Practice Exam Questions

vmware

Advanced Deploy VMware vSphere 7.x

EXAMKILLER

Help Pass Your Exam At First Try

VMware

Exam 3V0-22.21

Advanced Deploy VMware vSphere 7.x

Version: 3.0

[Total Questions: 17]

Question No : 1 CORRECT TEXT

The company's IT strategy is to adopt innovative and emerging technologies such as software-defined storage solution. The IT team has decided to run their business-critical workloads on an all-flash Virtual SAN (vSAN) as it provides excellent performance.

The IT team has purchased servers that are compatible with vSAN. However, all the solid-state drives (SSD) in the servers are shown incorrectly as hard-disk drives (HDD) instead.

In addition, some of the solid-state drives (SSD) will be used for other purposes instead of vSAN and should not be part of the vSAN cluster. These are the requirements for the vSAN cluster:

•In each server, use the 3GB SSD as the cache tier and the 11GB SSD as the capacity tier

• As a result the vSAN cluster will use a total of six SSDs (three SSDs for caching and three SSDs for capacity

• Ensure all the disks that will be used for vSAN are shown correctly as SSDs

• Provide storage savings by using deduplication and compression.

Next, the IT team wants to improve the performance and availability of the business-critical workloads on the vSAN-datastore.

Ensure the following configurations will be applied on existing and new workloads located on vSAN-datastore:

- Number of disk stripes per object: 2
- Primary level of failures to tolerate: 2
- Failure tolerance method: RAID-1 (Mirroring)
- Force provisioning; Yes

The new configurations should be applied by default.

You may create new storage policy but do not edit the default vSAN storage policy as it may be used by other vSAN clusters in the future. Name the policy "New vSAN Default'.

Nate-. All tasks should be executed in PROD-A host cluster.

Answer: see the solution below:

Explanation:

VMware vSphere ESXi can use locally attached SSDs (Solid State Disk) and flash devices in multiple ways. Since SSDs offer much higher throughput and much lower latency than traditional magnetic hard disks the benefits are clear. While offering lower throughput and higher latency, flash devices such as USB or SATADOM can also be appropriate for some

use cases. The potential drawback to using SSDs and flash device storage is that the endurance can be significantly less than traditional magnetic disks and it can vary based on the workload type as well as factors such as the drive capacity, underlying flash technology, etc.

This KB outlines the minimum SSD and flash device recommendations based on different technologies and use case scenarios.

SSD and Flash Device Use Cases

A non-exhaustive survey of various usage models in vSphere environment are listed below.

- Host swap cache
- Regular datastore
- vSphere Flash Read Cache (aka Virtual Flash)
- vSAN
- vSphere ESXi Boot Disk
- vSphere ESXi Coredump device
- vSphere ESXi Logging device

SSD Endurance Criteria

The flash industry often uses Tera Bytes Written (TBW) as a benchmark for SSD endurance. TBW is the number of terabytes that can be written to the device over its useful life. Most devices have distinct TBW ratings for sequential and random IO workloads, with the latter being much lower due to Write Amplification Factor (WAF) (defined below). Other measures of endurance commonly used are DWPD (Drive Writes Per Day) and P/E (Program/Erase) cycles.

Conversion formulas are provided here:

- Converting DWPD (Drive Writes Per Day) to TBW (Terabytes Written):
- Converting Flash P/E Cycles per Cell to TBW (Terabytes Written):

WAF is a measure of the induced writes caused by inherent properties of flash technology. Due to the difference between the storage block size (512 bytes), the flash cell size (typically 4KiB or 8KiB bytes) and the minimum flash erase size of many cells one write can force a number of induced writes due to copies, garbage collection, etc. For sequential workloads typical WAFs fall in the range of single digits while for random workloads WAFs can approach or even exceed 100. Table 1 contains workload characterization for the various workloads excepting the Datastore and vSphere Flash Read Cache workloads which depend on the characteristics of the Virtual Machines workloads being run and thus cannot be characterized here. A WAF from the table can be used with the above P/E to TBW formula.

