QUESTION 1
When creating a Windows Update Policy for a Workspace ONE solution, which option allows an administrator to utilize local network traffic only for peer traffic?

A. use peers on same NAT only
B. use peers on the same local network domain
C. simple download mode
D. use internet peers

Answer: B

QUESTION 2
An administrator has deployed a new NSX Distributed Firewall rule that allows only TLS 1.2 and TLS 1.3 HTTPS connections. The new rule is working, but TLS 1.0 and TLS 1.1 connections are still occurring.
What step is required to enforce the TLS policy restriction?

A. Configure a Context Profile and select DNS-TCP and DNS-UDP attributes.
B. Configure a Context Profile and select a FQDN attributes.
C. Configure a Context Profile and select TLS 1.2 and 1.3 attributes.
D. Configure a Context Profile and select HTTPS and HTTP attributes.

Answer: B

QUESTION 3
Which would be a cause for a device being flagged as compromised in the Workspace ONE UEM dashboard?

A. Device was stolen.
B. Device was lost.
C. Device was damaged.
D. Device was jailbroken.

Answer: A
Explanation:
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskCompliance.html

QUESTION 4
Where in the NSX UI does an administrator add an Active Directory Domain?

A. Go to System > Configuration > Identity Firewall AD > ADD ACTIVE DIRECTORY
B. Go to Inventory > Configuration > Identity Firewall AD > ADD ACTIVE DIRECTORY
C. Go to Home > Configuration > Identity Firewall AD > ADD ACTIVE DIRECTORY
D. Go to Security > Configuration > Identity Firewall AD > ADD ACTIVE DIRECTORY

Answer: A
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-8B60D22B-3119-48F6-AEAE-AE27A9372189.html

QUESTION 5
An administrator is trying to secure Workspace ONE components with firewall rules.
What port does the administrator need to allow for communication between the UEM Console Server and the UEM Database Server?

A. 443
B. 3389
C. 445
D. 1433

Answer: D
Explanation:
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2105/WS1_Assist/GUID-AWT-ARM-NETWORKSECURITYREQS.html

QUESTION 6
In a Workspace ONE deployment, which three are valid pre-configured sources for creating a baseline with the Baseline Wizard? (Choose three.)

A. GPO Connector
B. Registry File Import
C. Windows Security Baseline
D. CIS Benchmarks
E. Custom Baseline

Answer: CDE
Explanation:
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Windows_Desktop_Device_Management/GUID-uemWindeskUsingBaselines.html

QUESTION 7
A company has deployed a new application. Users are complaining they cannot connect. The administrator suspects there is an issue with the Distributed Firewall (DFW).
What three steps can be taken to troubleshoot the DFW? (Choose three.)

A. The administrator should confirm that SLOT 2, which is used by the DFW, is configured under the vNICs of the VMs.
B. The administrator should configure vRealize Log Insight using the Insight agent as the type and review the DFW rule logs in vRealize Log Insight.
C. The administrator should confirm if the DFW rule is set to log, and then look on the hypervisor where the VMs reside and look at logs at /var/log/dfwpktlogs.log.
D. The administrator should verify firewall rules exist to permit traffic and verify the hit counters are increasing.
E. The administrator should configure vRealize Log Insight using syslog as the type and review the DFW rule logs in vRealize Log Insight.

Answer: CDE

QUESTION 8
A consulting security firm was hired to inspect your infrastructure for vulnerabilities.
The firm inspected these items:
- badge readers to enter the datacenter
- locks on server racks
- security cameras in the datacenter

What type of infrastructure are they inspecting?

A. Virtual Infrastructure
B. Physical Infrastructure
C. Personnel Infrastructure
D. Logical Infrastructure

Answer: B
Explanation:
https://nces.ed.gov/pubs98/safetech/chapter5.asp

QUESTION 9
A security administrator receives an error with code 1001 while configuring a time-based firewall rule on an ESXi host.
Which two actions can resolve the problem? (Choose two.)

A. restarting the NSX firewall kernel module on the ESXi host
B. restarting the NTP service on the ESXi host
C. configuring the ESXi host with a remote NTP server
D. configuring the ESXi host with a local NTP server
E. reinstalling the NSX modules on the ESXi host

Answer: BE
Explanation:
https://arabitnetwork.files.wordpress.com/2018/12/nsx_64_troubleshooting-update4.pdf

QUESTION 10
What are the three types of NSX-T Data Center installation workflows? (Choose three.)

A. NSX-T for Bare Metal
B. NSX-T for OpenBox
C. NSX-T for VxRail
D. NSX-T for Hyper-V
E. NSX-T for KVM
F. NSX-T for vSphere

Answer: AEF

QUESTION 11
Which statements is true about IPFIX (Internet Protocol Flow Information Export)?

A. When you enable IPFIX, all configured host transport nodes will send IPFIX messages to the IPFIX collectors using port 80.
B. When you enable IPFIX, all configured host transport nodes will send IPFIX messages to the IPFIX collectors using port 3389.
C. When you enable IPFIX, all configured host transport nodes will send IPFIX messages to the IPFIX collectors using port 443.

