2V0-621$^{\text{Q\&As}}$

VMware Certified Professional 6 – Data Center Virtualization

QUESTION 1

An administrator needs to create an Integrated Windows Authentication (IWA) Identity Source on a newly deployed vCenter Server Appliance (VCSA).

Which two actions will accomplish this? (Choose two.)

A. Use a Service Principal Name (SPN) to configure the Identity Source.

B. Use a Domain administrator to configure the Identity Source.

C. Join the VCSA to Active Directory and configure the Identity Source with a Machine Account.

D. Create a computer account in Active Directory for the VCSA and configure the Identity Source.

Correct Answer: AC

A-) Configuring Active Directory as Identity Source for use with SSO 6.0 can be done in 2 ways

a.

Use the Machine Account(Any AD Account) b. Use with Service Principal Name

b.

Prerequisites :1. A domain account with domain administrator privileges is required when assigning a SPN to an account. 2. A domain account with domain user privileges is a minimum requirement for the account to be used as the SPN account.

c.

https://pubs.vmware.com/vsphere-60/index.jsp#com.vmware.vsphere.security.doc/GUID-4D24C6E863F5-4E35-862E-B59A03703254.html?resultof=%2522%2573%2570%256e%2522%2520

C-) VCSA- If you want to configure permissions for users and groups from an Active Directory domain to access the vCenter Server components, you must join its associated embedded or external Platform Services Controller instance to the Active Directory domain. https://pubs.vmware.com/vsphere60/index.jsp?topic=%2Fcom.vmware.vsphere.vcsa.doc%2FGUID08EA2F92-78A7-4EFF-880E-2B63ACC962F3.html

QUESTION 2

An administrator has configured three vCenter Servers and vRealize Orchestrator within a Platform Services Controller domain, and needs to grant a user privileges that span all environments.

Which statement best describes how the administrator would accomplish this?

A. Assign a Global Permission to the user.

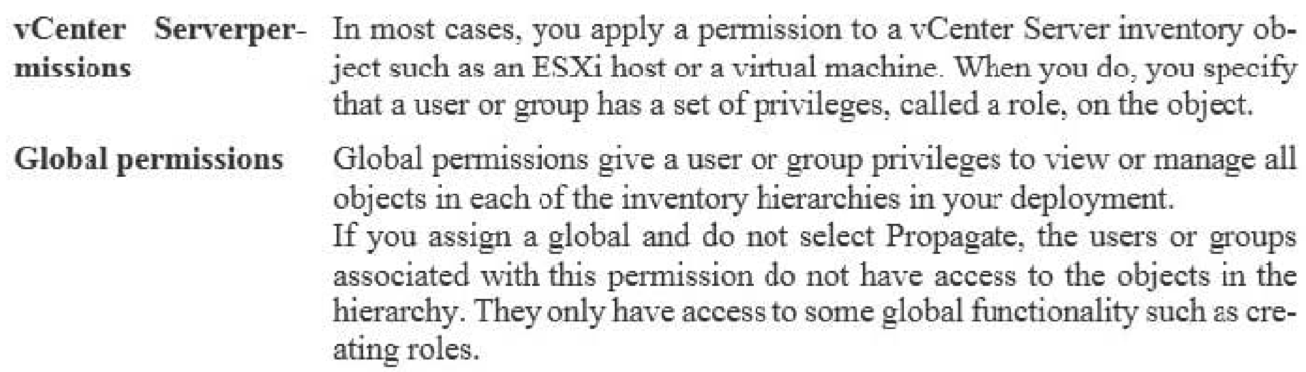
B. Assign a vCenter Permission to the user.

