PassQueen
a.k.a dumpsqueen.com

Juniper Networks Certified Internet Expert (JNCIE-SP)

Juniper JPR-961

Version Demo

Total Demo Questions: 8

Total Premium Questions: 85

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, BGP Routing	5
Topic 2, MPLS	8
Topic 3, Layer 2 VPNs	2
Topic 4, Layer 3 VPNs	4
Topic 5, Multicast	2
Topic 6, CoS	1
Topic 7, High Availability	3
Topic 8, Mix Questions	60
Total	85

QUESTION NO: 1

You work as the network administrator at ABC.com. The ABC.com network consists of a domain named ABC.com. The servers at the ABC.com network run Windows Server.

The ABC.com network has a Web server named ABC-SR11. During a routine monitoring you notice an increase in network traffic. Due to this you need to find out the MAC address of the workstation that initiated the transfers and the command that was used. However, you action must not effect ABC-SR11.

What actions must you take?

A. You must run the ipconfig/registerdns.

B. You must use the Netmon utility.

C. You must capture the IP traffic to ABC-SR11.

D. You must Enable Server Message Block (SMB) signing on all the workstations.

ANSWER: C

Explanation:

Capture the IP traffic to ABC-SR11. A passive packet capture is the appropriate approach because it lets the administrator observe the traffic exchanged with the web server without installing software, changing configuration, or otherwise interrupting service on ABC-SR11. The capture point can be a switch SPAN or port-mirroring destination, a network TAP, or another appropriately positioned monitoring interface. Ethernet frames in the capture contain the source MAC address, allowing the initiating workstation's Layer 2 address to be identified. Packet contents and protocol decoding can also reveal the application request or command used to initiate the transfer, subject to encryption and the protocol in use.

To ensure the capture is useful, filter on traffic whose source or destination is ABC-SR11's IP address, while retaining Layer 2 frame information. Capturing at a network device adjacent to the server is especially useful because it records the actual frames delivered toward the server and does not require any modification to the server itself. Microsoft documents packet capture capabilities in Packet Monitor (Pktmon); the general passive-observation principle and use of capture filters are also described in the Wireshark User's Guide.

QUESTION NO: 2

You work as the network administrator at ABC.com. The ABC.com network has a domain named ABC.com. The servers at the ABC.com network run Windows Server and the workstations, Windows XP Professional.

The ABC.com network has a server named ABC-SR10 that runs Windows Server Update Services (WSUS). During synchronization you notice that you cannot connect to the Windows Update servers, however, you can access to other Web site not residing in the intranet.

What actions must you take to connect to the Windows Update servers?

A. You must run the ipconfig/registerdns.

B. You must configure the forwarders on ABC-SR10.

C. You must set the authentication to the proxy server in the WSUS settings.

D. You must run the gpupdate /force command on ABC-SR10.

ANSWER: C

Explanation:

You must set the authentication to the proxy server in the WSUS settings. WSUS synchronizes update metadata and, where configured, update files by making outbound connections to Microsoft Update or Windows Update endpoints. In many enterprise networks, those outbound connections must traverse an HTTP proxy. Although the server may be able to reach

ordinary external websites, WSUS synchronization can still fail if the proxy requires credentials and WSUS has not been configured to supply them.

In the WSUS Administration Console, configure the proxy under the server's Update Source and Proxy Server settings. Enable use of a proxy server, specify its address and port, and provide proxy authentication credentials when required. The account must be permitted by the proxy to access the Microsoft update services used by WSUS. After saving the configuration, run a synchronization again so WSUS can establish its authenticated outbound connection and download the update catalog.

Microsoft documents the WSUS proxy-server configuration as part of WSUS deployment and synchronization configuration. See Configure WSUS and Synchronize WSUS.

QUESTION NO: 3

The ABC.com network consists of a single Active Directory domain named ABC.com. All client computers on the ABC.com network run Windows XP Professional.

You use your client computer named ABC-WS294. You want to use Microsoft Baseline Security Analyzer (MBSA) on ABC-WS294 to analyze network servers for security vulnerabilities.

Which of the following services are the minimum required to be running on the network servers for you to scan them with MBSA? (Choose all that apply.)

A. Remote Registry.

B. Workstation service.

C. Server service.

D. Print Spooler service.

ANSWER: A C

Explanation:

Remote Registry and Server service are the minimum services required on each target server for an MBSA remote vulnerability scan. MBSA obtains much of the configuration and security-update information needed for its assessment by remotely reading the target computer's registry. The Remote Registry service provides the necessary remote registry access, allowing the scanner to inspect security settings and installed-update information without an interactive session on the server.

The Server service is also required because it supplies the target's SMB file-and-print-sharing capability, including the administrative IPC$ connection used for remote management communication. With valid administrative credentials, the scanning workstation can use that connection to establish the remote access required for the assessment. These prerequisites apply to the systems being assessed; the scanning computer must additionally have network connectivity and appropriate administrative permissions for each target. Microsoft's MBSA documentation describes remote scanning and its administrative/network prerequisites, while Microsoft's SMB documentation explains the network file-sharing mechanism underlying these remote connections. See Microsoft Baseline Security Analyzer documentation and SMB overview for Windows Server.

