DUMPSBOSS.

Professional VMware Security

VMware 2V0-81.20

Version Demo

Total Demo Questions: 10

Total Premium Questions: 70

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which file can be used to validate repcli authentication was enabled for Carbon Black Cloud?

A. C:\Program Files\Confer\repcii.ini

B. C:\Program Files\Confer\config.ini

C. C:\Program Files\Confer\cfg.ini

D. C:\Program Files\Confer\cli.ini

ANSWER: A

Explanation:

Reference: https://community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Cloud-How-to-Enable-RepCLI-Authentication-on/ta-p/70393


Resolution

1. Enable bypass mode on the sensor from the Carbon Black Cloud Console
2. Open the **cfg.ini** file with Notepad (Notepad++.exe with Admin privilege is recommended)
   - Location of cfg.ini file can be found here
3. Add the following line (replace <DesiredSID> with actual AD Group or User SID)
   - Warning: Authenticated users will be able to run any repcli command on the device, please ensure SID only applies to a specific user or group trusted to execute repcli commands
   - Note: Only one SID can be specified
   - `AuthenticatedCLIUsers=<DesiredSID>`
4. Save changes to cfg.ini with "Save As" option, maintain the same file name and select a destination outside of the cfg.ini directory
5. Move the old cfg.ini file out of it's file path and keep as a backup
6. Move the new cfg.ini file with the SID entry back into the specified file path
7. Run the following repcli command

```
"c:\program files\confer\repcli" updateconfig
```

QUESTION NO: 2

An administrator is trying to create a new access policy rule in Workspace ONE Access.

Which two options are available when creating this new access policy rule. (Choose two.)

A. Device OS Version

B. Network Range

C. Compliance State

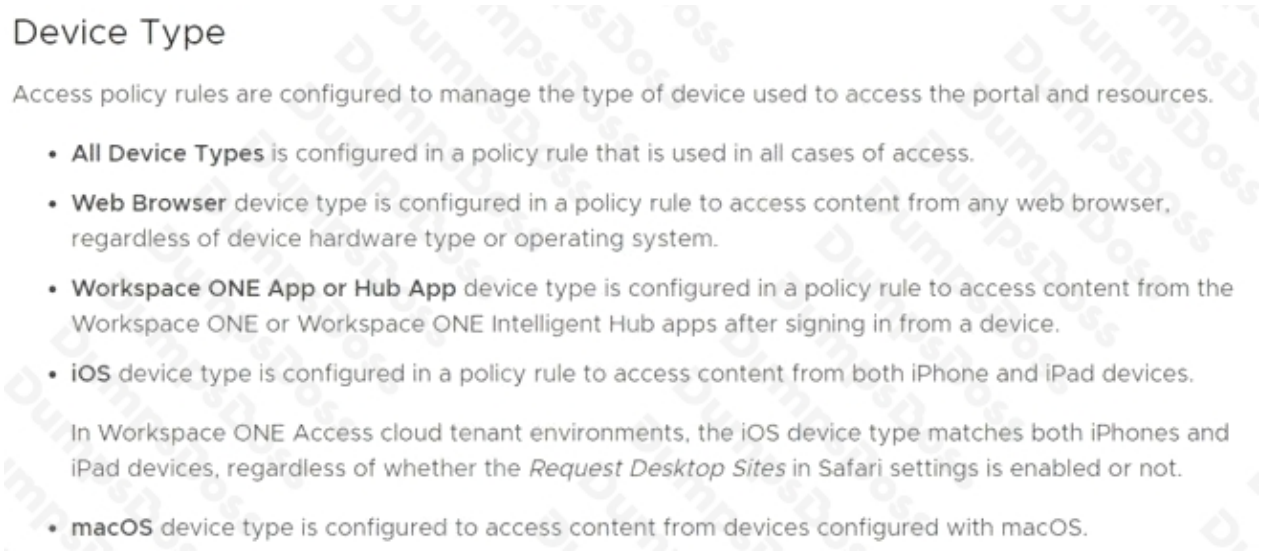
D. Device Ownership

E. Authentication Method

ANSWER: B E

Explanation:

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-Access/services/ws1_access_authentication_cloud/GUID-C2B03912-C7D8-4524-AE6E-8E8B901B9FD6.html



Device Type

Access policy rules are configured to manage the type of device used to access the portal and resources.