C. Assign vsphere.local membership to the user.

D. Assign an ESXi Permission to the user.

Correct Answer: A

Global Permissions Global permissions are applied to a global root object that spans solutions, for example, both vCenter Server and vCenter Orchestrator. Use global permissions to give a user or group privileges for all objects in all object hierarchies. Each solution has a root object in its own object hierarchy. The global root object acts as a parent object to each solution object. You can assign global permissions to users or groups, and decide on the role for each user or group. The role determines the set of privileges. You can assign a predefined role or create custom roles. See Using Roles to Assign Privileges. It is important to distinguish between vCenter Server permissions and global permissions.



vCenter Serverpermissions	In most cases, you apply a permission to a vCenter Server inventory object such as an ESXi host or a virtual machine. When you do, you specify that a user or group has a set of privileges, called a role, on the object.
Global permissions	Global permissions give a user or group privileges to view or manage all objects in each of the inventory hierarchies in your deployment. If you assign a global and do not select Propagate, the users or groups associated with this permission do not have access to the objects in the hierarchy. They only have access to some global functionality such as creating roles.

Reference: https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUIDC7702E31-1623-4189-89CB-E1136AA27972.html

QUESTION 3

Which three traffic types can be configured for dedicated VMkernel adapters? (Choose three.)

A. Discovery traffic

B. vMotion traffic

C. vSphere Replication NFC traffic

D. Provisioning traffic

E. vSphere Custom traffic

Correct Answer: BCD

Securing System Traffic

Take appropriate security measures to prevent unauthorized access to the management and system traffic in your vSphere environment. For example, isolate the vMotion traffic in a separate network that includes only the ESXi hosts that participate in the migration. Isolate the management traffic in a network that only network and security administrators are able to access. For more information, see vSphere Security and vSphere Installation and Setup.

System Traffic Types

You should dedicate a separate VMkernel adapter for every traffic type. For distributed switches, dedicate

a separate distributed port group for each VMkernel adapter.

Management traffic

Carries the configuration and management communication for ESXi hosts, vCenter Server, and host-tohost High Availability traffic. By default, when you install the ESXi software, a vSphere Standard switch is

created on the host together with a VMkernel adapter for management traffic. To provide redundancy, you

can connect two or more physical NICs to a VMkernel adapter for management traffic.

vMotion traffic

Accommodates vMotion. A VMkernel adapter for vMotion is required both on the source and the target

hosts. The VMkernel adapters for vMotion should handle only the vMotion traffic. For better performance,

you can configure multiple NIC vMotion. To have multi NIC vMotion, you can dedicate two or more port

groups to the vMotion traffic, respectively every port group must have a vMotion VMkernel adapter

associated with it. Then you can connect one or more physical NICs to every port group. In this way,

multiple physical NICs are used for vMotion, which results in greater bandwidth.

Note

vMotion network traffic is not encrypted. You should provision secure private networks for use by vMotion

only.

Provisioning traffic

Handles the data that is transferred for virtual machine cold migration, cloning, and snapshot creation.

IP storage traffic and discovery

Handles the connection for storage types that use standard TCP/IP networks and depend on the VMkernel

networking. Such storage types are software iSCSI, depended hardware iSCSI, and NFS. If you have two

or more physical NICs for iSCSI, you can configure iSCSI multipathing.ESXi hosts support only NFS

version 3 over TCP/IP. To configure a software FCoE (Fibre Channel over Ethernet) adapter, you must

have a dedicated VMkernel adapter. Software FCoE passes configuration information though the Data

Center Bridging Exchange (DCBX) protocol by using the Cisco Discovery Protocol (CDP)VMkernel

module.

Fault Tolerance traffic

Handles the data that the primary fault tolerant virtual machine sends to the secondary fault tolerant virtual machine over the VMkernel networking layer. A separate VMkernel adapter for Fault Tolerance logging is required on every host that is part of a vSphere HA cluster.

vSphere Replication traffic

Handles the outgoing replication data that the source ESXi host transfers to the vSphere Replication server. Dedicate a VMkernel adapter on the source site to isolate the outgoing replication traffic.

vSphere Replication NFC traffic

Handles the incoming replication data on the target replication site.

