DUMPSARENA

Professional VMware Security

VMware 2V0-81.20

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

In a Workspace ONE deployment, what two commands are available for a Windows policy when sending a command action as part of a compliance policy? (Choose two.)

A. Device Wipe

B. Enterprise Wipe

C. Apply Baseline

D. Apply Profile

E. Request Device Checkin

ANSWER: C D

QUESTION NO: 2

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:

Reference: 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 NO: 3

Which three statements are correct for Active Directory integration with Identity Firewalls (IDFW) in an NSX-T Data Center deployment? (Choose three.)

A. The IDFW can be used on both physical and virtual servers as long as supported operating system is installed.

B. The Thin Agent must be enabled in VMWare tools as it is not enabled by default.

C. The IDFW can be used for Virtual Desktops (VDI) or Remote desktop sessions (RDSH support).

D. Identity-based groups can be used as the source or destination in DFW rules.

E. User identity information is provided by the NSX Guest Introspection Thin Agent.

ANSWER: C D E

Explanation:

Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-281FD887-8AB2-4D4D-841E-DF02065F3E97.html

Note:

IDFW relies on the security and integrity of the guest operating system. There are multiple methods for a malicious local administrator to spoof their identity to bypass firewall rules. User identity information is provided by the NSX Guest Introspection Thin Agent inside guest VMs. Security administrators must ensure that thin agent is installed and running in each guest VM. Logged-in users should not have the privilege to remove or stop the agent.

QUESTION NO: 4

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

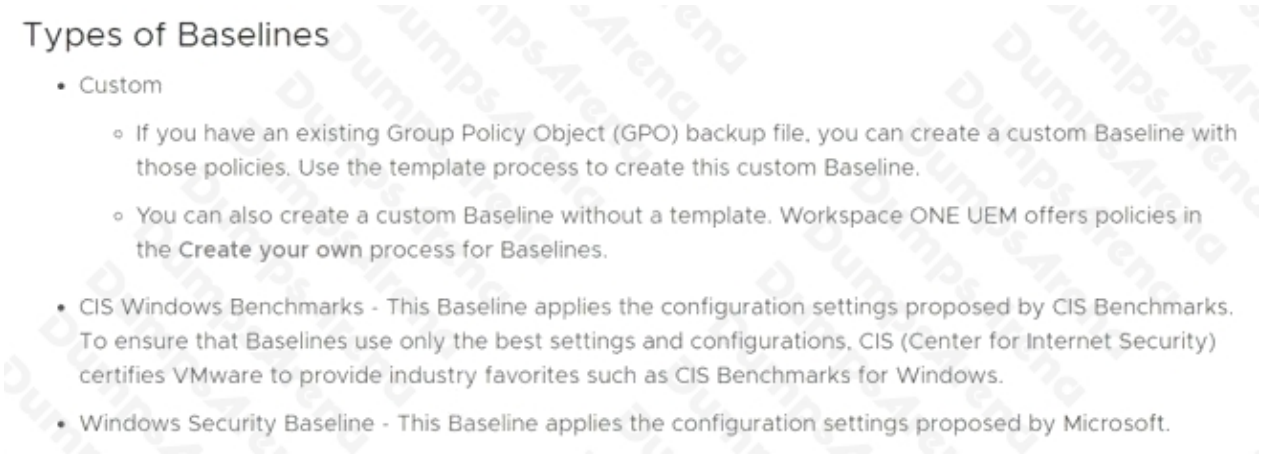
D. CIS Benchmarks

E. Custom Baseline

ANSWER: C D E

Explanation:

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



QUESTION NO: 5

How does an NSX-T Data Center firewall rule handle an Apply To setting for the firewall policy and firewall rule?

A. The rule Apply To will take precedent.

B. The first Apply To created will take precedent.

C. The last Apply To created will take precedent.

D. The policy Apply To will take precedent.

ANSWER: B

QUESTION NO: 6

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: A B

Explanation:

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

QUESTION NO: 7

When deploying a Carbon Black Cloud Sensor using GPO, which option is a required setting?

