PassQueen
a.k.a dumpsqueen.com

Advanced Deploy VMware vSphere 7.x

VMware 3V0-22.21

Version Demo

Total Demo Questions: 1

Total Premium Questions: 18

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Installing, Configuring, and Setup	10
Topic 2, Performance-tuning, Optimization, and Upgrades	3
Topic 3, Troubleshooting and Repairing	2
Topic 4, Administrative and Operational Tasks	3
Total	18

QUESTION NO: 1 - (SIMULATION)

As a member of the virtual infrastructure team, you have been tasked with creating a new guest customization specification and deploying a test virtual machine from an existing legacy template migrated from an old VMware VI3 environment

To complete this task:

ANSWER: See the explanation for the answer

Explanation:

Answer: Create a **Windows** guest OS customization specification that matches the operating system in the legacy VI3 template, then deploy a new VM from that template and select the new specification on the **Customize guest OS** page.

1. In the vSphere Client, open **Menu > Policies and Profiles > VM Customization Specifications** and select **Create**.
2. Select **Windows** as the target guest OS family. Give the specification the required name and description.
3. On the Windows options page, select **Generate new security ID (SID)**. This is important when cloning/deploying from a legacy template so that the deployed Windows VM does not retain the template's machine SID.
4. Configure the required computer-name option (normally **Use the virtual machine name**, unless the simulation explicitly requires a fixed name or a name entered during deployment).
5. Enter any required license/product key, administrator password, time zone, RunOnce commands, network values, and workgroup/domain join details. For a DHCP deployment, leave the adapter set to DHCP; for a static deployment, provide the specified IP address, mask/prefix, gateway, and DNS servers.
6. Finish and save the customization specification.
7. Right-click the migrated legacy template and select **New VM from This Template** (or **Deploy VM from this template**).
8. Enter the requested test VM name; select the requested inventory location, compute resource, datastore, and network.
9. At **Customize guest OS**, select **Customize using an existing customization specification** and choose the specification created above. Complete the deployment wizard.
10. Power on the test VM and verify that VMware Tools runs the customization: the computer name/network/domain-or-workgroup settings should match the specification and Windows should have a newly generated SID.

The supplied question text does not include the required VM name, customization-specification name, IP addressing, domain/workgroup, credentials, or placement targets. Therefore, those values cannot be determined from this JSON and must be entered exactly as provided in the interactive simulation environment.

QUESTION NO: 2 - (SIMULATION)

Your team is experiencing intermittent issues with esxi0la and you have been asked to configure the host to export its syslog data to a preconfigured syslog collector.

To complete this task, you must:

• Configure esxi0la.vciass.local to send syslog events to an external syslog collector on 172.20.10.10.

• Ensure that the ESXi host security policies allow the syslog traffic to pass.

ANSWER: See the explanation for the answer

Explanation:

On `esxi0la.vciass.local`, configure the remote syslog destination and enable the ESXi syslog firewall ruleset.

```
esxcli system syslog config set --loghost='udp://172.20.10.10:514'
esxcli system syslog reload
esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true
```

Verify the configuration:

```
esxcli system syslog config get
esxcli network firewall ruleset list | grep syslog
```

The required remote log host value is `udp://172.20.10.10:514`, and the `syslog` firewall ruleset must be enabled so outbound syslog traffic is permitted.

Equivalent vSphere Client steps: select the host, open **Configure > System > Advanced System Settings**, set `Syslog.global.logHost` to `udp://172.20.10.10:514`, then open **Configure > System > Firewall** and enable the **syslog** ruleset.