Virtual SAN traffic

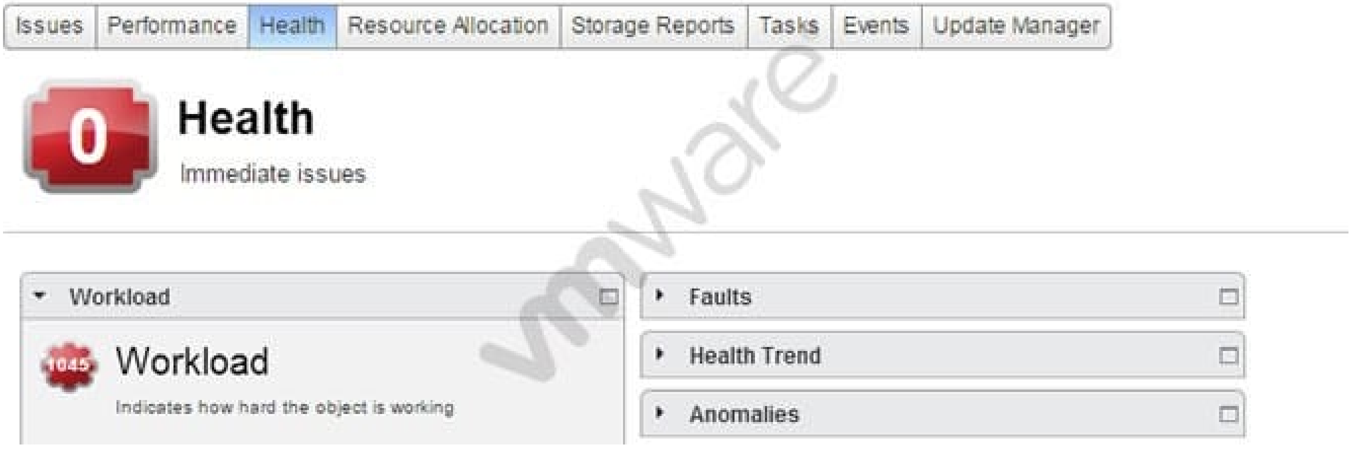
Every host that participates in a Virtual SAN cluster must have a VMkernel adapter to handle the Virtual SAN traffic.

Reference:

https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-D4191320-209E-4CB5-A709-C8741E713348.html

QUESTION 4

Refer to the Exhibit.



An administrator reviews the Health of a virtual machine, as shown in the Exhibit.

Based on the exhibit, which three metrics can be used to determine the virtual machine\\'s Workload characteristics? (Choose three.)

A. CPU

B. Memory

C. Network I/O

D. Threads

E. vNUMA Stats

Correct Answer: ABC

Virtual Machine Alert Definitions The vCenter adapter provides alert definitions that are generated on the virtual machines in your environment. Health/Symptom-based These alerts have the following impact and criticality information. Check the Link for detailed info: http://pubs.vmware.com/vrealizeoperationsmanager-61/index.jsp?topic=%2Fcom.vmware.vcom.core.doc%2FGUID-746FD64E-3380-44A6-A154-0BC63B4624F0.html

QUESTION 5

An administrator tries to capture network traffic for a virtual machine, but cannot see the expected traffic in the packet capture tool.

Which step can resolve the problem?

A. Migrate the virtual machine to a Distributed Virtual Switch.

B. Enable Promiscous Mode on the relevant port group.

C. Modify the default value of MAC Address changes.

D. Enable Forged Transmits on the virtual machine.

Correct Answer: B

Explanation: When promiscuous mode is enabled at the portgroup level, objects defined within that portgroup have the option of receiving all incoming traffic on the vSwitch. Interfaces and virtual machines within the portgroup will be able to see all traffic passing on the vSwitch, but all other portgroups within the same virtual switch do not.

Reference: https://kb.vmware.com/selfservice/microsites/search.do?
language=en_USandcmd=displayKCandexternalId=1002934