D. When you enable IPFIX, all configured host transport nodes will send IPFIX messages to the IPFIX collectors using port 4739.

Answer: D
Explanation:
When you enable IPFIX, all configured host transport nodes will send IPFIX messages to the IPFIX collectors using port 3389.

QUESTION 12
An administrator has been asked to install Guest Introspection Thin Agent using VMware Tools on a Windows 10 VDI solution.
Which statement is correct for enabling the Identity Firewall feature?

A. Guest Introspection drivers are included with VMware Tools for Windows and a reboot of the VM is required to initialize the drivers.
B. To install Guest Introspection on a Windows VM, you must perform a custom install and select the drivers.
C. Guest Introspection drivers are available from third-party providers and can be initialized without a VM reboot.
D. Select Guest Introspection Drivers to install File Introspection (vsepfit) and Network Introspection (vnetfit) drivers.

Answer: B
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.4/administration/GUID-756EF955-F2C1-47DD-946B-1B5E6DDC7BDA.html

QUESTION 13
Which three options are used to automate patch remediation based on CVEs for Windows devices using Workspace ONE Intelligence? (Choose three.)

A. Use Workspace ONE UEM console to approve patches.
B. Create Automated remediation based on Risk score.
C. Create automated remediation based on CVE vulnerabilities.
D. Identify vulnerable devices across the entire environment based on CVE information.
E. Create a dashboard to track CVE remediation.

Answer: CDE
Explanation:
https://techzone.vmware.com/meeting-security-slas-through-intelligent-patch-automation-vmware-workspace-one-operational-tutorial#_1089620

QUESTION 14
What traffic type is used to create an NSX Transport Zone to connect to the physical infrastructure?

A. Trunk
B. Vlan
C. Underlay
D. Overlay

Answer: B
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/installation/GUID-F739DC79-4358-49F4-9C58-812475F33A66.html

QUESTION 15

When creating a new Identity Provider (IdP) in Workspace ONE Access, which two methods are used to identify users? (Choose two.)

A. SAML Attribute
B. NameID Element
C. UserID Element
D. User Attribute
E. SAML Response

Answer: AB
Explanation:
https://docs.vmware.com/en/VMware-Workspace-ONE-Access/19.03/idm-administrator/GUID-0C459D5A-A0FF-4893-87A0-10ADDC4E1B8D.html

QUESTION 16
In an NSX-T Data Center deployment, when assigning user rights, what right would an administrator assign to a user to administer security compliance policies?

A. Auditor
B. Security Engineer
C. NSX Administrator
D. Security Administrator

Answer: D
Explanation:
https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-79F9067D-2F29-45DA-85C7-09EFC31549EA.html

QUESTION 17
Which three tasks are completed during the installation of NSX-T Data Center Workflow for vSphere? (Choose three.)

A. install NSX Edges, then create an NSX Edge cluster
B. create transport zones and set type to Overlay and VLAN; create host transport nodes and standard or enhanced N-VDS/VDS as needed
C. install the NSX Manager, configure a compute manager, deploy additional NSX Manager nodes to form a cluster
D. install NSX Tier-0 or Tier-1 gateways, then create an NSX Edge cluster
E. create transport zones and set type to VXLAN and VLAN; create host transport nodes and standard or enhanced N-VDS/VDS as needed

Answer: ABC
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/installation/GUID-414C33B3-674F-44E0-94B8-BFC0B9056B33.html

QUESTION 18
An administrator works for a company that supplies iOS devices to its employees. The administrator is notified there is a security vulnerability with the latest version of iOS. The administrator must prevent users from updating devices immediately. The administrator implements a device profile to configure the updates payload and prevent the devices from detecting the update.
How long can devices be prevented from accessing the update from Apple?

A. 90 Days
B. 60 Days
C. 30 Days
D. 180 Days

Answer: A
Explanation:
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/iOS_Platform/GUID-OSMgmt.html

QUESTION 19
In what order are NSX-T Distributed Firewall rules processed?

A. Top-to-bottom, left-to-right, finding a rule match the packet is processed per the rule and stops.
B. Left-to-right, top-to-bottom, finding a rule match the packet is processed per the rule and stops.
C. Left-to-right, top-to-bottom, finding a rule match the packet is processed per the rule and continues to next rule.
D. Top-to-bottom, left-to-right, finding a rule match the packet is processed per the rule and continues to next rule.

Answer: D
Explanation:
https://docs.vmware.com/en/VMware-NSX-T-Data-Center/2.3/com.vmware.nsxt.admin.doc/GUID-22DF2616-8B3F-4E13-8116-B7501D2A8E6D.html

QUESTION 20
As an IT administrator, you want to prevent users from launching a protected SaaS web application when they are not connected to the internal LAN. The application is federated with Workspace ONE Access.
What can be configured to prevent the application from launching?

A. Access Policy
B. IdP Response
C. SAML Attribute
D. Authentication Method

Answer: A
Explanation:
https://docs.vmware.com/en/VMware-Workspace-ONE-Access/19.03/com.vmware.wsp-resource/GUID-57B66680-A118-47DD-B3A3-81EAD6D6CAA7.html