QUESTION NO: 4

You work as a network administrator for ABC.com. The ABC.com network consists of a single Active Directory domain named ABC.com. There are currently 120 Web servers running Windows Server and are contained in an Organizational Unit (OU) named ABC_WebServers

ABC.com management took a decision to uABCrade all Web servers to Windows Server. You disable all services on the Web servers that are not required. After running the IIS Lockdown Wizard on a recently deployed web server, you discover that services such as NNTP that are not required are still enabled on the Web server.

How can you ensure that the services that are not required are forever disabled on the Web servers without affecting the other servers on the network? (Choose two.)

A. Set up a GPO that will change the startup type for the services to Automatic.

B. By linking the GPO to the ABC_WebServers OU.

C. Set up a GPO with the Hisecws.inf security template imported into the GPO.

D. By linking the GPO to the domain.

E. Set up a GPO in order to set the startup type of the redundant services to Disabled.

F. By linking the GPO to the Domain Controllers OU.

G. Set up a GPO in order to apply a startup script to stop the redundant services.

ANSWER: B E

Explanation:

By linking the GPO to the ABC_WebServers OU and setting the startup type of the redundant services to Disabled in that GPO, the administrator can centrally apply and continuously enforce the required service configuration only on the intended web-server computers. Group Policy objects linked to an organizational unit apply to computer accounts located in that OU, which provides the necessary scoping: web servers receive the policy while computers in other OUs are unaffected. This is preferable to a domain-level link when the configuration is specific to a server role.

The policy should configure each unnecessary service, such as NNTP, with a startup type of *Disabled*. Windows applies computer policy during startup and refreshes it periodically, so the desired service state is reasserted rather than relying solely on a one-time manual change. Combining an OU-scoped link with service startup configuration creates a manageable, repeatable baseline for all current and newly deployed members of the web-server OU. Microsoft documents Group Policy processing and scoping in its Group Policy overview, and documents the service startup controls available through System Services security settings.

QUESTION NO: 5

You administer your company's network. A single-domain Active Directory forest is configured on the network. All servers run Windows Server.

The network contains a server named Server5 that hosts confidential business datA. Access to Server5 must be restricted to only a few authorized personnel. You must ensure that those users, including designated Server5 administrators, cannot share Server5's desktop with other users. What should you do?

A. Disable Remote Assistance in the local policy on Server5.

B. Create a new OU, move Server5 to the OU, create a GPO that disables Remote Assistance, and link the GPO to the OU.

C. Create a new OU, move Server5 to the OU, create a GPO that disables Remote Desktop, and link the GPO to the OU.

D. Disable Remote Desktop in the local policy on Server5.

E. Disable Remote Assistance in System Properties on Server5.

F. Disable Remote Desktop in System Properties on Server5.

ANSWER: B

Explanation:

Create a new OU, move Server5 to the OU, create a GPO that disables Remote Assistance, and link the GPO to the OU. Remote Assistance is the Windows feature designed to let a user invite another person to view or control the user's interactive desktop session. Disabling it prevents Server5 users, including staff with administrative responsibilities on that server, from using Remote Assistance to expose the confidential server desktop to another user.

Applying the setting through a Group Policy Object scoped to a dedicated organizational unit is the appropriate domain-management approach. It targets the computer configuration to Server5 rather than relying on a user-specific setting,

provides centralized and auditable administration, and re-applies the desired configuration during Group Policy processing. A dedicated OU also creates a clean scope for this server-specific security requirement without unintentionally affecting other servers in the domain. The policy should disable the applicable Remote Assistance configuration so that Remote Assistance invitations and related assistance behavior are not available on Server5. Microsoft's Remote Assistance documentation describes the feature's role in sharing or controlling a remote user's session, while its Group Policy documentation explains centralized application of computer settings: Microsoft Remote Assistance documentation and Microsoft Group Policy overview.

QUESTION NO: 6

You operate an IS-IS Level 2 MPLS core. A newly deployed P router has formed IS-IS adjacencies with both core neighbors, but RSVP-TE LSPs cannot traverse the router.

Which two configuration requirements must be met for the router to participate as a transit router in RSVP-TE signaling? (Choose two.)

A. Enable RSVP on each core-facing interface.

B. Enable MPLS on each core-facing interface.

C. Configure LDP on each core-facing interface.

D. Configure IS-IS traffic engineering extensions.

E. Configure BGP labeled-unicast on each core-facing interface.

ANSWER: A B D

Explanation:

RSVP must be enabled on the transit interfaces because RSVP Path and Resv messages are exchanged hop by hop over the interfaces along the LSP path. Enabling MPLS on the same interfaces permits labeled packets to be forwarded after the RSVP LSP is established.

