings that you want to apply to the group under theComputer ConfigurationandUser Configurationnodes. For more information on how to edit a GPO, seeEdit a Group Policy Object.

Close theGroup Policy Management Editorand return to theGroup Policy Managementconsole. Right-click on the new GPO and selectScope. Here, you can specify the scope of management for the GPO, such as the links, security filtering, and WMI filtering.

Under theSecurity Filteringsection, click onAuthenticated Usersand then click onRemove. This will remove the default permission granted to all authenticated users and computers to apply the GPO.

Click onAddand then type the name of the group that you want to apply the GPO to, such asMemberServers. ClickOKto add the group to the security filter. You can also click onAdvancedto browse the list of groups available in the domain.

Optionally, you can also configure theWMI Filteringsection to further filter the GPO based on the Windows Management Instrumentation (WMI) queries. For more information on how to use WMI filtering, seeFilter the scope of a GPO by using WMI filters.

To link the GPO to an organizational unit (OU) or a domain, right-click on the OU or the domain in the left pane and selectLink an Existing GPO. Select the GPO that you created, such asGPO1, and clickOK. You can also change the order of preference by using theMove UpandMove Downbuttons.

Wait for the changes to replicate to other domain controllers. You can also force the update of the GPO by using thegpupdate /forcecommand on the domain controller or the client computers. For more information on how to update a GPO, seeUpdate a Group Policy Object.

Now, you have created a GPO named GPO1 that only applies to a group named MemberServers. You can verify the GPO application by using thegpresult /rcommand on a member server and checking theApplied Group Policy Objectsentry. You can also use theGroup Policy Resultswizard in theGroup Policy Managementconsole to generate a report of the GPO application for a specific computer or user. For more information on how to use the Group Policy Results wizard, seeUse the Group Policy Results Wizard.

Question 6

Question Type: **MultipleChoice**

SIMULATION

Task 11

You need to ensure that all DHCP clients that get an IP address from SRV1 will be configured to use DC1 as a DNS server.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

One possible solution to ensure that all DHCP clients that get an IP address from SRV1 will be configured to use DC1 as a DNS server is to use the DHCP scope options. DHCP scope options are settings that apply to all DHCP clients that obtain an IP address from a specific scope. You can use the DHCP scope options to specify the DNS server IP address, as well as other parameters such as the default gateway, the domain name, and the DNS suffix. Here are the steps to configure the DHCP scope options on SRV1:

On SRV1, openDNS Managerfrom theAdministrative Toolsmenu or by typingdnsmgmt.mscin the Run box.

In the left pane, expand your DHCP server and click onIPv4.

In the right pane, right-click on the scope that you want to configure and selectProperties.

In theScope Propertiesdialog box, click on theDNStab.

Check the boxEnable DNS dynamic updates according to the settings below. This option allows the DHCP server to register and update the DNS records for the DHCP clients.

Select the optionAlways dynamically update DNS records. This option ensures that the DHCP server updates both the A and PTR records for the DHCP clients, regardless of whether they request or support dynamic updates.

Check the boxDiscard A and PTR records when lease is deleted. This option allows the DHCP server to delete the DNS records for the DHCP clients when their leases expire or are released.

Check the boxDynamically update DNS records for DHCP clients that do not request updates. This option allows the DHCP server to update the DNS records for the DHCP clients that do not support dynamic updates, such as legacy or non-Windows clients.

In theDNS serverssection, click on theAddbutton to add a new DNS server IP address.

In theAdd Serverdialog box, enter the IP address of DC1, which is the DNS server that you want to use for the DHCP clients, and clickAdd.

ClickOKto close theAdd Serverdialog box and return to theScope Propertiesdialog box.

ClickOKto apply the changes and close theScope Propertiesdialog box.

Now, all DHCP clients that get an IP address from SRV1 will be configured to use DC1 as a DNS server. You can verify the DNS configuration by using theipconfig /allcommand on a DHCP client computer and checking theDNS Serversentry. You can also check the DNS records for the DHCP clients by using theDNS Managerconsole on DC1.

Question 7

Question Type: MultipleChoice

SIMULATION

Task 10

You need to configure Hyper-V to ensure that running virtual machines can be moved between SRV1 and SRV2 without downtime.

You do NOT need to move any virtual machines at this time.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

One possible solution to configure Hyper-V to ensure that running virtual machines can be moved between SRV1 and SRV2 without downtime is to use Live Migration. Live Migration is a feature of Hyper-V that allows you to move a running virtual machine from one host to another without any noticeable interruption of service. To set up Live Migration between SRV1 and SRV2, you need to perform the following steps:

On both SRV1 and SRV2, openHyper-V Managerfrom theAdministrative Toolsmenu or by typingvirtmgmt.mscin the Run box.