- **All Device Types** is configured in a policy rule that is used in all cases of access.
- **Web Browser** device type is configured in a policy rule to access content from any web browser, regardless of device hardware type or operating system.
- **Workspace ONE App or Hub App** device type is configured in a policy rule to access content from the Workspace ONE or Workspace ONE Intelligent Hub apps after signing in from a device.
- **iOS** device type is configured in a policy rule to access content from both iPhone and iPad devices.

  In Workspace ONE Access cloud tenant environments, the iOS device type matches both iPhones and iPad devices, regardless of whether the *Request Desktop Sites* in Safari settings is enabled or not.
- **macOS** device type is configured to access content from devices configured with macOS.

QUESTION NO: 3

Which two are features of a hybrid cloud model for networking and security when using NSX-T Data Center and VMware NSX Cloud? (Choose two.)

A. NSX Data Center provides consistent logical networking and security across protected and recovery sites.

B. NSX Data Center supports Layer 2 VPN between an NSX Edge and a Direct Connect Gateway.

C. NSX Data Center and VMware NSX Cloud stretch Layer 2 domains between public clouds using the Geneve overlay.

D. NSX Data Center supports secure, encrypted user access to private corporate applications (SSL VPN).

E. NSX Data Center supports remote sites (IPsec VPN) with optional VPN gateways or hardware routers from other vendors.

ANSWER: A E

Explanation:

Reference: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-datasheet.pdf

QUESTION NO: 4

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:

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


The following types of Web applications can be added to the catalog:

- SAML 2.0 applications
- SAML 1.1 applications

  SAML 1.1 is an older SAML authentication standard. For better security, implement SAML 2.0.
- WS-Federation 1.2 (supported for Office 365 only)
- OpenID Connect applications
- Applications that do not use a federation protocol
- Applications associated with third-party identity providers such as Okta, Ping, and ADFS.

  To add these applications, you must first configure the third-party identity provider as an application source in VMware Identity Manager. See

QUESTION NO: 5

An administrator has created a security policy from the NSX UI, but the firewall rules are not being applied to the traffic in the datapath.

Which two actions could be carried out by the administrator to resolve the problem? (Choose two.)

A. Modify the Direction of the rules in the security policy.

B. Modify the Action of the rules in the security policy.

C. Restart the workloads running on the impacted hosts.

D. Modify the Applied To field of the security policy.

E. Restart the nsx-proxy agent on the impacted hosts.

ANSWER: B C

QUESTION NO: 6

In a Workspace ONE environment, which two Risk Indicators are supported on the Windows 10 & MacOS platforms? (Choose two.)

A. Risky Setting

B. Compulsive App Download

C. App Collector

D. Rare App Collector

E. Laggard Update

ANSWER: B D

Explanation:

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-14_intel_user_risk_dashboard.html

Risk Indicators	Description	Risk
Anomalous Alert Activity	A device that produces an unusual number, type, or severity of security alerts.	An unusual number, type, or severity of threat alerts is an indication of a potentially compromised device.
App Collector	A person who installs an unusually large number of apps.	Any app can include known or unpatched vulnerabilities and these vulnerabilities can become attack vectors. The surface area for cyber-attacks increases with the number of apps on the device.
Compulsive App Download	A person who installs an atypical number of apps in a short period of time.	Users frenetically installing unusual apps on their devices have a greater risk of being a victim of malicious activity. Some apps disguise themselves as useful, friendly, or entertaining, when in fact they want to harm the user. Marketplace approaches to filtering unsafe content (malware) vary from vendor to vendor. A careless user can get tracked, hacked, or conned.
Excessive Critical CVEs	A device with an excessive number of unpatched critical CVEs (Common Vulnerability Exposure).	The greater the number of critical CVEs present on a device, the larger the device's attack surface.

QUESTION NO: 7

Which two options are needed to configure NSX-T Data Center to access the Active Directory? (Choose two.)

A. Domain Controller Name

B. Distinguished Name

C. username

D. Port

E. netBIOS name

ANSWER: B E

Explanation:

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

QUESTION NO: 8

In an NSX-T Data Center deployment, micro-segmentation via security policies is accomplished using which component?