IS-IS must also advertise traffic-engineering information for the router links. RSVP-TE path computation relies on link attributes, including reservable bandwidth and administrative groups, distributed by the IGP traffic-engineering extensions. An IS-IS adjacency alone supplies reachability but does not necessarily provide the TE database required for constrained path computation. Juniper documents the required RSVP and MPLS interface configuration in its RSVP configuration documentation and describes MPLS traffic engineering in its MPLS traffic engineering documentation.

QUESTION NO: 7

The ABC.com network consists of a single Active Directory domain named ABC.com. All servers on the ABC.com network run Windows Server Enterprise Edition and all client computers run Windows XP Professional. ABC.com has its headquarters in Chicago and a branch office in Dallas.

The Chicago and Dallas offices are connected by permanent leased line connection with a hardware router at each end of the connection.

Currently all client computers in both offices receive their IP configurations from a single Windows Server 2003 server located in the Chicago office.

You are designing a new DHCP architecture to improve the performance and reliability of the system.

How would you ensure that DHCP services will continue to function in the event of a failure of any single component? (Choose two.)

A. Set up two Windows Server computers as a DHCP server cluster in the Chicago office.

B. Install two Windows Server computers as a DHCP server cluster in the Dallas office.

C. Configure a Windows Server computer at the Dallas office as a DHCP relay agent.

D. Install a Windows Server computer as an additional DHCP server in the Dallas office.

E. Set up a Windows Server 203 computer at the Chicago office as a DHCP relay agent.

F. Configure one DHCP server to handle 75 percent of the IP address scope and the other DHCP server to handle 25 percent.

ANSWER: D F

Explanation:

Installing a Windows Server computer as an additional DHCP server in the Dallas office provides a DHCP service point local to the branch network. This removes dependence on the leased line, the WAN routers, and the Chicago DHCP host for Dallas clients to obtain or renew leases. If the interoffice connection fails, Dallas can continue serving its local subnet; likewise, Chicago retains its local DHCP capability. Configuring one DHCP server to handle 75 percent of the IP address scope and the other DHCP server to handle 25 percent implements the traditional split-scope design used before native DHCP failover was available. Each server has a defined, non-overlapping portion of the same scope available for lease allocation. The server holding the larger portion normally services the primary site, while the other maintains a reserve of addresses that can be issued if the primary DHCP server or its network path becomes unavailable. Together, the geographically distributed DHCP servers and split allocation improve both resiliency and normal branch-office performance. Microsoft describes DHCP server deployment and scope configuration concepts in its DHCP overview; the historical split-scope approach is also documented in the Windows Server 2003 DHCP documentation.

QUESTION NO: 8

You are the DNS administrator for TXGlobal, which is headquartered in Dallas and has branch offices in Austin, Houston, San Antonio and El Paso. The headquarters location hosts the parent domain, txglobal.com. Each branch office has been delegated a child domain. Austin hosts austin.txglobal.com, Houston hosts houston.txglobal.com, San Antonio hosts sanantonio.txglobal.com, and El Paso hosts elpaso.txglobal.com.

The primary DNS server in Dallas is named TXDNS. The primary DNS servers in the branch offices are named AUSDNS, HOUDNS, SADNS and EPDNS. The secondary DNS servers in the branch offices are named AUSDNS-2, HOUDNS-2, SADNS-2, and EPDNS-2.

To increase fault tolerance, you want to add another secondary DNS server in each location. The new DNS servers will be named AUSDNS-3, HOUDNS-3, SADNS-3, and EPDNS-3. You want TXDNS to be aware that the new servers are authoritative for their respective zones.

Which server or servers should host one or more stub zones?

A. AUSDNS, HOUDNS, SADNS and EPDNS

B. AUSDNS-3, HOUDNS-3, SADNS-3 and EPDNS-3

C. all of the DNS servers within the child domains

D. TXDNS

ANSWER: D

Explanation:

TXDNS is correct because it hosts the parent *txglobal.com* namespace and must maintain current referral information for each delegated child domain. A stub zone on TXDNS for each child domain—*austin.txglobal.com*, *houston.txglobal.com*, *sanantonio.txglobal.com*, and *elpaso.txglobal.com*—stores only the records needed to locate that child zone's authoritative servers: the SOA record, NS records, and required glue host records. It does not hold a complete copy of the child zone.

When the authoritative-server set for a child zone changes, such as when the additional secondary servers are introduced, the stub zone can refresh its data from the child zone's authoritative DNS infrastructure. This allows TXDNS to retain current awareness of the authoritative name servers and direct queries for the delegated namespaces appropriately, without administering full secondary copies of all branch zones. This use aligns with the purpose of stub zones: maintaining up-to-date authoritative-server information for another DNS zone while minimizing replicated zone data. Microsoft's DNS

documentation describes the records retained in stub zones and their role in identifying authoritative DNS servers: DNS zone types. Additional operational guidance is available in Manage DNS zones.