In the left pane, right-click on the name of the server and selectHyper-V Settings.

In theHyper-V Settingsdialog box, selectLive Migrationsin the navigation pane.

Check the boxEnable incoming and outgoing live migrations.

UnderAuthentication protocol, select the method that you want to use to authenticate the live migration traffic between the servers. You can choose eitherKerberosorCredSSP. Kerberos does not require you to sign in to the source server before starting a live migration, but it requires you to configure constrained delegation on the domain controller. CredSSP does not require you to configure constrained delegation, but it requires you to sign in to the source server through a local console session, a Remote Desktop session, or a remote Windows PowerShell session. For more information on how to configure constrained delegation, seeConfigure constrained delegation.

UnderPerformance options, select the option that best suits your network configuration and performance requirements. You can choose eitherTCP/IPorCompressionorSMB. TCP/IP uses a single TCP connection for the live migration traffic. Compression uses multiple TCP connections and compresses the live migration traffic to reduce the migration time and network bandwidth usage. SMB uses the Server Message Block (SMB) 3.0 protocol and can leverage SMB features such as SMB Multichannel and SMB Direct. For more information on how to choose the best performance option, seeChoose a live migration performance option.

UnderAdvanced Features, you can optionally enable theUse any available network for live migrationoption, which allows Hyper-V to use any available network adapter on the source and destination servers for live migration. If you do not enable this option, you need to specify one or more network adapters to be used for live migration by clicking on theAddbutton and selecting the network adapter from the list. You can also change the order of preference by using theMove UpandMove Downbuttons.

ClickOKto apply the settings.

Now, you have configured Hyper-V to enable live migration between SRV1 and SRV2. You can use Hyper-V Manager or Windows PowerShell to initiate a live migration of a running virtual machine from one server to another.

Question 8

Question Type: MultipleChoice

SIMULATION

Task 9

You plan to create group managed service accounts (gMSAs).

You need to configure the domain to support the creation of gMSAs.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To configure the domain to support the creation of gMSAs, you need to perform the following steps:

On a domain controller or a computer that has the Remote Server Administration Tools (RSAT) installed, open PowerShell as an administrator and run the following command to install the Active Directory module:

Install-WindowsFeature -Name RSAT-AD-PowerShell

Run the following command to create a Key Distribution Service (KDS) root key, which is required for generating passwords for gMSAs. You only need to do this once per domain:

Add-KdsRootKey -EffectiveImmediately

Wait for at least 10 hours for the KDS root key to replicate to all domain controllers in the domain. Alternatively, you can use the-EffectiveTimeparameter to specify a past date and time for the KDS root key, but this is not recommended for security reasons. For more information, seeAdd-KdsRootKey.

After the KDS root key is replicated, you can create and configure gMSAs using theNew-ADServiceAccountandSet-ADServiceAccountcmdlets. For more information, seeCreate a gMSAandConfigure a gMSA.

Question 9

Question Type: MultipleChoice

SIMULATION

Task 8

You need to create an Active Directory Domain Services (AD DS) site named Site2 that is associated to an IP address range of 192.168.2.0 to 192.168.2.255.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To create an AD DS site named Site2 that is associated to an IP address range of 192.168.2.0 to 192.168.2.255, you can follow these steps:

On a domain controller or a computer that has the Remote Server Administration Tools (RSAT) installed, openActive Directory Sites and Servicesfrom theAdministrative Toolsmenu or by typingdssite.mscin the Run box.

In the left pane, right-click onSitesand selectNew Site.

In theNew Object - Sitedialog box, enterSite2as theNameof the new site. Select a site link to associate the new site with, such asDEFAULTIPSITELINK, and clickOK. You can also create a new site link if you want to customize the replication frequency and schedule between the sites. For more information on how to create a site link, seeCreate a Site Link.

In the left pane, right-click onSubnetsand selectNew Subnet.

In theNew Object - Subnetdialog box, enter192.168.2.0/24as thePrefixof the subnet. This notation represents the IP address range of 192.168.2.0 to 192.168.2.255 with a subnet mask of 255.255.255.0. SelectSite2as theSite objectto associate the subnet with, and clickOK.

Wait for the changes to replicate to other domain controllers. You can verify the site and subnet creation by checking theSitesandSubnetscontainers in Active Directory Sites and Services.