A. NSX Bridge Firewall

B. NSX Gateway Firewall

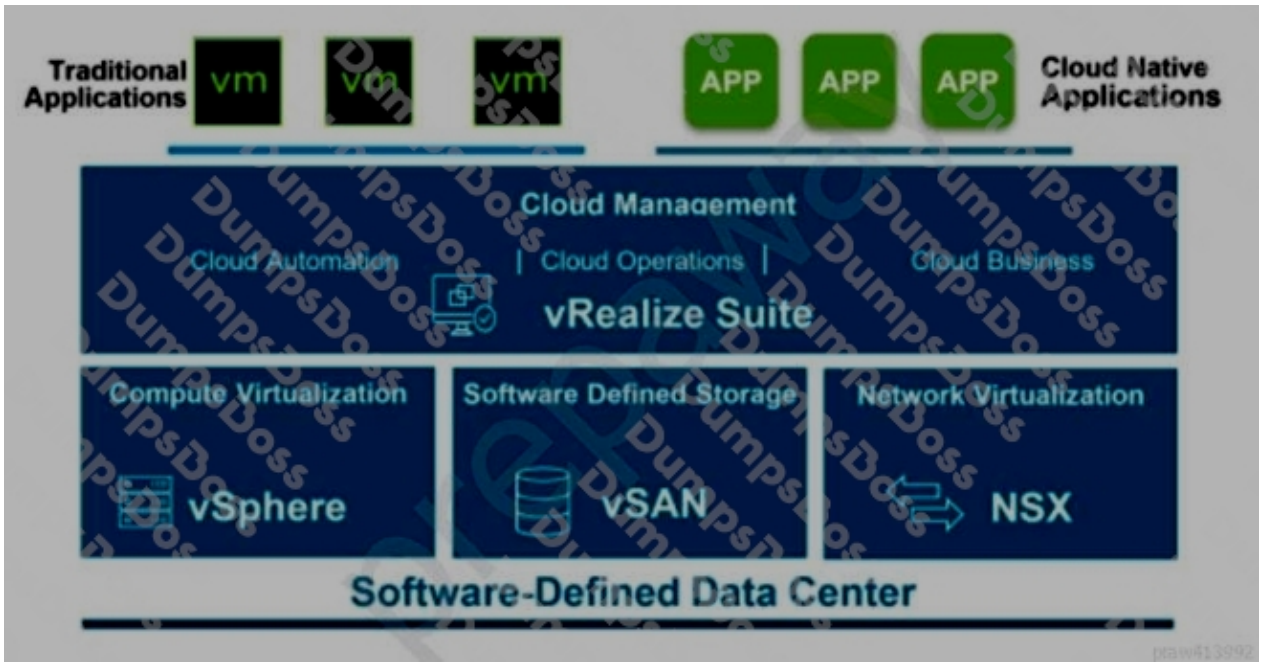
C. NSX Logical Router

D. NSX Distributed Firewall

ANSWER: D

Explanation:

Reference: https://infohub.delltechnologies.com/l/vmware-cloud-foundation-on-dell-emc-vxrail/vmware-sddc-vision-6#:~:text=NSX%20micro%2Dsegmentation%20is%20a,all%20hosts%20in%20the% 20environment



QUESTION NO: 9

Where in the NSX UI does an administrator deploy NSX Intelligence?

A. Go to Plan & Troubleshoot > Configuration > ADD NSX INTELLIGENCE APPLIANCE

B. Go to Security > Configuration > Appliances > ADD NSX INTELLIGENCE APPLIANCE

C. Go to System > Configuration > Appliances > ADD NSX INTELLIGENCE APPLIANCE

D. Go to Home > Configuration > Appliances > ADD NSX INTELLIGENCE APPLIANCE

ANSWER: C

Explanation:

Reference: https://docs.vmware.com/en/VMware-NSX-Intelligence/1.2/installation/GUID-45906AC9-7FD7-441E-83F9-E83CC68E8148.html

- Verify that the minimum NSX Intelligence system requirements are met for the appliance size you want to install. See Preparing for NSX Intelligence Installation.
- You must have an Enterprise Administrator role to install, configure, and use NSX Intelligence.
- Download the NSX Intelligence installer bundle file. See Download the NSX Intelligence Installer Bundle.
- Determine the size of the NSX Intelligence appliance to configure. Small size is for lab or proof-of-concept deployment, or small-scale production environment. Large size is for a large-scale production environment. See NSX Intelligence System Requirements.
- Synchronize time between an NTP server, the compute cluster on which the NSX Intelligence appliance is to be deployed, and with the NSX Manager server.
- Collect the IP addresses for the management subnet, gateway, DNS server, and NTP server that are required to configure the NSX Intelligence appliance.
- Ensure that the certificates used for the NSX Manager Unified Appliance node or cluster are compatible with the certificate types listed in Preparing for NSX Intelligence Installation.

QUESTION NO: 10

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