Question No : 2 CORRECT TEXT

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: Send us your suggestions.

Question No : 3 CORRECT TEXT

You are doing an audit for vCenter Server vcsa0la s inventory.

On the desktop, you will find a folder named "powercli-question". In the folder, there is a script named "vds-script.psl".

Your colleague needs some help to get it working as expected. Your task is to modify the script so that it exports a list of virtual machines, enables promiscuous mode on PCLI-Portgroup. and exports PCLI-Portgroup.

Answer: Send us your suggestions.

Question No : 4 CORRECT TEXT

Your security team is getting ready for an audit and wants to check the status of all ESXI hosts' outstanding security patches. Create a new fixed Update Manager baseline for all security ESXi host patches and name it "Security patches. "Use the patches available in the patch repository. Use VCSA01a in this task.

- Baseline Name: Security Patches
- Baseline Type: Host Patch
- Category: Security

Answer: See the Explanation below for Solution.

Explanation:

The Update Manager displays system managed baselines that are generated by vSAN. These baselines appear by default when you use vSAN clusters with ESXi hosts of version 6.0 Update 2 and later in your vSphere inventory. If your vSphere environment does not contain any vSAN clusters, no system managed baselines are created.
The system managed baselines automatically update their content periodically, which requires Update Manager to have constant access to the Internet. The vSAN system baselines are typically refreshed every 24 hours.
You use system managed baselines to upgrade your vSAN clusters to recommended critical patches, drivers, updates or the latest supported ESXi host version for vSAN. System managed baselines cannot be edited or deleted. You do not attach system managed baselines to inventory objects in your vSphere environment. You can create a baseline group of multiple system managed baselines, but you cannot add any other type of basline to that group. Similarly, you cannot add a system managed baseline to a baseline group that contains upgrade, patch, and extension baselines.

Question No : 5 CORRECT TEXT

The Virtual Infrastructure team wants to share a VM Template from vcsa0la to vcsa0lb via content libraries. Ensure that the content in the libraries is synchronized only when needed.

• Name of Published Content Library in vcsa0la: CL01

• Name of Subscribed Content Library in vcsa0lb: CL02

• For both content libraries, use the local datastore: SAN01

• VM Template to be shared: Core-Template

After the Core-Template has been synchronized from CL01 to CL02. deploy a virtual machine from VM-Template on vcsa0lb

• Name of virtual machine: CL-VM

• Host for virtual machine: »sxi03b

Answer: Send us your suggestions.

Question No : 6 CORRECT TEXT

The security team has decided to follow the VMware-recommended best practices in the vSphere hardening guide.

esxi02b:

Your first task is to create a local user in esxi02b:

• Name: SpecialUser

• Role: Administrator

Your second task is to ensure that SpecialUser is the ONLY user who is able to SSH into esxi02b via Putty.

Your final task is to enforce a strict lockdown on esxi02b.

Your second task is to ensure that SpecialUser is the ONLY user who is able to SSH into esxi02b via Putty.

Your final task is to enforce a strict lockdown on esxi02b.

Answer: See the solution below

Explanation:

Authentication and authorization govern access. vCenter Single Sign-On supports authentication, which means it determines whether a user can access vSphere components at all. Each user must also be authorized to view or manipulate vSphere objects.

vSphere supports several different authorization mechanisms, discussed in Understanding Authorization in vSphere. The focus of the information in this section is how the vCenter Server permission model works and how to perform user management tasks.

vCenter Server allows fine-grained control over authorization with permissions and roles. When you assign a permission to an object in the vCenter Server object hierarchy, you specify which user or group has which privileges on that object. To specify the privileges, you use roles, which are sets of privileges.

Initially, only the administrator user for the vCenter Single Sign-On domain, administrator@vsphere.local by default, is authorized to log in to the vCenter Server system. That user can then proceed as follows:

- Add an identity source in which users and groups are defined to vCenter Single Sign-On. See the Platform Services Controller Administration documentation.
- Give privileges to a user or group by selecting an object such as a virtual machine or a vCenter Server system and assigning a role on that object for the user or group.