Now, you have created an AD DS site named Site2 that is associated to an IP address range of 192.168.2.0 to 192.168.2.255. You can add domain controllers to the new site and configure the site links and site link bridges to optimize the replication topology.

Question 10

Question Type: MultipleChoice

SIMULATION

Task 7

You need to monitor the security configuration of DC1 by using Microsoft Defender for Cloud.

The required source files are located in a folder named \\dc1.contoso.com\install.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

One possible solution to monitor the security configuration of DC1 by using Microsoft Defender for Cloud is to use the Guest Configuration feature. Guest Configuration is a service that audits settings inside Linux and Windows virtual machines (VMs) to assess their compliance with your organization's security policies. You can use Guest Configuration to monitor the security baseline settings for Windows Server in the Microsoft Defender for Cloud portal by following these steps:

On DC1, open a web browser and go to the folder named \dc1.contoso.com\install. Download the Guest Configuration extension file (GuestConfiguration.msi) and save it to a local folder, such as C:\Temp.

Run the Guest Configuration extension file and follow the installation wizard. You can choose to install the extension for all users or only for the current user. For more information on how to install the Guest Configuration extension, seeInstall the Guest Configuration extension.

After the installation is complete, sign in to the Microsoft Defender for Cloud portal (2).

In the left pane, selectSecurity Centerand thenRecommendations.

In the recommendations list, find and selectVulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration).

In theRemediate Security Configurationspage, you can see the compliance status of your Windows VMs, including DC1, based on the Azure Compute Benchmark. The Azure Compute Benchmark is a set of rules that define the desired configuration state of your VMs. You can also see the number of failed, passed, and skipped rules for each VM. For more information on the Azure Compute Benchmark, seeMicrosoft cloud security benchmark: Azure compute benchmark is now available.

To view the details of the security configuration of DC1, click on the VM name and then selectView details. You can see the list of rules that apply to DC1 and their compliance status. You can also see the severity, description, and remediation steps for each rule. For example, you can see if DC1 has the latest security updates installed, if the firewall is enabled, if the password policy is enforced, and so on.

To monitor the security configuration of DC1 over time, you can use theCompliance over timechart, which shows the trend of compliance status for DC1 in the past 30 days. You can also use theCompliance breakdownchart, which shows the distribution of compliance status for DC1 by rule severity.

By using Guest Configuration, you can monitor the security configuration of DC1 by using Microsoft Defender for Cloud and ensure that it meets your organization's security standards. You can also use Guest Configuration to monitor the security configuration of other Windows and Linux VMs in your Azure environment.

Question 11

Question Type: MultipleChoice

SIMULATION

Task 6

You need to ensure that you can manage DC1 by using Windows Admin Center on SRV1.

The required source files are located in a folder named \\dc1.contoso.com\install.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

One possible solution to ensure that you can manage DC1 by using Windows Admin Center on SRV1 is to install Windows Admin Center on SRV1 and add DC1 as a managed server. Windows Admin Center is a web-based management tool that allows you to manage servers, clusters, Windows PCs, and Azure virtual machines (VMs) from a single interface. Here are the steps to install Windows Admin Center on SRV1 and add DC1 as a managed server:

On SRV1, open a web browser and go to the folder named \dc1.contoso.com\install. Download the Windows Admin Center installer file (WindowsAdminCenter.msi) and save it to a local folder, such as C:\Temp.

Run the Windows Admin Center installer file and follow the installation wizard. You can choose to install Windows Admin Center as a desktop app or as a service. For more information on how to install Windows Admin Center, seeInstall Windows Admin Center.

After the installation is complete, launch Windows Admin Center from the Start menu or the desktop shortcut. If you installed Windows Admin Center as a service, you can access it from a web browser by using the URL https://localhost:6516 or https://<SRV1>:6516, where <SRV1> is the name or IP address of SRV1.

On the Windows Admin Center dashboard, clickAddto add a new connection. SelectServeras the connection type and enter the name or IP address of DC1 in the Server name field. Optionally, you can specify the display name, description, and tags for the connection. ClickSubmitto add DC1 as a managed server.

On the Windows Admin Center dashboard, you should see DC1 listed under the Servers section. Click on DC1 to open the server overview page. From here, you can manage various aspects of DC1, such as roles and features, certificates, devices, events, files, firewall, processes, registry, services, and more. For more information on how to use Windows Admin Center to manage servers, seeManage servers with Windows Admin Center.

Now, you can manage DC1 by using Windows Admin Center on SRV1. You can also add more servers or other types of connections to Windows Admin Center and manage them from the same interface