A. COMPANY_CODE

B. LICENSE_CODE

C. CONNECT_LIMIT

D. AUTO_UPDATE

ANSWER: A

Explanation:

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Endpoint-Standard-How-to-Deploy-Windows-Sensors-using-GPO/ta-p/33306

- **To configure Group Policy to automatically create Windows Installer .msi log**

1. Open the Group Policy editor and expand Computer Configuration > Administrative Templates > Windows Components
2. Select **Windows Installer** and double click **Logging** or **Specify the types of events Windows Installer records in its transaction log** depending on the windows version
3. Select **Enabled**
4. In the **Logging** textbox, type voicewarmupx
5. Select **Save Changes**.

NOTE: The msixxx log file will be created in the Temp folder of the system volume C:\Windows\Temp\
NOTE: This setting will create an msi install log for all users in the GPO

QUESTION NO: 8

Which are two use cases for NSX Intelligence? (Choose two.)

A. Perform day 2 network operations and troubleshooting.

B. Provide end-to-end network visibility for physical, virtual, and third-party environments.

C. Identify security vulnerabilities and automatically quarantine affected workloads.

D. Gain insight about micro-segmentation traffic flows.

E. Simplify rule recommendation and deployment.

ANSWER: C D

Explanation:

The main use cases for NSX Intelligence are:

- **Automate micro-segmentation policy at scale**: Automatically recommends application groups and security policies to vastly simplify implementation of micro-segmentation and firewall rules.
- **Demonstrate and maintain policy compliance**: Delivers complete historical record of every flow in and out of every workload, detailed visualization of flows, as well as an audit trail for security policies
- **Simplify security incident troubleshooting:** Brings together a complete inventory of every workload, continuous layer 7 analysis and visualization of every flow between workloads without sampling, within a converged console in NSX

QUESTION NO: 9

Which is the built-in two factor authentication method in Workspace ONE Access?

A. VMware Verify

B. VMware SMS

C. VMware Auth

D. VMware Push

ANSWER: A

Explanation:

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/ws1_access_authentication_cloud/GUID-FE8A5B1C-BC17-4A5C-BC8D-614C5EE4057A.html

Users install the VMware Verify application on their devices and provide a phone number to register their device with the VMware Verify service. The device and phone number are also registered in the User & Groups user profile in the Workspace ONE Access console.

Users enroll their account once when they sign in using password authentication first and then enter the VMware Verify passcode that displays on their device. After the initial authentication, users can authenticate through one of these three methods.

- Push approval with OneTouch notification. Users approve or deny access from Workspace ONE Access with one click. Users click either Approve or Deny on the message that is sent.
- Time-based One Time Password (TOTP) passcode. A one-time passcode is generated every 20 seconds. Users enter this passcode on the sign-in screen.
- Text message. Phone SMS is used to send a one-time verification code in a text message to the registered phone number. Users enter this verification code on the sign-in screen.

QUESTION NO: 10

Which is true about Time-Based Firewall Policy rules?

A. Time-Based policy rules apply only to the NSX Distributed Firewall.

B. Time-Based policy rules apply to the NSX Gateway and Distributed Firewall.

C. Time-Based policy rules can only be used one time for NSX Gateway Firewall.

D. Time-Based policy rules apply only to the NSX Gateway Firewall.

ANSWER: B

Explanation:

Reference: https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/administration/GUID-8572496E-A60E-48C3-A016-4A081AC80BE7.html

1. Click the clock icon on the firewall policy you want to have a time window.

   A time window appears.

2. Click **Add New Time Window** and enter a **name**.

3. Select a time zone: UTC (Coordinated Universal Time), or the local time of the transport node. Distributed firewall only supports UTC with NTP service enabled, a change of time zone configuration is not supported.

4. Select the frequency of the time window - **Weekly** or **One time**.

5. Select the days of the week that the time window takes effect.

   NSX-T Data Center supports configuring weekly UTC time-windows for the local time-zone, when the entire time-window for the local time-zone is within the same day as the UTC time-zone. For example, you cannot configure a time window in UTC for a 7am-7pm PDT, which maps to UTC 2pm-2am of the next day.

6. Select the beginning and ending dates for the time window, and the times the window will be in effect.